SIEMENS

blue2net
LAN Access Point

Bluetooth™

User Guide

Issue January 2003, Version 4.0

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

Navigation in the PDF document (CD-ROM or download):

If you use Acrobat Reader, for example, you have to activate the tool  .

If you click on active elements in the PDF document, you can directly access the referenced views.

Active elements are:

- bookmarks on the left side of e.g. Acrobat Reader
- table of contents, list of figures, list of tables,
- hierarchy table (chapters, pages),
- references to chapters, pages, figures and tables,
- some URLs.

To return to your previous position, click on  .

Issue January 2003, Version 4.0 (valid for software with version numbers 4.0.x)

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).

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

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.

Contents

List of Figures

List of Tables

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 PAN Profile (Personal Area Networking Profile), which signifies a wireless Ethernet connection, or the LAN Access Profile, which means full IP integration over PPP (Point to Point Protocol).

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, which is connected via USB or PCMCIA adapter or as a compact flash card. In the following these devices will be referred to as "Bluetooth terminals".
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 travelers 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. In combination with an Ethernet switch, the LAN Access Point can also be used as access router for PCs/laptops (which in the following will be referred to as "Ethernet terminals") interconnected permanently via Ethernet cable.

2 QuickStart

This brief outline is intended to help you quickly access the information contained in this user guide.

There are a few things you absolutely need to know before you start up blue2net for the first time to enable you to work with blue2net securely and without problems. You can find this key information under "Must Read".

Once blue2net is ready to be taken live, with sufficient security settings for a given scenario, you can familiarize yourself with the individual parameters in detail and make individual adjustments where necessary. Neither do the first steps involve activating the firewall, performing software updates or setting up a device-specific homepage. All of this information is provided under "Look up later".

Certain items of information are not important until you want to make full and purpose-optimized use of the technical possibilities blue2net has to offer for professional or home use. Under the heading "For experts", experts will find the information they need. Conveying such information in such a way that non-experts will be able to fully understand it, might be out of the scope of this manual.

Note: In the PDF file (available on CD-ROM or from the Siemens blue2net-homepage), click on the chapter number to get to the corresponding chapter.

	QuickStart Guide	Details in chapter
1. Must Read	Make sure to read this chapter before starting up or configuring blue2net.	
Positioning and mounting	• For first start-up and basic configuration, you can place blue2net on the table next to the terminal. • Later, install blue2net in its final position (to select the optimum position, keep the directivity in mind as well as the distance specifications for cable connections, etc. - use the provided dimension diagram on the last page).	4.2 last page
Set up operation on LAN or xDSL modem	• For operation in a corporate LAN or with a cable modem, blue2net can in most cases be initially operated with the factory settings. • To operate blue2net on an xDSL modem, you need to configure it first before connecting it to the xDSL modem. You can rely on the provided use scenarios to find out how to configure your system in the way you want and how to define the highly important security settings.	4.3.1 4.3.2

	QuickStart Guide	Details in chapter
Security Technology-related security User-related security (e.g. handling of passwords)	From the technical point of view, blue2net is one of the most secure LAN Access Points on the market. However, you must make yourself familiar with the security functions to be able to put them to optimal use, and you have to comply with a few basic rules (e.g. how to handle passwords). Remember to adjust the security settings to your needs and aims, and strike your own balance between high-level security requirements and user convenience.	3 6.5
Registering terminals	This chapter describes a general procedure for setting up a Bluetooth connection between terminal (laptop, PDA,...) and blue2net (given the large variety of products, it is not possible to describe all the details required for each and every registration procedure. Please look up such details in the instructions coming with the terminal product you are using). Now you have access to the configuration (possible both via Bluetooth and LAN).	5
Access to the configuration page	Access the parameters via the web page provided in blue2net (please remember to specify the right address https://, with an s). Before doing so, check whether your web browser supports 128-bit encryption (cipher strength). If it doesn't, upgrade your browser).	6
Configuration	To ensure secure operation, you must not forget to define the security settings after you have registered the terminal for the first time. Likewise, different applications will require adequate settings for different parameters. To do so, you can either • choose one of several scenarios and set the parameters accordingly (recommended if you are not familiar with networking technology), or • set the parameters individually to suit your specific requirements. To be able to do so, you will have to familiarize yourself with the detailed parameter descriptions. Hierarchy numbers enclosed in square brackets - for example, [1.8.4] are designed to help you identify and find the required parameters.	6.5 7 8 8.3

	QuickStart Guide	Details in chapter
Use scenarios	This is the way to get quick results: Select one of several typical scenarios, which fall under 3 main categories: • Home use • Business • Public hot spots These scenarios help you to quickly arrive at good and secure configuration settings without the need to know all the complex details in the background (LAN or xDSL operation, security, access, exclusion, VIPs, etc.).	7.1 7.2 7.3
Preventing lockout	There are a few configuration parameters with which you have to be very careful. If set incorrectly and then inadvertently saved, such parameters may lead to blue2net becoming inaccessible via the Bluetooth connection or inaccessible at all. This is not a malfunction of blue2net, but a result of faulty configuration. It is important that you become aware of this face.	10 8.9
Saving the configuration settings	If you change configuration settings, you have to save them first before they can take effect. For this purpose, blue2net provides options you should become familiar with in order to avoid lockouts or loss of data and security problems.	8.9 8.9.1 8.9.2
2. Look up later	Detailed information on parameter and less frequently used functions.	
Description of the individual parameters	Detailed descriptions of all the parameters.	starting from 8.3
Firewall	Under certain circumstances, you can/should activate the built-in firewall. You can define rules to circumvent the firewall for the purposes of remote maintenance.	14 8.5.3 8.5.4
Software update	This chapter tells you how to download a software update from the Siemens homepage and upload it on blue2net. Please note the changes in the update procedure since Software version 4.0.0. For updating follow instructions provided for the previous software.	11
Specific homepage	You can load a specific homepage onto blue2net.	12

	QuickStart Guide	Details in chapter
3. For experts	This chapter is intended for people who want to know more about the network structures available for running blue2net.	
Network structures	blue2net has features that not only allow you to connect several terminals, but also to set up a small-scale network at low cost. However, doing so will require some specialist know-how. This User Guide provides a limited amount of details in this respect. If you are not a network administrator yourself, you might from time to time need the help of a network administrator or have to refer to the respective literature.	9

4. General information	These chapters provide general information about the device as such, about troubleshooting, and about the factory settings.	
Troubleshooting	This part of the manual gives you hints on troubleshooting so you will know how to handle typical problems that have already occurred several times.	13
Technical data	List of technical data.	21
Factory (default) settings	This section provides a list of all the factory settings for the configuration parameters. A deliberate reset will result in all of the factory settings taking effect again.	17 8.9.5
Conformity, CE, Bluetooth compliance	Information on conformity with industry standards, compliance with laws and the Bluetooth license.	15 23 16
Abbreviations & Terms	Provides explanations for the abbreviations and some of the terms used.	18
Customer service	Contact address for repairs, servicing, and inquiries.	19
Warranty and liability	Conditions for claims under warranty and liability.	20
Index	Helps you to find specific items of information.	22
Dimension diagram	Dimensions and drilling instructions for mounting blue2net.	last page

3 Security

Again and again, the security of wireless networks gives rise to discussions.

Siemens has decided to use the Bluetooth technology because it meets very high security standards.

3.1 Technology-related Security

This chapter compares the most important technological differences in terms of security between Bluetooth and the commonly used radio standard Wireless LAN (WLAN). WLAN here stands for the IEEE 802.11b standard.

Mechanisms to Find an Access Points

Bluetooth:

With Bluetooth, the terminal takes over the active part in looking for access points. The terminal sends out a search request and, provided this type of answering behavior has been activated, the LAN access point will reply by transmitting its Bluetooth address. If you don't want the LAN access point to be generally accessible, you can disable this answering behavior in the LAN access point. This makes it a lot more difficult for an attacker to find out whether potential access points exist, as they can no longer be identified via a simple search query.

WLAN:

In WLAN, the access point send messages to neighboring terminals within fixed time intervals to signal to them that it offers wireless access to a network. This fact is used by so called "war drivers" to find potential weak points.

Mechanisms for encrypting transferred data

All data transmission on the radio level is encrypted.In comparison to WLAN's WEP (Wireless Equivalent Privacy), Bluetooth's security mechanisms are significantly stronger.

Bluetooth:

Bluetooth uses the so-called E0 algorithm to encrypt data; here a new encryption key is used for each connection. Backtracking (recalculating) keys that use this algorithm requires considerably more effort and involves intercepting a much larger number of packages. Since a new encryption key is created each time a connection is established, it is practically impossible to backtrack the key.

WLAN:

WLAN uses the RC4 algorithm to encrypt data; here the same key is used to encrypt data for all connections. By passively intercepting data packages it is possible to backtrack (recalculate) the key after about 1,000.000 data

packages, after which all further data transmission can be passively read and decrypted.

Frequency Assignment for Data Transfers

Bluetooth:

The technology Bluetooth uses for assigning frequencies - frequency hopping (i.e. the frequency changes 1600 times per second) necessitates considerable technical effort for acquiring access and/or intercepting transmissions. At the same time, frequency hopping ensures a high level of protection against interference, which has a positive effect on data throughput.

WLAN:

Here, data transfers take place within a fixed frequency band. Passive interception is thus possible with the help of commonly available WLAN devices.

Range

It should not be underestimated that Bluetooth's shorter range (about 20 meters) also presents a security advantage. Only "attackers" who are situated within this short range can start such an attempt. "War-driver" attacks on corporate networks, a widely feared threat in WLAN systems, can be easily prevented by strategically positioning Bluetooth LAN access points (e.g. making use of blue2net's directivity) within the company premises by means of "physical measures" (see chapter 4.2).

3.2 User-related Security

Please always remember that users themselves carry a great deal of the responsibility for ensuring security:

a) Decision to use suitable passwords,

b) Striking a balance between high-security requirements and increased comfort, taking into account the intended use of the system (e.g. short passwords are of course easier to remember than passwords containing upper/lower case letters, numbers, and special characters),

c) Disciplined handling of passwords in order to prevent access to passwords (pay attention not to disclose passwords when assigning, storing or entering them).

4 Installation of blue2net

QuickGuide:

1. Mind the safety precautions.
2. Check the package contents.
3. Place blue2net on the table next to the laptop, for instance. Do not mount in final position before completing the initial installation.
4. Continue with chapter 4.3.1 (LAN operation, e.g. corporate network, Internet Service Provider cable modem) or 4.3.2 (xDSL modem operation).

4.1 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

4.2 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 (depending on the type of Bluetooth terminal used, the positioning of the blue2net unit, and the distance between terminal and blue2net, all the connected terminals together can share an effective net data throughput rate of up to 80 kByte/s. We would advise you to try out various 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

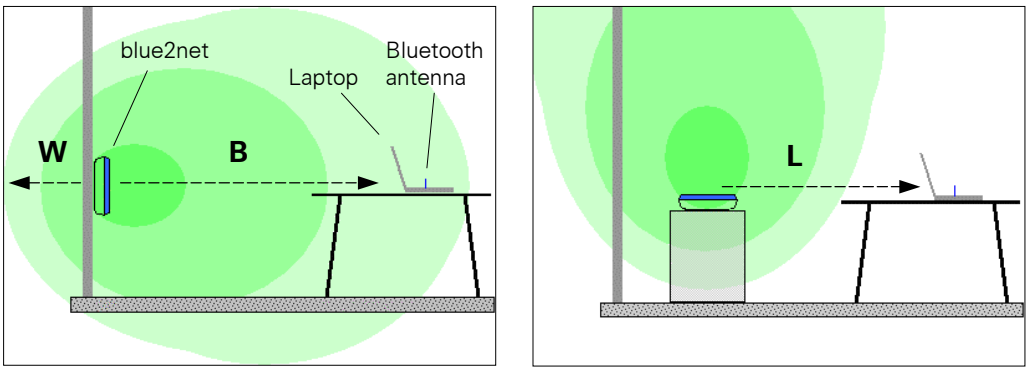


Figure 1 blue2net's directivity and how to achieve good transmission results

- 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.

4.3 Connecting blue2net to Your Ethernet

There are two ways to operate blue2net:

- on a LAN (e.g. corporate network, Internet Service Provider cable modem) (see chapter 4.3.1)
- on an xDSL modem (see chapter 4.3.2)

When shipped, blue2net comes configured for LAN operation.

Note: blue2net can serve as access router with both operation modes if you use an Ethernet switch for 10 Mbit/s.

4.3.1 Setting Up LAN Operation

Quick Guide:

How to proceed:

1. First, you need an IP address.
   Home users: Contact your Internet Service Provider (ISP). Register blue2net in the ISP's network, specifying the Ethernet MAC address (see label at the bottom side of the blue2net case).
   Corporate network: In most cases blue2net gets the IP address assigned automatically via a DHCP server. If not, contact the network administrator (keep blue2net's MAC address on hand, see label at the bottom side).
2. Connect blue2net via Ethernet cable to the LAN connector or cable modem (see Figure 2)
3. Plug in the power supply unit, the LED will start blinking. Wait for about 40 seconds until the indicator LED displays a steady light (in there is a problem, contact your network administrator or ISP).
4. Connect the terminal to blue2net via Bluetooth (see chapter 5)
5. Start your browser on the terminal (disable or bypass proxy settings, enable cookies).
6. Call up the web interface (homepage) via https://192.168.2.2 (see chapter 6.2)
7. Call up the configuration page (see chapter 6.4). Click "Configuration", enter "changeme" as password. Then immediately change the password and commit it to memory!
8. Define security settings and other configuration parameters. Choose a suitable scenario in chapter 7 (also see 6.5)
9. Permanently save the configuration (see chapter 8.9.2), The Bluetooth connection will automatically be aborted in the process.
10. To get access to the Internet, re-establish the Bluetooth connection (keep your Bluetooth password ready) and then start the browser on the Bluetooth terminal, unless it is already on.

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. If DHCP is used to assign IP addresses, your network administrator or ISP might ask you 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, 'MAC address').

If DHCP service is not available, blue2net will use its own fallback IP address. However, it is not possible to connect to the LAN with this IP address. You therefore need to ask your network administrator or ISP to assign a fixed IP address to your device and then configure it manually (see chapter 8.5.1).

How to proceed:

1. **First, connect 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 has 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, in particular ***security settings*** (for example, on the basis of the use scenarios provided in chapter 7), continue with chapter 6.5.

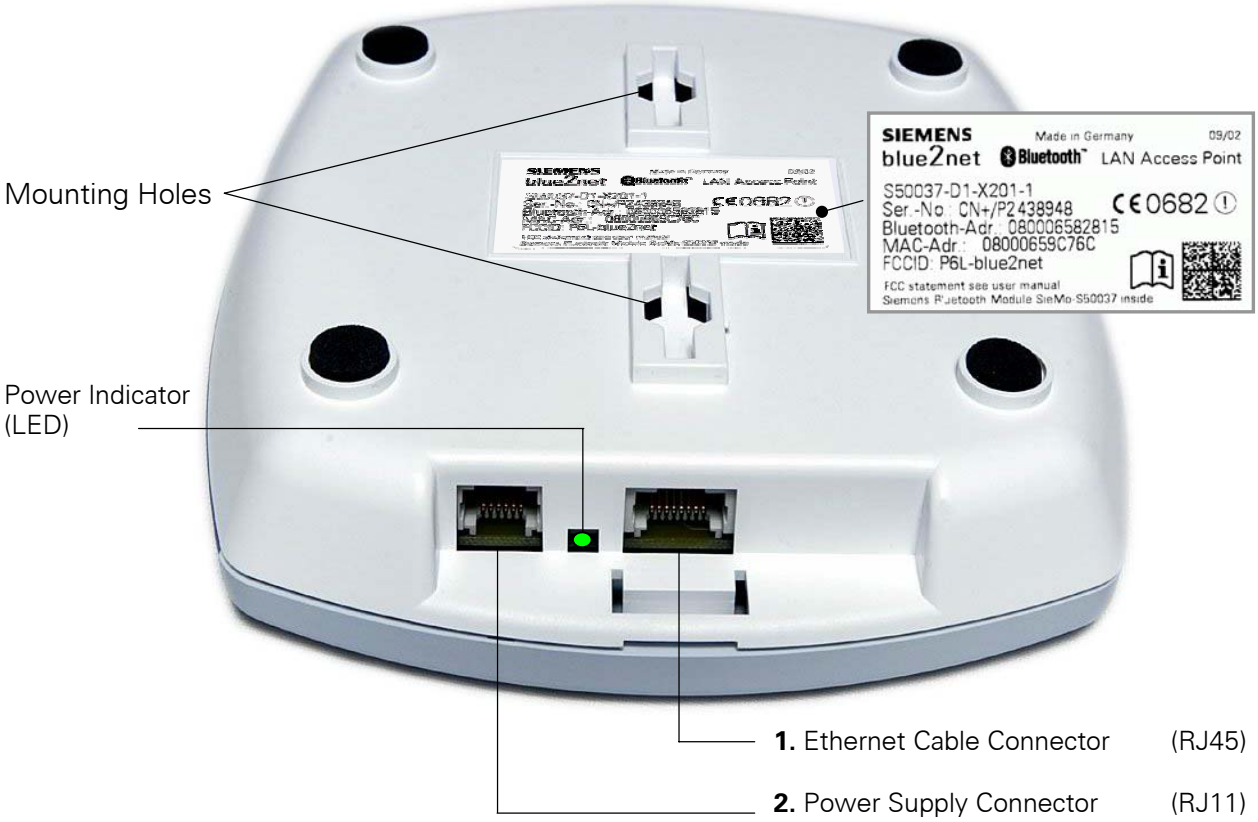


Figure 2 blue2net bottom view; connectors, mounting holes, LED, and label

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 (also indicated by the fact that this IP address is displayed on the Bluetooth terminal as suffix).

   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 the blue2net IP address manually (see chapter 8.5.1) .

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

After the manual blue2net IP configuration has been successfully carried out and a connection to the network is established, blue2net is basically ready to use. However, among other settings, you still need to define the ***security settings***. To choose suitable settings for your requirements, especially with respect to security, please refer to the use scenarios provided in chapter 7. Continue with chapter 6.5 ff.

4.3.2 Setting Up xDSL Modem Operation

Quick Guide:

When shipped, blue2net comes configured for LAN, so if you want to use it for xDSL, you have to reconfigure it first.

How to proceed:

1. Plug in the power supply unit, but don't connect to the xDSL modem yet (see Figure 2). Wait for about 2 minutes (indicator LED displays steady light).
2. Connect the terminal to blue2net via Bluetooth (see chapter 5)
3. Start your browser (disable or bypass proxy settings, enable cookies).
4. Call up the web interface (homepage) via https://192.168.2.2 (see chapter 6.2).
5. Call up the configuration page (see chapter 6.4).
   Click "Configuration", enter "changeme" as password. Then immediately change the password and commit it to memory!
6. Define the xDSL configuration and security settings. To be able to do so, select a suitable scenario in chapter 7.1.1 or chapter 7.3 (also see chapter 6.5 and 8.5.5)
7. Permanently save the configuration (see chapter 8.9.2), The Bluetooth connection will automatically be aborted in the process.
8. Connect blue2net via cable to the xDSL modem (see Figure 2).
9. To get access to the Internet, re-establish the Bluetooth connection (keep your Bluetooth password ready) (also see chapter 5) and then start the browser on the Bluetooth terminal, unless it is already on.

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) for the individual use scenarios provided in chapter 7.1.1 and 7.3, where you will also find proposals for suitable security settings without having to first study the parameter descriptions in detail. For a detailed description of all the parameters needed for the tunnel configuration required for xDSL operation, refer to chapter 8.5.5.

Remember not to set up the cable connection to the xDSL modem until after 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, PDA). 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 (green indicator LED emits a steady light).

2. Make xDSL configuration settings and then save settings to permanent memory:
   - For a listing of the parameters affected, refer to the xDSL scenarios in chapter 7.1.1 (parameters shown in **bold** print are, for technical reasons, absolutely mandatory for setting up an xDSL connection).
   - For information on how to set up a Bluetooth connection and how to access the configuration settings, refer to chapters 5 to 6.2 and 6.4.
   - For instructions on how to save data to permanent memory, refer to chapter 8.9.2.

   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 secure only if you have defined the security settings, e.g. based on a use scenario*** (see chapter 6.5).

4.4 Explanation of LED Behavior

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

Position of the indicator LED see Figure 2.

5 Connecting Terminal to blue2net via Bluetooth

Make sure that your Bluetooth terminal, such as a laptop, PDA or mobile phone, supports at least one of the following services:

- PAN-NAP (Personal Area Network - Network Access Point). A Bluetooth terminal with wireless connection will behave as if it were directly connected to the Ethernet via cable.

- LAP (LAN Access Profile). This profile is being replaced more and more by PAN-NAP.

Only applicable if you are using the "LAN Access Profile": if your Bluetooth terminal does not automatically set up a PPP connection (e.g. Remote Access Service under Windows operating systems, indicated by the  symbol in the status bar), you must set up such a connection yourself (for instructions on how to do this, refer to the User Guide of the Bluetooth module).

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

Basically, what you will have 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.

- Select the service you want ("PAN Network Access Point" service " or "LAN Access Profile").

- Connect your terminal to the selected device.
  In order to identify your blue2net device among several blue2net devices listed, look for its Bluetooth address . 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 ('Terminal Bluetooth Passkey [1.10.3]. By default, this Bluetooth passkey is set to '**1234**' on blue2net (see also chapters 8.1 and 8.3).

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 (LAN).

6.1 Required Browser Settings

- **Disable** the **proxy settings** on the Web browser of your PDA or laptop

  or

  bypass the proxy server. To stop the web browser from using the proxy server during the input of the blue2net IP address, enter, for example in IE 6.0, the blue2net IP address in the field below "Do not use proxy server for addresses beginning with:" (Proxy Settings/Exceptions).
- **Enable** the **cookies!**
- Make sure that your browser supports SSL 3.0 (for example, in the Internet Explorer, "Use SSL 3.0" should be selected under Tools > Internet Options > Advanced > Security.)

6.2 Access via Bluetooth

- You need an established Bluetooth connection to blue2net as described in chapter 5.
- Access blue2net's Web interface (Figure 3 shows the homepage) by entering the blue2net IP address in the address bar of the browser on the Bluetooth terminal:

  Please note the „**s**"!

  a) Applies only to status as shipped: Enter https://192.168.2.2 (Note that blue2net only supports secure access via https). This is the default IP address 'IP Masquerading' [2.5] that terminals connected via Bluetooth can use to access blue2net.

  b) If the 'IP Address Suffix Mode' is activated (factory setting), you will get the current bue2net IP address of the blue2net displayed after the Bluetooth Device Name. After a Bluetooth device inquiry, you can thus directly retrieve the IP address on the Bluetooth terminal and access the blue2net configuration pages by entering https://<retrieved IP address>

  c) If the 'IP Address Suffix Mode' is not activated, you will have to resort to written records to get the blue2net IP address.

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 the 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 6.2) and read the value of the parameter 'blue2net IP Address' (see 8.7.1).
- If the IP address was not assigned via DHCP, blue2net uses the fallback IP address (192.168.1.2). Make sure in that case that the IP address of the computer you use to carry out the configuration (= administration computer) and the blue2net fallback IP address are in the same subnet as blue2net (contact the network administrator, where necessary).
- Access blue2net's Web interface by entering **https://<blue2net IP address>** in the location/URL field of your Web browser (see Figure 3).

6.4 How to Get to the Configuration Page

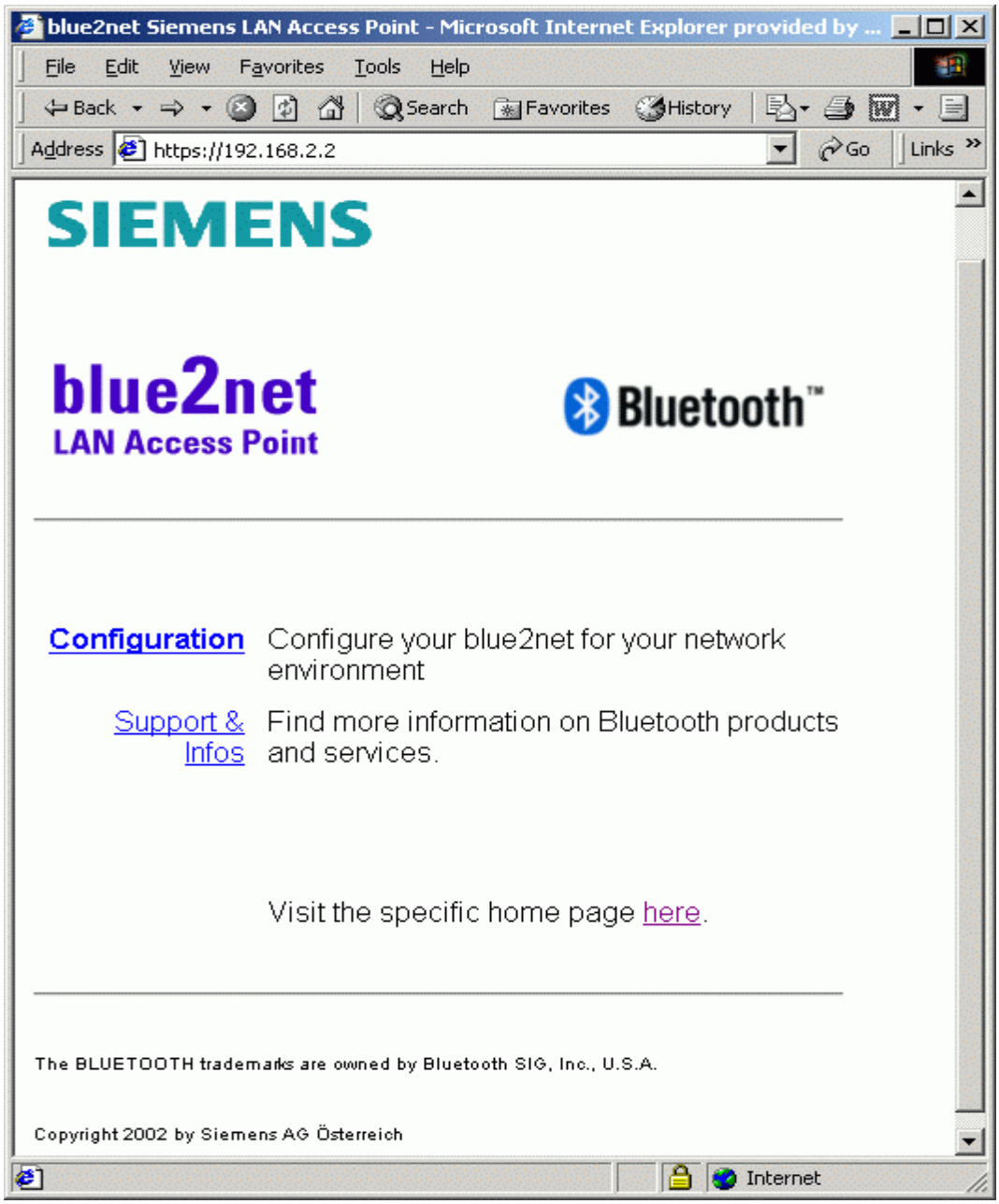


Figure 3 blue2net Web interface

- 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 8.8). 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 page. For more information on this essential issue, see chapter 10, "Preventing Lockout" !!.

6.5 Choosing Security Settings

Given the blu2net factory settings and provided you know the default passwords, you can use any Bluetooth terminal within a radio range of about 20 m to access the configuration pages and the LAN behind blue2net or to access the configuration pages from a PC via the LAN and make changes there as intended.

Be aware that your device will be secure only if you have defined and saved the security settings (as specified in the scenarios in chapter 7, for example).

- To prevent other people from accessing the blue2net configuration, change the default configuration password to a password of your choice.
- To prevent other people from using the Bluetooth connection, use features such as authorization, definition of passwords, restriction to certain terminals, strong encryption (e.g. 128-bit encryption), making blue2net non-discoverable, etc., but also by making use of blue2net's directivity.

LAN/cable modem operation:

After your blue2net has completed its start up phase it is basically ready to use. Be aware, however, that access to your blue2net is *secured only through the default passwords*.

To provide adequate security, choose one of the following options:

- Use the values from the use scenarios. Chapters 7.1.2, 7.1.3 and 7.2 provide settings for 3 typical use cases for LAN/cable modem.
- On the basis of the detailed description of all the parameters, choose the settings you want, e.g. because you want to configure blue2net to suit your own personal requirements. Chapter 8 provides details on each of the configuration settings.

xDSL modem operation:

To provide adequate security, choose one of the following options:

- When configuring the setting up of the tunnel connection, do *not use only the values shown in bold print* in the use scenarios provided in chapter 7.1.1 but also all the other settings applicable to your particular situation (home use in chapter 7.1.1 and 7.1.3, Hot Spot use in chapter 7.3).
- When configuring the setting up of the tunnel connection, do *use only the values shown in bold print* in the use scenarios shown in chapter 7.1.1 but configure the remaining values, for example, on the basis of the detailed descriptions of all the parameters on your own, e.g. because you want to configure blue2net to suit your own personal requirements. Chapter 8 provides details on each of the configuration settings.

7 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 10, "Preventing Lockout"

If you have just bought your blue2net, you only have to make the settings specified in the respective scenario; you can leave the remaining values just as they are (factory settings).

If you have already configured your blue2net, you can reset it to the factory settings (see chapter 8.9.5) and re-configure it in accordance with the recommendations given for the specific scenario.

Please take a brief look first at how you can change settings on blue2net (see chapters 8.1 and 8.2).

In the tables, each parameter comes with a hierarchy level, e.g. [1.8.4]. These hierarchy numbers, which are always enclosed in square brackets, also appear in the tables in chapter 8.3 ff and will frequently help you to identify and find the parameters you need.

Note: When you are setting up an in-house network with blue2net serving as router, it is generally preferable to use a switch rather than a hub, as there is a risk of data packet collisions in the network and resulting drops in the data rate.

7.1 Home Use Scenarios

7.1.1 Home Use Scenario with xDSL Modem (No Access Router))

Typical scenario: Several family members want to have access to the Internet via an xDSL modem. Only one person is authorized to edit the blue2net configuration parameters.
Characteristics: For security reasons, the blue2net unit needs to be protected against access by neighbors or unauthorized users outside the apartment or house (secure Bluetooth connections!)

This scenario applies to you only if you don't have an access router yet (your only Internet access so far was via PC, or your Internet access is completely new).

If you have been using a PC as access router for other PCs, you can now use blue2net instead. blue2net is noiseless (no moveable parts) and uses less energy than a PC in standby mode (<3.6W). As a small switch is cheaper than an access router, better use blue2net as access router.

If the only thing you want to do is to get wireless access to the WWW Internet, you can do without the devices shown in Figure 4 with a light-green background. In that case, connect blue2net directly to the xDSL modem. Likewise, you can skip the steps highlighted in light-green as explained in the configuration in Table 1 and Table 3.

Find out first whether your xDSL service provider is using PPPoE or PPtP as access protocol.

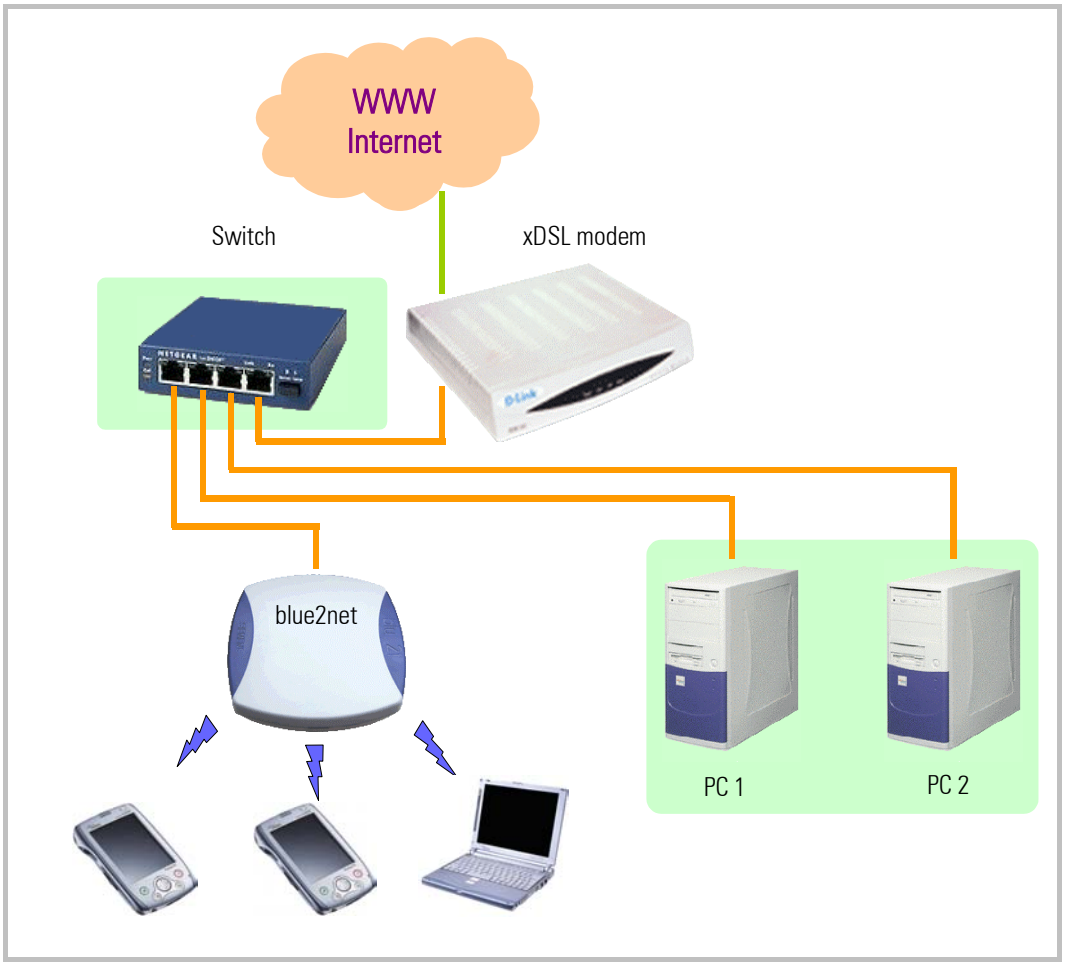


Figure 4 Scenario "Home use with xDSL modem"

xDSL modem with PPtP protocol (e.g. ADSL in Austria)

Make sure once more that your xDSL service provider uses PPtP as access protocol. Only in this case will the settings shown in the table below be suitable for your purposes.

Note: The parameters shown in bold print are the ones that absolutely have to be configured before you can connect blue2net for the first time with an xDSL modem (see chapter 4.3.2).

Parameter	Hier. lev.	Set to	Reason / Note
Bluetooth Device Name	[1.1.1]	Name of your choice (1...16 characters)	Required to identify your blue2net among other devices. Of course, you can retain the default name.
Default Access Mode	[1.11]	disabled	No access for everybody. Attention! Don't forget to make the settings in Table [1.10]!
Terminal Table	[1.10]	Bluetooth address [1.10.2], Bluetooth passkey [1.10.3] and Terminal IP address [1.10.4] of the terminals you are using most frequently. 'Allow Bluetooth Bonding' [1.10.5] is *enabled*	Here, you can enter the Bluetooth addresses of the Bluetooth devices of all family members. Each device has its own Bluetooth Passkey. If a device is to get the same IP address assigned at all times, enter it here as well (range from 192.168.2.71 to 192.168.2.253).
blue2net IP Address Resolution	[2.1]	predefined	The xDSL modem cannot reply to DHCP inquiries
Fixed blue2net IP Address	[2.2.1]	Example: [2.7.4]: is 10.0.0.138 (value predefined by the provider or derived from the description of the xDSL modem) [2.2.2]: 255.255.255.0 (blue2net factory setting) [2.2.1]: 10.0.0.140 'Fixed blue2net IP Address' lying in the same IP network as [2.7.4].	Set these parameters in such a way that 'Fixed blue2net IP Address' is in the same IP network as the IP address predefined by the xDSL modem, i.e. 'PPTP Server IP Address' [2.7.4]. So if the netmask is 255.255.255.0, [2.2.1] and [2.7.4] must be identical in the first 3 blocks, but must differ in the last block (less or greater than, min.1, max. 254).
Fixed blue2net Netmaks	[2.2.2]		
Fixed blue2net Gateway	[2.2.3]	0.0.0.0.	For this mode of operation this value is required

Parameter	Hier. lev.	Set to	Reason / Note
Default Firewall	[2.6.1]	enabled	Even though your devices (behind blue2net) are no longer reachable from the WWW Internet because of masquerading, you also enable the firewall to be absolutely sure to protect your in-house network against curiosity from the WWW.
Tunnel Mode	[2.7.1]	pptp	This table of settings is suitable for your purposes only if your xDSL provider uses PPtP as access protocol.
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'
PPTP Server IP Address	[2.7.4]	predefined IP address (could be e.g. 10.0.0.138)	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.
Additional IP Interface	[2.8.1]	enabled	Enables a second IP interface for the local in-house network. **If you are not operating an in-house network, you can omit this configuration step.**
Terminal IP Address Resolution	[3.1]	masquerading (default value)	With this kind of setting, the terminals do not require official IP addresses. You have already entered the devices of your family members in Table [1.10] 'Terminal Table'.
Local DHCP Server for Ethernet	[3.6.2]	enabled	Enables the internal blue2net DHCP server for Ethernet. **If you are not operating an in-house network, you can omit this configuration step.**

Parameter	Hier. lev.	Set to	Reason / Note
Fixed IP Addresses for Local Wired Network	[3.9]	[3.9.1] MAC address of the network cards [3.9.2] IP addresses for the network cards	You should enter the Ethernet-MAC addresses of the PCs/laptops participating (via cable) in your in-house network (address range 192.168.3.3 to 192.168.3.19). **If you are not operating an in-house network, you can omit this configuration step.**
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 1 Scenario "Home use with xDSL modem and PPtP", settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

Optional settings:

If you are frequently having problems accessing Internet pages (error message, for example, "The page cannot be displayed… Cannot find server or DNS Error"), a possible reason might be that the (external) DHCP server is not working reliably (also see chapter 13.3). In this case, you can make the following additional settings:

Parameter	Hier. lev.	Set to	Reason
Terminal DNS Server 1/2	[3.5.1] [3.5.2]	DNS server values as recommended by your service provider. Under 'Current Configuration' [4] >> 'Terminal Server Configuration' [4.3] you can find the values for the DNS server ([4.3.1] and [4.3.2]). (as long as the ISP's DHCP server is working)	Relevant only if your ISP's DHCP server does not work reliably.

Table 2 Scenario "Home use with xDSL modem and PPtP", optional settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

xDSL modem with PPPoE protocol (e.g. TDSL from Deutsche Telekom)

Please make sure once more that your xDSL service provider uses PPPoE as access protocol. Only in this case will the settings shown in the table below be suitable for your purposes.

Note: The parameters shown in bold print are the ones that absolutely have to be configured before you can connect blue2net for the first time with an xDSL modem (see chapter 4.3.2).

Parameter	Hier. lev.	Set to	Reason/Hints
Bluetooth Device Name	[1.1.1]	Name of your choice (1...16 characters)	Required to identify your blue2net among other devices. Of course, you can also retain the default name.
Default Access Mode	[1.11]	disabled	No access for everybody. Attention! Don't forget to make the settings in Table [1.10]!
Terminal Table	[1.10]	Bluetooth address [1.10.2], Bluetooth passkey [1.10.3] and Terminal IP address [1.10.4] of the terminals you are using most frequently. 'Allow Bluetooth Bonding' [1.10.5] is *enabled*	Here, you can enter the Bluetooth addresses of the Bluetooth devices of all family members. Each device has its own terminal Bluetooth passkey. If a device is to get the same IP address assigned at all times, enter it here as well (range from 192.168.2.71 to 192.168.2.253).
blue2net IP Address Resolution	[2.1]	predefined	The xDSL modem cannot reply to DHCP inquiries
Fixed blue2net IP Address	[2.2.1]	192.168.3.2	This the IP address of blue2net in your in-house network. **If you are not operating an in-house network, you can omit this configuration step.**.
Fixed blue2net Gateway	[2.2.3]	0.0.0.0.	For this mode of operation this value is required.

Parameter	Hier. lev.	Set to	Reason/Hints
Default Firewall	[2.6.1]	enabled	Even though your devices (behind blue2net) are no longer reachable from the WWW Internet because of masquerading, you also enable the firewall to be absolutely sure to protect your in-house network against curiosity from the WWW.
Tunnel Mode	[2.7.1]	pppoe	This table of settings is suitable for your purposes only if your xDSL provider uses PPPoE as access protocol.
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]	masqueradingpool	With this kind of setting, the terminals do not require official IP addresses.
Local DHCP Server for Ethernet	[3.6.2]	enabled	Enables the internal blue2net DHCP server for Ethernet. **If you are not operating an in-house network, you can omit this configuration step**.
Fixed IP Addresses for Local Wired Network	[3.9]	[3.9.1] MAC address of the network cards [3.9.2] IP addresses for the network cards	You should enter the Ethernet-MAC addresses of the PCs/laptops participating (via cable) in your in-house network (address range 192.168.3.3 to 192.168.3.19). **If you are not operating an in-house network, you can omit this configuration step.**
Configuration Password	[5.2]	Password of your choice (4…22 characters)	Only authorized persons (e.g. the family member who is most knowledgeable in network administrator) can configure blue2net. Attention! Make sure you remember the new password.

Table 3 Scenario "Home use with xDSL modem and PPPoE", settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

Optional settings:

If you are frequently having problems accessing Internet pages (error message, for example, "The page cannot be displayed… Cannot find server or DNS Error"), a possible reason might be that the (external) DHCP server is not working reliably (also see chapter 13.3). In this case, you can make the following additional settings:

Parameter	Hier. lev.	Set to	Reason
Terminal DNS Server 1/2	[3.5.1] [3.5.2]	DNS server values as recommended by your service provider. Under 'Current Configuration' [4] >> 'Terminal Server Configuration' [4.3] you can find the values for the DNS servers ([4.3.1] and [4.3.2]). (as long as the ISP's DHCP server is working)	Relevant only if your ISP's DHCP server does not work reliably.

Table 4 Scenario "Home use with xDSL modem and PPoE", optional settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

7.1.2 Home Use Scenario with Cable Modem (No Access Router)

Typical scenario: Several family members want to have access to the Internet via a cable modem. DHCP 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 activated to protect the PCs/laptops.

This scenario applies to you only if you do not have an access router yet (your only Internet access so far was via PC, or your Internet access is completely new).

If you have been using a PC as access router for other PCs, you can now use blue2net instead. blue2net is noiseless (no moveable parts) and uses less energy than a PC in standby mode (<3.6W). As a small switch is cheaper than an access router, better use blue2net as access router.

If the only thing you want to do is get wireless access to the WWW Internet, you can do without the devices shown in Figure 5 with a light-green background. In that case, connect blue2net directly to the cable modem. Likewise, you can skip the steps highlighted in light-green as explained in the configuration in Table 5.

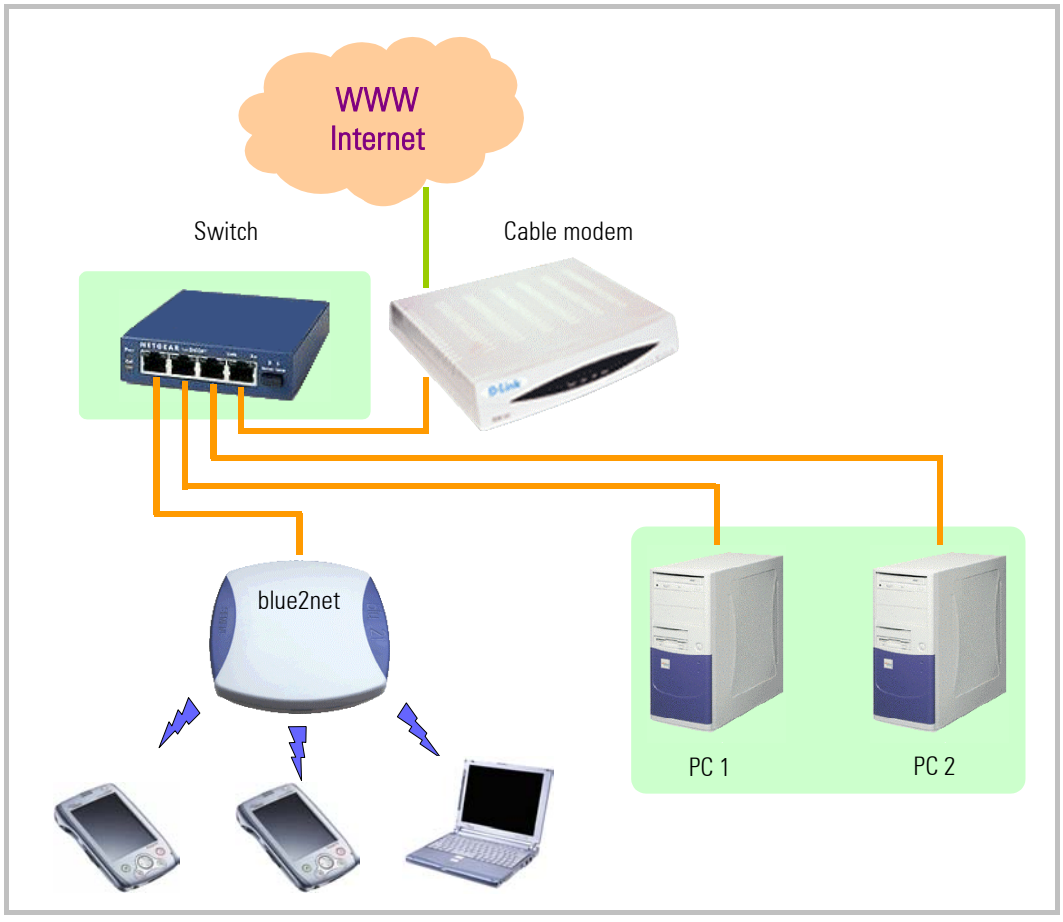


Figure 5 Scenario "Home use with cable modem"

Parameter	Hier. lev.	Set to	Reason/Hint
Bluetooth Device Name	[1.1]	Name of your choice (1...16 characters)	Required to identify your blue2net among other Bluetooth devices. Of course, you can retain the default name.
Terminal Table	[1.10]	Bluetooth address [1.10.2], Bluetooth passkey [1.10.3] and Terminal IP address [1.10.4] of the terminals you are using most frequently. 'Allow Bluetooth Bonding' [1.10.5] is *enabled*	Here, you can enter the Bluetooth addresses of the Bluetooth devices of all family members. Each device has its own terminal Bluetooth passkey. If a device is to get the same IP address assigned at all times, enter it here as well (range from 192.168.2.71 to 192.168.2.253).
Default Access Mode	[1.11]	disabled	No access for everybody. Attention! Don't forget to make the settings in Table [1.10]!
blue2net IP Address Resolution	[2.1]	dhcp (default value)	You Internet Service Provider will assign an official IP address via DHCP.
Default Firewall	[2.6.1]	enabled	Even though your devices (behind blue2net) are no longer reachable from the WWW Internet because of masquerading, you also enable the firewall to be absolutely sure to protect your in-house network against curiosity from the WWW.
Additional IP Interface	[2.8.1]	enabled	Enables a second IP interface for the local in-house network. **If you are not operating an in-house network, you can omit this configuration step.**
Local DHCP Server for Ethernet	[3.6.2]	enabled	Enables the DHCP server for Ethernet. **If you are not operating an in-house network, you can omit this configuration step.**

Parameter	Hier. lev.	Set to	Reason/Hint
Fixed IP Addresses for Local Wired Network	[3.9]	[3.9.1] MAC address of the network cards [3.9.2] IP addresses for the network cards	You should enter the Ethernet-MAC addresses of the PCs/laptops participating (via cable) in your in-house network (address range 192.168.3.3 to 192.168.3.19). **If you are not operating an in-house network, you can omit this configuration step.**
Configuration Password	[5.2]	Password of your choice (4…22 characters)	Only authorized persons (e.g. the system administrator) may configure blue2net. Attention! Do not forget the new password!

Table 5 Scenario "Home use with cable modem", settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

Optional settings:

If you are frequently having problems accessing Internet pages (error message, for example, "The page cannot be displayed… Cannot find server or DNS Error"), a possible reason might be that the (external) DHCP server is not working reliably (also see chapter 13.3). In this case, you can make the following additional settings:

Parameter	Hier. lev.	Set to	Reason
Fallback blue2net IP Address Fallback blue2net Netmask Fallback blue2net Gateway	[2.3.1] [2.3.2] [2.3.3]	IP parameter as supplied by service provider (Under 'Current Configuration' [4] >> 'blue2net IP Configuration' [4.2] you will find the values for the blue2net IP address [4.2.1],the netmask [4.2.2], and gateway. [4.2.3].	Most Internet service providers assign always the same IP parameters for services via cable modem If you enter these values as fallback values here, a short server failure at the ISP will not bother you if blue2net is restarting exactly at the time this happens.
Terminal DNS Server 1/2 Terminal WINS Server 1/2 Terminal Domain Name	[3.5.1] [3.5.2] [3.5.3] [3.5.4] [3.5.5]	DNS server values as recommended by your service provider (Under 'Current Configuration' [4] >> 'Terminal Server Configuration' [4.3] you will find the values for the DNS servers ([4.3.1] and [4.3.2]), the WINS servers ([4.3.3] and [4.3.4]) and domain name [4.3.5] (as long as the ISP's DHCP server is working).	Relevant only if your Internet provider's DHCP server does not work reliably.

Table 6 Scenario "Home use with cable modem", optional settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

7.1.3 Home Use Scenario with Access Router

Typical scenario: Several family members want to have access to the Internet via a cable modem or an xDSL modem. Only one person is authorized to edit the blue2net configuration parameters.
Additional assumptions: There is an access router in place to serve the cable modem or xDSL modem and to provide the Masquerading, Firewall, and DHCP functionalities (access router and cable modem/xDSL modem may be combined in one device).
Characteristics: For security reasons, the blue2net unit needs to be protected against access by neighbors or unauthorized users outside the apartment or house (secure Bluetooth connections!).

You may already have a small in-house network allowing all family members to access the Internet. Now you want to use blue2net to provide a wireless connection that enables you to comfortably surf the Net or read your e-mails from the sofa, using a PDA or laptop. Figure 6 illustrates the situation: devices shown against a white background are already in place, devices shown in the blue frame are supposed to be connected to the Internet and the in-house network.

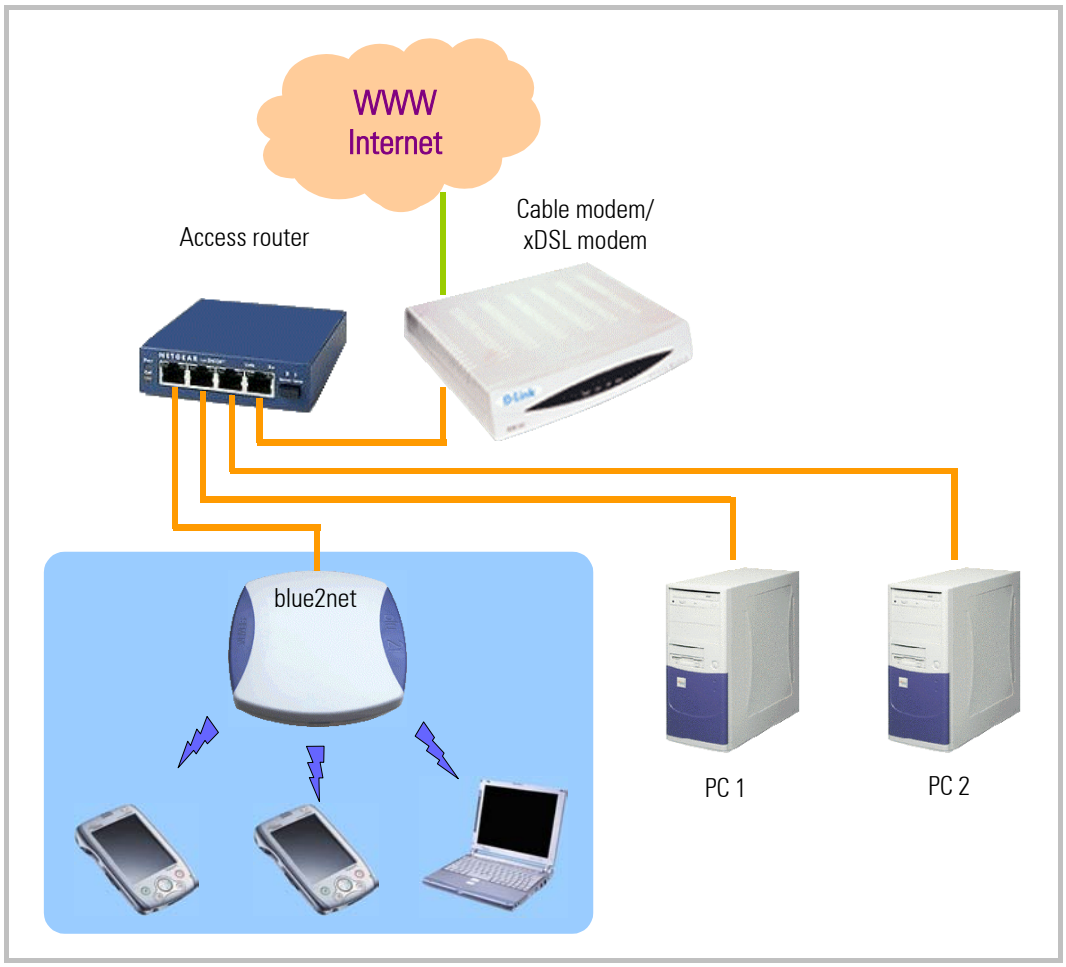


Figure 6 Scenario "Home use with access router"

Parameter	Hier. lev.	Set to	Reason
Bluetooth Device Name	[1.1.1]	Name of your choice (1...16 characters)	In an environment with many blue2net units, they should all have a unique name for clear differentiation. Of course, you can also retain the default name.
Terminal Table	[1.10]	All terminals are registered. The Bluetooth address [1.10.2) and the respective Bluetooth passkey [1.10.3] (**16 digits!!**) is already entered for you. The IP address [1.10.3] is set to *0.0.0.0*. 'Allow Bluetooth Bonding' [1.10.5] is enabled	All users have a Bluetooth password of their own which only provides access when combined with your Bluetooth device. Make use of all 16 digits of the Bluetooth passkey to ensure maximum security.
Default Access Mode	[1.11]	disabled	Only devices whose Bluetooth address is listed in [1.10] and which know the required Bluetooth passkey will be granted access.
Minimum Length of Key for Encryption	[1.13]	16	Encryption strength set to maximum (128 bit). This setting grants access only to devices supporting this encryption strength. **Caution!** Danger of lockout! Verify first whether or not your terminal supports 128 bit encryption (see chapters 10.2 and 13.2).
Terminal IP Address Resolution	[3.1]	dhcp	All Bluetooth devices get IP addresses and other information assigned by your internal blue2net DHCP server.
Local DHCP Server for NAP	[3.6.1]	disabled	As you have a DHCP server of your own attached to the access router, disable the DHCP server for NAP terminals on blue2net.
IP Connection Mode for NAP Terminals	[3.7]	bridging	Bluetooth devices that use the NAP service are connected directly to the Ethernet.
Configuration Password	[5.2]	Password of your choice	Only authorized persons (e.g. the system administrator) can

Parameter	Hier. lev.	Set to	Reason
		(4…22 characters)	configure blue2net. Attention! Do not forget the new password

Table 7 Scenario "Home use with access router", settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

Optional settings:

If you are frequently having problems accessing Internet pages (error message, for example, "The page cannot be displayed… Cannot find server or DNS Error"), a possible reason might be that the (external) DHCP server is not working reliably (also see chapter 13.3). In this case, you can make the following additional settings:

Parameter group	Hier. lev.	Set to	Reason
Fallback blue2net IP Address Fallback blue2net Netmask Fallback blue2net Gateway	[2.3.1] [2.3.2] [2.3.3]	Values blue2net normally receives via DHCP on the access router. Please enter the values you have reserved for blue2net on your DHCP server on the access router (also available under 'Current Configuration' [4] >> 'blue2net IP Configuration' [4.2] >> blue2net IP address [4.2.1], netmask [4.2.2] and gateway [4.2.3].	blue2net falls back on these values if your DHCP server fails temporarily during blue2net restart.
Terminal DNS Server 1/2 Terminal WINS Server 1/2 Terminal Domain Name	[3.5.1] [3.5.2] [3.5.3] [3.5.4] [3.5.5]	Values normally distributed via DHCP (DNS). Please enter the values your DHCP server on the access router would normally send to blue2net in the case of a DHCP inquiry (also available under 'Current Configuration' [4] >> 'Terminal Server Configuration' [4.3] >> DNS-Server [4.3.1] and [4.3.2]) and [4.3.2], WINS-Server [4.3.3] and [4.3.4] as well as Domain-Name [4.3.5] (as long as the ISP's DHCP server is working)	blue2net falls back on these values if your DHCP server fails temporarily during blue2net restart.

Table 8 Scenario "Home use with access router", optional settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

7.2 Business Scenarios

7.2.1 Business Scenario with Controlled General Access

Typical scenario: meeting rooms or conference rooms where participants (customers, visitors) are granted temporary access via the default Bluetooth passkey [1.12] .
Characteristics: The security level is medium; everybody knowing the Bluetooth passkey has access to the LAN; only authorized persons have access to the configuration settings.
For security reasons, blue2net should be set up on a separate network segment outside the company firewall in this scenario.
Connection: blue2net is connected to a company network segment and supplied with an IP address via the DHCP server of this separate network segment.

Parameter	Hier. lev.	Set to	Reason
Bluetooth Device Name	[1.1.1]	Name of your choice (1...16 characters)	In an environment with many blue2net units, they should all have a unique name for clear differentiation.
Auth. Level	[1.8.4]	noauth	You grant everybody who is able to detect your blue2net device access to the network blue2net is connected to. **Security note**: Since everybody is granted access, it is important that blue2net is set up on a separate network segment outside the company firewall.
Terminal Table	[1.10]	No terminals registered (Bluetooth address set to *00:00:00:00:00:00*) (default value)	All users should get access with the 'Default Bluetooth Passkey' [1.12] .
Default Bluetooth Passkey	[1.12]	Passkey or your choice (1…16 characters)	The password should be easy to obtain for the user.
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 9 Scenario "Business, controlled general access", settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

Optional settings:

If you are frequently having problems accessing Internet pages (error message, for example, "The page cannot be displayed… Cannot find server or DNS Error"), a possible reason might be that the (external) DHCP server is not working reliably (also see chapter 13.3). In this case, you can make the following additional settings:

Parameter group	Hier. lev.	Set to	Reason
Fallback blue2net IP Address Fallback blue2net Netmask Fallback blue2net Gateway	[2.3.1] [2.3.2] [2.3.3]	Values blue2net normally receives via DHCP. Please enter the values you have reserved for blue2net on your corporate DHCP server (also available under 'Current Configuration' [4] >> ,blue2net IP Configuration' [4.2] >> blue2net IP address [4.2.1, netmask [4.2.2], and gateway [4.2.3].	blue2net falls back on these values if your corporate DHCP server fails temporarily.
Terminal DNS Server 1/2 Terminal WINS Terminal Domain Name	[3.5.1] [3.5.2] [3.5.3] [3.5.4] [3.5.5]	Values normally distributed via DHCP (DNS). Please enter the values your corporate DHCP server would normally send to blue2net in the case of a DHCP inquiry (also available under 'Current Configuration' [4] >> ,Terminal Server Configuration' [4.3] >> DNS-Server [4.3.1] and [4.3.2]),]), the WINS servers ([4.3.3] and [4.3.4]) and domain name [4.3.5] (as long as the ISP's DHCP server is working).	blue2net falls back on these values if your corporate DHCP server fails temporarily.

Table 10 Scenario "Business, controlled general access", optional settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

7.2.2 Business Scenario with Secured Employee Access to Corporate Network

Typical scenario: Field service staff occasionally come in to submit reports, read and send e-mails or download new data onto their laptops or PDAs.
Characteristics: The security level is high, only Bluetooth devices listed in table [1.10] and authenticated with a device-specific passkey will get access to the local LAN (and Internet, where applicable). All data transfer is encrypted on the radio level. In contrast to WEP in WLANs, the Bluetooth security mechanisms are so strong that you can really feel secure with it.
Additional assumptions: It is assumed that you use a different device to run a DHCP server and another one to handle the Internet link-up of your corporate network. blue2net is integrated into your corporate network inside the firewall.

Parameter	Hier. lev.	Set to	Reason
Bluetooth Device Name	[1.1.1]	Name of your choice (1...16 characters)	In an environment with many blue2net units, they should all have a unique name for clear differentiation.
Discoverability Mode	[1.4]	nondiscoverable	This setting makes it more difficult for potential attackers to even discover your blue2net. Only when a new Bluetooth terminal is added is the setting temporarily switched to *discoverable*.
Terminal Table	[1.10]	All terminals are registered. For the terminals, the Bluetooth address [1.10.2) and the respective Bluetooth passkey [1.10.3] (**16 digits!!**) is already entered The IP address [1.10.3] is set to *0.0.0.0*. 'Allow Bluetooth Bonding' [1.10.5] is *enabled*	All users have a Bluetooth password of their own which only provides access when combined with your Bluetooth device. Please make use of all 16 digits of the Bluetooth passkey.
Default Access Mode	[1.11]	disabled	Only devices whose Bluetooth address is listed in [1.10] and which know the required Bluetooth passkey will be granted access.

Parameter	Hier. lev.	Set to	Reason
Minimum Length of Key for Encryption	[1.13]	16	Encryption strength set to maximum (128 bit). This setting grants access only to devices supporting this encryption strength. **Caution!** Danger of lockout! Verify first whether or not your terminal supports 128 bit encryption (see chapters 10.2 and 13.2).
Terminal IP Address Resolution	[3.1]	dhcp (default value)	All Bluetooth devices get IP addresses and other information assigned by the corporate DHCP server.
Local DHCP Server for NAP	[3.6.1]	disabled	As the company has a DHCP server of its own, disable the DHCP server for NAP terminals on blue2net.
IP Connection Mode for NAP Terminals	[3.7]	bridging	Bluetooth devices that use the NAP service are connected directly to the Ethernet.
Configuration Password	[5.2]	Password of your choice (4…22 characters)	Only authorized persons (e.g. the system administrator) can configure blue2net. Attention! Do not forget the new password

Table 11 Scenario "Business, secured employee access", settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

Optional settings:

If you are frequently having problems accessing Internet pages (error message, for example, "The page cannot be displayed… Cannot find server or DNS Error"), a possible reason might be that the (external) DHCP server is not working reliably (also see chapter 13.3). In this case, you can make the following additional settings:

Parameter group	Hier. lev.	Set to	Reason
Fallback blue2net IP Address Fallback blue2net Netmask Fallback blue2net Gateway	[2.3.1] [2.3.2] [2.3.3]	Values blue2net normally receives via DHCP. Please enter the values you have reserved for blue2net on your corporate DHCP server (also available under 'Current Configuration' [4] >> ,blue2net IP Configuration' [4.2] >> blue2net IP address [4.2.1, netmask [4.2.2], and gateway [4.2.3].	blue2net falls back on these values if your corporate DHCP server fails temporarily.
Terminal DNS Server 1/2 Terminal WINS Terminal Domain Name	[3.5.1] [3.5.2] [3.5.3] [3.5.4] [3.5.5]	Values normally distributed via DHCP (DNS). Please enter the values your corporate DHCP server would normally send to blue2net in the case of a DHCP inquiry (also available under 'Current Configuration' [4] >> ,Terminal Server Configuration' [4.3] >> DNS-Server [4.3.1] and [4.3.2]),]), the WINS servers ([4.3.3] and [4.3.4]) and domain name [4.3.5] (as long as the ISP's DHCP server is working).	blue2net falls back on these values if your corporate DHCP server fails temporarily.

Table 12 Scenario "Business, secured employee access", optional settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

7.3 Public Use Scenarios (Public Hot Spot)

7.3.1 Scenario with Public Access for a Small Number of Users (Small Hot Spot, xDSL)

Typical scenario: airport lounges, lounges in small hotels, small (Internet) cafes.
Characteristics: Quick and easy access, authorization for everybody, only authorized persons have access to the blue2net configuration settings, maximum number of simultaneous users: 7.
Additional assumptions: It is assumed, for example, that in addition to blue2net you have an xDSL modem with Ethernet connection and a contract with an xDSL Internet service provider.

Parameter	Hier. lev.	Set to	Reason
Bluetooth Device Name	[1.1.1]	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. You can use, for instance, the name of your Internet café or something similar.
Terminal Table	[1.10]	Bluetooth address [1.10.2], Bluetooth passkey [1.10.3] and Terminal IP address [1.10.4] of your most frequently used terminals 'Allow Bluetooth Bonding' [1.10.5] is *enabled*	If you want to support "VIPs" with a fixed terminal IP address, set 'Terminal IP Address Resolution' [3.1] to *masqueradingpool*.
Default Bluetooth Passkey	[1.12]	General Bluetooth passkey	The Bluetooth passkey may include a reference to the name of your Internet café, for example, to make it easier to remember for your customers.
blue2net IP Address Resolution	[2.1]	predefined	This setting is required to allow the use of the PPtP and PPPoE protocols.

Parameter	Hier. lev.	Set to	Reason
Fixed blue2net IP Configuration	[2.2]	Values as specified by the xDSL service provider	If your xDSL service provider uses PPtP as protocol, enter the values requested by the provider. If your xDSL provider uses PPPoE, you can retain the default settings. In both cases, set ‚Fixed blue2net Gateway' [2.2.3] to *0.0.0.0*
Tunnel Mode	[2.7.1]	pppoe or pptp	To find out which tunnel protocol to use for your xDSL access, contact your xDSL service provider
Tunnel Establishment Control	[2.7.2]	enabled or disabled	If your xDSL service provider charges you for online time, you should set the Tunnel-Establishment Control to *enabled* so you will be online only if somebody is actually using your hotspot.
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'
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.
Terminal Fixed Servers	[3.5]	DNS-Server 1 u. 2 [3.5.1] u. [3.5.2] Enter the values recommended by your xDSL service provider.	
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 13 Scenario "Public access (small hot spot)", settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) then wait for about 2 minutes. Then the device will be ready for use again.

Optional settings:

If you are frequently having problems accessing Internet pages (error message, for example, "The page cannot be displayed… Cannot find server or DNS Error"), a possible reason might be that the (external) DHCP server is not working reliably (also see chapter 13.3). In this case, you can make the following additional settings:

Parameter	Hier. level	Set to	Reasons
Terminal DNS Server 1/2	[3.5.1] [3.5.2]	DNS server values as recommended by your service provider. Under 'Current Configuration' [4] >> 'Terminal Server Configuration' [4.3] you can find the values for the DNS server ([4.3.1] and [4.3.2]). (as long as the ISP's DHCP server is working)	Relevant only if your ISP's DHCP server does not work reliably.

Table 14 Scenario "Public access (small hot spot)", optional settings

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) then wait for about 2 minutes. Then the device will be ready for use again.

7.3.2 Scenario with Public Access for a Large Number of Users (Large Hot Spot, xDSL)

Typical scenario: airport lounges, lounges in big hotels, larger (Internet) cafes.
Characteristics: Quick and easy access, authorization for everybody, only authorized persons have access to the blue2net configuration settings, maximum number of simultaneous users: 28.
Additional assumptions: It is assumed, for example, that in addition to several blue2net units you have an xDSL modem with Ethernet connection and a contract with an xDSL Internet service provider. You need a separate blue2net unit for every 7 users simultaneously accessing the Internet via Bluetooth.

You can grant simultaneous Internet access to more than 7 users by cascading several blue2net units.

In this case, there are 2 roles:

- The master blue2net is the device that serves the xDSL modem and supplies the customers' Bluetooth terminals (laptops, PDAs) with an IP address via DHCP.
- The remaining blue2net units are configured to act as slaves.

The master serves as access router, because its net use bandwidth on the Ethernet interface is about 300 kBps (kilobytes per second) or 2.4 Mbps (megabits per second). A blue2net unit has a net radio bandwidth of about 80 kBps, so you can operate 1 master and 3 slaves without restrictions.

Please note that you should also have a bandwidth of 300 kBps available via xDSL if you want to avoid restrictions when all users are active at the same time.

Technical information: As Bluetooth uses a fast frequency hopping procedure (1600 frequency changes per second) and has 79 frequencies at its disposal, which are used "at random", the operation of several access points (up to 10 and more) does not result in noticeable drops in performance.

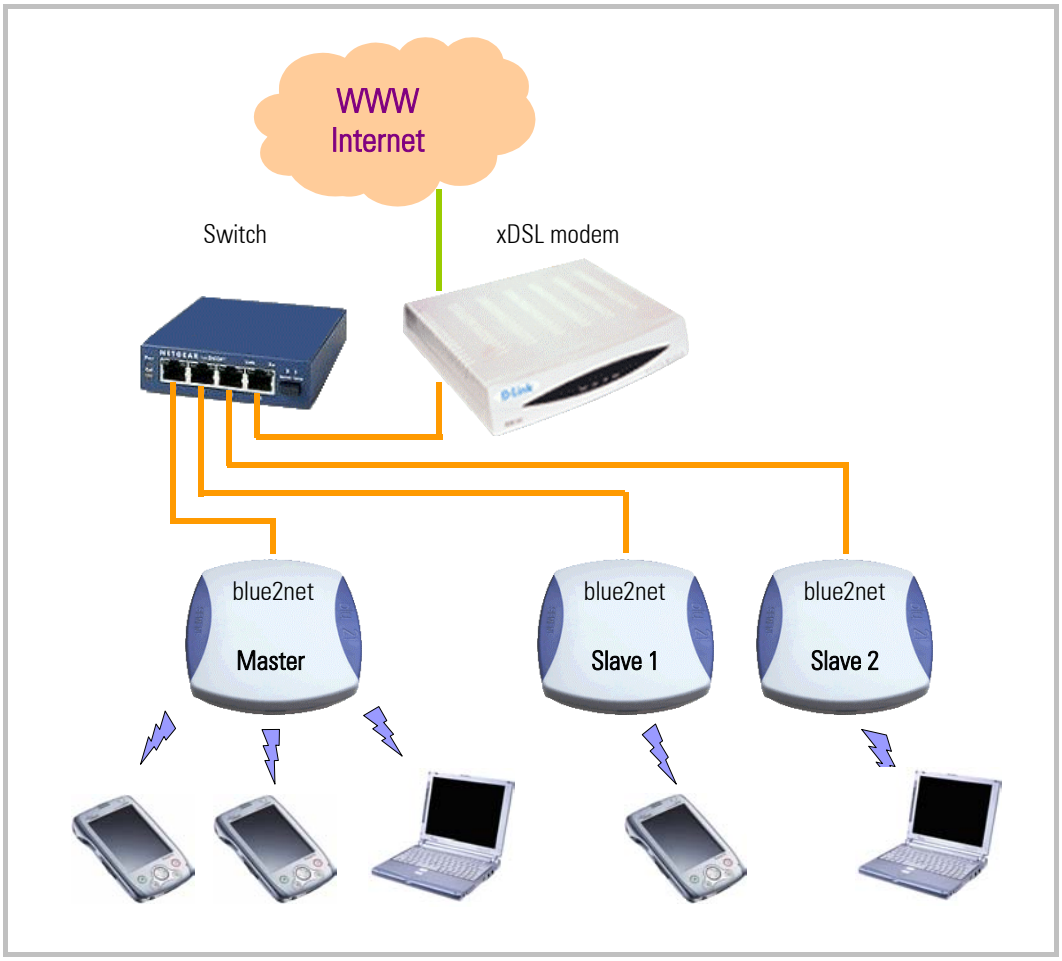


Figure 7 Scenario "Public access (large hot spot)" with master/slave configuration

Settings for the master blue2net:

Note on starting up the master blue2net: Since the master blue2net supplies the slave blue2nets with IP addresses, the master should be ready to operate before the slaves are switched on.

Parameter	Hier. lev.	Set to	Reason
Bluetooth Device Name	[1.1.1]	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. You can use, for instance, the name of your Internet café or something similar.
Terminal Table	[1.10]	Bluetooth address [1.10.2], Bluetooth passkey [1.10.3] and Terminal IP address [1.10.4] of your most frequently used terminals 'Allow Bluetooth Bonding' [1.10.5] is *enabled*	You want to support "VIPs" with a fixed terminal IP address. You should also enter the Ethernet-MAC addresses of the slave blue2nets as well as the Internet addresses specified for you in the 192.16.8.2.x network. (range 192.168.2.71-192.168.2.253)
Default Bluetooth Passkey	[1.12]	General Bluetooth passkey	The Bluetooth passkey may include a reference to the name of your Internet café, for example, to make it easier to remember for your customers.
blue2net IP Address Resolution	[2.1]	predefined	Via PPtP and PPPoE, there is no DHCP support..
Fixed blue2net IP Configuration	[2.2]	Values as specified by the xDSL service provider	If your xDSL service provider uses PPtP as protocol, enter the values requested by the provider. If your xDSL provider uses PPPoE, please enter the address given under 'IP Masquerading' [2.5], e.g. 192.168.2.2 . In both cases, please set ‚Fixed blue2net Gateway' [2.2.3] to *0.0.0.0*

Parameter	Hier. lev.	Set to	Reason
Tunnel Mode	[2.7.1]	pppoe or pptp	To find out which tunnel protocol to use for your xDSL access, contact your xDSL service provider
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'
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.
Additional IP Interface for blue2net	[2.8.1]	enabled/disabled second IP interface	If your xDSL service provider uses PPtP, change the setting to *enabled*. If your xDSL service provider uses PPPoE, leave the setting *disabled* unchanged
Local DHCP Server for Ethernet	[2.6.2]	enabled	Enable the internal blue2net DHCP server for Ethernet.
IP Connection Mode for NAP Terminals	[3.7]	bridging	Set the mode for the network access profile users to *bridging*
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 15 Scenario "Public access (large hot spot)", settings for master blue2net

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

Optional settings:

If you are frequently having problems accessing Internet pages (error message, for example, "The page cannot be displayed… Cannot find server or DNS Error"), a possible reason might be that the (external) DHCP server is not working reliably (also see chapter 13.3). In this case, you can make the following additional settings:

Parameter	Hier. lev.	Set to	Reason
Terminal DNS Server 1/2	[3.5.1] [3.5.2]	DNS server values as recommended by your service provider. Under 'Current Configuration' [4] >> 'Terminal Server Configuration' [4.3] you can find the values for the DNS server ([4.3.1] and [4.3.2]). (as long as the ISP's DHCP server is working)	Relevant only if your ISP's DHCP server does not work reliably.

Table 16 Scenario "Public access (large hot spot)", optional settings for master blue2net

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

Settings for the slave blu2nets:

Parameter	Hier. lev.	Set to	Reason
Bluetooth Device Name	[1.1.1]	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. You can use, for instance, the name of your Internet café or something similar.

Parameter	Hier. lev.	Set to	Reason
Terminal Table	[1.10]	Bluetooth address [1.10.2], Bluetooth passkey [1.10.3] and Terminal IP address [1.10.4] of your most frequently used terminals 'Allow Bluetooth Bonding' [1.10.5] is *enabled*	You want to support "VIPs" with a fixed terminal IP address. Leave the IP address of the VIP terminals at 0.0.0.0, as it is assigned by the master blue2net via DHCP. Note: Choose the same Bluetooth address [1.10.2] and Bluetooth passkey [1.10.3] as for the master blue2net (identical table except for the IP address).
Default Access Mode	[1.11]	enabled (default value)	Easy access for everybody
Default Bluetooth Passkey	[1.12]	General Bluetooth passkey	The Bluetooth passkey may include a reference to the name of your Internet café, for example, to make it easier to remember for your customers.
blue2net IP Address Resolution	[2.1]	dhcp (default value)	The slave blue2nets get their IP address assigned by the master blue2net.
Terminal IP Address Resolution	[3.1]	dhcp	The IP addresses of all terminals are managed by the master blue2net and distributed via DHCP.
Local DHCP Server for NAP	[3.6.1]	disabled	Disable the internal blue2net DHCP server for NAP, the master blue2net will take over this function.
IP Connection Mode for NAP Terminals	[3.7]	bridging	Set the mode for the network access profile users to *bridging*
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 17 Scenario "Public access (large hot spot)", settings for slave blue2net

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

Optional settings:

If you are frequently having problems accessing Internet pages (error message, for example, "The page cannot be displayed… Cannot find server or DNS Error"), a possible reason might be that the (external) DHCP server is not working reliably (also see chapter 13.3). In this case, you can make the following additional settings:

Parameter	Hier. lev.	Set to	Reason
Fallback blue2net IP Address Fallback blue2net Netmask Fallback blue2net Gateway	[2.3.1] [2.3.2] [2.3.3]	[2.3.1]: Enter the same IP parameters as you did for the master of this slave under [1.10.4] [2.3.2]: ‚Terminal netmask' [3.4] of the master blue2net, e.g. 255.255.255.0. [2.3.3]: Masquerading-IP ‚IP Masquerading' [2.5] of the master blue2net, e.g. 192.168.2.2 .	These values serve as fallback values only if the master blue2net fails during the restart of the slave.
Terminal DNS Server 1/2	[3.5.1] [3.5.2]	DNS server values as recommended by your service provider (Under 'Current Configuration' [4] >> 'Terminal Server Configuration' [4.3] you will find the values for the DNS servers ([4.3.1] and [4.3.2]), (as long as the ISP's DHCP server is working).	These values serve as fallback values only if the master blue2net fails during the restart of the slave.

Table 18 Scenario "Public access (large hot spot)", optional settings for slave blue2net

Do not forget to save the settings using 'Save Settings Permanently' [6.2] (see chapter 8.9.2) and then wait for about 2 minutes. Then the device will be ready for use again.

8 Configuration

8.1 Main Configuration Page

Click on **Configuration** on the Web interface (see Figure 3) to get the following overview (Figure 8). The numbers between square brackets indicate the place of a parameter in the hierarchy of the Web interface (see chapter 8.3 for details).

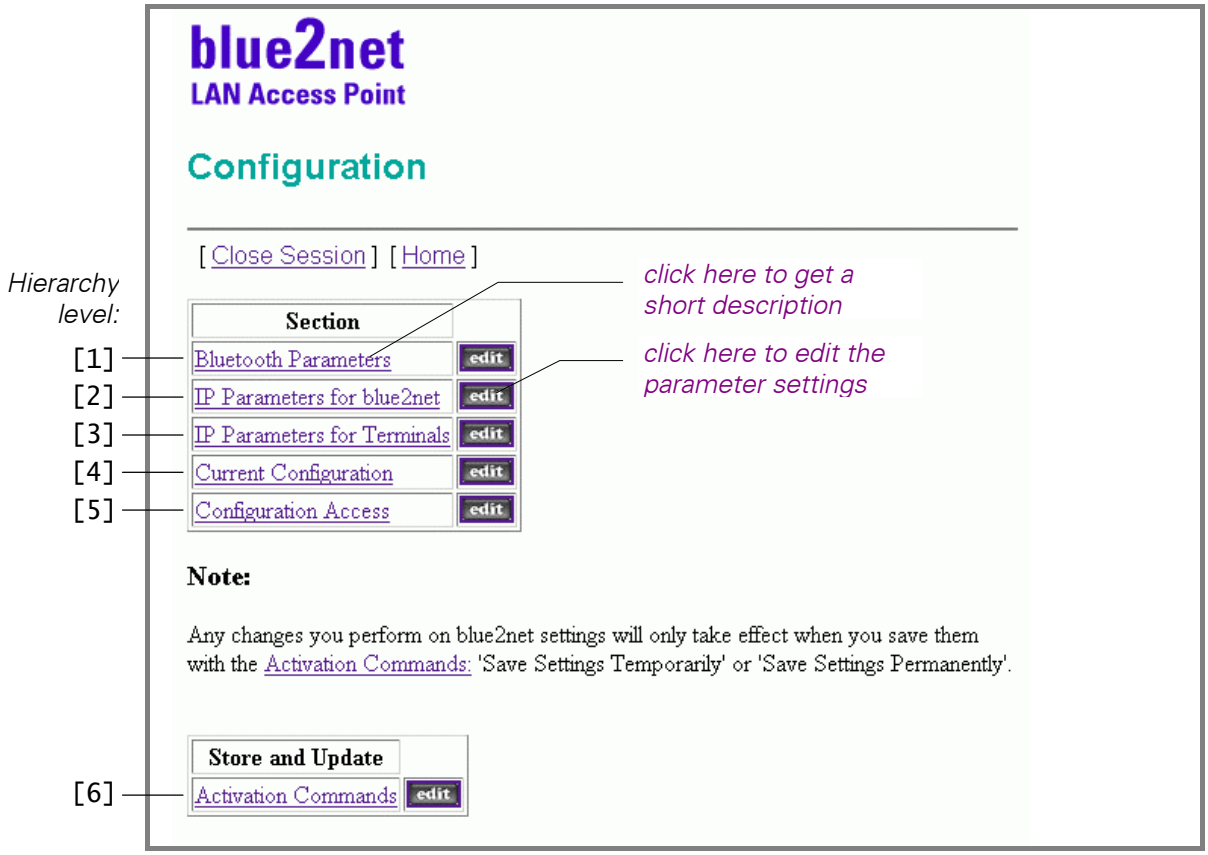


Figure 8 Main configuration page [0]

Click on one of the <edit> buttons. You will then be prompted to enter the configuration password (see Figure 9). The initial password is "**changeme**"

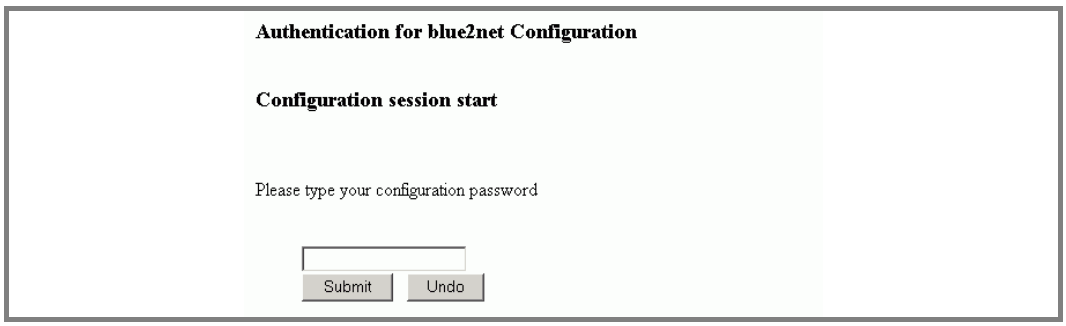


Figure 9 Authentication

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

For security reasons, you should then immediately change the password. Don't forget to save your changes: To do so, use the *activation commands* (see chapter 8.9)!

Note: Commit your new password to memory 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 10

Objects (see Figure 8)	**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 settings for the IP parameters for blue2net, e.g. whether IP addresses should be assigned via DHCP or whether permanently assigned IP addresses should be used. In addition, you can activate or deactivate a firewall, and activate and configure a second IP interface for using blue2net as access router.
IP Parameters for Terminals	[3]	Here you can define the IP parameter settings for the terminals to be connected, such as 'Terminal IP Address Resolution' and the pool of IP addresses that may be assigned to terminals ('Start/End of Terminal IP Address Pool Range'). Moreover, you can control the internal blue2net DHCP servers for Bluetooth PAN NAP and Ethernet.
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 19 Parameters on the main configuration page [0]

8.2 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 8.9).

Bluetooth connections (also the ones from other terminals) will be terminated if you use one of the activation commands to save changes (see chapter 8.9) !

After having made configuration changes, it is recommended to close the browser using the [Close Session] function. Otherwise, for security reasons you will have to wait up to 10 minutes before you can access the configuration menu again.

8.3 Hierarchy of Pages for Configuration Settings

The purpose of the following 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 change 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 on this parameter (edit, Submit) or
- a value to be displayed (number, address, domain, version)
- a table to be displayed
- objects to be displayed

[0] **Main Configuration Page** (chapter 8.1)		action / display of	page
[1] **Bluetooth Parameters** (chapter 8.4)			**54**
[1.1]	Bluetooth Device Name	➡ Objects	55
[1.1.1]	Bluetooth Device Name	edit, ▸ Submit	59
[1.1.2]	IP Address Suffix Mode	edit, ▸ Submit	59
[1.2]	Bluetooth Device Address	unique fixed address	55
[1.3]	Multipoint Mode	edit, ▸ Submit,	55
[1.4]	Discoverability Mode	edit, ▸ Submit	55
[1.5]	Connectability Mode	edit, ▸ Submit	56
[1.6]	Max. No. of Terminals Connected	edit, ▸ Submit	56
[1.7]	Number of Services	number	56
[1.8]	Service Table	➡ Table (3 rows)	56 & 62
[1.8.1]	Service Index	number	60
[1.8.2]	Service Name	edit, ▸ Submit	60
[1.8.3]	Service Description	edit, ▸ Submit	60
[1.8.4]	Auth. Level	edit, ▸ Submit	** 61
[1.8.5]	Service Provider	edit, ▸ Submit	61
[1.8.6]	Service URL	edit, ▸ Submit	61
[1.8.7]	Service ID	number	61
[1.8.8]	Bluetooth Service Class	service class	62
[1.8.9]	Activation	edit, ▸ Submit	62
[1.9]	Number of Terminals	number	56
[1.10]	Terminal Table	➡ Table (40 rows)	56
[1.10.1]	Terminal Index	number	65
[1.10.2]	Terminal Bluetooth Address	edit, ▸ Submit	65
[1.10.3]	Terminal Bluetooth Passkey	edit, ▸ Submit	65
[1.10.4]	Terminal IP Address	edit, ▸ Submit	66
[1.10.5]	Allow Bluetooth Bonding	edit, ▸ Submit	* 66
[1.11]	Default Access Mode	edit, ▸ Submit	57
[1.12]	Default Bluetooth Passkey	edit, ▸ Submit	57
[1.13]	Minimum Length of Key for Encryption	edit, ▸ Submit	* 58
[2] **IP Parameters for blue2net** (chapter 8.5)			**67**
[2.1]	blue2net IP Address Resolution	edit, ▸ Submit	67
[2.2]	Fixed blue2net IP Configuration	➡ Objects	68
[2.2.1]	Fixed blue2net IP Address	edit, ▸ Submit	69
[2.2.2]	Fixed blue2net Netmask	edit, ▸ Submit	69
[2.2.3]	Fixed blue2net Gateway	edit, ▸ Submit	69

Table 20 Hierarchy of pages for configuration settings (1)

[2]	**IP Parameters for blue2net** (chapter 8.5)			**67**
[2.3]	DHCP blue2net IP Objects	➡ Objects		68
[2.3.1]	Fallback blue2net IP Address	edit, ▸ Submit		70
[2.3.2]	Fallback blue2net Netmask	edit, ▸ Submit		70
[2.3.3]	Fallback blue2net Gateway	edit, ▸ Submit		70
[2.4]	Time Server IP	edit, ▸ Submit		68
[2.5]	IP Masquerading	edit, ▸ Submit		68
[2.6]	Firewall Settings	➡ Objects		68
[2.6.1]	Default Firewall	edit, ▸ Submit		71
[2.6.2]	Port Forwarding Rules	➡ Table (10 rows)	*	71
[2.6.2.1]	Index	number	*	72
[2.6.2.2]	Enable Rule	edit, ▸ Submit	*	73
[2.6.2.3]	Protocol	edit, ▸ Submit	*	73
[2.6.2.4]	Lower Port Number	edit, ▸ Submit	*	73
[2.6.2.5]	Enable Port Range	edit, ▸ Submit	*	74
[2.6.2.6]	Higher Port Number	edit, ▸ Submit	*	74
[2.6.2.7]	Fwd. Destination IP Addr.	edit, ▸ Submit	*	74
[2.6.2.8]	Fwd. Source IP Address	edit, ▸ Submit	*	74
[2.6.2.9]	Fwd. Source IP Add. Netm.	edit, ▸ Submit	*	74
[2.6.3]	Number of Port Forwarding Rules	number	*	71
[2.7]	Tunnel Configuration (PPPoE / PPTP)	➡ Objects		68
[2.7.1]	Tunnel Mode	edit, ▸ Submit		76
[2.7.2]	Tunnel Establishment Control	edit, ▸ Submit		77
[2.7.3]	Authentication Parameters	➡ Objects		77
[2.7.3.1]	Tunnel User Name	edit, ▸ Submit		78
[2.7.3.2]	Tunnel User Password	edit, ▸ Submit		78
[2.7.4]	PPTP Server IP Address	edit, ▸ Submit		77
[2.8]	Access Router	➡ Objects	*	68
[2.8.1]	Additional IP Interface	edit, ▸ Submit	*	80
[2.8.2]	Fixed Additional IP Interface	➡ Objects	*	80
[2.8.2.1]	Fixed b2n Addl. IP Address	edit, ▸ Submit	*	80
[2.8.2.2]	Fixed b2n Addl. IP Netmask	edit, ▸ Submit	*	80
[3]	**IP Parameters for Terminals** (chapter 8.6)			**72**
[3.1]	Terminal IP Address Resolution	edit, ▸ Submit		81
[3.2]	Start of Terminal IP Address Pool Range	edit, ▸ Submit	***	83
[3.3]	End of Terminal IP Address Pool Range	edit, ▸ Submit	***	83
[3.4]	Terminal Net Mask	edit, ▸ Submit		83
[3.5]	Terminal Fixed Servers	➡ Objects		83
[3.5.1]	Terminal DNS Server 1	edit, ▸ Submit		85
[3.5.2]	Terminal DNS Server 2	edit, ▸ Submit		85
[3.5.3]	Terminal WINS Server 1	edit, ▸ Submit		86
[3.5.4]	Terminal WINS Server 2	edit, ▸ Submit		86
[3.5.5]	Terminal Domain Name	edit, ▸ Submit		86
[3.6]	Local DHCP Server Objects	➡ Objects	*	83
[3.6.1]	Local DHCP Server for NAP	edit, ▸ Submit	*	87
[3.6.2]	Local DHCP Server for Ethernet	edit, ▸ Submit	*	87
[3.7]	IP Connection Mode for NAP Terminals	edit, ▸ Submit	*	84
[3.8]	Available IP Addresses for Local Wired Network	➡ Objects	*	84
[3.8.1]	Lowest IP Address of Range	edit, ▸ Submit	*	88
[3.8.2]	Highest IP Address of Range	edit, ▸ Submit	*	88
[3.9]	Fixed IP Addresses for Local Wired Network	➡ Table (40 rows)	*	84
[3.9.1]	Index	number	*	89
[3.9.2]	MAC Address	edit, ▸ Submit	*	89
[3.9.3]	IP Address	edit, ▸ Submit	*	89
[3.10]	Number of Fixed IP Addresses	number	*	84

Table 21 Hierarchy of pages for configuration settings (2)

[4]	**Current Configuration** (chapter 8.7)			**90**
[4.1]	MAC Address		unique fixed address	90
[4.2]	blue2net IP Configuration	➡ Objects		91
[4.2.1]	blue2net IP Address		address	91
[4.2.2]	blue2net Netmask		address	91
[4.2.3]	blue2net Gateway		address	91
[4.3]	Terminal Server Configuration	➡ Objects		92
[4.3.1]	Terminal DNS Server 1		address	92
[4.3.2]	Terminal DNS Server 2		address	92
[4.3.3]	Terminal WINS Server 1		address	92
[4.3.4]	Terminal WINS Server 2		address	92
[4.3.5]	Terminal Domain Name		domain	92
[4.4]	Version Information	➡ Objects		93
[4.4.1]	Module Firmware Version		version	93
[4.4.2]	PPCBoot Version		Version	93
[4.4.3]	blue2net Software Version		Version	93
[4.4.4]	blue2net Hardware Version		version	93
[4.4.5]	SieMo Module Info		version	93
[4.5]	Tunnel Status (PPPoE/PPTP)	➡ Objects		90
[4.5.1]	Tunnel Status		status of tunnel conn.	94
[4.5.2]	IP Address of Tunnel Endpoint on b2n		address	* 94
[5]	**Configuration Access** (chapter 8.8)			**95**
[5.1]	SNMP Access		edit, ▸ Submit	95
[5.2]	Configuration Password		edit, ▸ Submit	95
[6]	**Activation Commands** (chapter 8.9)			**96**
[6.1]	Save Settings Temporarily		edit, ▸ Submit	98
[6.2]	Save Settings Permanently		edit, ▸ Submit	99
[6.3]	Reset blue2net		edit, ▸ Submit	99
[6.4]	Update Software		edit, ▸ Submit	100
[6.5]	Restore Default Settings		edit, ▸ Submit	100
[6.6]	Store Specific Homepage		edit, ▸ Submit	100

Table 22 Hierarchy of pages for configuration settings (3)

Change history:

As compared to the previous SW version 3.0.0 / user guide V 3.0, the following changes have been made (also refer to chapter 11.3):

*) new parameter

**) factory setting (default value) changed!

***) function changed

[3.2] and [3.3] have been renamed and now provide a different functionality

[3.3.1] and [3.3.2] have been omitted

[5.2.1] is now called [5.2]

8.4 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 a brief online description (see Figure 10).

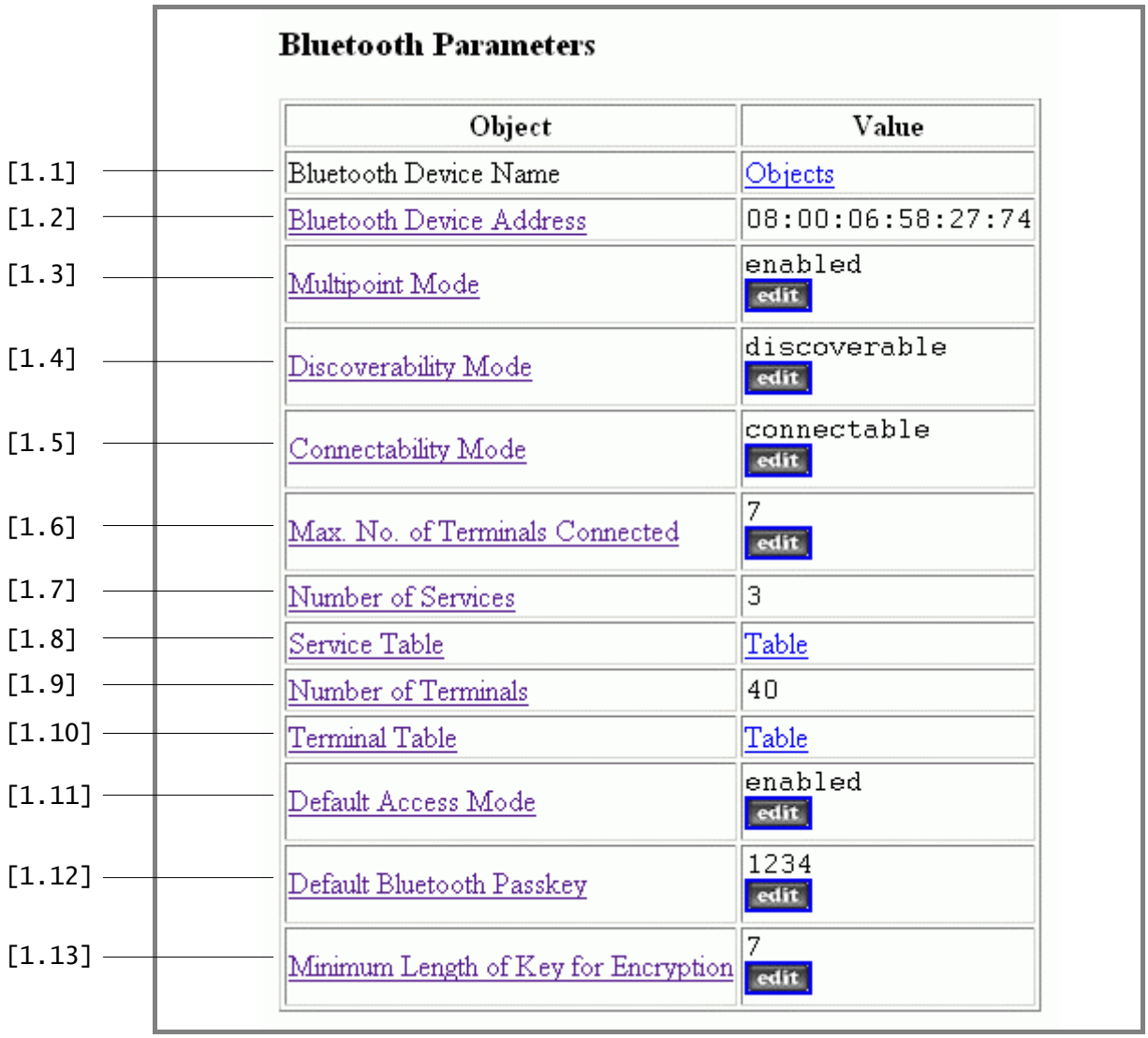


Figure 10 Bluetooth Parameters [1]

Objects (see Figure 10)	**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
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 enforced by 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. **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 10) Terminals whose software does not allow for direct input of a Bluetooth address for connection set-up must have "seen" blue2net at least once and have saved the respective data before you can set up a connection.

Objects (see Figure 10)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
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* terminal. **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 10)
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 10)
Number of Services	[1.7]	3 (three) (read only)	This is the number of services presented to the terminals.
Service Table	[1.8]		A list of entries regarding services (see chapter 8.4.1).
Number of Terminals	[1.9]	40 (fourty) (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 8.4.3).

Objects (see Figure 10)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
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 10)
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. The passkey should be 16 characters long and comprise upper/lower case letters, numbers and special characters. **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 10)

Objects (see Figure 10)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Minimum Length of Key for Encryption	[1.13]	7 Other value of your choice (1...16) 16 = 128 bit 7 = 56 bit 5 = 40 bit	This object allows you to define the minimum required key length for Bluetooth services whose Auth. Level [1.8.4] is set to 'authandenc'. The value represents the number of octets used for encryption. A value of 7 corresponds to 7 times 8 = 56 bits The key length for services is negotiated between blue2net and the terminals. Maximum protection against interception is afforded by a key length of 16 (= 128 bits). **Caution!** Danger of lockout! Verify first whether or not your terminal supports 128 bit encryption (see chapters 10.2 and 13.2). Terminals which do not support the full key length of 128 bits (e.g. if 16 is set, which corresponds to 128 bits) cannot use the services (and will be excluded from the data transfer) If you select a suitable 'Minimum Length of Key for Encryption', you can also achieve encryption with a shorter key length, which will, however, increase the risk of interception.

Table 23 Bluetooth Parameters [1]

8.4.1 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 (see Figure 11). A Bluetooth device inquiry can retrieve the user-friendly name of your blue2net unit plus its current IP address and display it on your Bluetooth terminal.

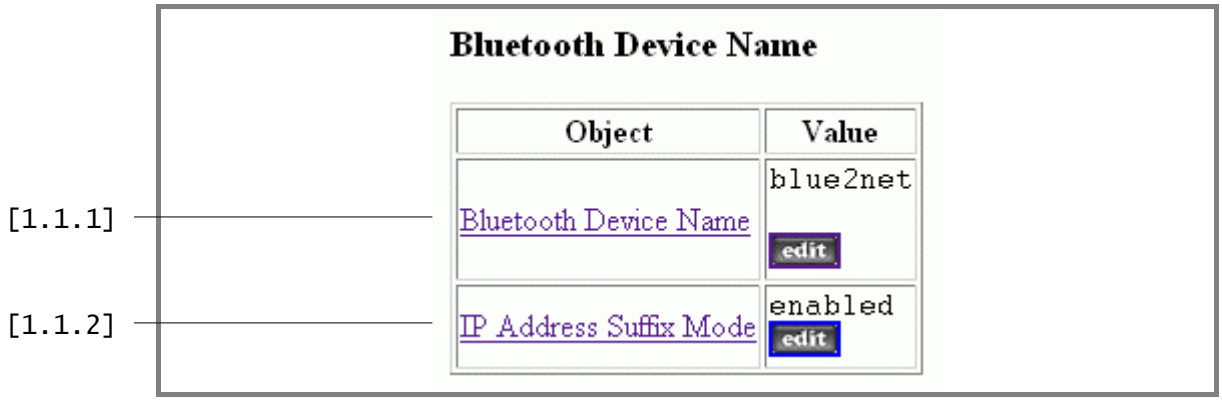


Figure 11 Bluetooth Device Name [1.1]

Objects (see Figure 11)	**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 24 Bluetooth Device Name [1.1]

8.4.2 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.

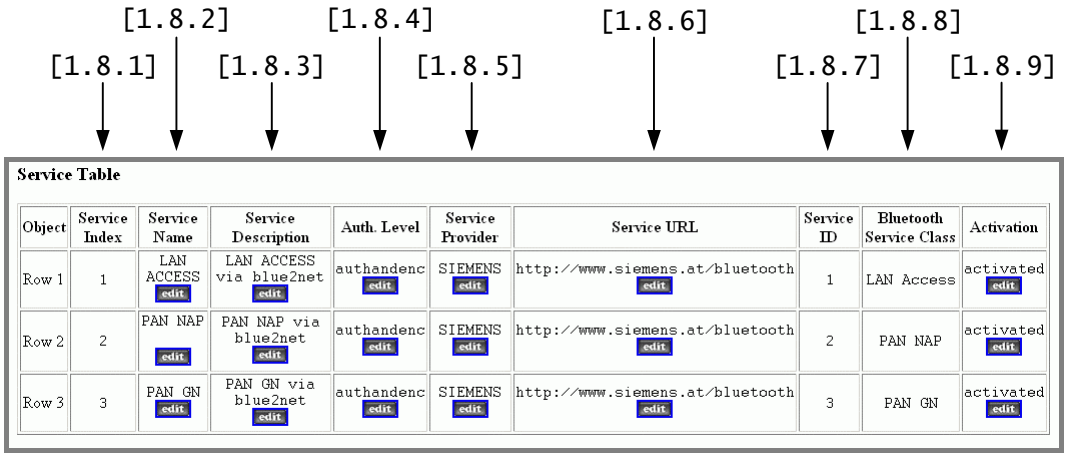


Figure 12 Service Table [1.8]

Objects (see Figure 12)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Service Index	[1.8.1]	1 / 2 / 3 (read-only)	A unique value for each service.
Service Name	[1.8.2]	LAN ACCESS 1/ PAN NAP/ PAN GN 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 / PAN NAP / PAN GN / via blue2net other description of your choice (1...31 characters)	Service description display. Does not influence the functionality.

Objects (see Figure 12)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Auth. Level	[1.8.4]	authandenc noauth auth	There are various security mechanisms available for the terminals. 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 [1.12] or [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 [1.12] or [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 10)
Service Provider	[1.8.5]	SIEMENS other entry of your choice (1...15 characters)	Provider of the service presented to a client (Bluetooth terminal/Bluetooth device) via 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 (Bluetooth terminal/Bluetooth device) via SDP.
Service ID	[1.8.7]	1 / 2 / 3 (read-only)	Value of Service Record Handle subfield presented to a client using SDP.

Objects (see Figure 12)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Bluetooth Service Class	[1.8.8]	LAN Access / PAN NAP / PAN GN (read-only)	Description of the Service Class (Bluetooth profile) offered by blue2net.
Activation	[1.8.9]	activated deactivated	If the corresponding Bluetooth Service Class is set to *activated*, it can be used by a client (Bluetooth- terminal / Bluetooth device). **Caution!** Danger of lockout if **all 3** entries are set to *deactivated*! Verify this parameter carefully! (see chapter 10)

Table 25 Service Table [1.8]

8.4.3 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 for 'LAN Access Profile', 'Terminal IP Address Resolution' [3.1] has to be set to *predefined* or *masqueradingpool*.

In order to be able to assign an IP address to the terminal when using the PAN NAP service, the DHCP server for NAP terminals [3.6.1] must be set to *enabled* (see chapter 8.6.2)

If you want all Bluetooth terminals to authenticate with a separate Bluetooth passkey, but still get IP addresses assigned from the pool, set 'Default Access Mode' [1.11] to *disabled*. In the terminal table, enter only the Bluetooth addresses [1.10.2] and Bluetooth passkeys [1.10.3], but leave the IP addresses [1.10.4] set to *0.0.0.0*.

If the 'IP Connection Mode for NAP Terminals' [3.7] (see chapter. 8.6, page 84) is set to *bridging*, the terminal table can be used also for computers that are connected to blue2net via Ethernet. Such computers will then be configured with DHCP provided 'Local DHCP Server for Ethernet' [3.6.2] was set to *enabled*.

You then have to enter the Ethernet address of the network card of the computer in question as terminal Bluetooth address [1.10.2]. In this case 'Terminal Bluetooth Passkey' [1.10.3] is irrelevant. If 'IP Connection Mode for NAP Terminals' [3.7] is set to *routing*, please use values table for 'Fixed Addresses for Local Wired Network' [3.9] to assign IP addresses to the computer network cards.

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 pool of terminal IP addresses (between 'Start/End of Terminal IP Address Pool Range' [3.2] and [3.3]).

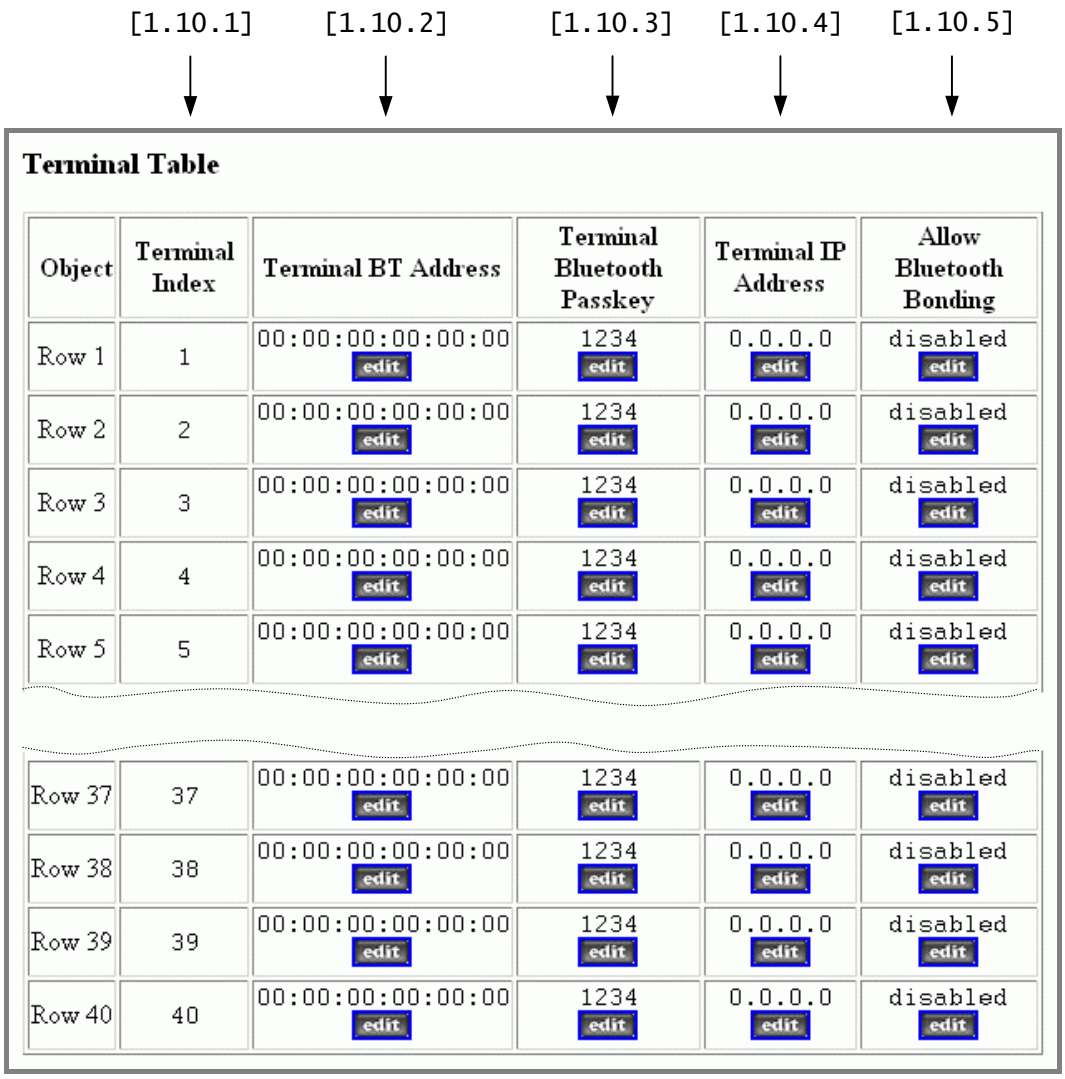


Figure 13 Terminal Table [1.10]

Objects (see Figure 13)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Terminal Index	[1.10.1]	1-40 (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 or the Ethernet address of a computer network card, provided 'IP Connection Mode for NAP Terminals' [3.7] is set to *bridging* and a computer is to be configured via DHCP. 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 10 and 10.1)
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 10)

Objects (see Figure 13)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
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 provided it uses "LAN Access Profile". In the case of "PAN NAP Service" the terminal IP address will be assigned if 'Local DHCP Server for NAP' [3.6.1] is set to *enabled*. If it is an Ethernet address, 'Terminal IP Address' will be assigned to the computer via DHCP provided 'Local DHCP Server for NAP' [3.6.1] is set to *enabled*, and 'IP Connection Mode for NAP Terminals' [3.7] is set to *bridging*. If 'Terminal IP Address' contains *0.0.0.0*, a value from the pool of terminal IP addresses between 'Start/End of Terminal IP Address Pool Range' [3.2] and [3.3] will be assigned to this terminal.
Allow Bluetooth Bonding	[1.10.5]	disabled enabled	If 'Allow Bluetooth Bonding' is set to *enabled*, the internal information required to authenticate this Bluetooth device will be saved in blue2net's permanent memory. Input of the Bluetooth passkey [1.10.3] is required only the first time the connection is set up. After that, the devices "know each other", and it is no longer necessary to enter the Bluetooth passkey [1.10.3].

Table 26 Terminal Table [1.10]

8.5 IP Parameters for blue2net [2]

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

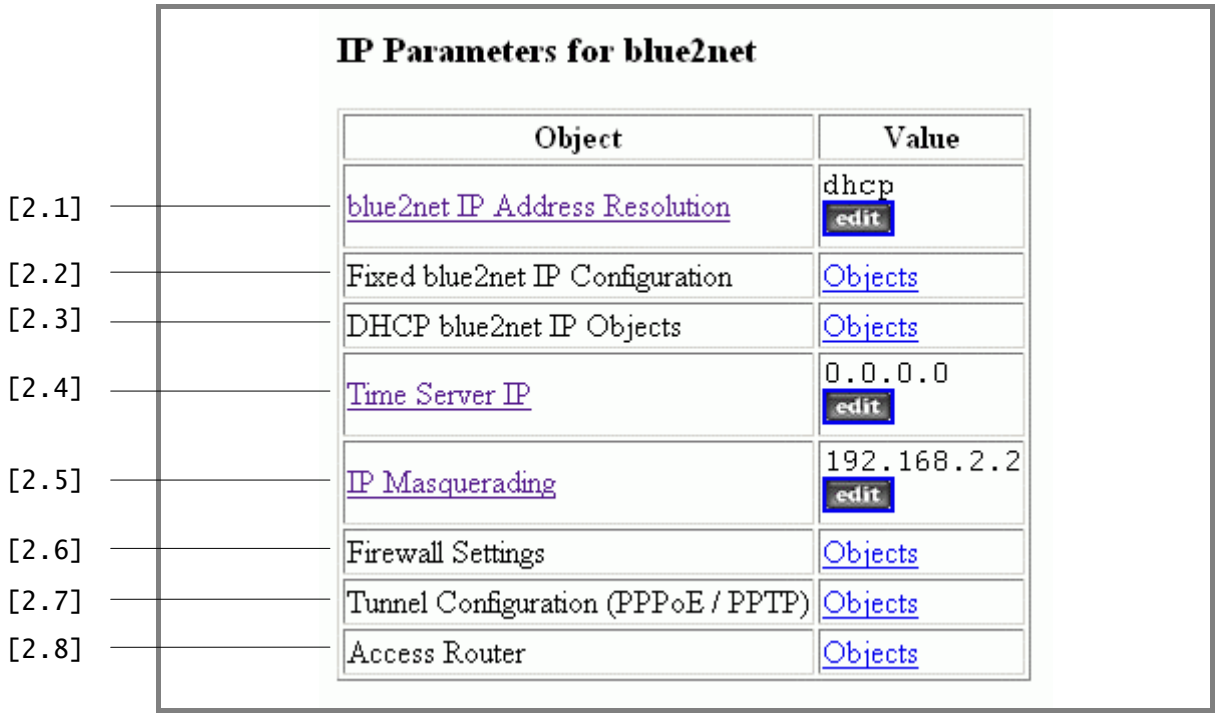


Figure 14 IP Parameters for blue2net [2]

Objects (see Figure 14)	**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 10)

Objects (see Figure 14)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Fixed blue2net IP Configuration	[2.2]		The IP addresses assigned to blue2net if the blue2net address resolution mode [2.1] is set to *predefined*.
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. If you have set 'IP Connection Mode for NAP Terminals' to *routing*, this value should be different from 'Fixed blue2net Additional IP Address' [2.8.2.1] provided 'Additional IP Interface' [2.8.1] is set to *enabled*.
Firewall Settings	[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 17). You can also configure "Port Forwarding" here.]
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).
Access Router	[2.8]		Configuration of a second IP interface at the Ethernet port in order to be able to operate blue2net as access router.

Table 27 IP Parameters for blue2net [2]

8.5.1 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.

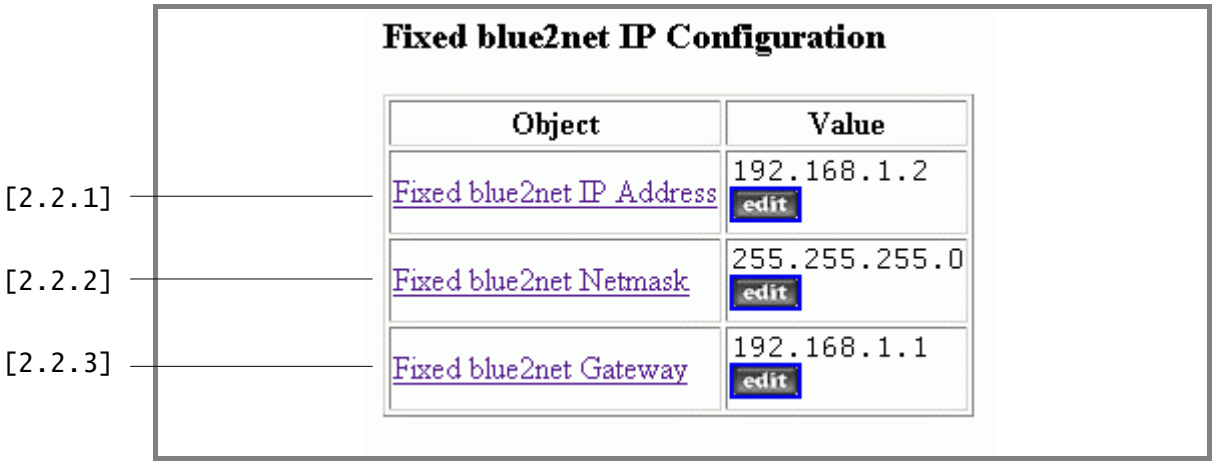


Figure 15 Fixed blue2net IP Configuration [2.2]

Objects (see Figure 15)	**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 28 Fixed blue2net IP Configuration [2.2]

8.5.2 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 4.3.

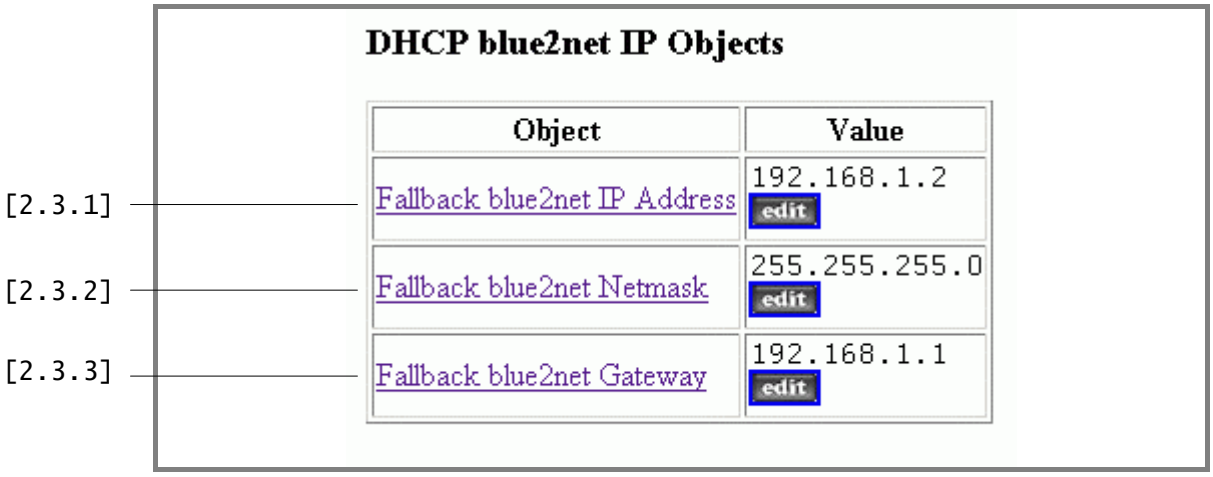


Figure 16 DHCP blue2net IP Objects, DHCP setup [2.3]

Objects (see Figure 16)	**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 29 DHCP blue2net IP Objects, DHCP setup [2.3]

8.5.3 Firewall Option (Firewall Settings [2.6])

The firewall in blue2net may be enabled in order to prevent attacks coming from the Ethernet side (e.g. over LAN, cable modem or xDSL connection). However, it is possible to allow defined access paths through the firewall to the computers in the local network behind blue2net (e.g. remote computer maintenance). For more details on how to define such access rules, refer to 8.5.4.

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

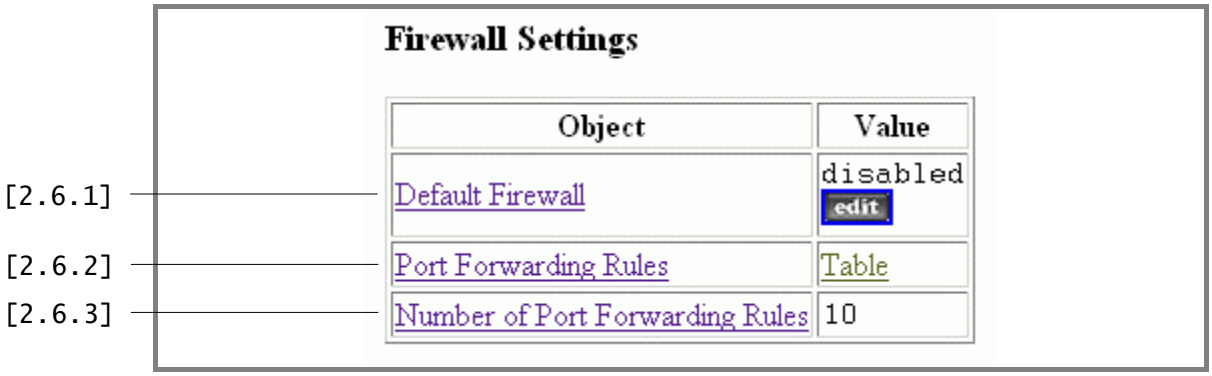


Figure 17 Firewall Settings [2.6]

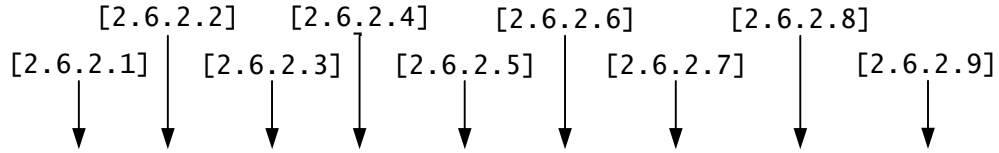
Objects (see Figure 17)	Hier. level	Factory setting, other values, value range	Explanation
Default Firewall	[2.6.1]	disabled enabled	If 'Default Firewall' is set to *enabled*, a default set of firewall rules (see chapter 14) will be activated.
Port Forwarding Rules]	[2.6.2]		Table of port forwarding rules; important, for example, for remote server maintenance
Number of Port Forwarding Rules	[2.6.3]	10 (read only)	Maximum number of active port forwarding rules [2.6.2]

Table 30 Firewall Settings [2.6]

8.5.4 Port Forwarding Rules [2.6.2]

Port forwarding takes effect if you want to use blue2net as access router with masquerading and provide a service on the local computer that is accessible from the Internet (local computer connected via Ethernet or Bluetooth).

A possible application would be if you make a PPTP or PPPoE server available on a computer to allow secure VPN access from the Internet into your network.



Port Forwarding Rules

Object	Index	Enable Rule	Protocol	Lower Port Number	Enable Port Range	Higher Port Number	Forwarding Destination IP Address	Forwarding Source IP Address	Forwarding Source IP Address Netmask
Row 1	1	disabled edit	17 edit	0 edit	disabled edit	65535 edit	0.0.0.0 edit	0.0.0.0 edit	0.0.0.0 edit
Row 2	2	disabled edit	17 edit	0 edit	disabled edit	65535 edit	0.0.0.0 edit	0.0.0.0 edit	0.0.0.0 edit
Row 3	3	disabled edit	17 edit	0 edit	disabled edit	65535 edit	0.0.0.0 edit	0.0.0.0 edit	0.0.0.0 edit
Row 4	4	disabled edit	17 edit	0 edit	disabled edit	65535 edit	0.0.0.0 edit	0.0.0.0 edit	0.0.0.0 edit
Row 5	5	disabled edit	17 edit	0 edit	disabled edit	65535 edit	0.0.0.0 edit	0.0.0.0 edit	0.0.0.0 edit
Row 6	6	disabled edit	17 edit	0 edit	disabled edit	65535 edit	0.0.0.0 edit	0.0.0.0 edit	0.0.0.0 edit
Row 7	7	disabled edit	17 edit	0 edit	disabled edit	65535 edit	0.0.0.0 edit	0.0.0.0 edit	0.0.0.0 edit
Row 8	8	disabled edit	17 edit	0 edit	disabled edit	65535 edit	0.0.0.0 edit	0.0.0.0 edit	0.0.0.0 edit
Row 9	9	disabled edit	17 edit	0 edit	disabled edit	65535 edit	0.0.0.0 edit	0.0.0.0 edit	0.0.0.0 edit
Row 10	10	disabled edit	17 edit	0 edit	disabled edit	65535 edit	0.0.0.0 edit	0.0.0.0 edit	0.0.0.0 edit

Figure 18 Port Forwarding Rules [2.6.2]

Objects (see Figure 18)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Index	[2.6.2.1]	1-10 (read only)	Unique value for each rule. blue2net checks, for each rule and one after the other, whether or not it is true. If it is, it will be applied, and the remaining rules will be skipped.

Objects (see Figure 18)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Enable Rule	[2.6.2.2]	disabled enabled	Enables or disables this one specific rule. The rule as such remains in place even if disabled and can be reactivated if required by simply setting this flag back to *enabled*.
Protocol	[2.6.2.3]	17 Other protocol number (0-255)	Number of the IP protocol to be forwarded: 6.....tcp, 17.....udp, 47.....gre, 255.....all protocols **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 10) If you forward all protocols (= value 255) and thus have not *enabled* an 'Additional IP Interface' [2.8.1], blue2net is no longer configurable from the Ethernet connection.
Lower Port Number	[2.6.2.4]	0 Other port number (0 ... 65535), which should not be higher than [2.6.2.6]	If 'Enable Port Range' [2.6.2.5.] is *disabled*, this is the number of the single port to be forwarded (relevant only if the value in 'Protocol' [2.6.3.2] is set to 6 (tcp) or 17 (udp)). If 'Enable Port Range' [2.6.2.5.] is *enabled*, this is the lowest number in a port number range (inclusive). **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 10) If you forward a tcp port range that contains the value 447 and have not activated a second IP interface ('Additional IP Interface' [2.8.1] set to *enabled*), blue2net is no longer configurable from the Ethernet connection.

Objects (see Figure 18)	Hier. level	Factory setting, other values, value range	Explanation
Enable Port Range	[2.6.2.5]	disabled enabled	Set this flag to *enabled* if you want to forward a contiguous port range. The range is defined through 'Lower Port Number' [2.6.2.4] and 'Higher Port Number' [2.6.2.6]. Applies only to tcp and udp (6 or 17 in 'Protocol' [2.6.2.3]).
Higher Port Number	[2.6.2.6]	65535 Other port number (0 ... 65535), which should not be lower than [2.6.2.4])	If 'Enable Port Range' [2.6.2.5.] is *enabled*, this is the number of the highest port (inclusive) from the range to be forwarded. If 'Enable Port Range' [2.6.2.5.] is *disabled*, this parameter will have no effect. **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 10) If you forward a tcp port range that contains the value 447 and have not activated a second IP interface ('Additional IP Interface' [2.8.1] set to *enabled*), blue2net is no longer configurable from the Ethernet connection.
Forwarding Destination IP Address	[2.6.2.7]	0.0.0.0	This is the destination IP address for forwarding, i.e. the IP address of the computer on which the service(s) actually execute(s).
Forwarding Source IP Address	[2.6.2.8]	0.0.0.0	IP address of the computer or computer network that is allowed to use the service(s).
Forwarding Source IP Address Netmask	[2.6.2.9]	0.0.0.0	Mask for the source address (all address parts that feature (binary) 1 in the mask must be identical with the address specified in 'Forwarding Source IP Address' [2.3.6.8]).

Table 31 Port forwarding rules [2.6.2]

Examples:

If you are running a server for which you want to perform remote maintenance from the Internet, you can install a PPTP server program on this server and enter the following two rules on blue2net in order to forward PPTP to this server (interesting for small companies that have their IT infrastructure servicing outsourced).

Index	Enable Rule	Protocol	Lower Port Number	Enable Port Range	Higher Port Number
x	enabled	47 (gre)	0	disabled	65535
x+1	enabled	6 (tcp)	1723	disabled	65535

Table 32 Example of a port forwarding rule for PPTP tunnels

You can achieve the same goal with l2tp, if you have an L2TP server program (LNS) running on your server and activate the following rule:

Index	Enable Rule	Protocol	Lower Port Number	Enable Port Range	Higher Port Number
x	enabled	17 (udp)	1701	disabled	65535

Table 33 Example of a port forwarding rule for L2TP tunnels

If you want to be able to reach a computer in the local network with SSH from the WWW Internet, you have to run an SSH service on this computer and activate the rules specified in Table 33.

Index	Enable Rule	Protocol	Lower Port Number	Enable Port Range	Higher Port Number
x	enabled	6 (tcp)	22	disabled	65535
x+1	enabled	17 (udp)	22	disabled	65535

Table 34 Example of a port forwarding rule for SSH tunnels

8.5.5 Tunnel Configuration (PPPoE / PPTP) [2.7]

When an xDSL modem is connected to a terminal device, in most cases a tunnel protocol will execute "on top of" the Ethernet protocol. Before it is possible to exchange data with the Internet, a tunnel protocol must be set up between the terminal (blue2net) and the xDSL modem. blue2net supports the tunnel protocols PPPoE (RFC 2516) and PPTP (RFC 2637).

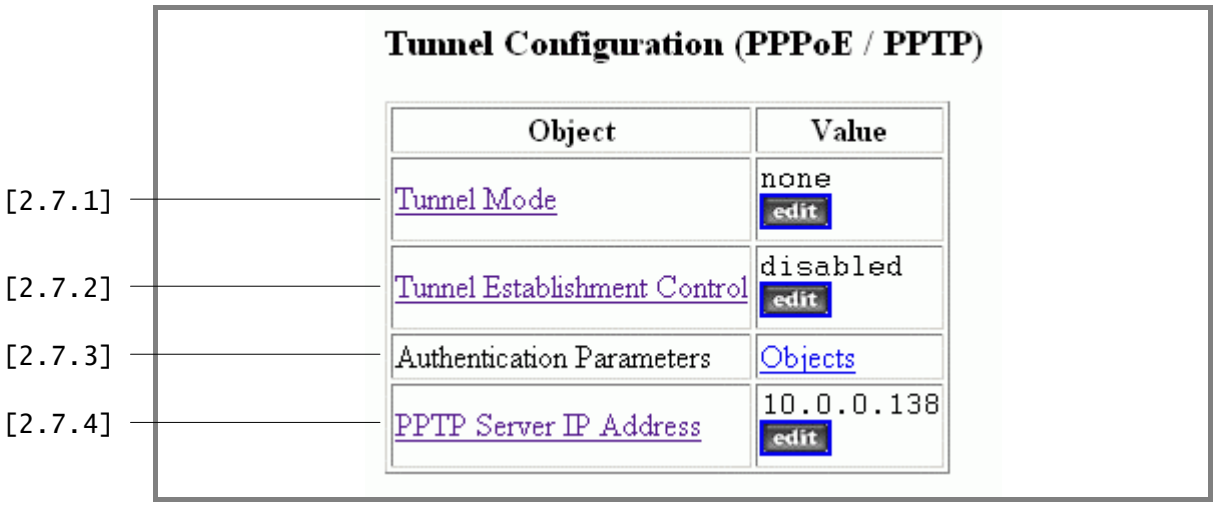


Figure 19 Tunnel Configuration (PPPoE / PPTP) [2.7]

Objects (see Figure 19)	**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 'pptp', 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.

Objects (see Figure 19)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
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 the tariff model of your xDSL service provider does not charge you for online time (e.g. flat rate). 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 in the tariff model of your xDSL provider. Attention! If blue2net acts as access router and [2.7.2] is set to *enabled*, the tunnel will not be automatically established for PCs connected to the wired Ethernet! This means that in that case you must not change the setting to *enabled*.
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 address	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 35 Tunnel Configuration (PPPoE / PPTP) [2.7]

8.5.6 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.

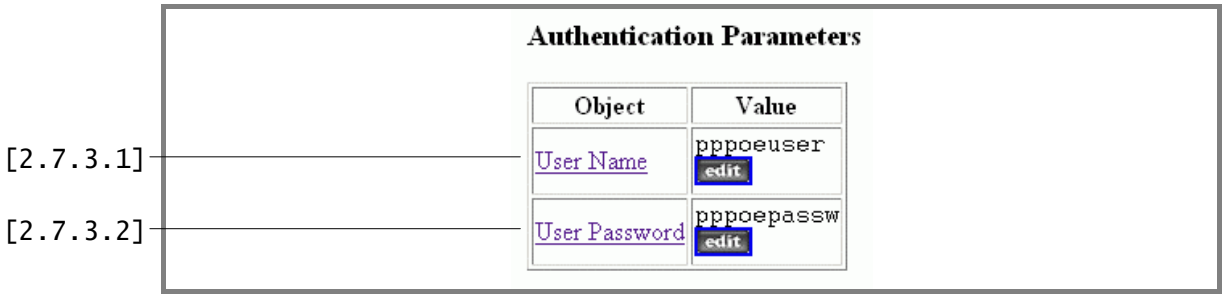


Figure 20 Authentication Parameters [2.7.3]

Objects (see Figure 20)	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 user authentication (e.g. user ID assigned by your ISP).
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 by your ISP).

Table 36 Authentication Parameters [2.7.3]

8.5.7 Access Router [2.8]

You can use blue2net as access router. To do so, change the factory settings for the parameters under 'Access Router' [2.8] (unless you are setting up the link to the WWW via an xDSL modem using PPPoE (see 'Authentication Parameters' [2.7.3] in chapter 8.5.6).

Set 'Additional IP Interface' [2.8.1] to *enabled* in order to activate a second IP interface for a small home network.

If 'IP Connection Mode for NAP Terminals' [3.7] is set to *bridging* and 'Terminal IP Address Resolution' is set to *masquerading* or *masqueradingpool*, the IP address and netmask as specified in 'IP Masquerading' [2.5] and in 'Terminal Netmask' [3.4] will be used for the second IP interface. Otherwise the values entered under 'Fixed Additional IP Interface' [2.8.2] will be used in "bridging mode".

If 'IP Connection mode for NAP Terminals' [3.7] is set to *routing*, you should use an IP address for the second IP interface that is not located in the same subnet as the Bluetooth terminals with PAN NAP Service. Provided 'Terminal IP Address Resolution' [3.1] is set to *masquerading* or *masqueradingpool*. this will be the IP address from 'IP Masquerading' [2.5] and the netmask from [3.4].

Note: The use bandwidth of blue2net as access router is about 300 kBps (kiloBytes per second). Do not position blue2net with enabled access router functionality directly after an additional hardware router together with a hub, as such routers may generate quick bursts that may lead to a drop in the data throughput rate for Ethernet terminals. The reason for this are possible collisions between data packets sent from the WWW Internet to blue2net and packets sent from blue2net to the computers on your home LAN. In such a case, it is better to directly use your hardware router for PCs connected to the Ethernet.

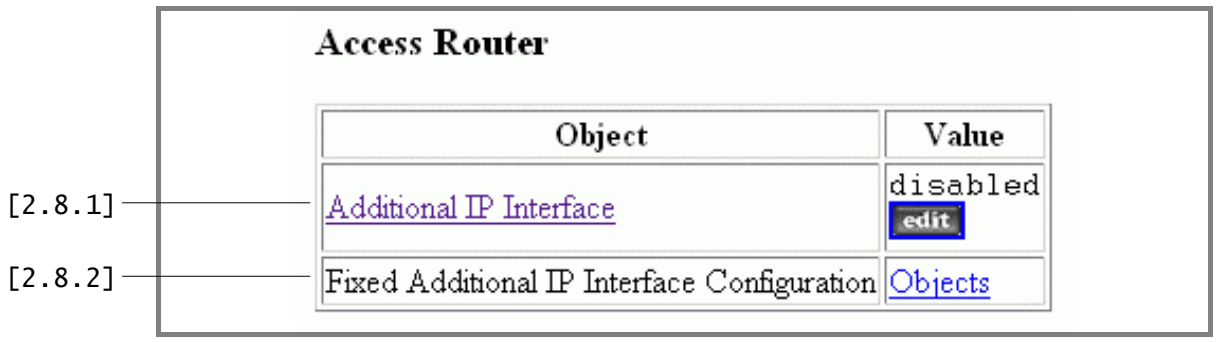


Figure 21 Access Router [2.8]

Objects (see Figure 21)	Hier. level	Factory setting, other values, value range	Explanation
Additional IP Interface	[2.8.1]	disabled enabled	Enables/disables a second IP interface on blue2net.
Fixed Additional IP Interface Configuration	[2.8.2]		Menu for configuring the second IP interface.

Table 37 Access router [2.8]

8.5.8 Fixed Additional IP Interface Configuration [2.8.2]

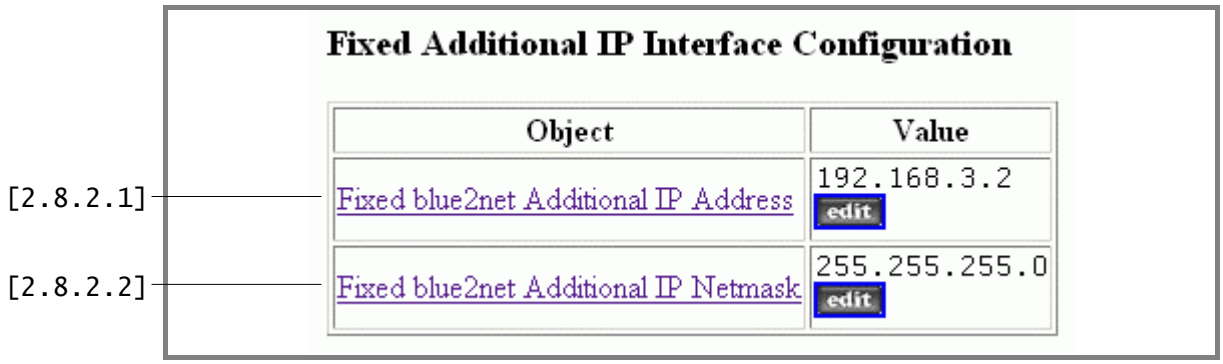


Figure 22 Fixed Additional IP Interface Configuration [2.8.2]

Objects (see Figure 22)	Hier. level	Factory setting, other values, value range	Explanation
Fixed blue2net Additional IP Address	[2.8.3.1]	192.168.3.2 other IP address	IP address of the second IP interface (used only if 'IP Connection Mode for NAP Terminals' [3.7] is set to *routing*). If you use "masquerading", i.e. if 'Terminal IP Address Resolution' [3.1] is set to *masquerading*, this IP address must be different from 'IP Masquerading' [2.5]!
Fixed blue2net Additional IP Netmask	[2.8.3.2]	255.255.255.0 other netmask	Subnetmask for the second IP interface (used only if 'IP Connection Mode for NAP Terminals' [3.7] is set to *routing*).

Table 38 Fixed Additional IP Interface Configuration [2.8.2]

8.6 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.

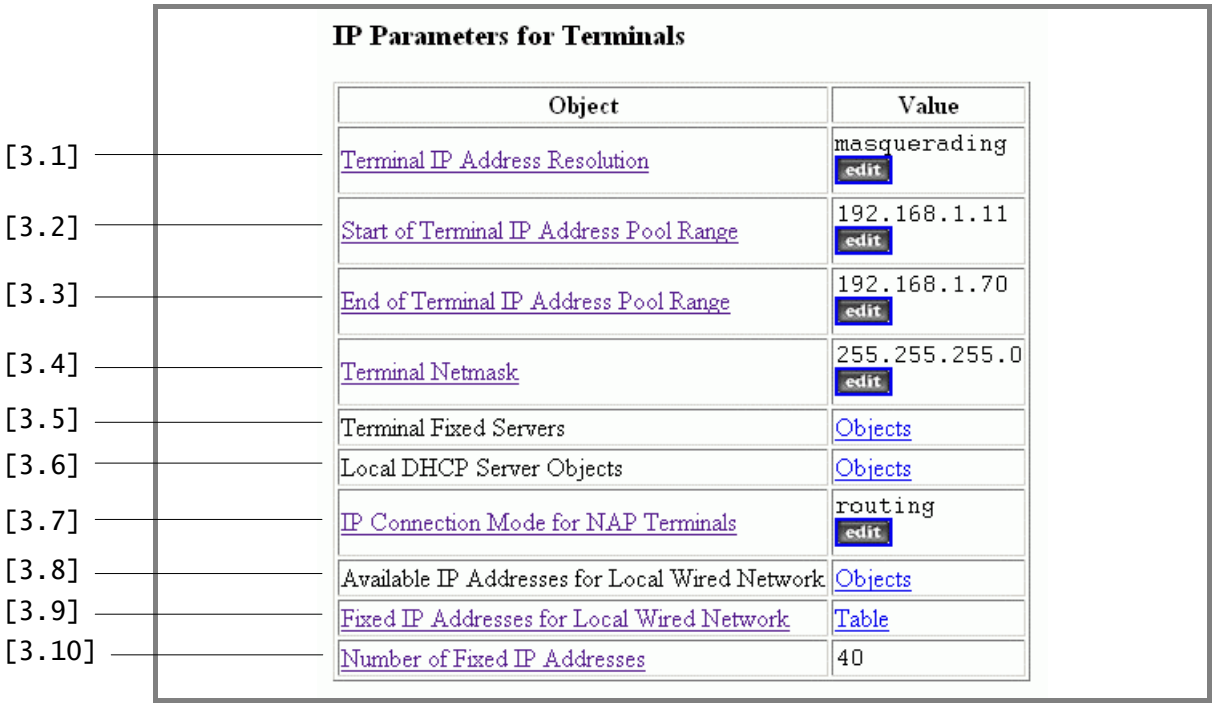


Figure 23 IP Parameters for Terminals [3]

Objects (see Figure 23)	**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 Bluetooth terminals with LAP profile (this is the recommended setting for home users with cable modem or xDSL modem). For your ISP, only the official blue2net IP is visible. For PAN NAP, you should in this case enable the DHCP server ('Local DHCP Server for NAP' [3.6.1] set to *enabled*). Continued →

Objects (see Figure 23)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Terminal IP Address Resolution Continued	[3.1]	masquerading dhcp predefined masqueradingpool	If the mode is set to *dhcp*, blue2net will issue a DHCP inquiry containing the Bluetooth address of the terminal during connection set-up. To get the same treatment for PAN NAP terminals, you should set 'IP Connection Mode for NAP Terminals' [3.7] to *bridging* and disable the DHCP server for NAP terminals ('Local DHCP Server for NAP' [3.6.1] to *disabled*). 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 'Start/End of Terminal IP Address Pool Range' [3.2] and [3.3]. If the terminal is registered in the 'Terminal Table [1.10], blue2net will use the IP address assigned there (see 8.4.3). For PAN NAP, you should in this case enable the DHCP server ('Local DHCP Server for NAP [3.6.1]' to *enabled*) 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 8.4.3). **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 10)

Objects (see Figure 23)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Start of Terminal IP Address Pool Range (Attention! Name and function changed as compared to v 3.0 !)	[3.2]	192.168.2.11	Lowest IP address of the range for "LAN Access Profile"-Terminals und PAN terminals (provided 'Local DHCP Server for NAP' [3.6.1] is *enabled*). If 'IP Connection Mode for NAP Terminals' [3.6.2] is set to *bridging* and 'Access Router' [2.8] – 'Additional IP Interface' [2.8.1] to *enabled*, and 'Local DHCP Server for Ethernet' [3.6.2] to *enabled* – the range will also be used for assigning addresses to computers connected to the local Ethernet.
End of Terminal IP Address Pool Range (Attention! Name and function changed as compared to v 3.0 !) [3.3.1] and [3.3.2]. have been omitted	[3.3]	192.168.2.70	Highest address in the IP address range. If you want to assign IP addresses only to terminals with a registered MAC address (see table for 'Fixed IP Address for Local Wired Network' [3.9], set [3.2] and [3.3] to *0.0.0.0*
Terminal Netmask	[3.4]	255.255.255.0 other value	The subnet mask associated with the IP address out of 'Start/End of Terminal IP Address Pool Range' [3.2]-[3.3]
Terminal Fixed Servers	[3.5]		While the PPP connection is being established these parameters will be sent to the Bluetooth terminal. These values are also passed on to PAN NAP and Ethernet terminals on the local DHCP server.
Local DHCP Server Objects	[3.6]		Here you can start and stop the DHCP server for Bluetooth PAN terminals or Ethernet terminals.

Objects (see Figure 23)	Hier. level	Factory setting, other values, value range	Explanation
IP Connection Mode for NAP Terminals	[3.7]	routing bridging	Connection of Bluetooth terminals to the Ethernet interface in the case of PAN NAP service. *routing* – no connection to Ethernet interface, IP data is routed. *bridging* – direct connection of PAN NAP terminals to Ethernet interface (on Ethernet protocol level).
Available IP Addresses for Local Wired Network	[3.8]		Pool of IP addresses assigned via DHCP to Ethernet terminals (PCs/laptops) provided 'IP Connection Mode for NAP Terminals' [3.7] is set to *routing* and 'Local DHCP Server for Ethernet' [3.6.2] to *enabled*.
Fixed IP Addresses for Local Wired Network	[3.9]		Table of Ethernet addresses and associated IP addresses assigned via DHCP to the respective Ethernet terminals (PCs/Laptops) provided 'IP Connection Mode for NAP Terminals' [3.7] is set to *routing* and 'Local DHCP Server for Ethernet' [3.6.2] to *enabled*.
Number of Fixed IP Addresses	[3.10]	40 (read only)	Maximum possible number of entries in 'Fixed IP Address for Local Wired Network' table [3.9].

Table 39 IP Parameters for Terminals [3]

Please note that the setting for 'IP Connection Mode for NAP Terminals' [3.7] also has an impact on which ranges will be used for address assignment to Ethernet terminals via DHCP (see [3.6], [3.9] and [3.10]).

The reason for this is that in "Bridging-Mode" for 'IP Connection Mode for NAP Terminals' [3.7], Ethernet and PAN NAP are linked on the Ethernet protocol level. This means that between a Bluetooth terminal connected with "PAN NAP Profile" and a PC/laptop on the local LAN, the information packets will be forwarded directly with the Ethernet protocol. As in this case no routing is required on the IP level, the PCs/laptops and the Bluetooth-PAN NAP terminals may even be located in the same IP subnet.

However, if 'IP Connection Mode for NAP Terminals' [3.7] is set to *routing*, the information packets exchanged between the PCs/laptops on the local LAN and the Bluetooth PAN NAP terminals must be routed on the IP level. For this to work, these terminals must then be located in different IP subnets.

8.6.1 Terminal Fixed Servers [3.5]

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

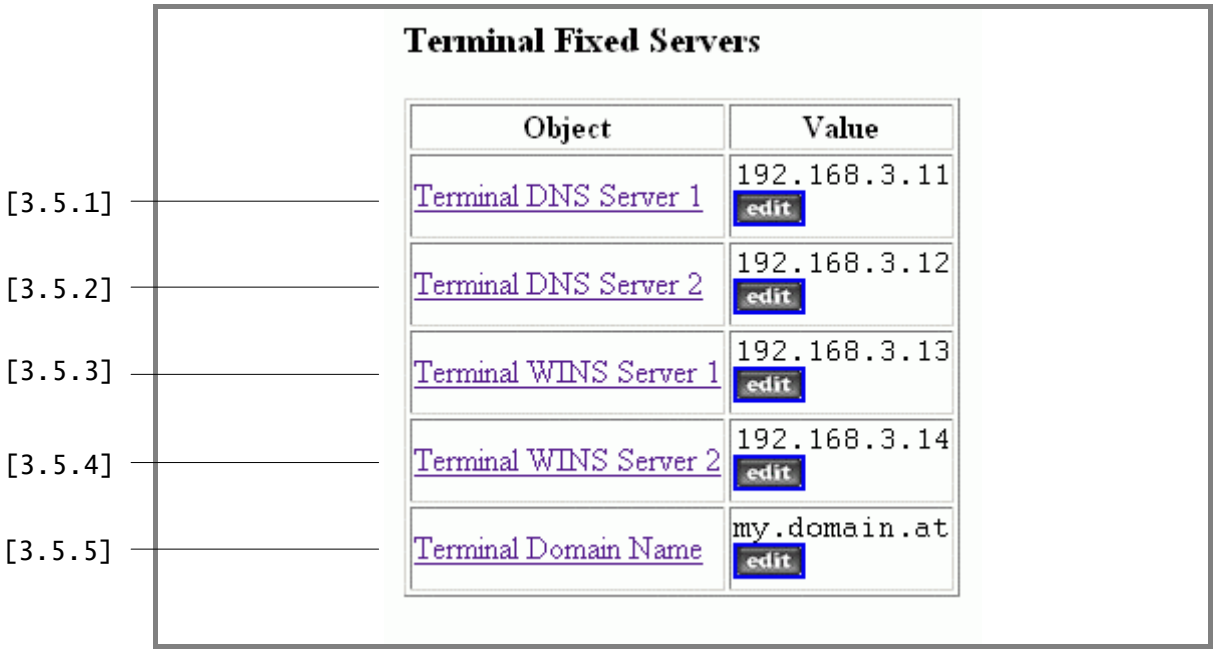


Figure 24 Terminal Fixed Servers [3.5]

Objects (see Figure 24)	**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*. Enter the correct DNS IP address manually if this DNS IP address cannot be transmitted correctly by the DHCP server.
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*.

Objects (see Figure 24)	Hier. level	Factory setting, other values, value range	Explanation
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 40 Terminal Fixed Servers [3.5]

8.6.2 Local DHCP Server Objects [3.6]

Here, you can assign IP addresses, via DHCP, to Bluetooth terminals that use the "PAN NAP Service" to connect, and to computers that are wire-connected to the local Ethernet.

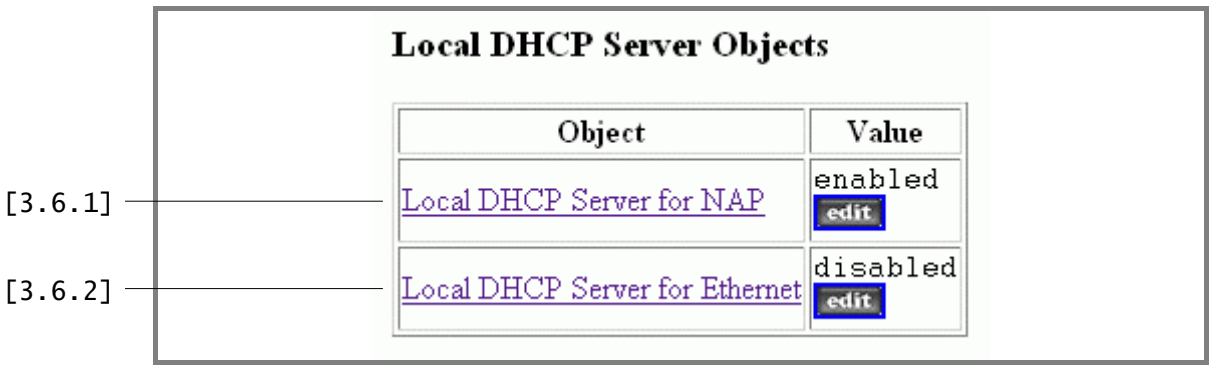


Figure 25 Local DHCP Server Objects [3.6]

Objects (see Figure 25)	Hier. level	Factory setting, other values, value range	Explanation
Local DHCP Server for NAP	[3.6.1]	enabled disabled	Here you can enable or disable the DHCP server for Bluetooth terminals that use the "PAN NAP Service" to connect.
Local DHCP Server for Ethernet	[3.6.2]	disabled enabled	Here you can enable or disable the DHCP server for Ethernet terminals (PCs/laptops). This setting is ineffective in "bridging mode".

Table 41 Local DHCP Server Objects [3.6]

In case 'IP Connection Mode for NAP Terminals" [3.7] is set to *bridging*, it is not possible to enable [3.6.1] and [3.6.2] independently of each other. In such a case, the DHCP server will serve both Bluetooth terminals via "PAN NAP Service" and Ethernet terminals (PCs/laptops on the local LAN) as soon as flag [3.6.1] is set to *enabled*.

8.6.3 Available IP Addresses for Local Wired Network [3.8]

The IP addresses lying within the specified range are assigned by the DHCP server to the Ethernet terminals (PCs/laptops on the local LAN). Of course, this will happen only if 'Local DHCP Server for Ethernet' [3.6.2] is set to *enabled*. Moreover, this range of IP addresses will be used only if 'IP Connection Mode for NAP Terminals' is set to *routing*.

If 'IP Connection Mode for NAP Terminals' is set to *bridging*, the range between [3.2] and [3.3] will also be used for the Ethernet terminals (PCs/laptops on the local LAN) provided the DHCP server is set to *enabled* in [3.6.1] or [3.6.2].

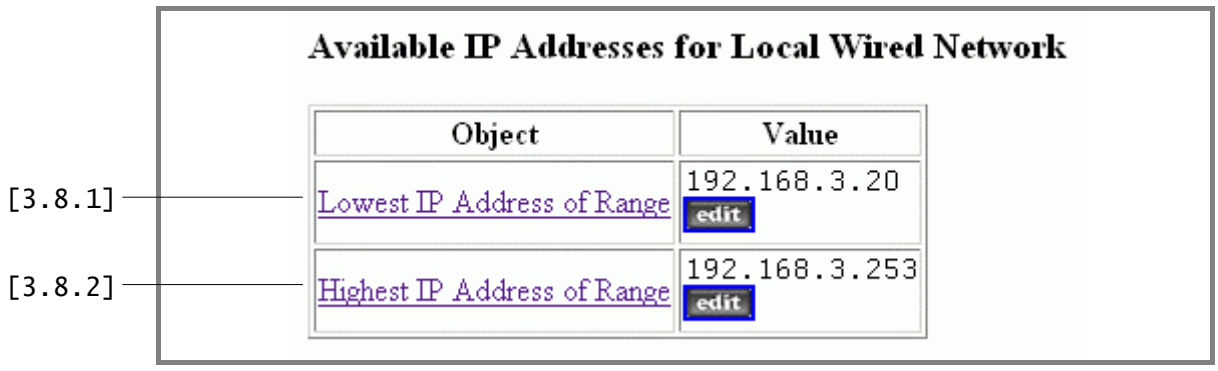


Figure 26 Available IP Addresses for Local Wired Network [3.8]

Objects (see Figure 26)	Hier. level	Factory setting, other values, value range	Explanation
Lowest IP Address of Range	[3.8.1]	192.168.3.20	The lowest IP address (inclusive) of the range the DHCP server uses to assign IP addresses to Ethernet terminals (PCs/laptops on the local LAN) if the Ethernet address is not specified explicitly in 'Fixed IP Addresses for Local Wired Network' [3.9].
Highest IP Address of Range	[3.8.2]	192.168.3.253	The highest (inclusive) IP address of the range. If you want to assign IP addresses only to terminals with a registered MAC address (see table for 'Fixed IP Address for Local Wired Network' [3.9], set [3.2] and [3.3] to *0.0.0.0*

Table 42 Available IP Addresses for Local Wired Network [3.8]

The DHCP server uses this range of IP addresses to assign IP addresses to PCs/laptops on the local LAN if the Ethernet addresses of the PCs/laptops are not listed in Table [3.9] and 'IP Connection Mode for NAP Terminals' [3.7] is set to *routing*.

The IP addresses within the range should be in the same subnet as the IP addresses for the second IP interface under [2.8.2].

If you are using an xDSL- modem and PPPoE as access protocol, the IP addresses within the range should be in the same subnet as the IP addresses for the first IP interface of blue2net under [2.2].

8.6.4 Fixed IP Addresses for Local Wired Network [3.9]

Here you can assign fixed IP addresses, via DHCP, to computers connected to the local Ethernet. This table will be used only if 'IP Connection Mode for NAP Terminals'[3.7] is set to *routing* and the DHCP server specified in [3.6] is enabled.

If the second IP interface is enabled, these IP addresses should lie in the same subnet as the IP address of the second IP interface of blue2net under [2.8.2]. Otherwise, these IP addresses should lie in the same subnet as the IP address of the first IP interface of blue2net under [2.2].

If you are using an xDSL- modem and PPPoE as access protocol, the IP addresses should be in the same subnet as the IP address of the first IP interface of blue2net under [2.2].

Note: Make sure that none of the 'Fixed IP Addresses for Local Wired Network' [3.9.3] overlap with the IP address range [3.8.1] to [3.8.2] ('Available IP Addresses for Local Wired Network').

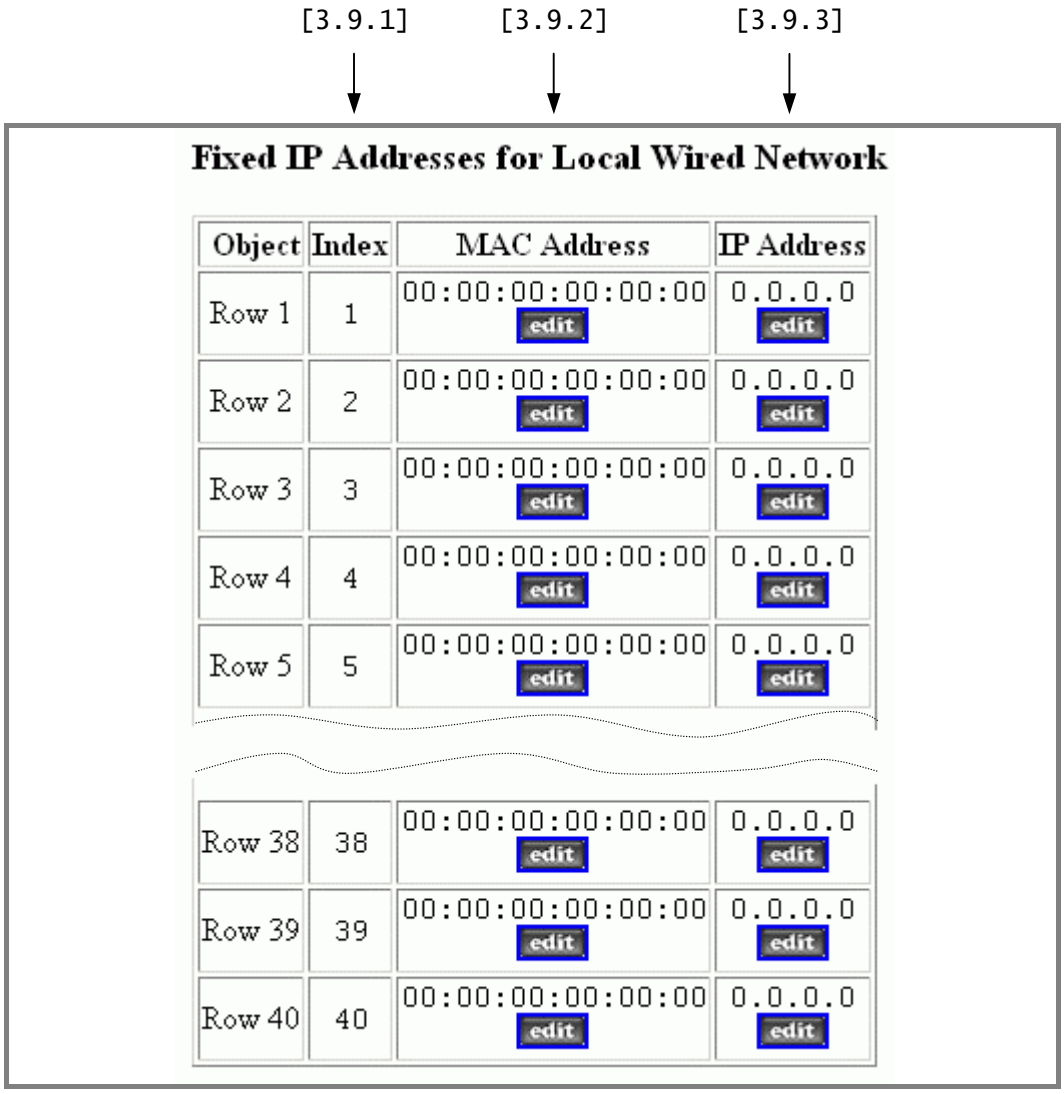


Figure 27 Fixed IP Addresses for Local Wired Network [3.9]

Objects (see Figure 27)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Index	[3.9.1]	1-40 Number of the entry (read only)	not relevant
MAC Address	[3.9.2]	XX:XX:XX:XX:XX X ... 0-9 und A-F	Ethernet address of the network card of the Ethernet terminal (PCs/laptops) (in hexadecimal format)
IP Address	[3.9.2]	AAA.BBB.CCC.DDD Internet address	IP address to be set via DHCP on the network card of the Ethernet terminal (PCs/laptops on the home network).

Table 43 Fixed IP Addresses for Local Wired Network [3.9]

8.7 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.

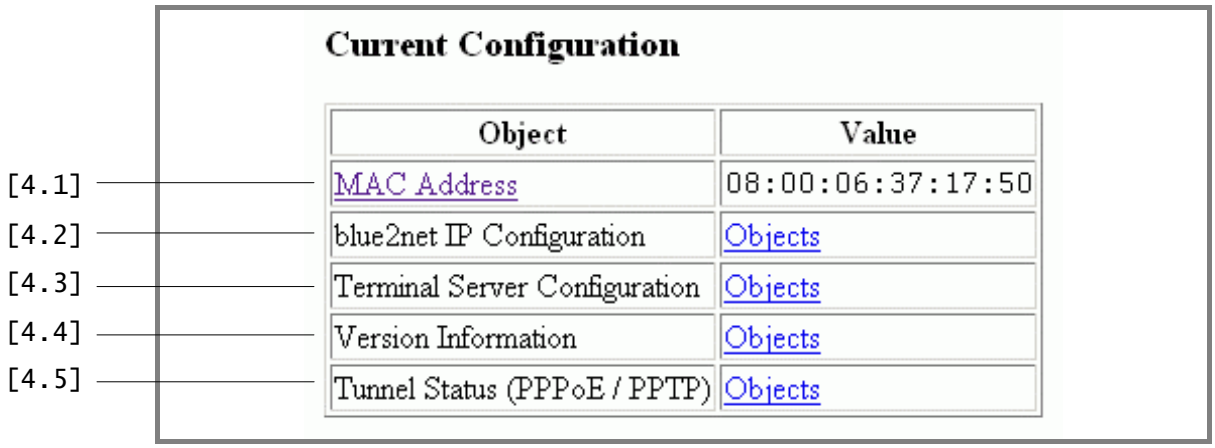


Figure 28 Current Configuration [4]

Objects (see Figure 28)	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 45
Terminal Server Configuration	[4.3]	see Table 46
Version Information	[4.4]	see Table 47
Tunnel Status (PPPoE / PPTP)	[4.5]	see Table 48 and Table 49

Table 44 Current Configuration [4]

8.7.1 blue2net IP Configuration [4.2]

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

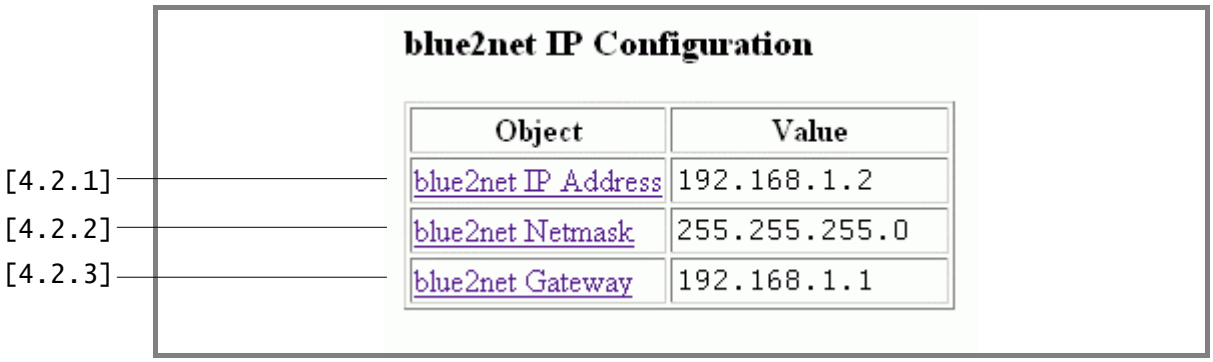


Figure 29 blue2net IP Configuration [4.2]

Objects (see Figure 29)	**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 assigned to blue2net. If the 'blue2net IP Address Resolution' [2.1] is set to *dhcp*, this value was retrieved via a DHCP request.

Table 45 blue2net IP Configuration [4.2]

8.7.2 Terminal Server Configuration [4.3]

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

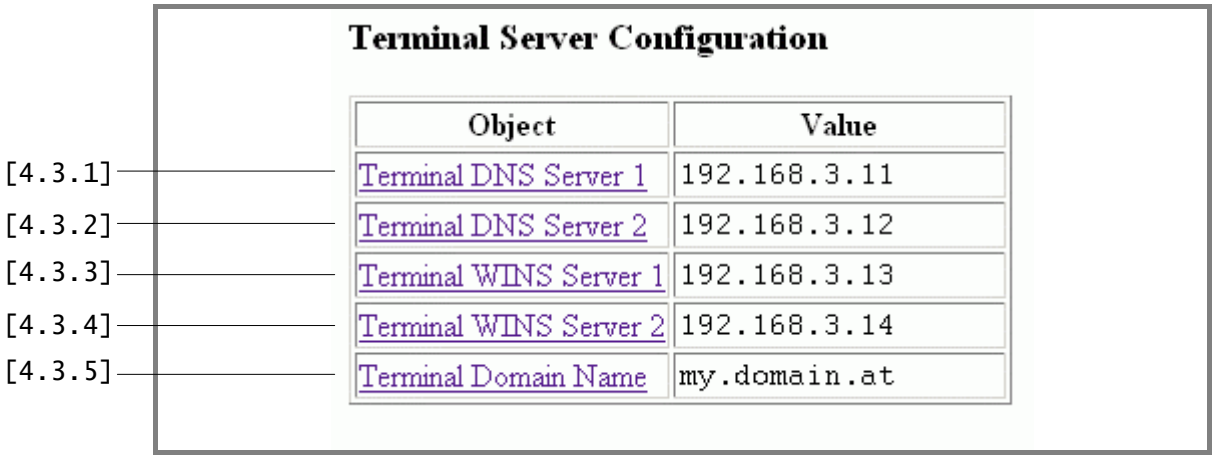


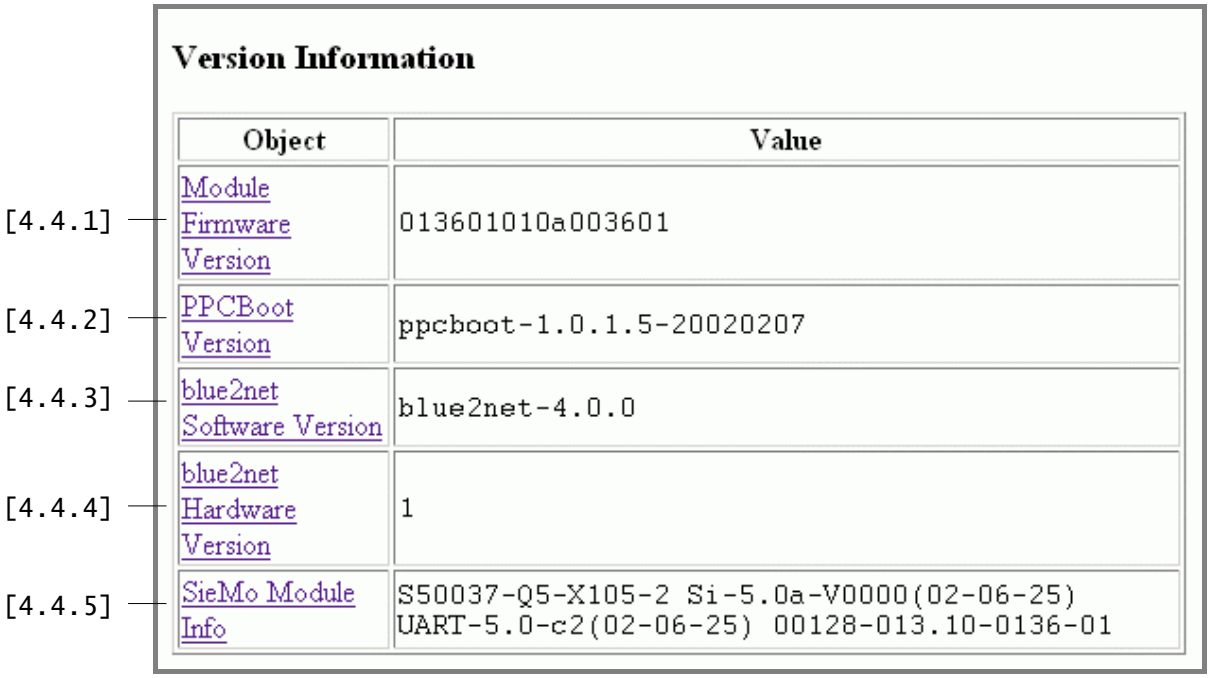
Figure 30 Terminal Server Configuration [4.3]

Objects (see Figure 30)	**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 46 Terminal Server Configuration [4.3]

8.7.3 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	013601010a003601
[4.4.2]	PPCBoot Version	ppcboot-1.0.1.5-20020207
[4.4.3]	blue2net Software Version	blue2net-4.0.0
[4.4.4]	blue2net Hardware Version	1
[4.4.5]	SieMo Module Info	S50037-Q5-X105-2 Si-5.0a-V0000(02-06-25) UART-5.0-c2(02-06-25) 00128-013.10-0136-01

Figure 31 Version Information [4.4] (example)

Objects (see Figure 31)	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 47 Version Information [4.4]

8.7.4 Tunnel Status (PPPoE / PPTP) [4.5]

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

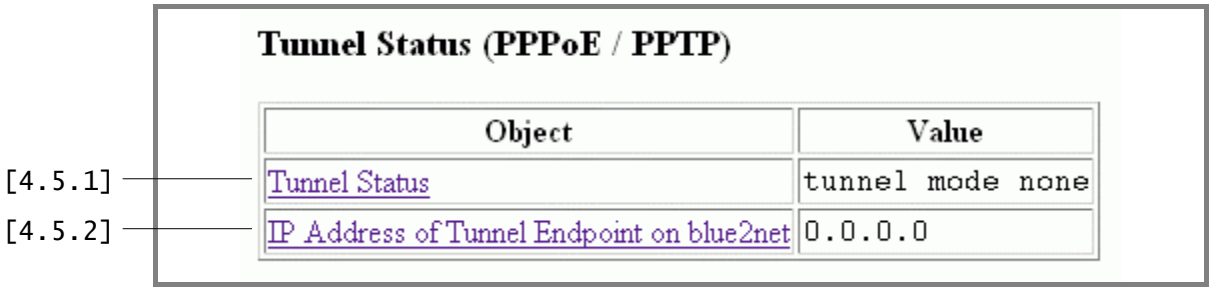


Figure 32 Tunnel Status (PPPoE / PPTP) [4.5]

Objects (see Figure 32)	Hier. level	Explanation
Tunnel Status	[4.5.1]	Current status of the "tunnel".
IP Address of Tunnel Endpoint on blue2net	[4.5.2]	Current value for the IP address of the tunnel endpoint on blue2net.

Table 48 Tunnel Status (PPPoE / PPTP) [4.5]

A few examples of status messages relating to [4.5.1]::

Message	Description
... 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 49 Status messages (examples)

8.8 Configuration Access [5]

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

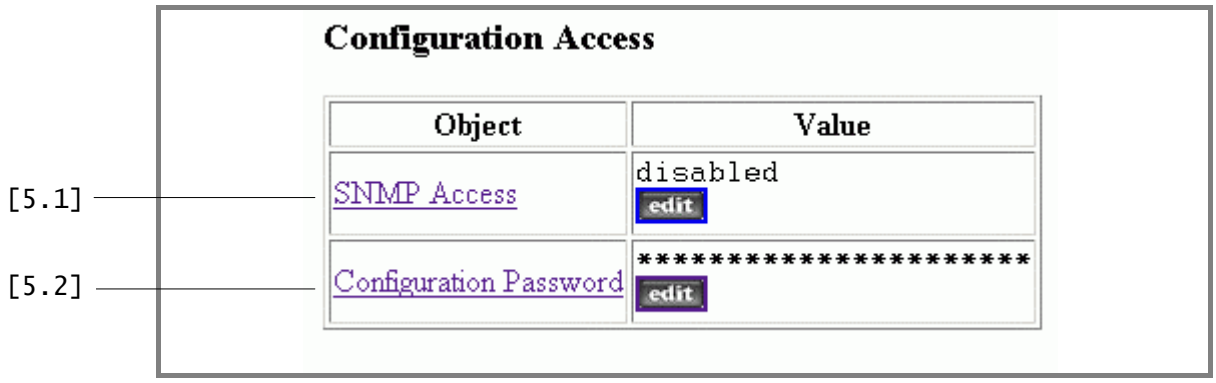


Figure 33 Configuration Access [5]

Objects (see Figure 33)	**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 10)

Table 50 Configuration Access [5]

8.8.1 Change of Configuration Password [5.2]

You have to enter the password twice (see Figure 34).

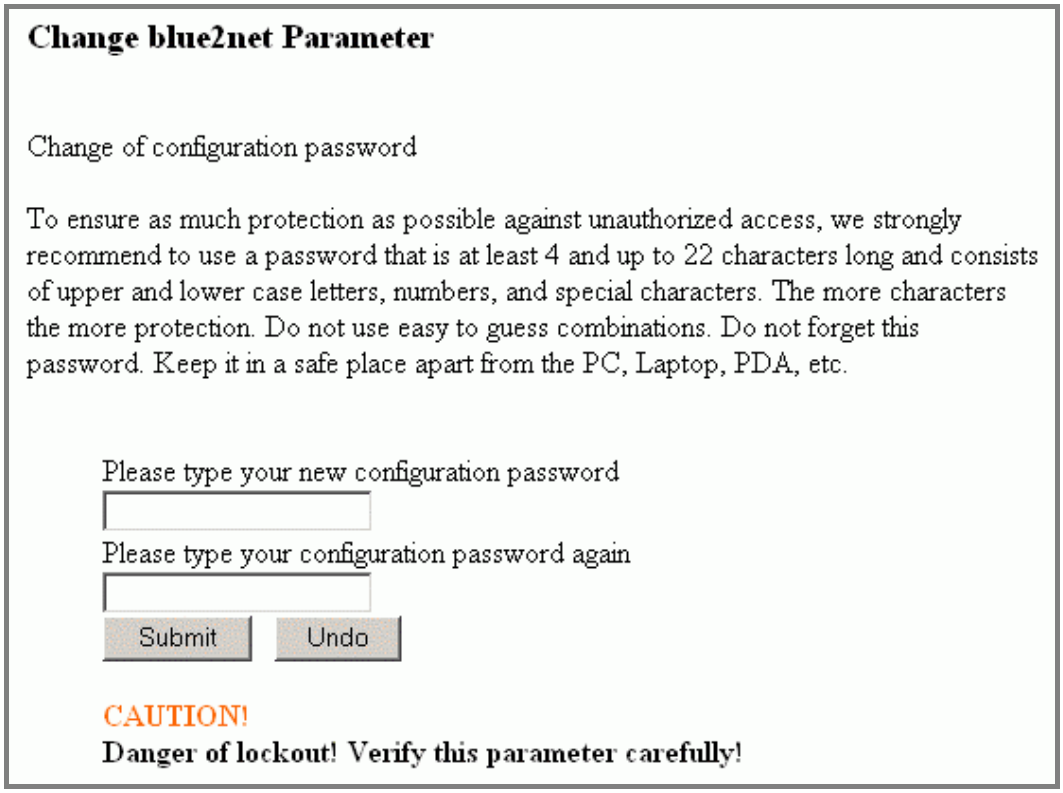


Figure 34 Change of Configuration Password [5.2]

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 8.9.1 and 8.9.2).

8.9 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'. This fact has certain advantages, for instance in the case of a possible lockout after incorrect settings (also refer to chapter 10). However, it is important to always remember this, especially with respect to the security settings.

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

After downloading updated software or loading a file for your own specific blue2net homepage, you have to save the changes you made in order to let them take effect.

Mind the warnings in order to prevent locking yourself out from access via Bluetooth or LAN (see also chapter 10).

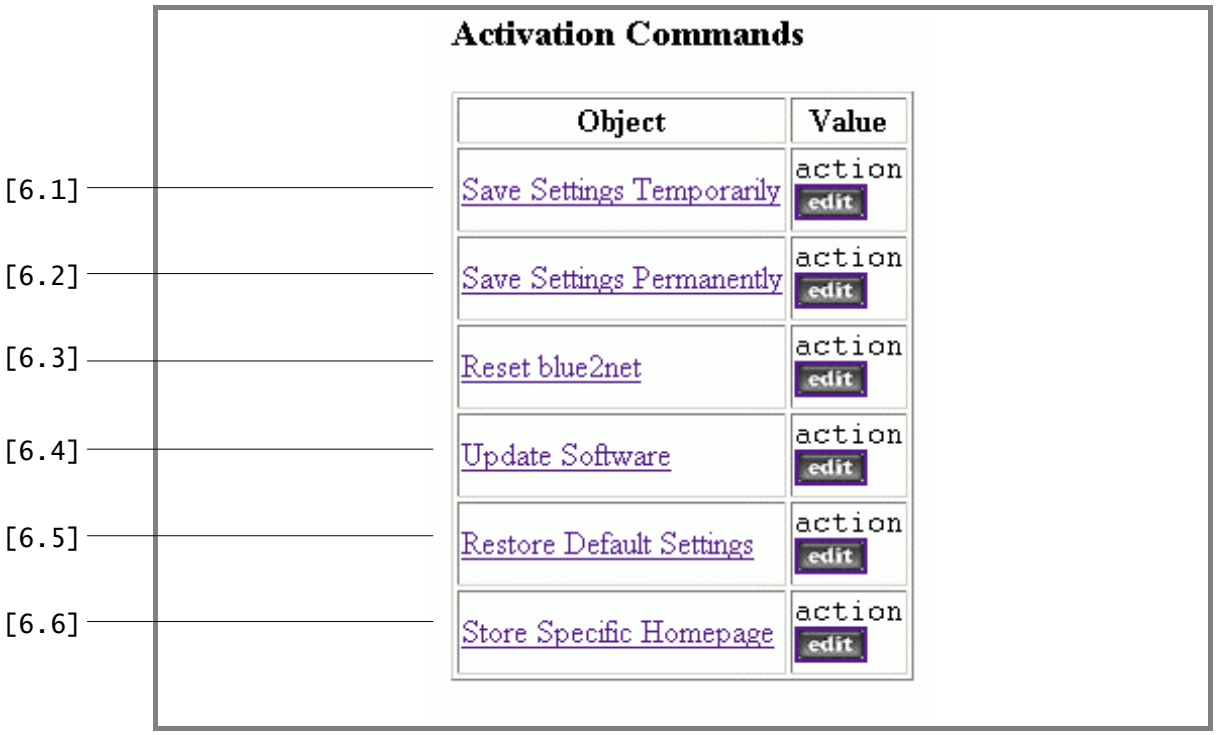


Figure 35 Activation Commands [6]]

Click on the <edit> button to get a page like the one displayed below (see Figure 36).

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

Figure 36 Activation Command (Save Settings Temporarily [6.1]

8.9.1 Save Settings Temporarily [6.1]

Any changes you make in one or more blue2net parameters will not take effect unless you save them. Always remember this, especially with respect to the security settings.

You can save changes either

- *temporarily* (e.g. for the current session) by selecting 'Save Settings Temporarily' [6.1], or
- *permanently* (until further changes are saved to memory) by selecting 'Save Settings Permanently' [6.2].

'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 (e.g. [6.3], 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 [6.3] 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' [1.#] and/or 'IP Parameters for Terminals' [3.#] 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 on how to prevent this, see chapter 10, “Preventing Lockout”

If you have locked yourself out, 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 [4.2.1] required!), click the <edit> button next to 'Activation Commands [6]', click the <edit> button next to 'Reset blue2net' [6.3] 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 the user manual.

8.9.2 Save Settings Permanently [6.2]

Any changes you make in one or more settings will not take effect unless you save them. Always remember this, especially with respect to the security settings.

You can save changes either

- *temporarily* (e.g. for the current session) by selecting 'Save Settings Temporarily' [6.1], or
- *permanently* (until further changes are saved to memory) by selecting 'Save Settings Permanently' [6.2] .

'Save Settings Permanently' saves the changed parameters in permanent memory, until further changes are save there.

If you have configured 'Bluetooth Parameters' [1.#] and/or 'IP Parameters for Terminals' [3.#] 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' (chapter 8.9.1), for in case you *lock yourself out* by saving the wrong settings in permanent memory, your only option in the worst case (see chapter 10.1) is to send the unit in to the service center (chapter 19) and have it reset to the factory settings there. For more information on how to prevent lock-out, see chapter 10.

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

8.9.3 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 a waiting time of 2 minutes 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 the user manual.

8.9.4 Update Software [6.4]

The blue2net manufacturer provides software updates to improve the performance of the device or to eliminate bugs or defects.

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 the service homepage.

For details on how to proceed, please see chapter 11

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

8.9.5 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 17.

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 by resetting all your own settings to the factory settings and then reconfiguring them.

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

8.9.6 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. You can then call it up on the Web interface homepage (see Figure 3).

For details on how to proceed, please see chapter 12.1.

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

9 Overview of Network Structures

This chapter is intended for readers wanting to know more about network structure issues related to the operation of blue2net.

If terms such as Internet protocol, Ethernet, and routing don't mean much to you, just skip this chapter and resort to the use scenario in chapter 7 that is most adequate for your purposes.

- If 'IP Connection Mode for NAP Terminals' [3.7] is set to *bridging*, the devices using this service are connected to the local network over blue2net's Ethernet interface in such a way as if they were directly plugged in there with a network card. They are thus able to use all the protocols starting from layer 2 (Ethernet Standard IEEE 802.3).

  Bluetooth devices using "LAN Access Profile" as access profile can use all protocols starting from layer 3 (Internet protocol). blue2net can use DHCP to get configuration information for you from an external DHCP server by using the Bluetooth address as MAC address. With the help of the "proxy_arp" technology, the LAP terminals appear, for IP transaction purposes, to other Ethernet participants as if they were directly connected to the Ethernet cable.

- If 'IP Connection Mode for NAP Terminals' [3.7] is set to *routing*, blue2net acts as router for those Bluetooth devices that use NAP as access service. All Bluetooth devices should preferably be in the same subnet. DHCP inquiries from Bluetooth NAP terminals don't reach the local Ethernet, so it is best to enable "Local DHCP Server for NAP Terminals". Bluetooth devices can then be distinguished from devices connected to the local Ethernet on the basis of the IP subnet in which they lie. As blue2net does not support any router information protocol (RIP, IGP), routers working on the local Ethernet cannot send data packets directly to Bluetooth devices. For this reason, it is necessary to use masquerading and/or port forwarding in this case. Only if you are running a purely "insular" solution without routers or Internet access can you do without masquerading.

9.1 Network Structure with 'IP Connection Mode for NAP Terminals' [3.7] Set to "routing"

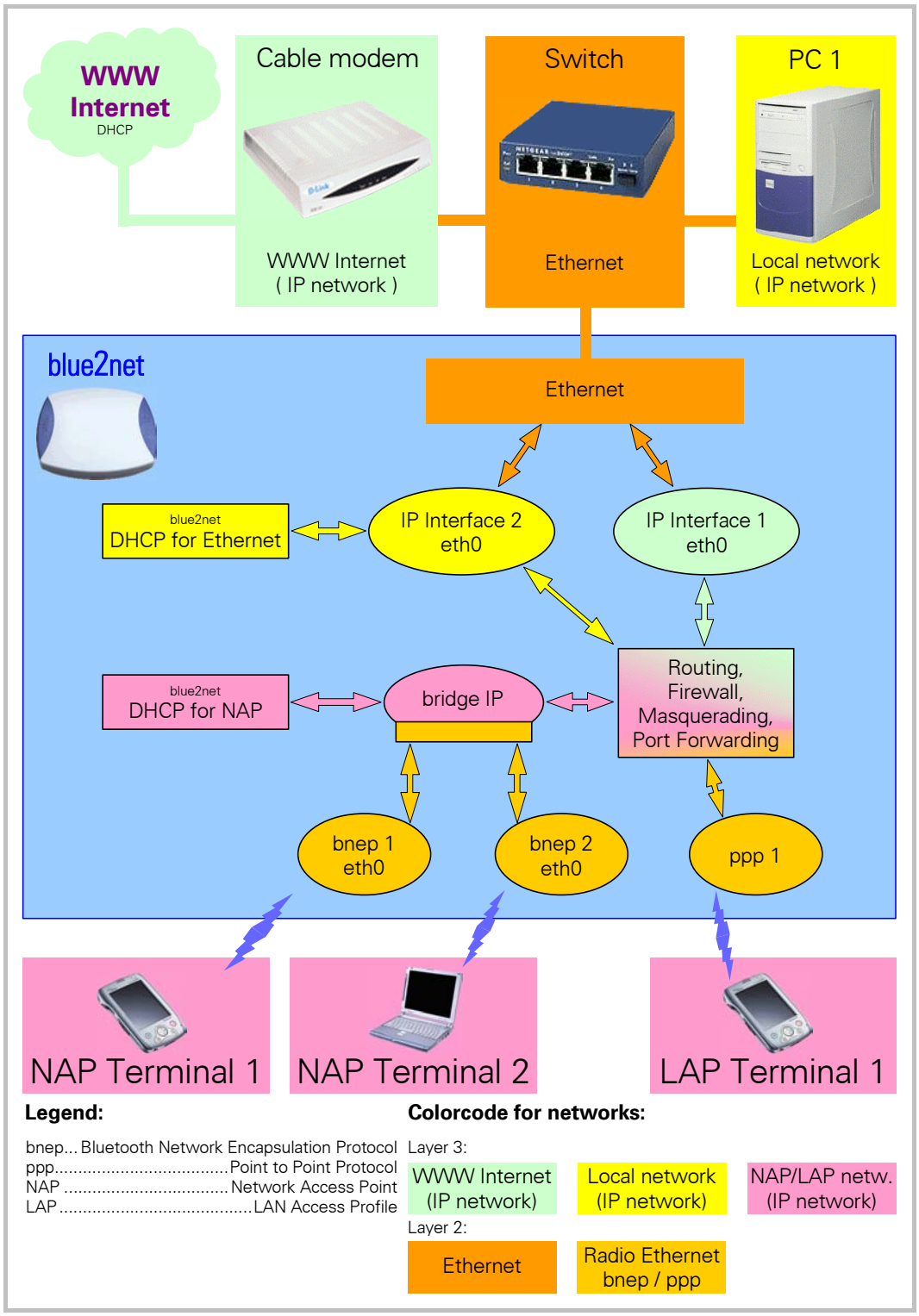


Figure 37 Network structure for blue2net with the 'IP Connection Mode for NAP Terminals' mode [3.7] set to "routing"

Figure 37 illustrates the network structure when blue2net is used as router for Bluetooth NAP terminals.

This is the typical use case if you want to connect blue2net to the Internet via a cable modem at home.

Bluetooth LAN Access Profile terminals and Bluetooth-NAP terminals are located in the same IP subnet and are configured for NAP by means of the internal blue2net DHCP server. In this case (masquerading enabled), blue2net shows the Masquerading IP [2.5] on the "bridge". The NAP terminals are linked on blue2net on the Ethernet level (e.g. ARP).

PC1 is located in a local IP subnet, blue2net has a separate second IP interface in this subnet. blue2net uses an internal blue2net DHCP server to configure PC1 for Ethernet terminals.

As routing is not possible if IP interface 2 and bridge IP (IP masquerading from [2.5]) are located in the same subnet, make sure that 'Fixed blue2net Additional IP Address' [2.8.3.1] is not in the same subnet as 'IP Masquerading' [2.5] with netmask from 'Terminal Net Mask' [3.4].

The connection to the Internet service provider is set up via blue2net's first IP interface. blue2net gets the IP data for this interface for example via a DHCP server provided by the ISP.

All IP packets going from and to the Internet must pass through the "Routing, Firewall, Masquerading, Port Forwarding" block, as the ISP recognizes only the IP address of IP interface 1. The local PC, PC1, also sends data packets destined for the Internet first to blue2net where they are masqueraded (i.e. the sender IP address is replaced with the blue2net IP address on interface 1) and routed onwards to the Internet. The packets from the Internet destined for PC1 arrive at blue2net via IP interface 1, are de-masqueraded in the routing block (i.e. the sender IP address of PC 1, which was replaced above, is again written to the IP packet as destination address instead of the IP address of blue2net IP interface 1) and are then forwarded to PC1 via IP interface 2.

9.2 Network Structure with 'IP Connection Mode for NAP Terminals' [3.7] Set to "bridging"

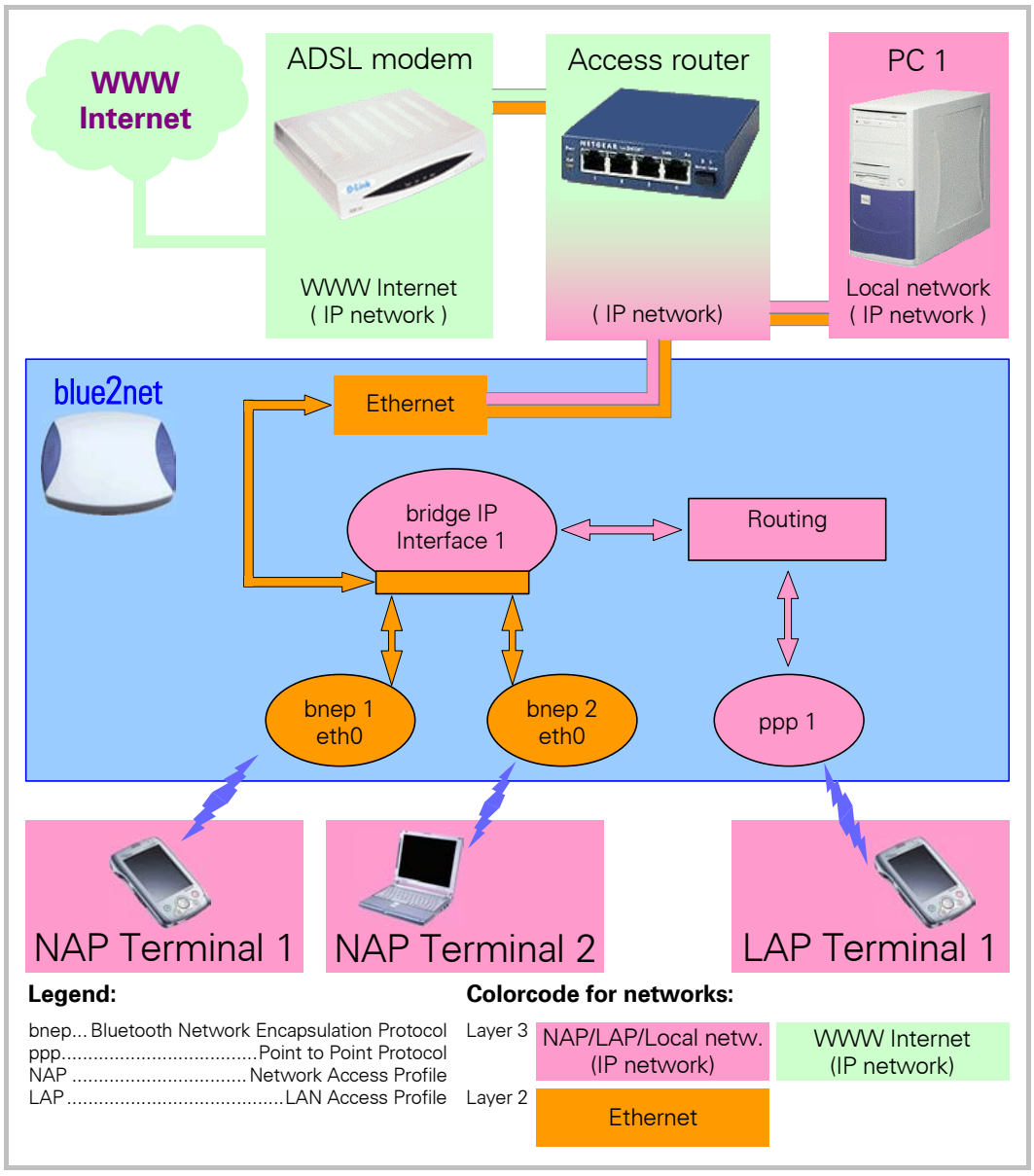


Figure 38 Network structure for blue2net with the 'IP Connection Mode for NAP Terminals' mode [3.7] set to "bridging"

Figure 38 illustrates a typical network structure where blue2net is used with 'IP Connection Mode for NAP Terminals' [3.7] set to *bridging*. The figure specifically shows a situation where you are already using another device as access router which offers you the following functions

- operation of ADSL modem
- device configuration via DHCP
- firewall against the WWW Internet

This device may of course also be another blue2net combined with a low-priced switch. In "bridging mode", all Ethernet devices on blue2net are connected with one another as if they were connected directly to the Ethernet. The laptop "NAP Terminal 2" and the PDA "NAP Terminal 1" are also directly connected to the local Ethernet on the access router via the interfaces "bnep1" and "bnep2" and the "bridge". For this reason "PC 1" can, for instance, reach "NAP Terminal 1" directly, without a detour via routing. In the local network, blue2net appears with the IP address you defined as fixed IP address in [2.1] to [2.3], e.g.192.168.2.2 .

The Bluetooth NAP terminals, the Bluetooth terminals that use LAP, and the other devices on the local Ethernet all get the information for their IP interfaces from the access router, via its DHCP server. For this to work it is necessary for the Bluetooth NAP terminals to be able to directly access the local Ethernet by means of the "bridging mode", because DHCP uses Ethernet broadcast. (See use scenario 7.1.3). For the LAP terminals, blue2net can execute the DHCP protocol (using the terminals' Bluetooth addresses as hardware addresses) and then forward the configuration data thus retrieved to the Bluetooth LAP terminals via PPP.

If, with 'IP Connection Mode for NAP Terminals' [3.7] set to *bridging*, you enable the second IP interface, it will appear as second IP interface on the "bridge". As it can be assumed that you want to use the second IP interface for the local network and that the IP packets from the local network are to be masqueraded if 'Terminal IP Address Resolution' [3.1] is set to *masquerading* or *masqueradingpool*, the second IP interface will automatically get the IP address from 'IP Masquerading' [2.5]. Only if you have set 'Terminal IP Address Resolution' [3.1] to *dhcp* or *predefined* will the IPs from [2.8.2] become effective.

9.3 IP Addresses for Terminals

Table 51 to Table 58 are designed to help you enter the correct values for the IP addresses of terminals on the blue2net configuration user interface.

The tables always come in pairs: a parameter table and a solution table.

In the first table (parameter table), look for the row containing the parameter setting you have selected (highlighted in blue and gray). Then, in the green columns in this row, select the type of terminal that is interesting for you, remember the index number shown there and look for it in the subsequent solution table.

There, you can see where the IP address of the terminal comes from. If the cell in the parameter table or the row in the solution table is highlighted in pink, blue2net will not ensure automatically that the IP address of the terminal is in the correct subnet. In that case the system administrator will have to take care of this matter. The contents of cells highlighted in gray do not change in a parameter table, while the contents of cells highlighted in blue will.

An example:
'IP Connection Mode for NAP Terminals' [3.7] is set to *bridging*, 'Additional IP Interface' [2.8.1] is set to *enabled*, 'Terminal IP Address Resolution' [3.1] is set to *masquerading*, 'Local DHCP Server for NAP' [3.6.1] is set to *enabled*, 'Local

DHCP Server for Ethernet' [3.6.2] is set to *enabled*, and MAC address+ IP address in Terminal Table [1.10] for a terminal intending to use LAP do not exist.

This setting corresponds to row 3 in Table 51, the cell for LAP terminal holds the index number 3. As the cell is not highlighted in red, blue2net will automatically ensure that the IP address of the terminal will be located in the correct subnet by generating the subnet part of the IP address.

In solution Table 52, row 3 shows you that the LAP terminal gets its IP address from "Terminal IP Address Pool Range" [3.2]-[3.3]. In addition, it also tells you that the terminal IP address will be automatically placed into the subnet defined through 'IP Masquerading' [2.5] and 'Terminal Netmask' [3.4].

IP Connection Mode for NAP Terminals [3.7]	Additional IP Interface [2.8.1]	Terminal IP Address Resolution [3.1]	Local DHCP Server for NAP [3.6.1]	Local DHCP Server for Ethernet [3.6.2]	MAC address + IP address exist in 'Terminal Table' [1.10]	Terminal type -> Index in Table 52		
						Bluetooth LAP	Bluetooth NAP	Ethernet
bridging	enabled	masquerading	enabled	irrelevant	yes	1	1	1
bridging	enabled	masquerading	disabled	irrelevant	yes	1	6	6
bridging	enabled	masquerading	enabled	irrelevant	no	3	3	3
bridging	enabled	masquerading	disabled	irrelevant	no	3	6	6
bridging	enabled	masqueradingpool	enabled	irrelevant	yes	7	7	7
bridging	enabled	masqueradingpool	disabled	irrelevant	yes	7	6	6
bridging	enabled	masqueradingpool	enabled	irrelevant	no	1	1	1
bridging	enabled	masqueradingpool	disabled	irrelevant	no	1	6	6
bridging	enabled	predefined	enabled	irrelevant	yes	4	4	4
bridging	enabled	predefined	disabled	irrelevant	yes	4	2	2
bridging	enabled	predefined	enabled	irrelevant	no	5	5	5
bridging	enabled	predefined	disabled	irrelevant	no	2	2	2
bridging	enabled	dhcp	irrelevant	irrelevant	irrelevant	2	2	2
bridging	disabled	masquerading	enabled	irrelevant	yes	1	1	1
bridging	disabled	masquerading	disabled	irrelevant	yes	1	6	6
bridging	disabled	masquerading	enabled	irrelevant	no	3	3	3
bridging	disabled	masquerading	disabled	irrelevant	no	3	6	6
bridging	disabled	masqueradingpool	enabled	irrelevant	yes	7	7	7
bridging	disabled	masqueradingpool	disabled	irrelevant	yes	7	6	6
bridging	disabled	masqueradingpool	enabled	irrelevant	no	3	3	3
bridging	disabled	masqueradingpool	disabled	irrelevant	no	3	6	6
bridging	disabled	predefined	enabled	irrelevant	yes	10	10	10
bridging	disabled	predefined	disabled	irrelevant	yes	10	12	12
bridging	disabled	predefined	enabled	irrelevant	no	11	11	11
bridging	disabled	predefined	disabled	irrelevant	no	11	12	12
bridging	disabled	dhcp	irrelevant	irrelevant	irrelevant	12	12	12

Table 51 Parameter table: impact of settings on terminal IP and terminal netmasks if 'IP Connection Mode for NAP Terminals' is set to *bridging*

Index	Subnet for terminal IP	Subnetmask for terminal	Automati-cally in correct subnet ?	IP address for terminal derived from ? This entry must be in the correct subnet
1	Masquerading IP [2.5]	Terminal Netmask [3.4]	yes	Entry in Terminal Table [1.10]
2	Fixed blue2net Additional IP Addr. [2.8.2.1]	Terminal Netmask [3.4]	no	External DHCP server
3	Masquerading IP [2.5]	Terminal Netmask [3.4]	yes	Terminal IP Address Pool Range [3.2]-[3.3]
4	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	no	Entry in Terminal Table [1.10]
5	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	no	Terminal IP Address Pool Range [3.2]-[3.3]
6	Masquerading IP from [2.5]	Terminal Netmask [3.4]	no	External DHCP server
7	Masquerading IP from [2.5]	Terminal Netmask [3.4]	no	Entry in Terminal Table [1.10]
10	blue2net IP from [2.1]-[2.3]	blue2net Netmask [2.1]-[2.3]	no	Entry in Terminal Table [1.10]
11	blue2net IP from [2.1]-[2.3]	blue2net Netmask [2.1]-[2.3]	no	Terminal IP Address Pool Range [3.2]-[3.3]
12	blue2net IP from [2.1]-[2.3]	blue2net Netmask [2.1]-[2.3]	no	External DHCP server

Table 52 Solution table for Table 51

IP Connection Mode for NAP Terminals [3.7]	Additional IP Interface [2.8.1]	Terminal IP Address Resolution [3.1]	Local DHCP Server for NAP [3.6.1]	Local DHCP Server for Ethernet [3.6.2]	MAC address+ IP address exist in 'Terminal Table' [1.10]	Terminal type -> Index in Table 54	
						Bluetooth LAP	Bluetooth NAP
routing	irrelevant	masquerading	enabled	irrelevant	yes	1	1
routing	irrelevant	masquerading	disabled	irrelevant	yes	1	2
routing	irrelevant	masquerading	enabled	irrelevant	no	3	3
routing	irrelevant	masquerading	disabled	irrelevant	no	3	2
routing	irrelevant	masqueradingpool	enabled	irrelevant	yes	4	4
routing	irrelevant	masqueradingpool	disabled	irrelevant	yes	4	2
routing	irrelevant	masqueradingpool	enabled	irrelevant	no	3	3
routing	irrelevant	masqueradingpool	disabled	irrelevant	no	3	2
routing	irrelevant	predefined	enabled	irrelevant	yes	4	4
routing	irrelevant	predefined	disabled	irrelevant	yes	4	2
routing	irrelevant	predefined	enabled	irrelevant	no	5	5
routing	irrelevant	predefined	disabled	irrelevant	no	5	2
routing	irrelevant	dhcp	irrelevant	irrelevant	irrelevant	6	2

Table 53 Parameter table: impacts of settings on terminal IP and terminal netmasks for Bluetooth terminals if 'IP Connection Mode for NAP Terminals' is set to *routing*

Index	Subnet for terminal IP	Subnetmask for terminal	Automatically in correct subnet?	IP address for terminal derived from ? This entry must be in the correct subnet
1	Masquerading IP [2.5]	Terminal Netmask [3.4]	yes	Entry in Terminal Table [1.10]
2	Masquerading IP [2.5]	Terminal Netmask [3.4]	no	Fixed configuration at terminal
3	Masquerading IP [2.5]	Terminal Netmask [3.4]	yes	Terminal IP Address Pool Range [3.2]-[3.3]
4	Masquerading IP [2.5]	Terminal Netmask [3.4]	no	Entry in Terminal Table [1.10]
5	Masquerading IP [2.5]	Terminal Netmask [3.4]	no	Terminal IP Address Pool Range [3.2]-[3.3]
6	Masquerading IP [2.5]	Terminal Netmask [3.4]	no	External DHCP server

Table 54 Solution table for Table 53

IP Connection Mode for NAP Terminals [3.7]	Additional IP Interface [2.8.1]	Terminal IP Address Resolution [3.1]	Local DHCP Server for NAP [3.6.1]	Local DHCP Server for Ethernet [3.6.2]	MAC address+ IP address exist in 'Fixed IP Address for Local Wired Network' [3.9]	Terminal type -> Index in Table 56
						Ethernet
routing	enabled	masquerading	irrelevant	enabled	yes	1
routing	enabled	masquerading	irrelevant	disabled	yes	2
routing	enabled	masquerading	irrelevant	enabled	no	3
routing	enabled	masquerading	irrelevant	disabled	no	2
routing	enabled	masqueradingpool	irrelevant	enabled	yes	4
routing	enabled	masqueradingpool	irrelevant	disabled	yes	2
routing	enabled	masqueradingpool	irrelevant	enabled	no	3
routing	enabled	masqueradingpool	irrelevant	disabled	no	2
routing	enabled	predefined	irrelevant	enabled	yes	4
routing	enabled	predefined	irrelevant	disabled	yes	2
routing	enabled	predefined	irrelevant	enabled	no	5
routing	enabled	predefined	irrelevant	disabled	no	2
routing	enabled	dhcp	irrelevant	irrelevant	irrelevant	2

Table 55 Parameter table: impacts of settings on terminal IP and terminal netmasks for Ethernet terminals if 'IP Connection Mode for NAP Terminals' is set to *routing* and the second IP interface is enabled

Index	Subnet for terminal IP	Subnetmask for terminal	Automatically in correct subnet?	IP address for terminal derived from ? This entry must be in the correct subnet
1	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	yes	Entry in 'Fixed IP Address for Local Wired Network' [3.9]
2	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	no	Fixed setting on terminal or external DHCP server
3	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	yes	Available IP Addresses for Local Wired Network [3.8]
4	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	no	Entry in 'Fixed IP Address for Local Wired Network' [3.9]
5	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	no	Available IP Addresses for Local Wired Network [3.8]

Table 56 Solution table for Table 55

IP Connection Mode for NAP Terminals [3.7]	Additional IP Interface [2.8.1]	Terminal IP Address Resolution [3.1]	Local DHCP Server for NAP [3.6.1]	Local DHCP Server for Ethernet [3.6.2]	MAC address+ IP address exist in 'Fixed IP Address for Local Wired Network' [3.9]	Terminal type -> Index in Table 58
						Ethernet
routing	disabled	not dhcp	irrelevant	enabled	yes	1
routing	disabled	not dhcp	irrelevant	enabled	no	2
routing	disabled	dhcp	irrelevant	irrelevant	irrelevant	3

Table 57 Parameter table: impacts of settings on terminal IP and terminal netmasks for Ethernet terminals if 'IP Connection Mode for NAP Terminals' set to *routing* and the second IP interface is not enabled

Index	Subnet for terminal IP	Subnetmask for terminal	Automatically in correct subnet?	IP address for terminal derived from ? This entry must be in the correct subnet
1	blue2net IP from [2.1]-[2.3]	blue2net Netmask [2.1]-[2.3]	no	Entry in 'Fixed IP Address for Local Wired Network' [3.9]
2	blue2net IP from [2.1]-[2.3]	blue2net Netmask [2.1]-[2.3]	no	Available IP Addresses for Local Wired Network [3.8]
3	blue2net IP from [2.1]-[2.3]	blue2net Netmask [2.1]-[2.3]	no	External DHCP or fixed setting on terminal

Table 58 Solution table for Table 57

10 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 via either Bluetooth and Ethernet (LAN) or both.

This is not a malfunction of blue2net. Some settings are unavoidable for security reasons, 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 this information in a safe place separate from the blue2net unit, the PDA or laptop.

Also keep in mind the instructions regarding the saving of settings as described in chapter 8.9.2, and record *permanently saved settings*.

10.1 Lockout from Access via Bluetooth and Ethernet (LAN)

Parameter	Hier. level	Before setting it to	remember
Configuration Password	[5.2]	Your own new password	When you change the Configuration Password (which you should always do for security reasons), make sure to always remember 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 factory settings.

Table 59 Lockout scenarios: Lockout from Bluetooth and Ethernet (LAN)

10.2 Lockout from Access via Bluetooth

Parameter	Hier. level	Before setting it to	remember
Discoverability Mode	[1.4]	nondiscoverable	Some terminals need to have "seen" blue2net at least once and have saved the respective data before you can set up a connection. Ensure that (each) terminal "discovers" blue2net at least once (Bluetooth inquiry + service browsing) with the 'discoverable' setting enabled on blue2net.
Connectability Mode	[1.5]	nonconnectable	The only possibility to access your blue2net is via Ethernet (LAN). No Bluetooth connection is possible any more!
Max. No. of Terminals Connected]	[1.6]	0	
Auth. Level	[1.8.4]	authandenc or auth	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].
Activation	[1.8.9]	deactivated	If you set all 3 entries (LAN Access, PAN NAP, PAN GN) for the Bluetooth Service Class to *deactivated*, it is no longer possible to establish a Bluetooth connection. Then, the only way to access your blue2net is via Ethernet (LAN).
Default Access Mode	[1.11]	disabled	Only terminals listed 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]	new password	When you change the 'Default Bluetooth Passkey' (which you should always do for security reasons), make sure to always remember the new passkey. If you have no terminals registered in the terminal table [1.10], you will have no access.

Parameter	Hier. level	Before setting it to	remember
Minimum Length of Key for Encryption	[1.13]	16	It could happen that an older Bluetooth terminal doesn't support more than 56-bit encryption. In this case, it is not possible to set up a connection.
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 60 Lockout scenarios: Lockout from Bluetooth access

10.3 Lockout from Access via Ethernet (LAN)

Parameter	Hier. level	Before setting it to	remember
blue2net IP Address Resolution	[2.1]	predefined	Make sure you remember your fixed blue2net IP addresses [2.2.1] and fixed blue2net netmask [2.2.2]
blue2net IP Address Resolution	[2.1]	dhcp but DHCP service not available	Make sure you remember your fallback blue2net IP addresses [2.3.1] and fallback blue2net netmask [2.3.2]
Protocol Lower Port Number Enable Port Range Higher Port Number (Port Forwarding Rules)	Combination of [2.6.2.3] [2.6.2.4] [2.6.2.5] or [2.6.2.3] [2.6.2.4] [2.6.2.5] [2.6.2.6]	 6 443 disabled 6 ≤ 443 enabled ≥ 443	If you forward tcp port443 without having a second IP interface enabled (i.e. ‚Additional IP Interface' [2.8.1] set to *disabled*), blue2net can no longer be configured via the Ethernet-connection. Attention! tcp port 443 must not lie within the 'Port Range' between [2.6.2.4] and [2.6.2.6].
Lower/Higher Port Number + Enable Port Range (Port Forwarding Rules)	Combination of [2.6.2.4] [2.6.2.5] [2.6.2.6]	 0 enabled 65535 (tcp port 443 is included)	If you forward all the ports (range between [2.6.2.4] / [2.6.2.6]) without having enabled a second IP interface (i.e. ‚Additional IP Interface' [2.8.1] set to *disabled*), blue2net can no longer be configured via the Ethernet-connection.

Parameter	Hier. level	Before setting it to	remember
Protocol (Port Forwarding Rules)	[2.6.2.3]	255 (tcp port 443 is included)	If you forward "all protocols" (= value 255 in [2.6.2.3]) without having enabled a second IP interface (i.e. ‚Additional IP Interface' [2.8.1] set to *disabled*), blue2net can no longer be configured via the Ethernet-connection.

Table 61 Lockout scenarios: Lockout from access via Ethernet (LAN)

11 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. Settings that were stored in permanent memory will remain as they were (but note the information provided in chapter 11.1).

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

A software update takes effect only after a blue2net reboot.

11.1 Information for Upgrades from Previous SW Versions

Settings permanently saved before a software update will not be lost through a software update, but will remain unchanged. However, each new SW version might come with new parameters due to enhancements or changes to the scope of functions provided, while other parameters may become obsolete or factory settings may be changed, for example, due to security reasons.

To avoid that values from earlier software versions impact the functioning of blue2net in an uncontrollable manner, we recommend to proceed as follows:

- BEFORE the SW update:
  - download the software from the homepage and save it;
  - record the values of all parameters;
  - if you are using xDSL:
    - shut down the xDSL connection (set ‚Tunnel Mode' [2.7.1] to *none*),
    - save the values using ‚Save Settings Permanently' [6.2];
  - perform a reset using 'Reset blue2net' [6.3] (existing Bluetooth connection will be aborted!)
- only THEN:
  - perform the software update;
  - reset all values to the factory settings (see chapter 8.9.5);
  - reconfigure the values for all blue2net parameters; destroy records for security reasons.

Of course, you could also find out first which values have changed (see Change History) by referring to the tables in the new version's User Guide (e.g. "Hierarchy of Pages for Configuration Settings", chapter 8.3 and "Factory Settings", chapter 17 in the present document), check these values individually and correct them, where necessary (e.g. new factory setting). To do so, proceed as follows:

- BEFORE the SW update:
  - download the software from the homepage and save it;
  - record the values of all parameters having been changed or omitted;
  - if you are using xDSL:
  - shut down the xDSL connection (set ‚Tunnel Mode' [2.7.1] to none),
  - save the values using ‚Save Settings Permanently' [6.2];
  - perform a reset using 'Reset blue2net' [6.3] (existing Bluetooth connection will be aborted!)
- only THEN:
  - perform the software update;
  - reset all values to the factory settings (see chapter 8.9.5);
  - reconfigure the values for all changed and new parameters; destroy records for security reasons.

11.2 How to Download New Software

ATTENTION! The procedure described below is no longer applicable for previous versions!
If you want to update from an earlier SW version (see 'Current Configuration' [4] > [4.4.3]), follow the instructions provided for that earlier version installed on blue2net (The user guide featuring version x.y also goes together with software version x.y.z, for example 4.0 corresponds to 4.0.z).
Reason: the procedure described below for the current version has changed as against the one used up to the previous versions).

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

During the update the LED flashes rapidly.

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

How to obtain a new software version?

1. Use a PC or laptop that is connected to the Internet.
2. Visit our homepage at 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. Make sure all other users have properly closed down the Bluetooth connections they have set up.

5. Record the values of all parameters.

6. If you are using xDSL:
   - shut down the xDSL connection (set ‚Tunnel Mode' [2.7.1] to *none*),
   - save the values using ‚Save Settings Permanently' [6.2].

7. Perform a reset using 'Reset blue2net' [6.3] or simply cut the power supply for a short time (existing Bluetooth connection will be aborted!).

8. Set up a connection to your blue2net via LAN or Bluetooth and link up with the blue2net configuration page (also see 6.4 "How to Get to the Configuration Page").

   Click on <edit> next to 'Activation Commands' [6], then on <edit> next to 'Store Specific Homepage' [6.4]. The following page will be displayed:

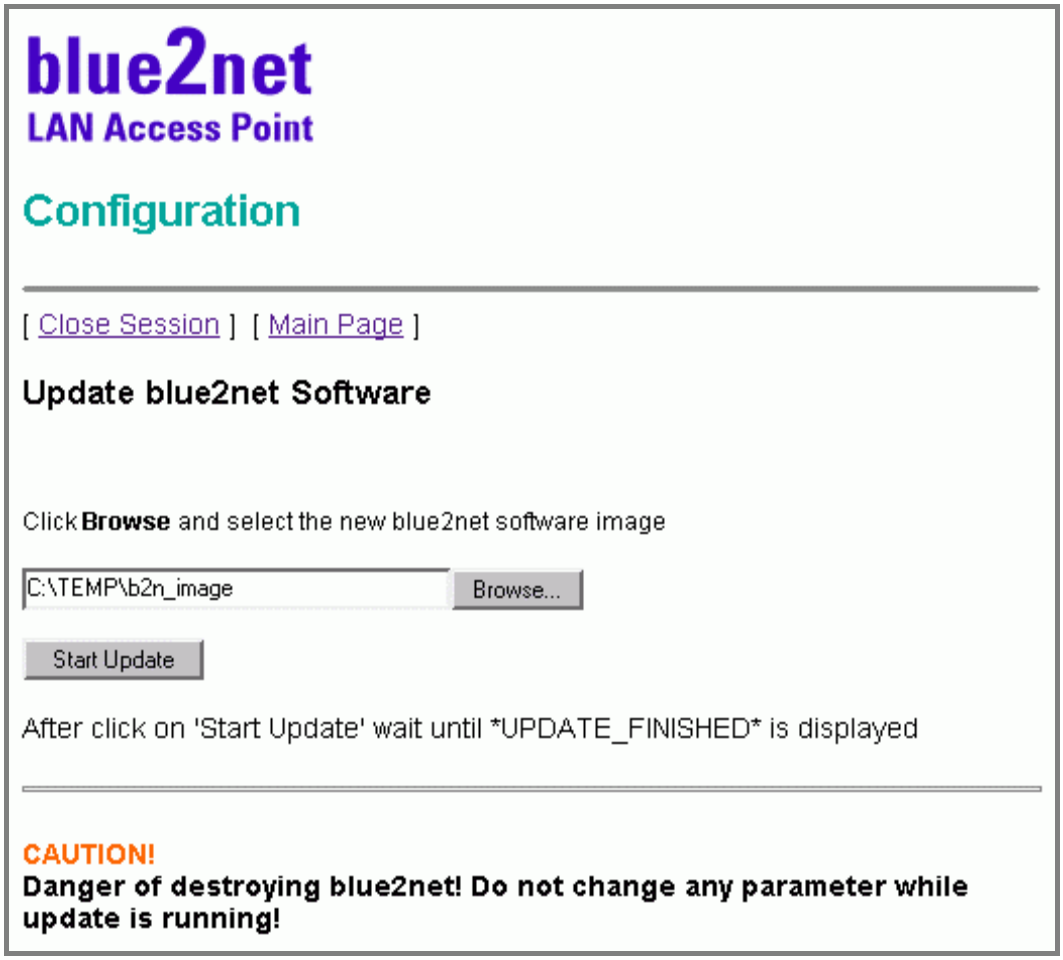


Figure 39 Software update: Selecting the new blue2net software

9. Use <Browse> to select the blue2net software version you previously downloaded from the Internet. Then click on <Start Update> to save the new software and make it take effect after a reboot.

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 (see Figure 40).

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.

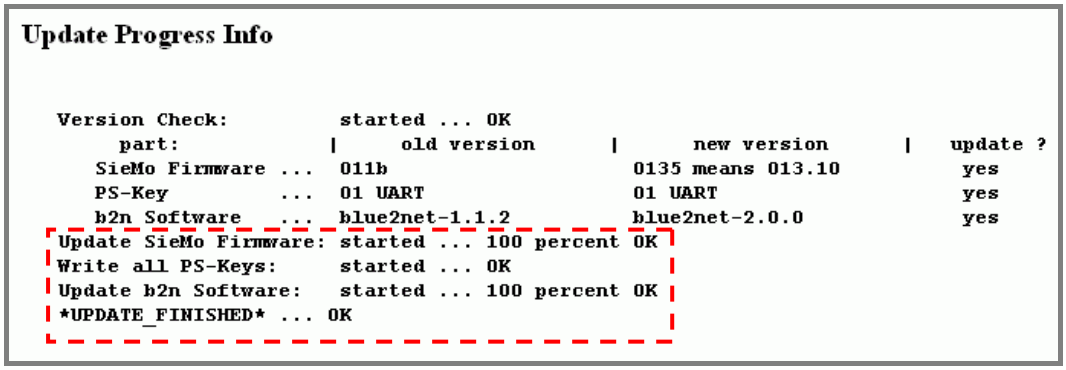


Figure 40 Progress of the software update process (example)

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.

10. Check 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 takes about 2 minutes (normal, slow blinking of the LED). Settings already stored in permanent memory will remain unchanged (also see the information provided in chapters 11.1 and 11.3).

- **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 19), keeping the Web browser status output ready in the case of questions (only if update was initiated via LAN).

11. Reset all values to the factory settings using ‘Restore Default Settings’ [6.5] (see chapter 8.9.5),

12. Reconfigure the values of all blue2net parameters, then destroy records for security reasons.

    The new software is now ready to use.

11.3 Future Software Updates

Future SW versions may come with changes to the parameters, both in terms of the number of parameters and their factory settings.

For future software updates, we therefore recommend the same procedure as the one described here in chapter 11.1 “Information for Upgrades from Previous SW Versions”.

The information provided in the User Guide of the respective follow-up version will serve as change history.

12 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.

12.1 How to Load Your Specific Homepage

Loading your own specific homepage file onto your blue2net is similar to performing a software update (see chapter 11.2).

Loading the file for the specific homepage:

1. Make sure all other users have properly closed down the Bluetooth connections they have set up.

2. Set up a connection via LAN or Bluetooth to your blue2net. and link up with the blue2net configuration page (also see 6.4 „How to Get to the Configuration Page“).

   Click on <edit> next to 'Activation Commands', then on <edit> next to 'Store Specific Homepage'. The following page will be displayed:

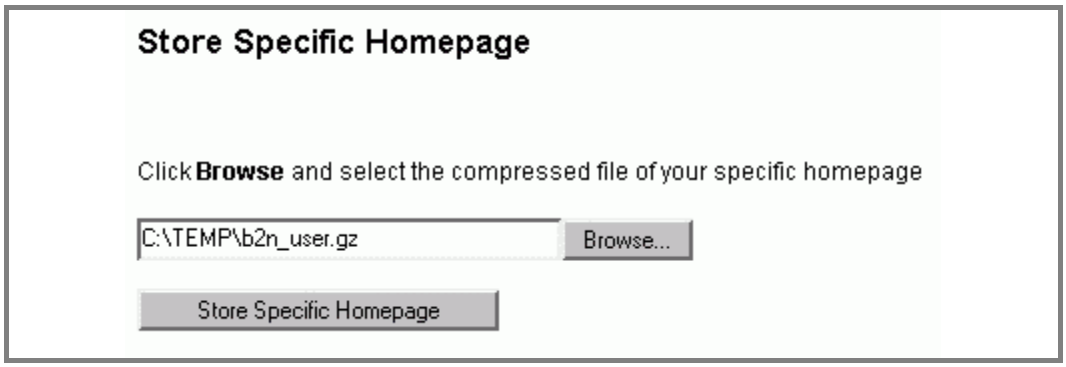


Figure 41 Specific homepage: Selecting the new specific homepage

3. Use <Browse> to select the file created previously with Linux “tar”. Then click on <Store Specific Homepage> to temporarily save the new specific homepage.

ATTENTION! This step does not mean that the homepage is now permanently saved. You can check first whether or not the homepage is being displayed correctly on the screen.

Once you have completed checking, you can permanently save the homepage.

Permanently saving the specific homepage:

4. Make sure all other users exit the Bluetooth connections they have established.
5. Open the blue2net main configuration page (see Figure 8).
6. Click on the <edit> button next to 'Activation Commands' [6]
7. Click on the <edit> button next to 'Save Settings Permanently' [6.2].
8. Save your specific homepage by clicking on the <Submit> button.
9. blue2net will now be rebooted. This might take up to 2 minutes.

Now your specific homepage is ready to use.

13 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 the terminal side.

13.1 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 62 Troubleshooting: Hardware

13.2 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*
	Terminal has never before been registered with ‘Discoverability Mode’ [1.4] set to ‘discoverable’.	Some terminals must have “seen” blue2net at least once and have saved the respective data before you can set up a connection. Ensure that (each) terminal registers at least one while blue2net is discoverable.
You cannot discover 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*

Symptoms	Possible cause	Possible solution
You cannot connect to blue2net with your Bluetooth terminal	Some terminals support neither the LAN access profile nor PAN services, e.g. mobile phones support only Bluetooth Headset.	Future generation mobile phones will support the profiles/services offered in blue2net (LAN Access Profile/PAN Services, Network Access Point, and Group Networking) more and more.
	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].
	All 3 services have been deactivates in the 'Service Table' [1.8].	Access the configuration page via LAN and activate at least one (1) service under 'Activation' [1.8.9] .
	'Minimum Length of Key for Encryption' [1.13]:set too high. It may happen that an older Bluetooth terminal does not support more than 56-bit encryption. To check this, a) take a look into the user guide for the Bluetooth terminal b) try it out provided you have another way of access via Ethernet/ LAN or another Bluetooth terminal if something goes wrong	Reduce [1.13] to 7 or 5 or upgrade the firmware of your Bluetooth terminal to 128-bit encryption capability, if possible, or use a Bluetooth terminal that supports 128-bit encryption.
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 4.2).

Table 63 Troubleshooting: Bluetooth connection

13.3 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 and/or blue2net does not get an IP address assigned from the DHCP server.	Check the IP parameters for blue2net [2]. Ask your system administrator or Internet Service Provider for correct IP parameters for blue2net Enter the fallback blue2net IP parameter [2.3.x] as described in chapter 7.1.2 under "Optional Settings".
You can reach external computers (Internet) via their IP address, but not via their names (e.g. www.siemens.at). (Error Message: "The page cannot be displayed… Cannot find server or DNS Error)	The DNS IP address configuration is wrong (see chapter 8.6.1 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*	Being undiscoverable and protected against access from outside is one of the reasons for using a firewall. However, using "Port Forwarding", you can make individual services discoverable from outside (see chapter 8.5.4). But if 'Terminal Address Resolution' [3.1] is set to *masquerading*, the Bluetooth terminal will still not be reachable from the Internet.

Table 64 Troubleshooting: LAN access

13.4 Software Update

Symptoms	Possible cause	Possible solution
The image file cannot be stored on blue2net.	You have copied the wrong image file (too large) to blue2net.	Restart blue2net (see chapter 8.9.3). It is recommended to copy only blue2net software files (b2n_image) to your blue2net.

Table 65 Troubleshooting: Software update

13.5 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 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**://....
	Older devices featuring browser versions not yet supporting 128-bit encryption cannot access the configuration page.	Verify whether or not the browser installed on the terminal supports 128-bit encryption. To do so, click on “Info” in the browser’s menu bar. For Internet Explorer.00 there is an update available under http://www.microsoft.com/windows/ie/downloads/recommended/128bit/default.asp
You are prompted repeatedly for the configuration password.	Cookies are not enabled on your Web browser.	Enable cookies on you Web browser.

Table 66 Troubleshooting: Configuration access

14 Firewall

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

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

Note: When the firewall is enabled, the pre-programmed security settings may lead to restrictions with certain applications (e.g. games via Internet).

When 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
DHCP (from source port 68 only)	tcp / udp	67
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 (on/off), 68 (off/on)
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 67 Services that can be used while the firewall is enabled

In addition, you will be able to use services you forward using the 'Port Forwarding Rules' [2.6.2] on Ethernet terminals (PCs/laptops in the home LAN. It is your responsibility to prevent misuse on the destination devices.
Transactions for all services listed in table Table 67 can be started only from inside the firewall (from a device connected via Bluetooth or via Ethernet terminals (PCs/Laptops in the home LAN)

Even when the firewall is enabled, you can configure blue2net from the LAN side, because this is done via https and password protection is used. The same holds for software updates and the loading of a specific homepage. This was not possible in previous SW versions. blue2net thus now fully supports remote maintenance.

For information on how to enable/disable the firewall, see chapters 6.4, 8.5, and 8.5.3.

15 Regulatory Statement

15.1 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.

15.2 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 68 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 42 CE Conformity Marking

15.3 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.

16 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.

17 Factory Settings

To restore default settings use the activation command ‘Restore Default Settings’ as described in chapter 8.9.5.

[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 address for BT 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	(1)	LAN ACCESS 1
	(2)	PAN NAP
	(3)	PAN GN
[1.8.3] Service Description	(1)	LAN ACCESS via blue2net
	(2)	PAN NAP via blue2net
	(3)	PAN GN via blue2net
[1.8.4] Auth. Level		authandenc **(changed !)** **
[1.8.5] Service Provider		SIEMENS
[1.8.6] Service URL		http://www.siemens.at/bluetooth
[1.8.7] Service ID		– (read only)
[1.8.8] Bluetooth Service Class		– (read only)
[1.8.9] Activation	(all 3)	activated
[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
[1.10.5] Allow Bluetooth Bonding		disabled *
[1.11] Default Access Mode		enabled
[1.12] Default Bluetooth Passkey		1234
[1.13] Minimum Length of Key for Encryption		7 *
[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

Table 69 Factory settings (default values) (1)

[Hier.level] Parameter & Objects	Factory setting	
[2] **IP Parameters for blue2net**	–	
[2.6] Firewall Settings	–	
[2.6.1] Default Firewall	disabled	
[2.6.2] Port Forwarding Rules	–	*
[2.6.2.1] Index	– (read only)	*
[2.6.2.2] Enable Rule	disabled	*
[2.6.2.3] Protocol	17	*
[2.6.2.4] Lower Port Number	0	*
[2.6.2.5] Enable Port Range	disabled	*
[2.6.2.6] Higher Port Number	65535	*
[2.6.2.7] Fwd. Destination IP Addr.	0.0.0.0	*
[2.6.2.8] Fwd. Source IP Address	0.0.0.0	*
[2.6.2.9] Fwd. Source IP Add. Netm.	0.0.0.0	*
[2.6.3] Number of Port Forwarding Rules	– (read only)	*
[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 Password	pppoepassw	
[2.7.4] PPTP Server IP Address	10.0.0.138	
[2.8] Access Router	–	*
[2.8.1] Additional IP Interface	disabled	*
[2.8.2] Fixed Additional IP Interface	–	*
[2.8.2.1] Fixed b2n Addl. IP Address	192.168.3.2	*
[2.8.2.2] Fixed b2n Addl. IP Netmask	255.255.255.0	*
[3] **IP Parameters for Terminals**	–	
[3.1] Terminal IP Address Resolution	masquerading	
[3.2] Start of Terminal IP Addr. Pool Range	192.168.1.11	***
[3.3] End of Terminal IP Address Pool Range	192.168.1.70	***
[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	
[3.6] Local DHCP Server Objects	–	*
[3.6.1] Local DHCP Server for NAP	enabled	*
[3.6.2] Local DHCP Server for Ethernet	disabled	*
[3.7] IP Connection Mode for NAP Terminals	routing	*
[3.8] Available IP Addresses for Local Wired Network	–	*
[3.8.1] Lowest IP Address of Range	192.168.3.20	*
[3.8.2] Highest IP Address of Range	192.168.3.253	*
[3.9] Fixed IP Addresses for Local Wired Network	–	*
[3.9.1] Index	– (read only)	*
[3.9.2] MAC Address	00:00:00:00:00:00.	*
[3.9.3] IP Address	0.0.0.0	*
[3.10] Number of Fixed IP Addresses	– (read only)	*

Table 70 Factory settings (default values) (2)

[Hier.level] Parameter & Objects		Factory setting
[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)
[4.5.2]	IP Address of Tunnel Endpoint on b2n	– (read-only) *
[5] Configuration Access		–
[5.1]	SNMP Access	disabled
[5.2]	Configuration Password	changeme
[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 71 Factory settings (default values) (3)

Change history:

As compared to the previous SW version v 3.0.0 / user guide v 3.0, the following changes have been made (also refer to chapter 11.3):

*) new parameter

**) factory setting (default value) changed!

***) function changed

[3.2] and [3.3] have been renamed and now provide a different functionality

[3.3.1] and [3.3.2] have been omitted

[5.2.1] is now called [5.2]

18 Abbreviations and Terms

Term	Explanation
ARP	Address Resolution Protocol (used to find the Ethernet address related to an IP address)
Authentication	A security procedure
Authorization	A security procedure where a device is given permission to access a particular service
BT	Bluetooth
CE	Conformity Europe
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	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IMAP	Internet Mail Access Protocol
IMAP SEC	Internet Mail Access Protocol secure
IP	Internet Protocol
ISP	Internet Service Provider
KPOP	Post Office Protocol Kerberos
LAN	Local Area Network
LAP	LAN Access Protocol
LED	Light Emitting Diode
MAC	Medium Access Control
PAN	Personal Area Networking
PAN GN	Personal Area Networking Group Network
PAN NAP	Personal Area Networking Network Access Point
Passkey	Another name for PIN
PCMCIA	Personal Computer Memory Card Int'l Association, synonym for a standard for PC-Cards, such as Bluetooth cards, modem cards and Fax cards
PDA	Personal Digital Assistant
PIN	Personal Identification Number

Table 72 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 73 Abbreviations and terms (2)

19 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 http://www.siemens.at/bluetooth > Products > blue2net ... / Contact

20 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.

21 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 Profile
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	4.4 V, 600 mA, ext. 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	via built-in Web server
blue2net IP address assignment	DHCP or predefined (fixed)
Terminal IP address assignment	masquerading or DHCP (external/internal) or predefined (fixed)
xDSL protocols	PPPoE (RFC 2516) PPtP (RFC 2637)
Access router functionality	second IP interface with internal DHCP server bridging/routing for PAN
Cascadability for blue2net	one master, several slaves (for hot spots)
Port forwarding	all IP protocols, all ports
Security	configuration: Password and HTTPS, Bluetooth passkeys, built-in firewall
Homepage loadable on blue2net	up to 60 Kbytes in zipped form can be stored on blue2net
Software upgrades with https (remote maintenance option)	available at http://www.siemens.at/bluetooth
More information	http://www.siemens.at/bluetooth

Table 74 Technical Data

22 Index

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X

23 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, 18.3.02

Head of Quality Assurance
Herbert Haunschmid
Vienna, 15.3.02

Figure 43 Declaration of Conformity

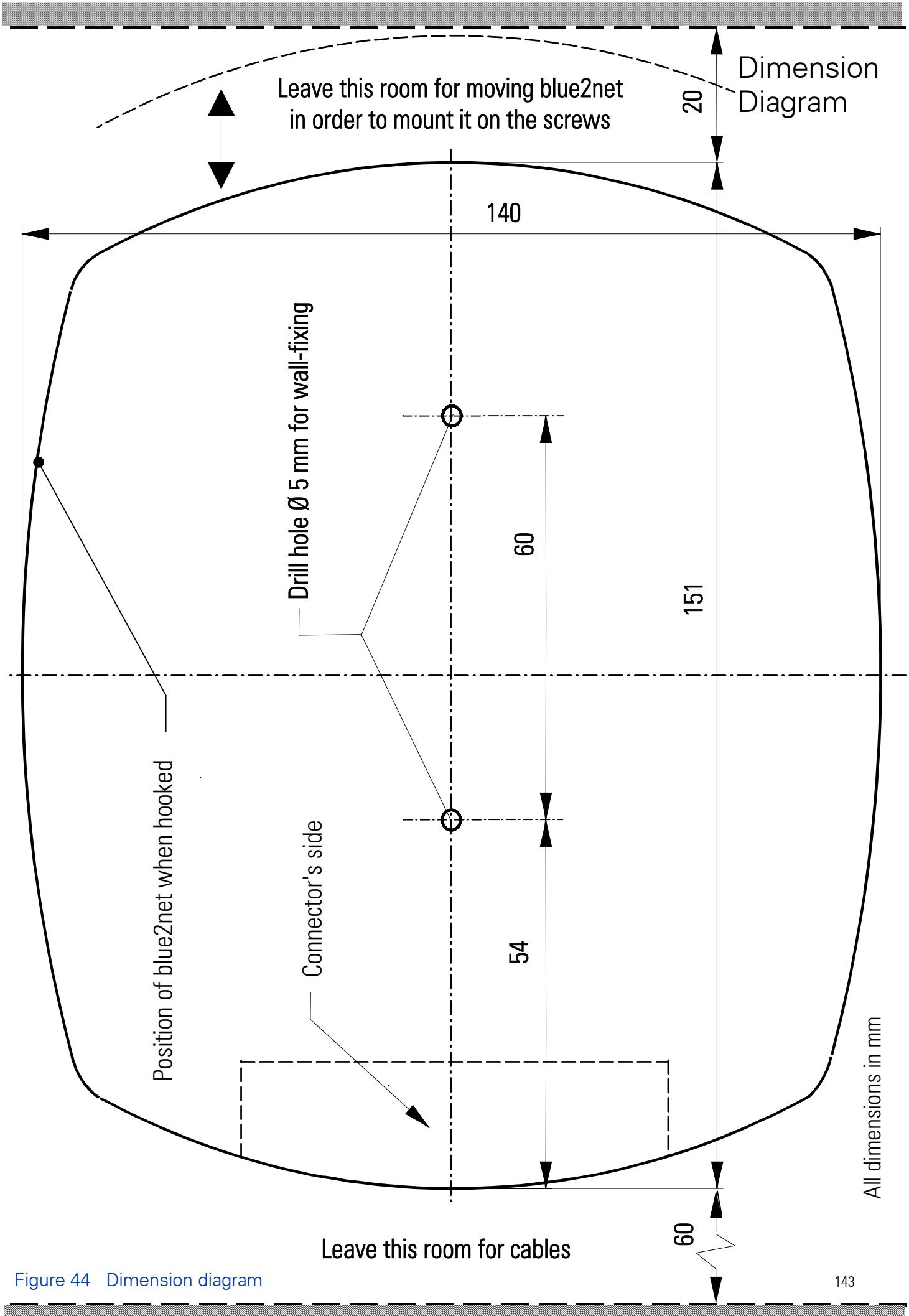


Figure 44 Dimension diagram