SIEMENS

blue2net
LAN Access Point

Bluetooth™

Bedienungsanleitung

Ausgabe August 2002, Version 2.0

Die Informationen in diesem Handbuch sowie die beschriebene Software können ohne vorherige Ankündigung zum Zwecke der technischen Verbesserung geändert werden.

Information über Siemens Bluetooth™ Produkte:

http://www.siemens.at/bluetooth

Ausgabe August 2002, Version 2.0

Sicherheitshinweise

Netzgerät:

Verwenden Sie für blue2net nur das mitgelieferte Netzgerät:

Best.Nr.: N4 EFS3 3W 4.4V (EU-Ausführung)
N4 GFS3 3W 4.4V (UK-Ausführung)
N4 UFS3 3W 4.4V (US-Ausführung)

Vor Inbetriebnahme überprüfen Sie bitte, ob die Netzspannung und die am Netzgerät angegebene Eingangsspannung übereinstimmen.

Eine gewisse Gehäuseerwärmung ist normal und unbedenklich.

Darf nur für informationstechnische Geräte eingesetzt werden.

Vor Spritzwasser schützen.

Nur in geschlossenen Räumen betreiben.

Das Netzgerät sollte im Betrieb nicht bedeckt und nicht in der Nähe von Heizkörpern oder unter direkter Sonnenbestrahlung betrieben werden.

Nur mit einem trockenen Tuch reinigen. Keine Lösungsmittel verwenden.

blue2net:

Andere elektrische Einrichtungen (z.B. medizinische Geräte) können bei Gebrauch des Gerätes beeinträchtigt werden. Stellen Sie deshalb das Gerät nur an Orten auf, wo es keine Störungen bei derartigen Einrichtungen bewirkt.

Stellen Sie das Gerät nicht in Dusch- oder Waschräumen auf.

Betreiben Sie das Gerät nicht in Umgebungen mit Explosionsgefahr (z.B. Lackiererei, Tankstelle, Kraftstoffdepot etc.).

Das Gerät oder das Netzgerät dürfen in keinem Fall vom Benutzer geöffnet werden. Durch Änderungen am Gerät werden Garantie- und Gewährleistungsansprüche sowie die Benützungsbewilligung ungültig.

Sorgen Sie dafür, dass die Bedienungsanleitung dem Gerät beiliegt, wenn es an Dritte weitergegeben wird.

Das Gerät muss am Ende seines Lebenszyklus umweltfreundlich entsorgt werden. Da Umweltschutzbestimmungen und Entsorgungseinrichtungen von Land zu Land verschieden sind, kontaktieren Sie bitte zur Beratung örtliche Behörden, den Umweltschutzbeauftragten Ihrer Firma oder Ihren Händler.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

Was ist blue2net?

blue2net bietet dem Benutzer die Möglichkeit, über eine Bluetooth-Funkverbindung Zugriff auf alle Dienste und Ressourcen eines LAN (Local Area Network) zu erhalten.

Es können bis zu 7 Terminals gleichzeitig über Bluetooth an blue2net angebunden werden. Gemäß Bluetooth-Spezifikation 1.1 verwendet blue2net das „LAN Access Profile“, das bedeutet eine vollständige IP-Anbindung über PPP (Point to Point Protocol).

Vielfältige Sicherheitsoptionen sowie eine integrierte Firewall regeln die Zugriffsberechtigung bzw. verhindern einen unerlaubten Verbindungsaufbau.

Der LAN Access Point wird einfach an eine Ethernet-Schnittstelle angeschlossen und ist in einem Umkreis von ca. 10 - 30 Metern einsatzbereit.

Auf Benutzerseite benötigt man lediglich einen PC, Laptop oder PDA mit entsprechendem Bluetooth-Modul. Solche Adapter können per USB oder PCMCIA angesteckt werden. Bei vielen Notebooks ist Bluetooth bereits eingebaut.

Der auf Embedded Linux basierende Siemens LAN Access Point arbeitet mit allen gängigen Bluetooth-Adaptern zusammen. Die Konfiguration erfolgt über ein Web-Interface mit üblichen Internet-Browsern. Bei einer größeren Anzahl von Access Points bietet sich für Administratoren die Möglichkeit, die Konfiguration über SNMP vorzunehmen.

Einsatzgebiete:

Teilnehmer einer Besprechung können ohne lästige Kabel im Firmen-Netzwerk arbeiten. In einem Bürogebäude können Außendienstmitarbeiter bequem und schnell ihre Daten mit dem Server aktualisieren und synchronisieren.

Öffentliche Plätze wie Flughäfen, Bahnhöfe, Hotels, Restaurants, Einkaufszentren, Internet-Cafes können Reisenden oder ihren Kunden verschiedenste Informationen und Dienste zur Verfügung stellen. Diese Informationen sind dann auch gratis abrufbar, da für die Bluetooth-Funkverbindung keine Lizenzgebühren anfallen.

Heimanwender können drahtlos vom Sofa aus im Internet surfen und ihre E-Mails abrufen – der Access Point stellt die Verbindung über ein Kabel-Modem (z.B. Chello) oder xDSL-Modem her.

2 Erste Installation von blue2net

2.1 Überprüfung des Packungsinhalts

1 blue2net-Gerät

1 Netzgerät in EU-Ausführung: N4 EFS3 3W 4.4V oder
UK-Ausführung: N4 GFS3 3W 4.4V oder
US-Ausführung: N4 UFS3 3W 4.4V

1 blue2net-Bedienungsanleitung als CD-ROM oder Handbuch

4 selbstklebende Gummifüße

2 Schrauben samt Dübel

2.2 Installationshinweise

- Beachten Sie bitte die Sicherheitshinweise.
- Nur in Innenräumen innerhalb eines Temperaturbereiches von 0 bis +40 °C verwenden.
- Eine 220/230V~ (110/120V~)-Steckdose und ein Ethernetanschluss sollten nahe dem Aufstellungsort von blue2net vorhanden und leicht zugänglich sein.
- Verwenden Sie nur das mitgelieferte Original-Netzgerät.
- Für die Erstinstallation, bei der zum ersten Mal eine Verbindung zum LAN hergestellt wird und grundlegende Konfigurations-Einstellungen vorgenommen werden, kann das Gerät z.B. auf den Tisch neben den Laptop gestellt werden. Eine fixe Platzierung, wie im nächsten Punkt beschrieben, sollte erst vorgenommen werden, wenn die Erstinstallation abgeschlossen ist.
- Die eingebaute Antenne von blue2net hat eine Richtcharakteristik (siehe Abb. 1). Mit zunehmender Entfernung zwischen blue2net und den Bluetooth-Geräten wird es immer wichtiger, diese zu berücksichtigen, um beste Reichweiten und Datenübertragungsraten zu erzielen. Wir empfehlen, die optimale Position von blue2net durch Ausprobieren herauszufinden, bevor Sie Löcher für die Befestigungsschrauben bohren.

Abhängigkeit der Übertragungs-ergebnisse von der Richtwirkung:

B .. Beste Ergebnisse
W . Weniger gute Erg.
S... Schlechteste Ergebnisse

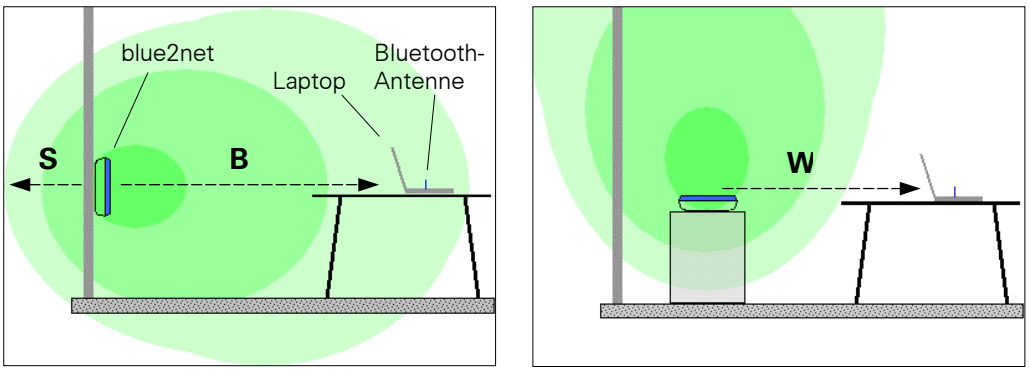

Abb. 1 Richtcharakteristik von blue2net und Erzielung guter Reichweiten

- Andererseits kann diese Richtcharakteristik dazu genützt werden, das Gerät so aufzustellen, dass z.B. in Nachbarbereiche möglichst gering abgestrahlt wird (Datenschutz, Störungen).
- Der Aufstellungsort sollte sich nicht in unmittelbarer Nähe von Geräten befinden, die im gleichen Frequenzbereich arbeiten (z.B. Mikrowellenherde).
- Das Gerät kann an einer Wand oder Decke installiert werden oder auf einer ebenen, nicht rutschigen Fläche aufgestellt werden. Von der Aufstellung am Boden wird wegen der Beschädigungs- und Stolpergefahr abgeraten.
- Installieren Sie das Gerät an einem zentralen Ort, z.B. in einem Gang. Versuchen sie eine Platzierung zu vermeiden, bei der die Funksignale von Hindernissen (z.B. dicke Mauern) abgeschattet werden.
- Lassen Sie bei der Befestigung des Gerätes auf der Anschlussseite min. 60 mm Abstand für die Wegführung der Kabel und auf der gegenüberliegenden Seite ca. 20 mm Abstand für die notwendige Bewegung zum Einrasten in den Schrauben. Auf der vorletzten Seite der Bedienungsanleitung finden Sie ein Maßbild zum Bohren der Befestigungslöcher.
- Die Gerätefüße hinterlassen normalerweise keine Abdrücke auf den Aufstellflächen. Wegen der Vielfalt der verwendeten Lacke und Polituren können Abdrücke jedoch nicht vollkommen ausgeschlossen werden.

2.3 Anschluss von blue2net am Ethernet

Für blue2net sind grundsäzlich zwei Betriebsarten vorgesehen:

- Betrieb am LAN (z.B. Firmennetzwerk, Kabelmodem eines Internet-Service-Providers)
- Betrieb an einem xDSL-Modem

blue2net ist im Auslieferungszustand für den Betrieb am LAN konfiguriert.

2.3.1 Betrieb am LAN

Grundsätzlich braucht man zum Betrieb eines Gerätes wie blue2net am LAN eine *IP-Adresse*.

DHCP (Dynamic Host Configuration Protocol) ist der am meisten verwendete Mechanismus in Firmennetzwerken und bei Kabel-Modem-(Internet-)Providern, um Clients wie blue2net IP-Adressen zuzuweisen. Wenden Sie sich bitte an Ihren Netzwerk-Administrator oder ISP (Internet Service Provider) und fragen Sie dort, ob bei Ihrem LAN DHCP zur Verfügung steht. Bei IP-Zuweisung über DHCP könnten Sie von Ihrem Netzwerk-Administrator oder ISP nach der *MAC-Adresse* fragt werden. Diese ist am Typenschild an der Unterseite Ihres Gerätes aufgedruckt (siehe Abb. 2, 'MAC-Adr.').

Falls der DHCP-Dienst *nicht* verfügbar ist, verwendet blue2net seine eigene Rückfall-IP-Adresse. Mit dieser IP-Adresse ist aber keine Verbindung zum LAN möglich. Sie müssen sich von Ihrem Netzwerk-Administrator oder ISP fixe IP-Adressen für Ihr Gerät zuweisen lassen und diese anschließend manuell konfigurieren.

Vorgehensweise:

1. Schließen Sie **zuerst das Ethernet-Kabel** an den Ethernet-Kabelanschluss (Stecker RJ45) an (Das Kabel ist nicht Teil des Lieferumfangs) und dann das Netzgerät an den Stromversorgungsanschluss (Stecker RJ11) (siehe Abb. 2).

2. Prüfen Sie nach ca. 40 Sekunden, ob die Anzeige-LED (siehe Abb. 2) dauerhaft leuchtet. Wenn ja, können Sie sicher sein, dass blue2net seine IP-Adressen über DHCP zugewiesen bekommen hat.

   blue2net ist jetzt zur Benützung bereit, ***aber nicht abgesichert***.

   Sie müssen anschließend die für Ihren Anwendungsfall geeigneten Einstellungen, insbesondere ***Sicherheitseinstellungen***, vornehmen. Lesen Sie dazu zunächst weiter im Kapitel 2.8.

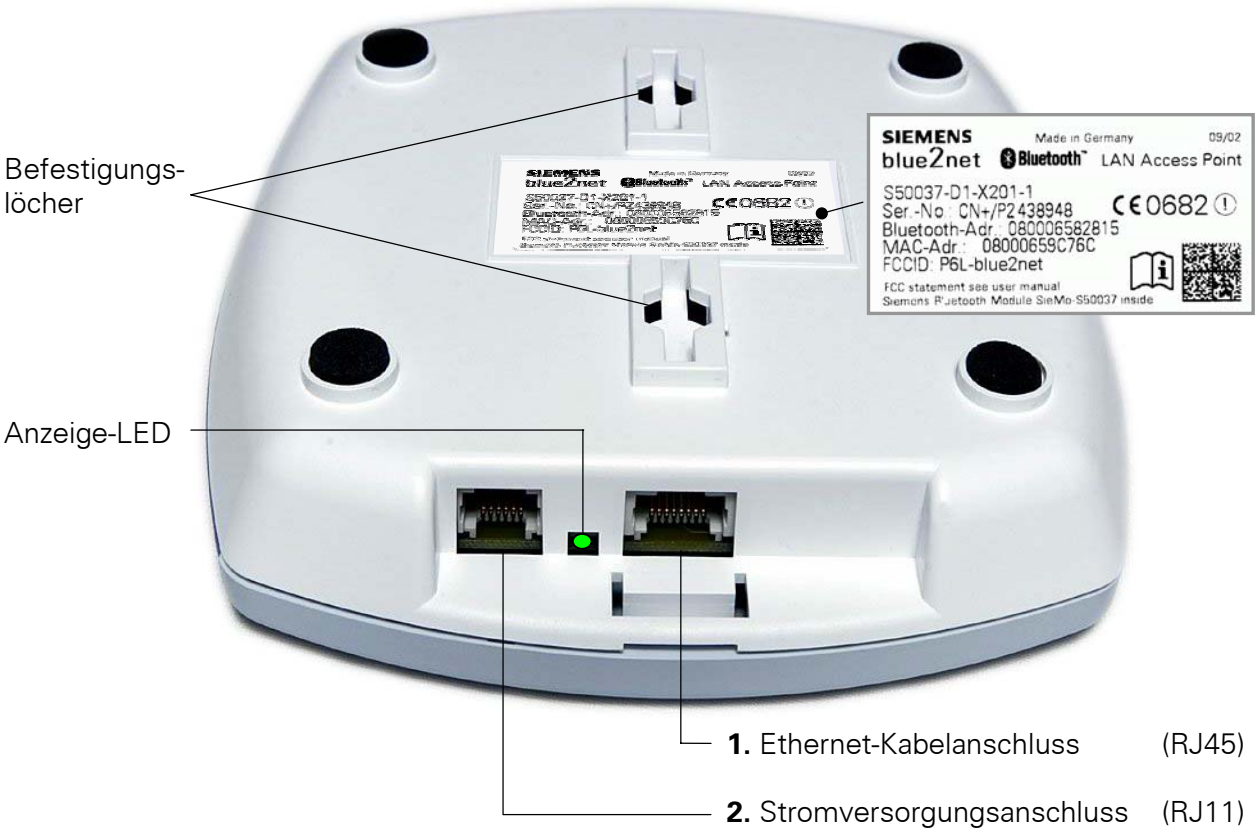

Abb. 2 Unterseite des Gerätes: Anschlüsse, Befestigungslöcher, LED und Typenschild

3. Wenn die LED erst nach ungefähr 2 Minuten dauerhaft leuchtet, ist kein DHCP-Dienst verfügbar, und blue2net wird seine eigene Rückfall-IP-Adresse (192.168.1.2) verwenden, um starten zu können. Mit dieser IP-Adresse kann blue2net aber keine Verbindung zum LAN herstellen. Sie haben jetzt 2 Möglichkeiten:

   - Fragen Sie beim Netzwerk-Administrator oder ISP (Internet Service Provider) nach, warum kein DHCP-Dienst verfügbar war.
   - Wenn der DHCP-Dienst nicht verfügbar ist, müssen Sie blue2net manuell konfigurieren.

Ziehen Sie in diesem Fall einen Experten für Netzwerktechnik zu Rate (z.B. den Netzwerk-Administrator Ihrer Firma oder des ISP), um eine Verbindung zum LAN zu bekommen.

Nachdem die manuelle Konfiguration erfolgreich durchgeführt und eine Netzverbindung aufgebaut wurde, ist blue2net betriebsbereit. Es müssen dann aber noch die ***Sicherheitseinstellungen*** vorgenommen werden. Um die für Ihre Anforderungen geeigneten Einstellungen, besonders hinsichtlich Sicherheit, auszuwählen, fahren Sie bitte mit Kapitel 2.8 ff fort.

2.3.2 Betrieb an einem xDSL-Modem

blue2net ist im Auslieferungszustand für den Betrieb am LAN bzw. Kabel-Modem konfiguriert.

Für den Betrieb an einem xDSL-Modem sind Einstellungen an bestimmten Parametern zwingend erforderlich (Sie finden eine Aufzählung dieser Parameter (fett gedruckt) in Kapitel 4.4. Eine detaillierte Beschreibung aller Parameter für die dazu vorgesehene Tunnel-Konfiguration finden Sie in Kapitel 3.5.4).

Darüber hinaus dürfen Sie die Kabelverbindung zum xDSL-Modem erst herstellen, nachdem blue2net passend zu Ihrem xDSL-Zugang konfiguriert ist.

In der Regel wird die Konfiguration vom Heimanwender am Bluetooth-Terminal (z.B. Laptop) über eine Bluetooth-Verbindung durchgeführt werden. Die Konfiguration ist auch über Ethernet möglich, dazu wird aber erweitertes Netzwerk-Know-How vorausgesetzt.

Vorgehensweise:

1. Netzgerät an den Stromversorgungsanschluss anschließen (Stecker RJ11) (siehe Abb. 2).

   Hinweis: Sie können erst 2 min. nach Anschluss der Stromversorgung, wenn blue2net die Startphase durchlaufen hat, mit dem nächsten Schritt fortfahren.

2. Konfiguration für xDSL durchführen und Werte anschließend permanent speichern:
   - Eine Aufzählung der Parameter finden Sie im Kapitel 4.4 (fett gedruckt)
   - Den Aufbau einer Bluetooth-Verbindung und den Zugang zur Konfiguration lesen Sie in den Kapiteln 2.5, bis 2.6.2 und 3 .
   - Anweisungen zum permanenten Abspeichern finden Sie in Kapitel 3.9.2

   Hinweis: nach der Konfiguration findet ein Reset mit anschließendem Neustart statt. Alle Bluetooth-Verbindungen werden abgebrochen!

3. Stellen Sie erst nach der Konfiguration die Kabelverbindung (Kabel ist nicht Teil des Lieferumfangs) zum xDSL-Modem her (Stecker RJ45) (siehe Abb. 2).

blue2net ist danach zur Benützung bereit, ***aber nicht abgesichert***.

Es müssen daher noch die ***Sicherheitseinstellungen*** vorgenommen werden. Um die für Ihre Anforderungen geeigneten Einstellungen, besonders hinsichtlich Sicherheit, auszuwählen, fahren Sie bitte mit Kapitel 2.8 ff fort.

2.4 Bedeutung des Verhaltens der LED-Anzeige

Verhalten	**Bedeutung**
Kein Licht	Keine Stromversorgung
Dauerlicht	Betriebsbereit, IP-Adresse zugewiesen
Normales Blinken	blue2net-Startphase
Langsames Blinken	Verbindungsaufbau zum Netz
Schnelles Blinken	Software-Update

2.5 Verbinden zu blue2net über Bluetooth

Stellen Sie sicher, dass Ihre verwendeten Bluetooth-Geräte/Terminals (z.B. Laptop oder PDA) das „LAN Access Profile“ unterstützen.

Folgen Sie den Anweisungen in der **Bedienungsanleitung** Ihres **Bluetooth-Terminals**.

Grundsätzlich werden Sie folgendes tun müssen:

- Starten Sie Bluetooth auf Ihrem Bluetooth-Terminal.
- Suchen Sie mit Ihrem Bluetooth-Terminal nach erreichbaren Bluetooth-Geräten (Bluetooth device inquiry).
- Wählen Sie Ihr blue2net in der angezeigten Geräteliste und verbinden Sie sich damit.
  Um Ihr blue2net unter den anderen angezeigten Geräten zu identifizieren, brauchen Sie seine Bluetooth-Adresse, welche auf dem Typenschild auf der Unterseite des blue2net-Gehäuses zu finden ist (siehe Abb. 2).
- Wenn ein Login-Fenster auf Ihrem Terminal erscheint, müssen Sie das Bluetooth-Passwort ('Bluetooth-Passkey') eingeben. Das voreingestellte Passwort lautet '**1234**'.
- Stellen Sie sicher, dass Ihr Terminal eine PPP-Verbindung aufbaut wie z.B. Windows DFÜ.

2.6 Zugriff auf den eingebauten blue2net-Web-Server

Der in blue2net eingebaute Web-Server stellt für die Konfiguration der Parameter, für die Überprüfung der Einstellungen und für die Ausführung eines Software-Updates ein Web-Interface bereit. Es gibt zwei Möglichkeiten, auf den Web-Server zuzugreifen: über Bluetooth oder über Ethernet (LAN).

2.6.1 Erforderliche Browser-Einstellung

- **Deaktivieren** Sie die **Proxy-Einstellungen** im Web-Browser Ihres PDA oder Laptop.
- **Aktivieren** Sie die **Cookies!**

2.6.2 Zugang über Bluetooth

- Für den Zugriff brauchen Sie eine bestehende Bluetooth-Verbindung zu blue2net wie in Kapitel 2.5 beschrieben.
- Geben Sie in der Adressleiste des Browsers http**s**://192.168.2.2 ein, um auf das Web-Interface von blue2net zuzugreifen (beachten Sie bitte, dass blue2net nur den sicheren Zugang über http**s** unterstützt). Bei dieser IP-Adresse handelt es sich um die voreingestellte IP-Adresse für Terminals, die über Bluetooth verbunden sind. Abb. 3 zeigt die Homepage des blue2net-Web-Interface.

2.6.3 Zugang über Ethernet (LAN)

Der Zugang zur Konfigurationsfunktion über Ethernet (LAN) wird nur Fachleuten empfohlen. Gehen Sie im Wesentlichen nach den folgenden Anweisungen vor:

- Wenn die IP-Adresse über DHCP zugewiesen wurde, müssen Sie zunächst ihren aktuellen Wert herausfinden. Es gibt dafür drei Wege:
  a) Am Bluetooth-Terminal: Im Auslieferungsszustand ist blue2net so konfiguriert, dass die aktuelle IP-Adresse nach dem Bluetooth-Geräte-Namen (Bluetooth Device Name) Ihres blue2net angezeigt wird. Sie können somit die IP- Adresse nach einer Bluetooth-Geräte-Abfrage (Bluetooth device inquiry) am Bluetooth-Terminal direkt ablesen.
  b) Fragen Sie Ihren Netzwerk-Administrator oder Internet Service Provider.
  c) Greifen Sie auf blue2net über Bluetooth zu (siehe Kapitel 2.6.2) und lesen Sie den Wert des Parameters ‘blue2net IP Address’ ab (siehe Kapitel 3.7.1).
- Wenn die IP-Adresse nicht über DHCP zugewiesen wurde, verwendet blue2net die Rückfall-IP-Adresse ('Fallback IP Address' 192.168.1.2). Vergewissern Sie sich, dass die IP-Adresse am Client (Bluetooth-Terminal) und die von blue2net im gleichen Subnetz liegen.
- Greifen Sie auf das Web-Interface durch Eingabe von **https://<IP-Adresse von blue2net>** in die Adressleiste Ihres Web-Browsers zu (siehe Abb. 3).

2.7 Wie Sie zur Konfigurations-Seite gelangen

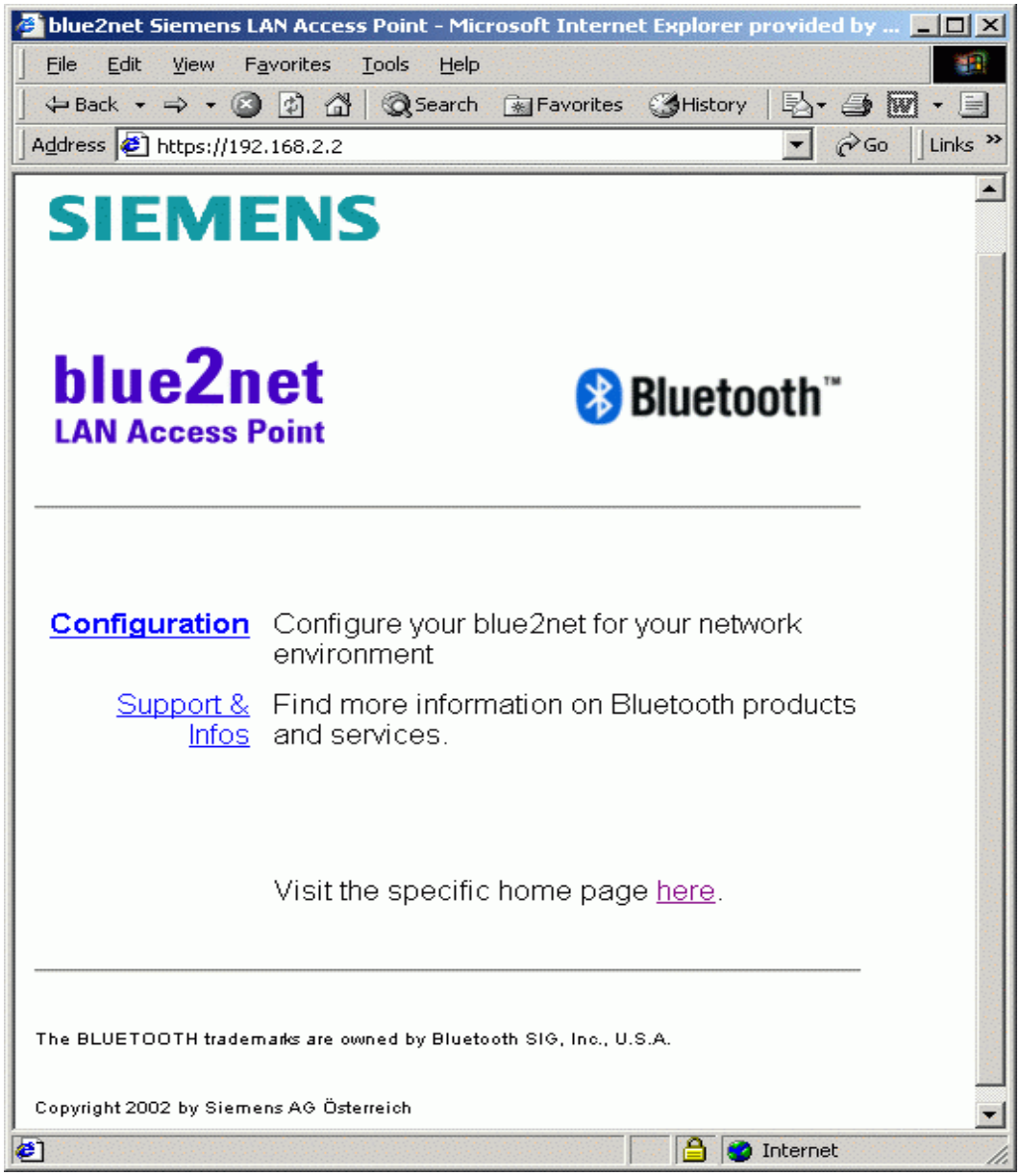

Abb. 3 blue2net-Web-Interface (Homepage)

- Klicken Sie auf **Configuration** auf der ersten Seite des Web-Interface von blue2net (siehe Abb. 3).
- Das voreingestellte Passwort für den Konfigurationszugang lautet „**changeme**“. Es wird empfohlen, das Passwort nach der ersten Verwendung sofort zu ändern (siehe Kapitel 3.8). Bewahren Sie das Passwort getrennt vom Gerät, der Betriebsanleitung, dem Laptop, PDA oder PC an einem sicheren Ort auf.

Vorsicht! Wenn Sie das Konfigurations-Passwort vergessen, haben Sie keinen Zugang mehr zu den Einstellungen von blue2net. Sie sind dann von der Konfigurationsseite ausgesperrt. Informieren Sie sich genau zu diesem wesentlichen Punkt in Kapitel 5, „Aussperrung verhindern“.

2.8 Auswahl von Sicherheitseinstellungen

Nachdem blue2net seine Startphase abgeschlossen hat, ist es grundsätzlich bereit zur Benützung. Der Zugriff ist aber noch *nicht abgesichert*. Mit den Vorgabewerten der Werkseinstellung ist es möglich, von jedem in Funkreichweite befindlichen Bluetooth-Terminal auf die Konfiguration von blue2net und das LAN oder von einem PC über das LAN auf die Konfiguration zuzugreifen.

Um einen entsprechend abgesicherten Zugriff zu erreichen, können Sie eine der folgenden Vorgangsweisen wählen:

- Kapitel 1 zeigt Einstellungen für 4 typische Anwendungsfälle.
- Kapitel 3 zeigt detailliert die Konfigurationseinstellungen, um blue2net nach Ihren persönlichen Anforderungen einrichten zu können.

2.9 Wichtige Werkseinstellungen

Ihr blue2net wird mit den folgenden Werkseinstellungen (Default-Werte) für Bluetooth- und IP-Parameter geliefert:

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

Tabelle 1 Wichtige Werkseinstellungen

1) Siehe Kapitel 3.3
2) Default-IP-Adresse für den Zugriff auf den Web-Server über Bluetooth
3) Dieser Wert muss für einige Bluetooth-Terminals manuell eingestellt werden (sehen Sie in der Betriebsanleitung Ihres Bluetooth-Terminals nach)

Eine komplette Aufstellung der voreingestellten Werte aller Parameter finden Sie in Kapitel 12

3 Konfiguration

3.1 Haupt-Konfigurations-Seite

Klicken Sie auf **Configuration** im Web-Interface (Abb. 3), um zu der folgenden Übersicht (Abb. 4) zu gelangen. Die Nummern in den eckigen Klammern zeigen den Platz eines Parameters in der Hierarchie des Web-Interface an (Details dazu in Kapitel 3.3).

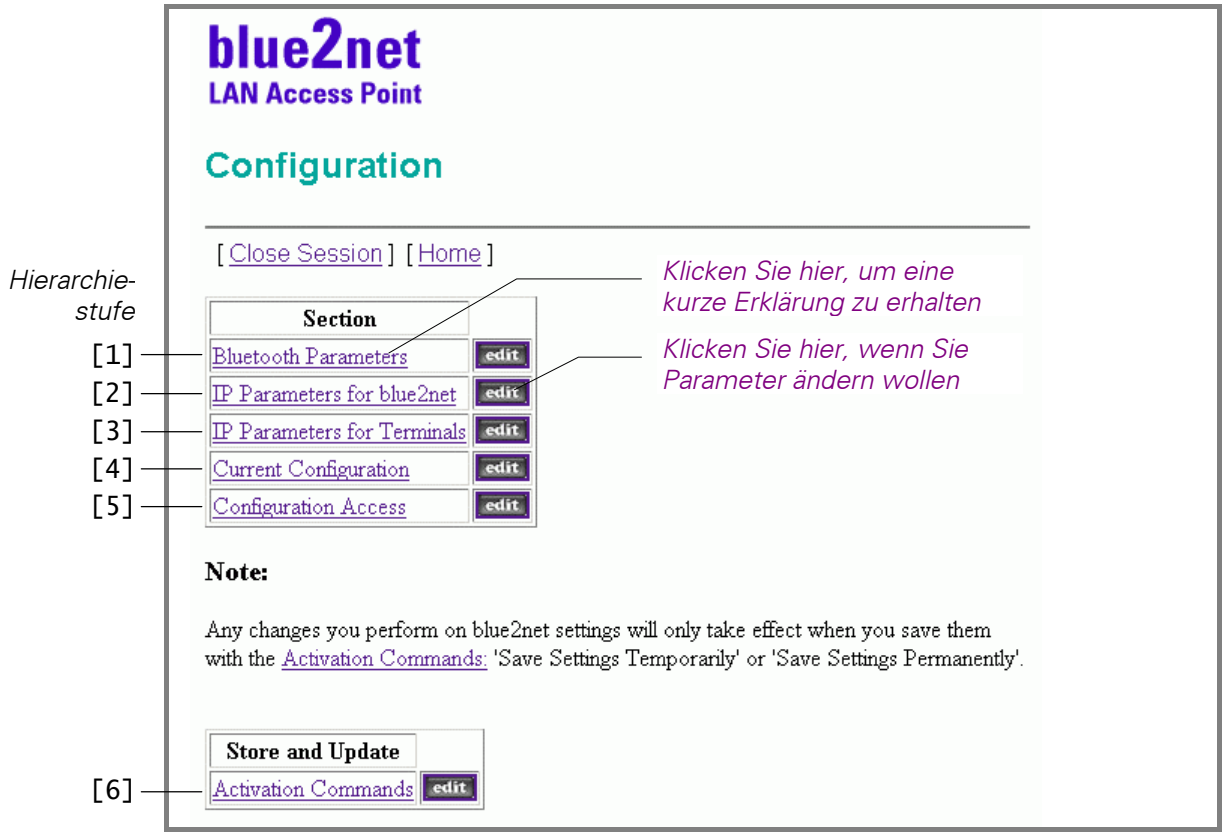

Abb. 4 Haupt-Konfigurations-Seite [0]

Klicken Sie auf eine der <edit>-Schaltflächen und geben Sie das Konfigurations-Passwort ein (Abb. 5). Das voreingestellte Passwort lautet „**changeme**".

Abb. 5 Authentifizierung (Authentication)

Klicken Sie auf <Submit>, dann wird die Haupt-Konfigurations-Seite angezeigt.

Aus Sicherheitsgründen sollten Sie das Passwort sofort ändern. Vergessen sie bitte nicht, dass Sie die Änderung anschließend abspeichern müssen. Verwenden Sie dazu die '*Activation Commands*' (siehe Kapitel 3.9)!

Hinweis: Merken Sie sich bitte das neue Passwort oder bewahren Sie es an einem sicheren Ort auf. Wenn es einmal geändert ist, ist der Zugang zur Konfiguration nur mehr mit dem *neuen* Passwort möglich! Siehe dazu Kapitel 5.

Objekte (siehe Abb. 4)	**Hierarchie stufe**	**Erklärung**
Bluetooth Parameters	[1]	Hier können Sie alle Parameter ändern, die für die Bluetooth-Verbindung maßgeblich sind, z.B. Bluetooth-Gerätename (Bluetooth device name), Mehrfachzugang (multipoint mode), Sichtbarkeit/Auffindbarkeit (discoverability), Verbindungsbereitschaft (connectability), vorgegebene Zugriffsart (default access mode) und vorgegebenes Bluetooth-Passwort (default Bluetooth passkey).
IP Parameters for blue2net	[2]	Hier können Sie Einstellungen zu IP-Parametern für blue2net vornehmen, z.B. ob IP-Adressen über DHCP zugewiesen werden sollen oder ob fix zugewiesene IP-Adressen verwendet werden. Ferner kann hier eine Firewall aktiviert oder deaktiviert werden.
IP Parameters for Terminals	[3]	Hier können Sie Einstellungen zu IP-Parametern für die anzuschließenden Terminals vornehmen, z.B. den Mechanismus der Zuteilung von IP-Adressen zu den Terminals (Terminal IP address resolution) und den Vorrat an IP-Adressen, die Terminals zugeordnet werden können (Terminal IP address pool).
Current Configuration (Aktuelle Einstellungen)	[4]	Hier können Sie sich über die aktuellen Einstellungen der IP-Adressen von blue2net und der Bluetooth-Terminals sowie über die im Gerätes eingesetzten SW- und HW-Versionen informieren.
Configuration Access (Zugang zur Konfiguration)	[5]	Hier können Sie das Konfigurations-Passwort ändern und SNMP aktivieren oder deaktivieren.
Activation Commands (Aktivierungs-befehle)	[6]	Hier können Sie Konfigurationsänderungen entweder vorläufig (temporarily) oder dauerhaft (permanently) speichern. Hier können Sie auch eine ggf. verfügbare neue Software oder eine geräteeigene Homepage aktivieren. Weitere Befehle bewirken die Rücksetzung der Parameter auf die Werkseinstellungen oder Werte im Permanent-Speicher.

Tabelle 2 Parametergruppen auf der Haupt-Konfigurations-Seite [0]

3.2 Ändern von Parametern

Klicken Sie auf die Schaltfläche <edit> bei dem Parameter, den Sie ändern wollen. Im folgenden Eingabefenster wird der Wert eingegeben oder eingestellt.

Wenn Sie bereits eingegebene Änderungen wieder auf den zuvor angezeigten Wert zurücksetzen wollen, klicken Sie auf <Undo>.

Durch Klicken auf <Zurück>/<Back> beim Web-Browser gelangen Sie zur vorhergehenden Seite, ohne dass Änderungen wirksam werden.

Wenn Sie überzeugt sind, dass Ihre Eingabe richtig ist, klicken Sie auf <Submit>. Darauf folgt eine Bestätigung der Änderung oder ggf. eine Fehlermeldung.

Jegliche Änderungen, die Sie an blue2net-Einstellungen vornehmen, werden erst wirksam, nachdem Sie diese mit einem der Speicherbefehle der *Aktivierungs-befehle* abgespeichert haben (siehe Kapitel 3.9)!

Bluetooth-Verbindungen (auch die anderer Terminals) werden abgebrochen, wenn Sie mit einem der Aktivierungsbefehle abspeichern (siehe Kapitel 3.9)!

Es wird empfohlen, den Browser nach dem Vornehmen von Konfigurationen mit [Close Session] zu schließen, da man ansonsten aus Sicherheitsgründen bis zu 10 Minuten warten muss, um erneut ins Konfigurationsmenü einsteigen zu können.

3.3 Hierarchie der Parameter für die Konfiguration

Die folgende Tabelle soll es Ihnen erleichtern, die Parameter auf den Seiten des Web-Interfaces zu lokalisieren. Ferner ist die Identifikation der Parameter bei Querverweisen dadurch leichter möglich. Jeder Parameter und jede Parametergruppe hat eine Nummer, die den Platz in der Hierarchie darstellt. Diese Nummer zwischen eckigen Klammern - [x.y] - wird immer wieder in Abbildungen, Tabellen und Querverweisen angeführt, z.B. [1.8.4] für ‚Auth. Level'.

Auf der rechten Seite der Tabelle können Sie folgendes sehen:

- eine Aktion, die man an dem Parameter durchführen kann (edit, Submit), oder
- einen Wert, der angezeigt wird (Nummer, Adresse, Domäne, Version), oder
- eine Tabelle, die gezeigt wird, oder
- Objekte, die gezeigt werden.

[0] **Haupt-Konfigurations-Seite** (Kapitel 3.1)	Aktion / Anzeige	Seite
[1] **Bluetooth Parameters** (Kapitel 3.4)		**16**
[1.1] Bluetooth Device Name	➡ Objects	17
[1.1.1] Bluetooth Device Name	edit, ▸ Submit	20
[1.1.2] IP Address Suffix Mode	edit, ▸ Submit	20
[1.2] Bluetooth Device Address	eindeutige, fixe Adresse	17
[1.3] Multipoint Mode	edit, ▸ Submit,	17
[1.4] Discoverability Mode	edit, ▸ Submit	17
[1.5] Connectability Mode	edit, ▸ Submit	17
[1.6] Max. No. of Terminals Connected	edit, ▸ Submit	18
[1.7] Number of Services	Nummer	18
[1.8] Service Table	➡ Table (1 Reihe)	18 & 20
[1.8.1] Service Index	Nummer	21
[1.8.2] Service Name	edit, ▸ Submit	21
[1.8.3] Service Description	edit, ▸ Submit	21
[1.8.4] Auth. Level	edit, ▸ Submit	22
[1.8.5] Service Provider	edit, ▸ Submit	22
[1.8.6] Service URL	edit, ▸ Submit	22
[1.8.7] Service ID	edit, ▸ Submit	20
[1.9] Number of Terminals	Nummer	18
[1.10] Terminal Table	➡ Table (10 Reihen)	18
[1.10.1] Terminal Index	Nummer	24
[1.10.2] Terminal Bluetooth Address	edit, ▸ Submit	24
[1.10.3] Terminal Bluetooth Passkey	edit, ▸ Submit	24
[1.10.4] Terminal IP Address	edit, ▸ Submit	24
[1.11] Default Access Mode	edit, ▸ Submit	18
[1.12] Default Bluetooth Passkey	edit, ▸ Submit	19
[2] **IP Parameters for blue2net** (Kapitel 3.5)		**25**
[2.1] blue2net IP Address Resolution	edit, ▸ Submit	25
[2.2] Fixed blue2net IP Configuration	➡ Objects	26
[2.2.1] Fixed blue2net IP Address	edit, ▸ Submit	27
[2.2.2] Fixed blue2net Netmask	edit, ▸ Submit	27
[2.2.3] Fixed blue2net Gateway	edit, ▸ Submit	27
[2.3] DHCP blue2net IP Objects	➡ Objects	26
[2.3.1] Fallback blue2net IP Address	edit, ▸ Submit	28
[2.3.2] Fallback blue2net Netmask	edit, ▸ Submit	28
[2.3.3] Fallback blue2net Gateway	edit, ▸ Submit	28
[2.4] Time Server IP	edit, ▸ Submit	26
[2.5] IP Masquerading	edit, ▸ Submit	26
[2.6] Firewall Settings	➡ Objects	26
[2.6.1] Default Firewall	edit, ▸ Submit	29

Tabelle 3 Hierarchie in den Seiten für die Konfigurationseinstellungen (1)

		Aktion / Anzeige	Seite
[2.7]	Tunnel Configuration (PPPoE / PPTP)	➡ Objects	26
[2.7.1]	Tunnel Mode	edit, ▶ Submit	30
[2.7.2]	Tunnel Establishment Control	edit, ▶ Submit	31
[2.7.3]	Authentication Parameters	➡ Objects	31
[2.7.3.1]	Tunnel User Name	edit, ▶ Submit	32
[2.7.3.2]	Tunnel User Pasword	edit, ▶ Submit	32
[2.7.4]	PPTP Server IP Address	edit, ▶ Submit	31
[3] IP Parameters for Terminals (Kapitel 3.6)			**32**
[3.1]	Terminal IP Address Resolution	edit, ▶ Submit	33
[3.2]	Number of Terminal IP Address Pool Entries	Nummer	33
[3.3]	Terminal IP Address Pool Table	➡ Table (7 Reihen)	34
[3.3.1]	Terminal IP Address Index	Nummer	35
[3.3.2]	Terminal IP Address Pool Value	edit, ▶ Submit	35
[3.4]	Terminal Net Mask	edit, ▶ Submit	34
[3.5]	Terminal Fixed Servers	➡ Objects	34
[3.5.1]	Terminal DNS Server 1	edit, ▶ Submit	36
[3.5.2]	Terminal DNS Server 2	edit, ▶ Submit	36
[3.5.3]	Terminal WINS Server 1	edit, ▶ Submit	37
[3.5.4]	Terminal WINS Server 2	edit, ▶ Submit	37
[3.5.5]	Terminal Domain Name	edit, ▶ Submit	37
[4] Current Configuration (Kapitel 3.7)			**38**
[4.1]	MAC Address	eindeutige, fixe Adresse	38
[4.2]	blue2net IP Configuration	➡ Objects	39
[4.2.1]	blue2net IP Address	Adresse	39
[4.2.2]	blue2net Netmask	Adresse	39
[4.2.3]	blue2net Gateway	Adresse	39
[4.3]	Terminal Server Configuration	➡ Objects	40
[4.3.1]	Terminal DNS Server 1	Adresse	40
[4.3.2]	Terminal DNS Server 2	Adresse	40
[4.3.3]	Terminal WINS Server 1	Adresse	40
[4.3.4]	Terminal WINS Server 2	Adresse	40
[4.3.5]	Terminal Domain Name	Domäne	40
[4.4]	Version Information	➡ Objects	41
[4.4.1]	Module Firmware Version	Version	41
[4.4.2]	PPCBoot Version	Version	41
[4.4.3]	blue2net Software Version	Version	41
[4.4.4]	blue2net Hardware Version	Version	41
[4.4.5]	SieMo Module Info	Version	41
[4.5]	Tunnel Status (PPPoE/PPTP)	➡ Objects	38
[4.5.1]	Tunnel Status	Status d.Tunnel-Verbind.	42
[5] Configuration Access (Kapitel 3.8)			**43**
[5.1]	SNMP Access	edit, ▶ Submit	43
[5.2]	Configuration Password	edit	43
[5.2.1]	Change of configuration password	▶ Submit	44
[6] Activation Commands (Kapitel 3.9)			**44**
[6.1]	Save Settings Temporarily	edit, ▶ Submit	46
[6.2]	Save Settings Permanently	edit, ▶ Submit	47
[6.3]	Reset blue2net	edit, ▶ Submit	47
[6.4]	Update Software	edit, ▶ Submit	48
[6.5]	Restore Default Settings	edit, ▶ Submit	48
[6.6]	Store Specific Homepage	edit, ▶ Submit	49

Tabelle 4 Hierarchie in den Seiten für die Konfigurationseinstellungen (2)

3.4 Bluetooth-Parameter [1]

Dieses Kapitel beschreibt Bluetooth-Parameter für das Gerät blue2net und die Bluetooth-Terminals.

Werte, die mit einer Schaltfläche <edit> versehen oder über einen Link ‚Table' in einer untergeordneten Tabelle über eine Schaltfläche <edit> zugänglich sind, können Sie ändern. Wenn Sie auf einen der unterstrichenen Objektnamen klicken, erhalten Sie eine kurze Online-Beschreibung.

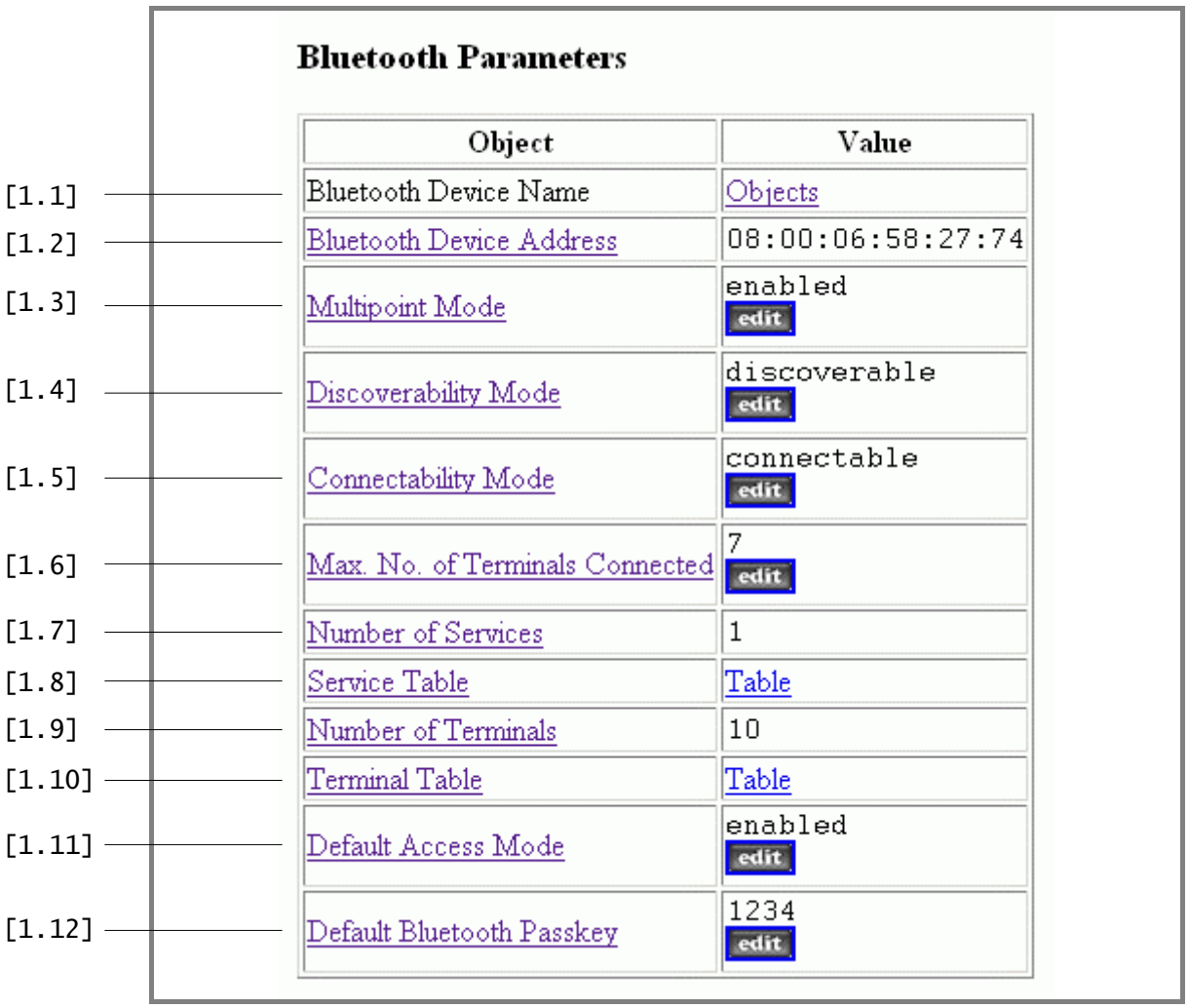

Abb. 6 Bluetooth Parameters [1]

Objekte (siehe Abb. 6)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Bluetooth Device Name	[1.1]		Zugang zur Konfiguration des benutzerfreundlichen Namens von blue2net und zur Aktivierung der Anzeige der IP-Adresse.
Bluetooth Device Address	[1.2]	fixer, eindeutiger Wert	Das ist die eindeutige Bluetooth-Adresse Ihres blue2net. Sie finden diese Adresse auch auf dem Typenschild an der Unterseite des blue2net-Gehäuses aufgedruckt (Bluetooth-Adr.).
Multipoint Mode	[1.3]	enabled disabled	Wenn 'Multipoint Mode' auf *enabled* gesetzt ist, können bis zu 7 Geräte gleichzeitig eine Verbindung zu blue2net herstellen. Wenn 'Multipoint Mode' auf *disabled* gesetzt ist, kann nur ein Gerät verbunden werden, und der „Master-Slave-Switch“ wird von blue2net nicht erzwungen. Hinweis: Einige ältere Bluetooth-Terminals werden nur einsatzfähig sein, wenn 'Multipoint Mode' auf *disabled* gesetzt ist.
Discoverability Mode	[1.4]	discoverable nondiscoverable	Wenn blue2net auf *discoverable* gesetzt ist, ist es für andere Geräte bei der Bluetooth-Geräte-Abfrage (Bluetooth device inquiry) „sichtbar“. Wenn blue2net auf *nondiscoverable* gesetzt ist, ist es für andere Geräte bei der Bluetooth-Geräte-Abfrage (Bluetooth device inquiry) „unsichtbar”.
Connectability Mode	[1.5]	connectable nonconnectable	Wenn blue2net auf *connectable* gesetzt ist, kann ein Bluetooth-Terminal eine Verbindung zu ihm aufbauen. Wenn blue2net auf *nonconnectable* gesetzt ist, kann *kein* Terminal eine Verbindung zu ihm aufbauen. **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 5)

Objekte (siehe Abb. 6)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Max. No. of Terminals Connected	[1.6]	7 (sieben) anderer Wert (Bereich: 0…7)	Diese Zahl gibt an, wieviele Terminals maximal gleichzeitig mit blue2net verbunden werden können. Wenn dieser Wert auf „0“ eingestellt ist, wird *kein* Terminal eine Verbindung zu blue2net aufbauen können. **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 5)
Number of Services	[1.7]	1 (eins) (nur Anzeige)	Das ist die Anzahl der Dienste, die den Terminals angeboten werden.
Service Table	[1.8]		Eine Liste von Einträgen betreffend die Dienste. (siehe Kapitel 3.4.1).
Number of Terminals	[1.9]	10 (zehn) (nur Anzeige)	Die höchstmögliche Anzahl an Terminals, die in die Tabelle' Terminal Table' [1.10] von blue2net aufgenommen werden können.
Terminal Table	[1.10]		Eine Aufstellung von Einträgen, welche die Terminals betreffen (siehe Kapitel 3.4.3).
Default Access Mode	[1.11]	enabled disabled	Wenn 'Default Access Mode' auf *enabled* gesetzt ist, können Terminals, die nicht in der Tabelle 'Terminal Table' [1.10] aufgelistet sind, eine Verbindung zu blue2net herstellen. Der 'Default Bluetooth Passkey' [1.12] kommt dabei für die Bluetooth-Authentifizierung zum Einsatz. **Sicherheitshinweis:** Wenn 'Default Access Mode' auf *enabled* gesetzt ist, wird jedem Terminal Zugang zu blue2net gewährt. Wenn 'Default Access Mode' auf *disabled* gesetzt ist, können nur Terminals, die in der Tabelle 'Terminal Table' [1.10] aufgelistet sind, eine Verbindung zu blue2net herstellen. **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 5)

Objekte (siehe Abb. 6)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Default Bluetooth Passkey	[1.12]	1234 anderes Passwort Ihrer Wahl (1...16 Zeichen)	Bluetooth-Passwort, welches Terminals zugewiesen wurde, die nicht in der Tabelle 'Terminal Table' [1.10] aufgelistet sind. Dieses Passwort gewährt so einem Terminal nur dann Zugang, wenn 'Default Access Mode' [1.11] auf *enabled* gesetzt ist. **Sicherheitshinweis:** Sie sollten dieses Passwort sofort nach der Installation von blue2net ändern. **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 5)

Tabelle 5 Bluetooth Parameters [1]

3.4.1 Bluetooth Device Name [1.1]

'Bluetooth Device Name' [1.1.1] und 'IP Address Suffix Mode' [1.1.2] helfen, blue2net unter mehreren Bluetooth-Geräten identifizieren und/oder auswählen zu können. Bei einer Bluetooth-Geräte-Abfrage (Bluetooth device inquiry) kann ein benutzerfreundlicher Name samt aktueller IP-Adresse des blue2net auf Ihrem Bluetooth-Terminal angezeigt werde

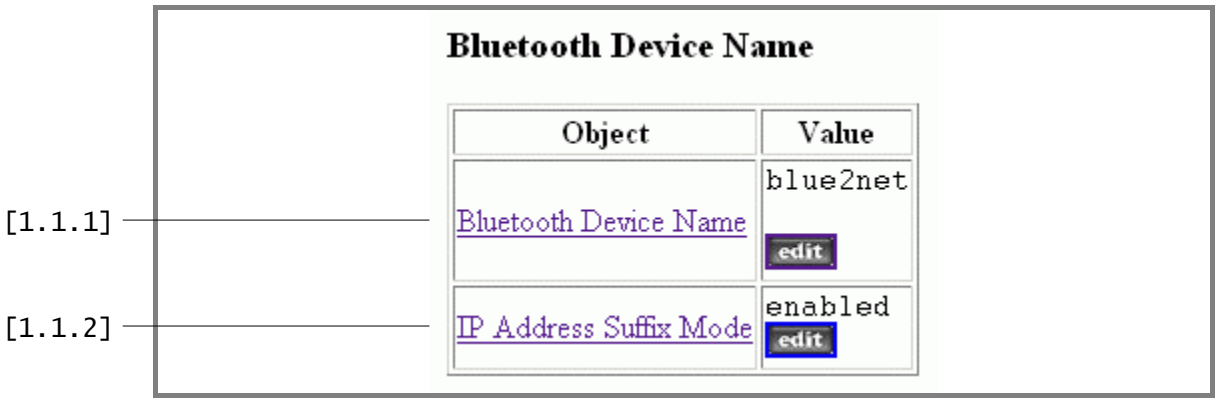

Abb. 7 Bluetooth Device Name [1.1]

Objekte (siehe Abb. 7)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Bluetooth Device Name	[1.1.1]	blue2net anderer Name (1...16 Zeichen)	Der benutzerfreundliche Name Ihres blue2net
IP Address Suffix Mode	[1.1.2]	enabled disabled	Wird 'IP Address Suffix Mode' auf *enabled* eingestellt, so wird die aktuelle IP- Adresse von blue2net an den 'Bluetooth Device Name' angefügt. Die IP-Adresse ist dann bei der Bluetooth-Geräte-Abfrage (Bluetooth device inquiry) am Bluetooth-Terminal ablesbar und ermöglicht das rasche Feststellen der aktuellen blue2net IP-Adresse.

Tabelle 6 Bluetooth Device Name [1.1]

3.4.2 Service Table [1.8]

Der wichtigste Wert in dieser Tabelle ist 'Auth. Level' [1.8.4]. Dieser steuert die bei blue2net verwendeten Bluetooth-Sicherheits-Funktionen *Authentifizierung* und *Verschlüsselung*).

Die anderen Werte werden Bluetooth-Geräten bei einer Bluetooth-Geräte-Abfrage (Bluetooth device inquiry) über SDP übermittelt.

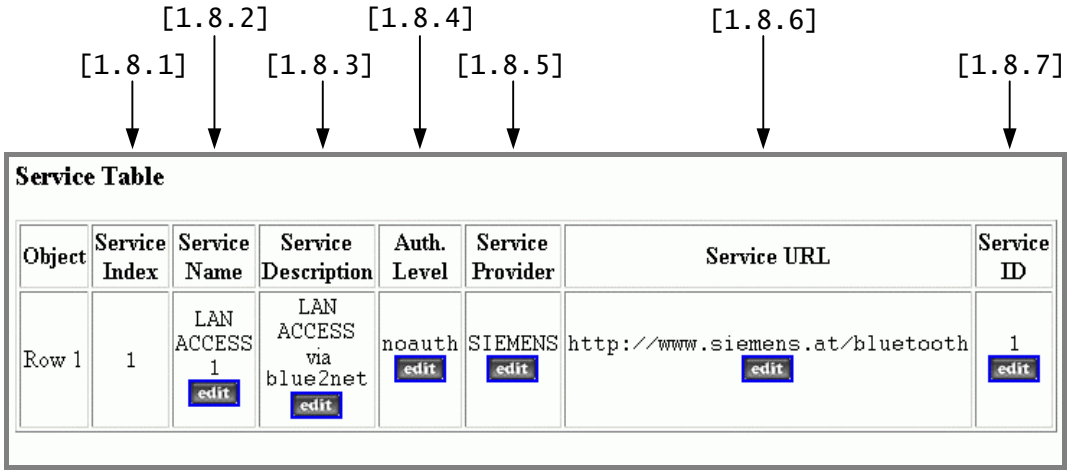

Abb. 8 Service Table [1.8]

Objekte (siehe Abb. 8)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Service Index	[1.8.1]	1 (eins) (nur Anzeige)	Ein eindeutiger Wert für jeden Dienst
Service Name	[1.8.2]	LAN ACCESS 1 anderer Name Ihrer Wahl (1...23 Zeichen)	Der Name des Dienstes, der einem Client über SDP übermittelt wird
Service Description	[1.8.3]	LAN ACCESS via blue2net andere Beschreibung Ihrer Wahl (1...31 Zeichen)	Anzeige der Dienste-Beschreibung. Beeinflusst nicht die Funktionalität.

Objekte (siehe Abb. 8)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Auth. Level	[1.8.4]	noauth auth authandenc	Es gibt Sicherheitsmechanismen für Terminals. Ein Dienst mit dem Attribut *noauth* (keine Authentifizierung) kann ohne jede Sicherheitsschranke verwendet werden. **Sicherheitshinweis:** Wenn 'Auth.Level' auf *noauth* gesetzt ist, gibt es keine Beschränkungen für irgendein Bluetooth-Terminal, auf blue2net und das dahinterliegende LAN zuzugreifen. Für Dienste mit dem Attribut *auth* (Authentifizierung) wird nach einem Bluetooth-Passwort [1.10.3] gefragt, bevor der Benutzer irgendeinen Datentransfer durchführen kann. Für Dienste mit dem Attribut *authandenc* (Authentifizierung und Verschlüsselung) wird nach einem Bluetooth-Passwort [1.10.3] gefragt, bevor der Benutzer irgendeinen verschlüsselten Datentransfer durchführen kann. **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 5)
Service Provider	[1.8.5]	SIEMENS anderer Eintrag Ihrer Wahl (1...15 Zeichen)	Provider des Dienstes, der einem Client (Bluetooth-Terminal / Bluetooth-Gerät) über SDP übermittelt wird.
Service URL	[1.8.6]	http://www.siemens.at/bluetooth anderer Eintrag Ihrer Wahl (1…47 Zeichen)	URL des Dienstes, der einem Client (Bluetooth-Terminal / Bluetooth-Gerät) über SDP übermittelt wird.
Service ID	[1.8.7]	1 (eins)	Wert (Service Record Handle Subfield), der einem Client übermittelt wird, der SDP verwendet (vorbereitet für zukünftige Anwendungen).

Tabelle 7 Service Table [1.8]

3.4.3 Terminal Table [1.10]

Diese Terminal-Tabelle kann dazu verwendet werden, ausgewählten Bluetooth-Terminals, die durch ihre spezifische Bluetooth-Geräte-Adresse (Bluetooth device address) [1.10.2] identifiziert sind, Zugang zu blue2net zu gewähren.

Wenn Sie alle Terminals, die nicht in der Terminal-Tabelle registriert sind, ausschließen wollen, müssen Sie den 'Default Access Mode' [1.11] auf *disabled* setzen.

Für jedes in dieser Tabelle registrierte Terminal können Sie eine eindeutige IP-Adresse ('Terminal BT Address') [1.10.2] und ein eigenes Terminal-Bluetooth-Passwort ('Terminal Bluetooth Passkey') [1.10.3] konfigurieren. Um eine eindeutige IP-Adresse für ein spezifisches Terminal zu erhalten, muss 'Terminal IP Address Resolution' [3.1] auf *predefined* oder *masqueradingpool* gesetzt sein

Wenn die 'Terminal IP Address' [1.10.4] nicht konfiguriert (d.h. auf 0.0.0.0 eingestellt) ist, erhalten Terminals ihre IP-Adressen aus dem Vorrat an Terminal-IP-Adressen ('Terminal IP Address Pool Table') [3.3] .

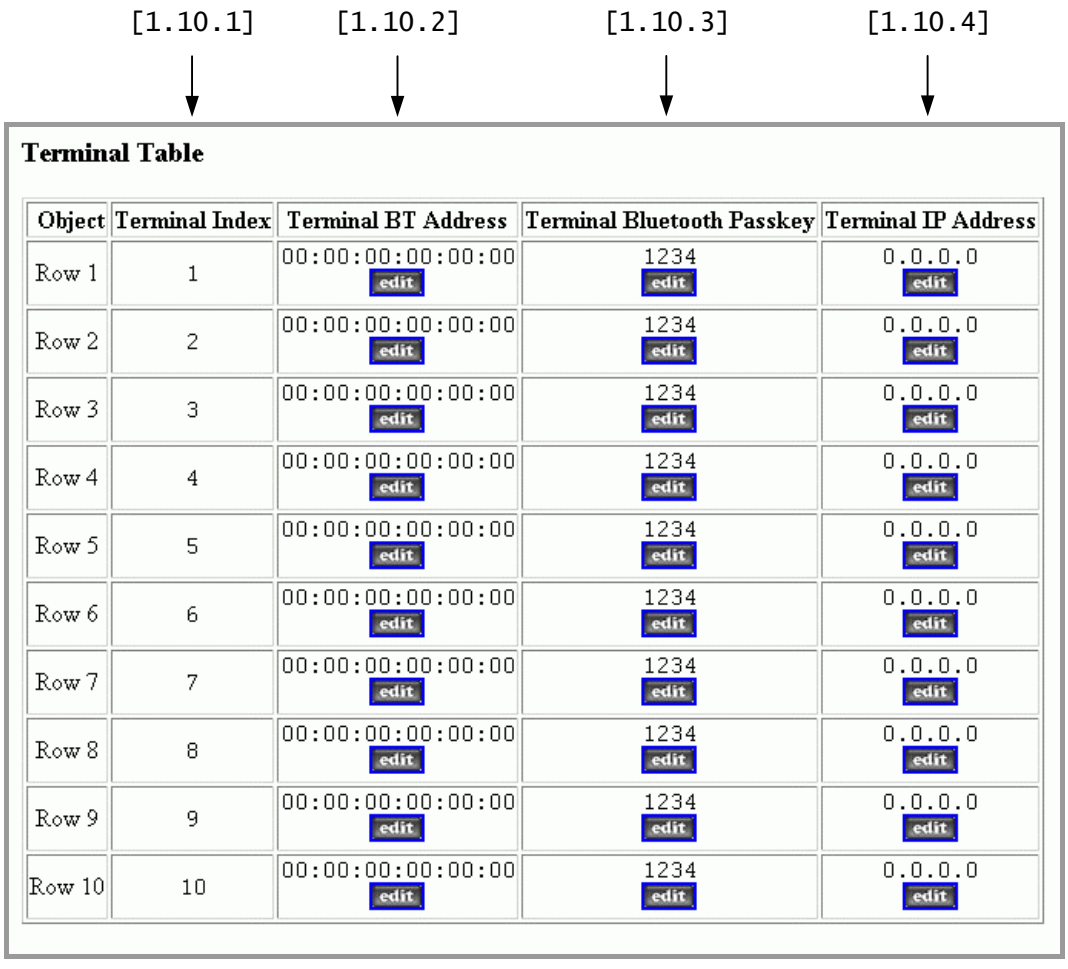

Abb. 9 Terminal Table [1.10]

Objekte (siehe Abb. 9)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Terminal Index	[1.10.1]	1-10 (Nur Anzeige)	Eindeutiger Wert für jedes Terminal (bewegt sich zw. 1 und dem Wert von 'Number of Terminals' [1.9])
Terminal Bluetooth Address	[1.10.2]	00:00:00:00:00:00 andere Bluetooth-Adresse	Eindeutige Bluetooth-Adresse eines Terminals, das berechtigt ist, dieses blue2net zu benützen. Hinweis: Wenn die Terminal-Bluetooth-Adresse auf 00:00:00:00:00:00 gesetzt ist (voreingestellter Wert), wird blue2net dieses Terminal nicht als registriert erkennen, selbst wenn das Passwort [1.10.3] und/oder die Terminal-IP-Adresse [1.10.4] konfiguriert sind. Wenn eine andere Bluetooth-Adresse eingetragen ist: **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 5 und 5.1)
Terminal Bluetooth Passkey	[1.10.3]	1234 anderer Wert Ihrer Wahl (1...16 Zeichen)	Bluetooth-Passwort, das diesem Terminal für den Zugang zu blue2net zugewiesen wird. **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 5)
Terminal IP Address	[1.10.4]	0.0.0.0 andere IP-Adresse	Wenn 'Terminal IP-Address Resolution' [3.1] auf *predefined* oder *masqueradingpool* gesetzt ist, wird die 'Terminal IP Address' dem Terminal zugewiesen. Wenn aber bei 'Terminal IP-Address' *0.0.0.0* eingetragen ist, wird dem Terminal ein Wert aus dem Vorrat von 'Terminal IP Address Pool Entries' [3.2] zugewiesen.

Tabelle 8 Terminal Table [1.10]

3.5 IP Parameters for blue2net [2]

Dieses Kapitel beschreibt IP-Parameter, die für das Gerät blue2net selbst relevant sind.

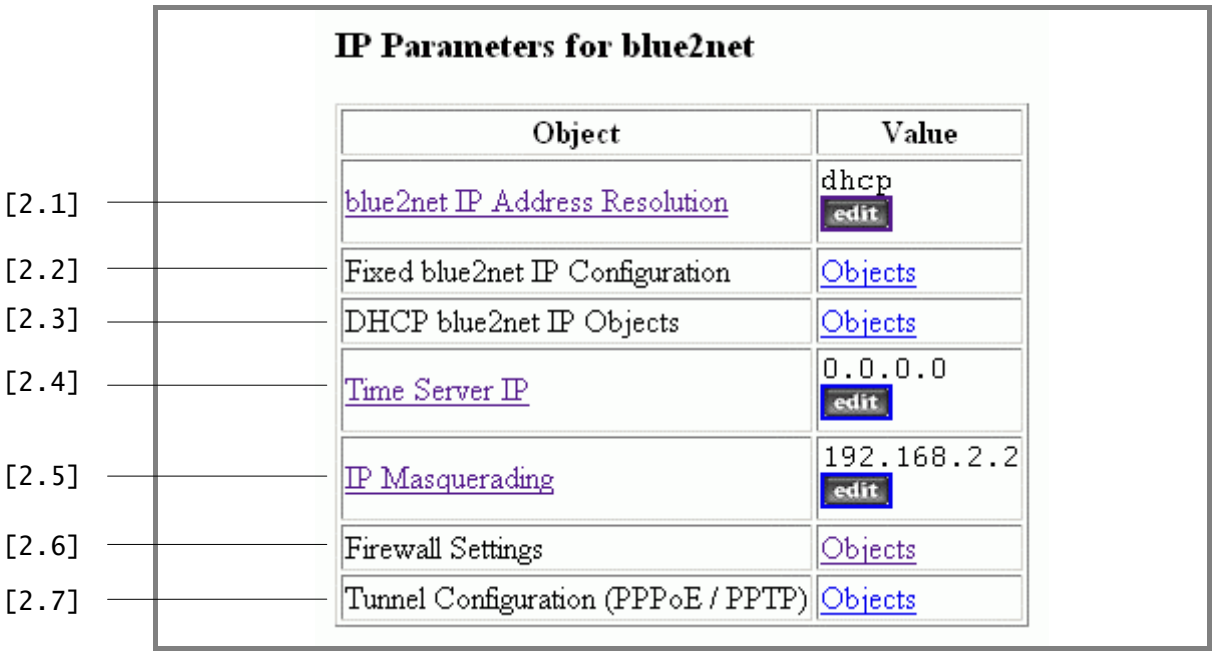

Abb. 10 IP Parameters for blue2net [2]

Objekte (siehe Abb. 10)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
blue2net IP Address Resolution	[2.1]	dhcp predefined	Dieses Objekt bestimmt den Mechanismus, der für die Zuordnung von IP-Adress-Werten an blue2net eingesetzt wird. Wenn als Verfahren *dhcp* eingestellt ist, wird blue2net eine DHCP-Anforderung aussenden, um während des Hochlaufens IP-Adress-Werte zu empfangen. Wenn als Verfahren *predefined* eingestellt ist, wird blue2net die Werte verwenden, die unter 'Fixed blue2net IP Configuration' [2.2] eingegeben sind. Für xDSL-Betrieb ist dieses Verfahren einzustellen. **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 5)

Objekte (siehe Abb. 10)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Fixed blue2net IP Configuration	[2.2]		IP-Adressen, die blue2net zugewiesen sind, wenn das Adress-Auflösungsverfahren 'blue2net IP Address Resolution' [2.1] auf *predefined* eingestellt ist.
DHCP blue2net IP Objects („Fallback“ IP).	[2.3]		IP-Adressen, die blue2net zugewiesen sind, wenn das Adress-Auflösungsverfahren 'blue2net IP Address Resolution' [2.1] auf *dhcp* eingestellt ist.
Time Server IP	[2.4]	0.0.0.0 andere IP-Adresse	IP-Adresse eines Time-Servers in Ihrem Netzwerk (vorbereitet).
IP Masquerading	[2.5]	192.168.2.2 andere IP-Adresse	IP-Adresse von blue2net im maskierten Netz, in Fällen, wo 'Terminal IP Address Resolution' [3.1] auf *masquerading* oder *masqueradingpool* eingestellt ist. Hinweis: Sorgen Sie dafür, dass dieser Wert nicht identisch ist mit der IP-Adresse des blue2net.
Firewall Settings	[2.6]	⇒ [2.6.1]	Wenn 'Default Firewall'[2.6.1] auf *enabled* gesetzt ist, werden die voreingestellten Firewall-Regeln aktiviert (siehe auch Abb. 13).
Tunnel Configuration (PPPoE / PPTP)	[2.7]		Viele Internet-Service-Provider verwenden ein Tunnel-Protokoll, um einen Breitband-Internetzugang auf Basis von DSL bereitzustellen. blue2net unterstützt 2 häufig verwendete Tunnel-Protokolle: PPPoE (RFC 2516) und PPTP (RFC 2637).

Tabelle 9 IP Parameters for blue2net [2]

3.5.1 Fixed blue2net IP Configuration [2.2]

Wenn 'blue2net IP Address Resolution' [2.1] auf *predefined* eingestellt ist, werden die im Folgenden gezeigten Werte wirksam. Diese Werte werden Ihrem blue2net Gerät vom Netzwerk-Administrator oder ISP zugewiesen .

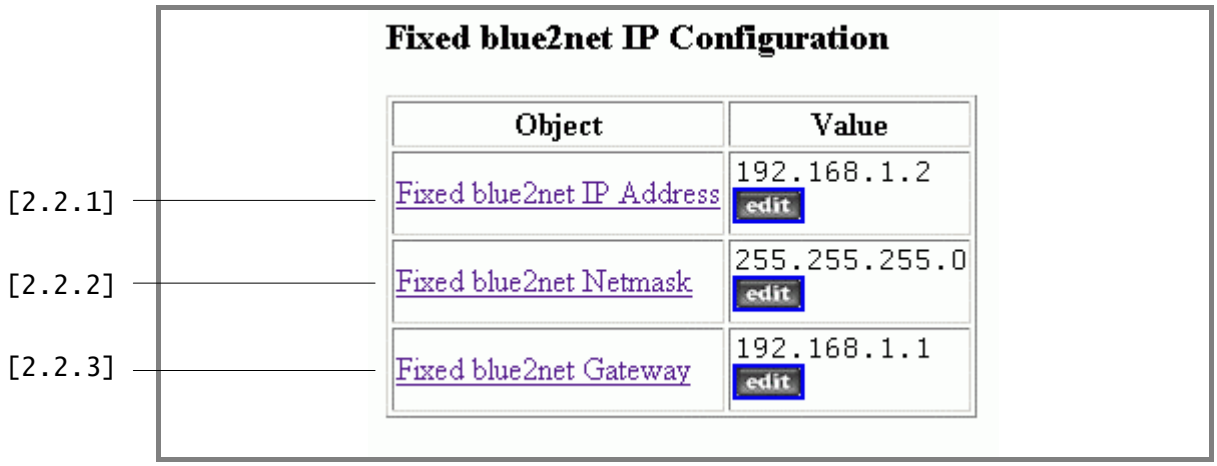

Abb. 11 Fixed blue2net IP Configuration [2.2]

Objekte (siehe Abb. 11)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Fixed blue2net IP Address	[2.2.1]	192.168.1.2 andere IP-Adresse	IP-Adresse, die blue2net zugewiesen wird, unter der Voraussetzung, dass 'blue2net Address Resolution' [2.1] auf *predefined* eingestellt ist.
Fixed blue2net Netmask	[2.2.2]	255.255.255.0 andere Netzmaske	Subnetzmaske, welche zur IP-Adresse 'Fixed blue2net IP Address' [2.2.1] gehört, in Fällen, wo 'blue2net Address Resolution' [2.1] auf *predefined* eingestellt ist.
Fixed blue2net Gateway	[2.2.3]	192.168.1.1 anderes Gateway	IP-Adresse des voreingestellten Gateway auf blue2net, in Fällen, wo 'blue2net Address Resolution' [2.1] auf *predefined* eingestellt ist.

Tabelle 10 Fixed blue2net IP Configuration [2.2]

3.5.2 IP Address Resolution: DHCP [2.3]

Wenn 'blue2net IP Address Resolution' [2.1] auf *dhcp* gesetzt ist und kein DHCP-Dienst verfügbar ist, kommen die unten beschriebenen Werte zum Einsatz. Um herauszufinden, ob DHCP in Ihrem Netzwerk zur Verfügung steht, lesen Sie bitte Kapitel 2.3.

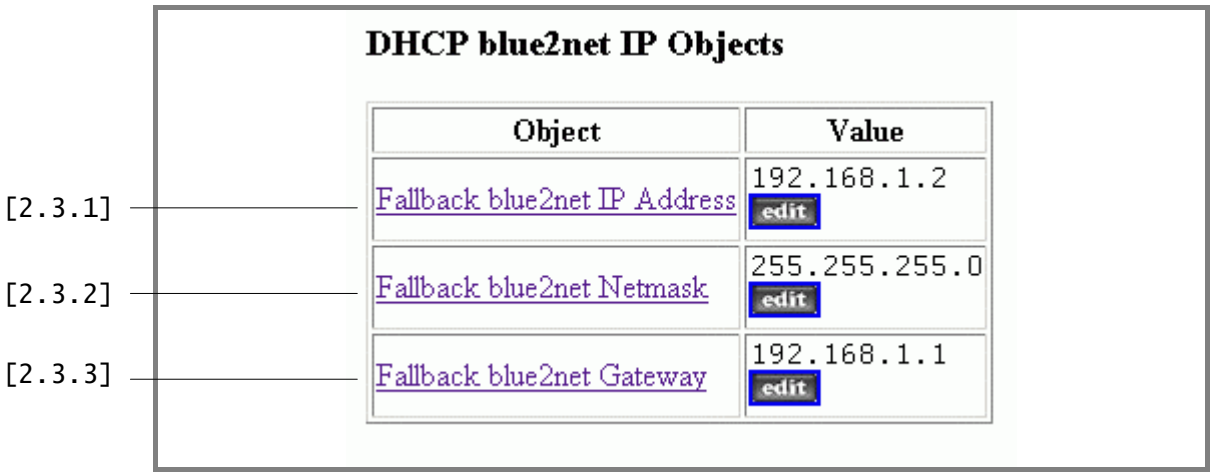

Abb. 12 DHCP blue2net IP Objects [2.3]

Objekte (siehe Abb. 12)	**Hierarchy stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Fallback blue2net IP Address	[2.3.1]	192.168.1.2 andere IP-Adresse	IP-Adresse, die blue2net zugewiesen wird, wenn 'blue2net Address Resolution' [2.1] auf *dhcp* eingestellt ist, die DHCP-Anforderung des Wertes aber fehlgeschlagen ist.
Fallback blue2net Netmask	[2.3.2]	255.255.255.0 andere Netzmaske	Subnetzmaske, welche zur IP-Adresse 'Fallback blue2net IP Address' [2.3.1] gehört, in Fällen, wo 'blue2net Address Resolution' [2.1] auf *dhcp* eingestellt ist, die DHCP-Anforderung des Wertes aber fehlgeschlagen ist.
Fallback blue2net Gateway	[2.3.3]	192.168.1.1 anderes Gateway	IP-Adresse des voreingestellten Gateway auf blue2net, in Fällen, wo 'blue2net Address Resolution' [2.1] auf *dhcp* eingestellt ist, die DHCP-Anforderung des Wertes aber fehlgeschlagen ist.

Tabelle 11 DHCP blue2net IP Objects [2.3]

3.5.3 Firewall Settings [2.6]

Die Firewall in blue2net kann aktiviert werden, um Angriffen von Ethernet-Seite (z.B. über LAN, Kabel-Modem oder xDSL-Anschluss) vorzubeugen.

Hinweis: Bei Aktivierung der Firewall kann es durch die vorprogrammierten Sicherheits-Einstellungen bei gewissen Anwendungen (z. B. Spiele über Internet) zu Einschränkungen kommen.

Ein Software-Update oder das Laden einer spezifischen Homepage über LAN ist nur möglich, wenn die Firewall deaktiviert / *disabled* ist (siehe auch 6.1 und 9).

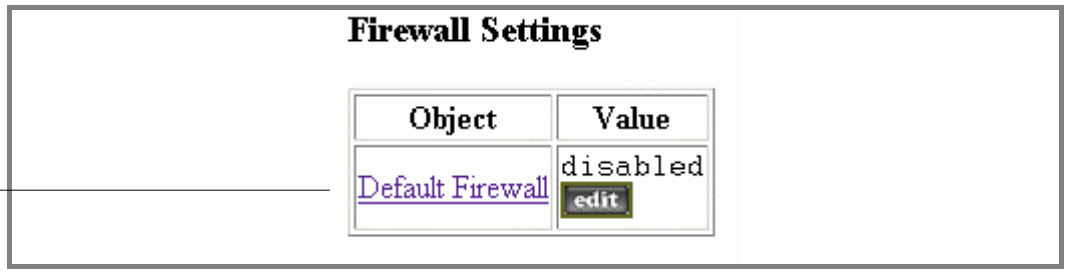

Abb. 13 Firewall Settings [2.6]

Objekte (siehe Abb. 13)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Default Firewall	[2.6.1]	disabled enabled	Wenn 'Default Firewall' auf *enabled* gesetzt ist, werden die voreingestellten Firewall-Regeln aktiviert (siehe Kapitel 9).

Tabelle 12 Firewall Settings [2.6]

3.5.4 Tunnel Configuration (PPPoE / PPTP) [2.7]

Bei der Anbindung von einem xDSL-Modem an ein Endgerät ist meist „über“ dem Ethernet -Protokoll noch ein sogenanntes Tunnel-Protokoll "zwischengeschaltet". Bevor Daten mit dem Internet ausgetauscht werden können, muss ein Tunnel-Protokoll zwischen dem Endgerät (blue2net) und dem xDSL Modem aufgebaut werden. blue2net unterstützt die Tunnel-Protokolle PPPoE (RFC 2516) und PPTP (RFC 2637).

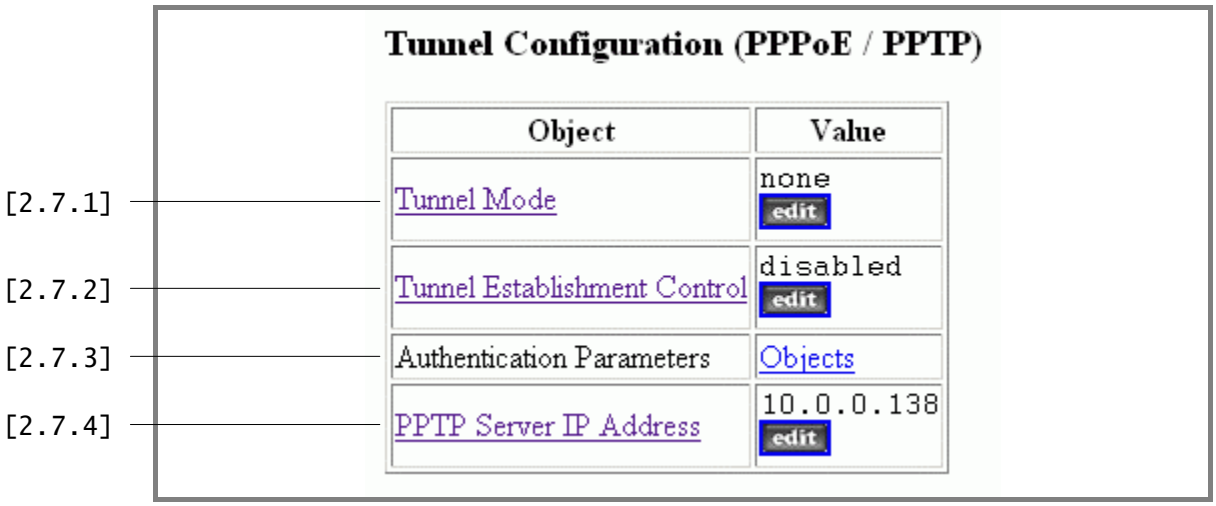

Abb. 14 Tunnel Configuration (PPPoE / PPTP) [2.7]

Objekte (siehe Abb. 14)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Tunnel Mode	[2.7.1]	none pppoe pptp	Wenn 'Tunnel Mode' auf *none*, eingestellt ist, wird kein Tunnel-Protokoll von blue2net aktiviert. Wenn 'Tunnel Mode' auf *pppoe* eingestellt ist, wird blue2net das PPPoE Tunnel-Protokoll (RFC 2516) aktivieren. Wenn 'Tunnel Mode' auf *pptp*, eingestellt ist, wird blue2net das PPTP Tunnel-Protokoll (RFC 2637) aktivieren. Welches Tunnel-Protokoll für ihren xDSL-Zugang zu verwenden ist, erfahren Sie bei Ihrem xDSL-Provider.

Objekte (siehe Abb. 14)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Tunnel Establishment Control	[2.7.2]	disabled enabled	Dieser Parameter ist nur relevant, wenn 'Tunnel Mode' auf *pppoe* oder *pptp* eingestellt ist. Wenn 'Tunnel Establishment Control' auf *disabled* eingestellt ist, baut blue2net beim Start eine Tunnel-Verbindung auf. Der Tunnel bleibt aufrecht, bis blue2net abgeschaltet wird. Diese Einstellung verwenden, wenn ‚Flat-Rate' das Tarifmodell Ihres xDSL-Anbieters ist. Wenn 'Tunnel Establishment Control' auf *enabled* eingestellt ist, baut blue2net eine Tunnel-Verbindung auf, sobald sich das erste Bluetooth-Terminal zu blue2net verbindet. Die Tunnel-Verbindung wird abgebrochen, sobald sich das letzte Bluetooth-Terminal von blue2net getrennt hat. Diese Einstellung verwenden, wenn Online-Zeit für das Tarifmodell Ihres xDSL-Anbieters maßgebend ist.
Authentication Parameters	[2.7.3]		Authentifizierung (User Name und User Passwort) für die Tunnel-Verbindungen.
PPTP Server IP Address	[2.7.4]	10.0.0.138 andere IP-Adresse	Dieser Parameter ist nur relevant, wenn 'Tunnel Mode' auf *pptp* eingestellt ist. 'PPTP Server IP Address' ist die IP-Adresse des PPTP-Servers/xDSL--Modems. Entnehmen sie diese IP-Adresse aus den Unterlagen ihres xDSL-Modems oder kontaktieren sie ihren xDSL-Anbieter.

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

Authentication Parameters [2.7.3]

Die Tunnel-Protokolle PPPoE und PPTP führen beim Aufbau des Tunnels eine Authentifizierung mittels 'User Name' und 'User Password' durch. Die Werte für diese Parameter werden Ihnen von Ihrem xDSL-Provider zugewiesen.

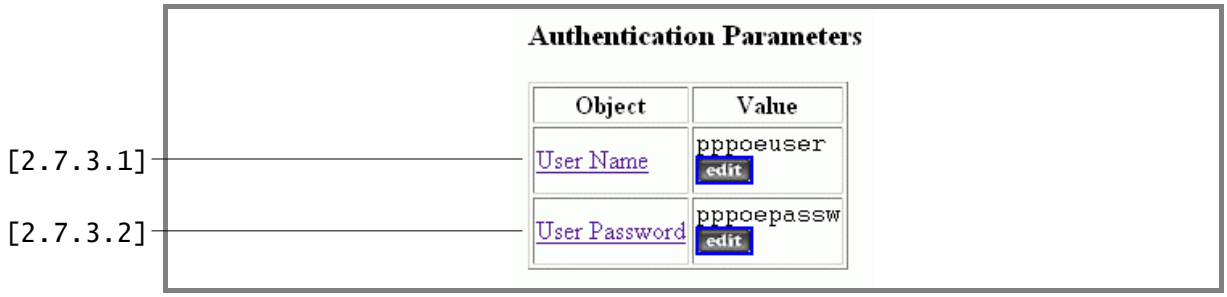

Abb. 15 Authentication Parameters [2.7.3]

Objekte (siehe Abb. 15)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
User Name	[2.7.3.1]	pppoeuser anderer Wert Ihrer Wahl (1...100 Zeichen)	Der 'User Name' wird für die Authentifizierung des Benützers verwendet (dieser wird Ihnen z.B. vom Internet-Service-Provider zugewiesen).
User Password	[2.7.3.2]	pppoepassw anderer Wert Ihrer Wahl (1...100 Zeichen)	Das 'User Password' wird für die Authentifizierung des Benützers verwendet. (dieses wird Ihnen z.B. vom Internet-Service-Provider zugewiesen).

Tabelle 14 Authentication Parameters [2.7.3]

3.6 IP Parameters for Terminals [3]

Dieses Kapitel beschreibt die IP-Parameter für Terminals, die mit blue2net verbunden sind. Während die PPP-Verbindung aufgebaut wird, werden diese Parameter (ausgenommen [3.1] und [3.2]) an das Bluetooth-Terminal geschickt.

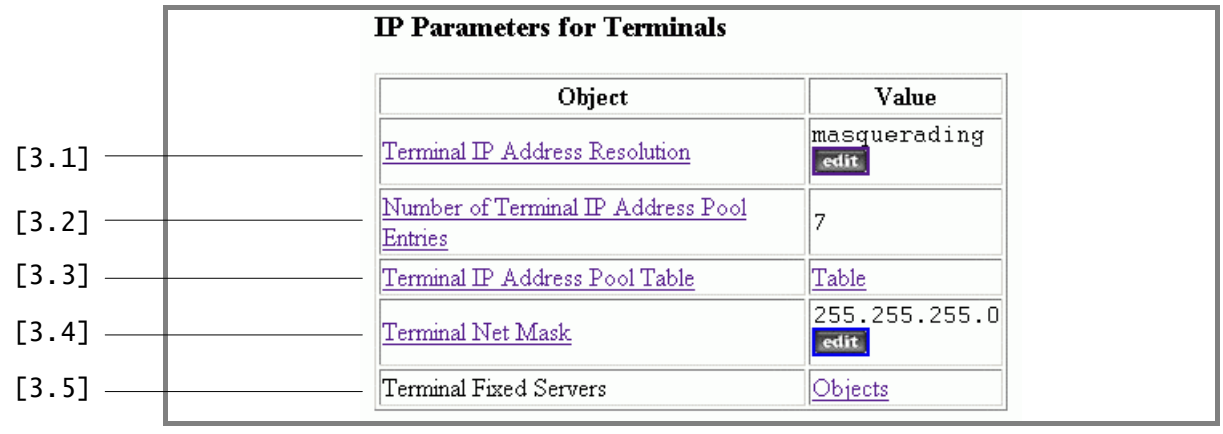

Abb. 16 IP Parameters for Terminals [3]

Objekte (siehe Abb. 16)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Terminal IP Address Resolution	[3.1]	masquerading dhcp predefined masqueradingpool	Dieses Objekt bestimmt den Mechanismus, der eingesetzt wird für die Zuordnung von IP-Adress-Werten zu Terminals, die mit blue2net verbunden sind. Wenn als Verfahren *masquerading* eingestellt ist, ist keine IP-Adress-Konfiguration für die Terminals erforderlich (empfohlene Einstellung für Heimanwender mit Kabel-Modem oder xDSL-Modem). Wenn als Verfahren *dhcp* eingestellt ist, wird blue2net während des Verbindungsaufbaus eine DHCP-Anfrage aussenden, welche die Bluetooth-Adresse des Terminals enthält. Wenn als Verfahren *predefined* eingestellt ist, wird blue2net eine IP-Adresse aus einem Vorrat von fixen IP-Adressen verwenden. Dieser Vorrat ist definiert in der Tabelle 'Terminal IP Address Pool Table' [3.3]. Wenn das Terminal in der Tabelle 'Terminal Table' [1.10] registriert ist, wird blue2net eine von dort zugewiesene IP-Adresse verwenden (siehe auch 3.4.3) Wenn als Verfahren *masqueradingpool* eingestellt ist, geht die Zuweisung genau so vor sich, wie beim Verfahren *masquerading* erwähnt, ausgenommen sind jedoch die in der Tabelle 'Terminal Table' [1.10] registrierten Terminals (siehe auch 3.4.3). **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 5)
Number of Terminal IP Address Pool Entries	[3.2]	7 (nur Anzeige)	Anzahl der IP-Adressen im Vorrat der Terminal-IP-Adressen ('Terminal IP Address Pool Table' [3.3]).

Objekte (siehe Abb. 16)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Terminal IP Address Pool Table	[3.3]		Liste der IP-Adressen, die blue2net Terminals zuweisen kann.
Terminal Netmask	[3.4]	255.255.255.0 other value	Subnetzmaske, welche zu den IP-Adressen aus der Tabelle 'Terminal IP Address Pool Table' [3.3] gehört.
Terminal Fixed Servers	[3.5]		Während die PPP-Verbindung aufgebaut wird, werden diese Parameter an das Bluetooth-Terminal gesendet.

Tabelle 15 IP Parameters for Terminals [3]

3.6.1 Terminal IP Address Pool Table [3.3]

Eine Liste von IP-Adressen, die blue2net den Terminals zuordnen kann. Diese IP-Adressen sind nur relevant, wenn 'Terminal IP Address Resolution' [3.1] *nicht* auf *dhcp* gesetzt ist.

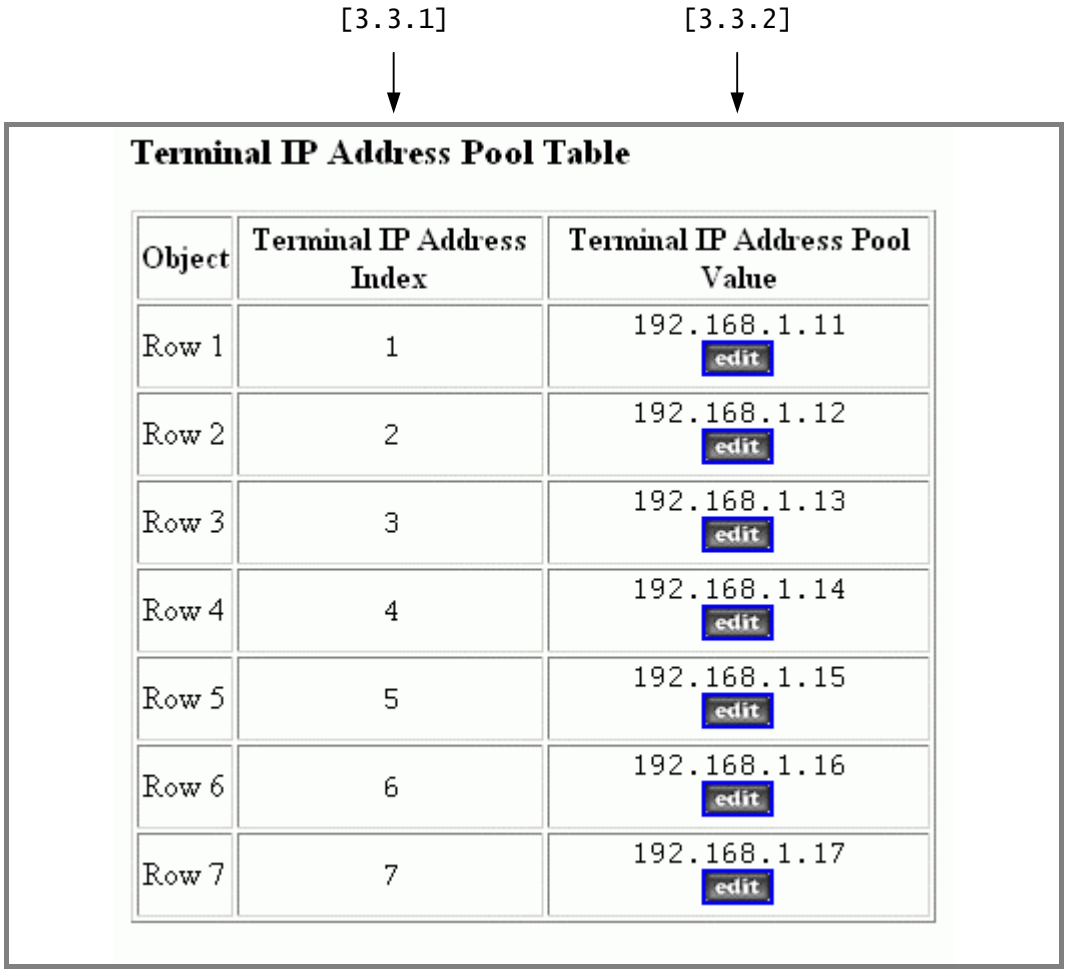

Abb. 17 Terminal IP Address Pool Table [3.3]

Objekte (siehe Abb. 17)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Terminal IP Address Index	[3.3.1]	1-7 (nur Anzeige)	Ein nur einmal vergebener Wert
Terminal IP Address Pool Value	[3.3.2]	192.168.1.11…17	Das sind die IP-Adressen, welche den Terminals zugewiesen werden, in Fällen, wo 'Terminal IP Address Resolution' [3.1] auf *predefined* gesetzt ist.

Tabelle 16 Terminal IP Address Pool Table [3.3]

3.6.2 Terminal Fixed Servers [3.5]

Server IP-Adressen in Fällen, wo das Verfahren 'Terminal IP Address Resolution' [3.1] *nicht* auf *dhcp* gesetzt ist.

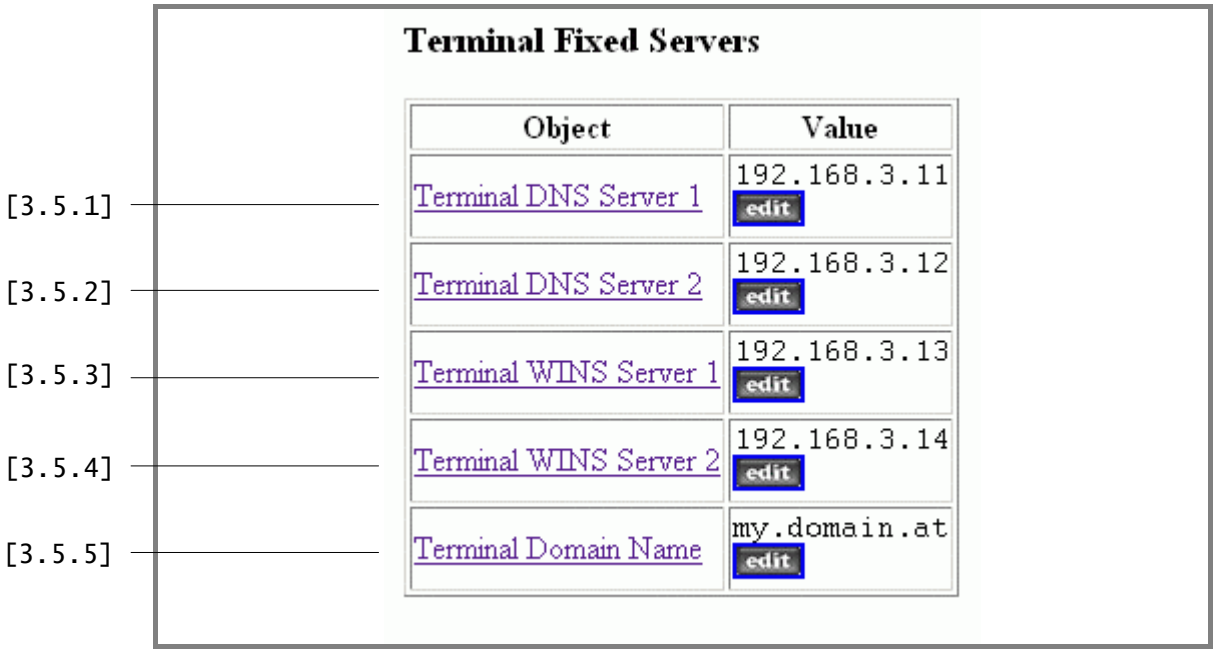

Abb. 18 Terminal Fixed Servers [3.5]

Objekte (siehe Abb. 18)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Terminal DNS Server 1	[3.5.1]	192.168.3.11 andere IP-Adresse	IP-Adresse des DNS Server 1, welcher den Terminals zugewiesen wird, wenn das Verfahren 'Terminal IP Address Resolution' [3.1] nicht auf *dhcp* gesetzt ist und 'blue2net IP Address Resolution' [2.1] auf *predefined* gesetzt ist. Bitte tragen Sie die korrekten DNS-IP-Adressen (DNS 1 u. 2) manuell ein, falls diese durch den DHCP-Server nicht richtig übermittelt werden können (siehe Kapitel 8.3).
Terminal DNS Server 2	[3.5.2]	192.168.3.12 andere IP-Adresse	IP-Adresse des DNS Server 2, welcher den Terminals zugewiesen wird, wenn das Verfahren 'Terminal IP Address Resolution' [3.1] nicht auf *dhcp* gesetzt ist und 'blue2net IP Address Resolution' [2.1] auf *predefined* gesetzt ist.

Objekte (siehe Abb. 18)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Terminal WINS Server 1	[3.5.3]	192.168.3.13 andere IP-Adresse	IP-Adresse des WINS Server 1, welcher den Terminals zugewiesen wird, wenn das Verfahren 'Terminal IP Address Resolution' [3.1] nicht auf *dhcp* gesetzt ist und 'blue2net IP Address Resolution' [2.1] auf *predefined* gesetzt ist.
Terminal WINS Server 2	[3.5.4]	192.168.3.14 andere IP-Adresse	IP-Adresse des WINS Server 2, welcher den Terminals zugewiesen wird, wenn das Verfahren 'Terminal IP Address Resolution' [3.1] nicht auf *dhcp* gesetzt ist und 'blue2net IP Address Resolution' [2.1] auf *predefined* gesetzt ist.
Terminal Domain Name	[3.5.5]	my.domain.at anderer Domänen-Name (1…100 Zeichen)	Domänen-Name, welcher den Terminals zugewiesen wird, wenn das Verfahren 'Terminal IP Address Resolution' [3.1] nicht auf *dhcp* gesetzt ist und 'blue2net IP Address Resolution' [2.1] auf *predefined* gesetzt ist.

Tabelle 17 Terminal Fixed Servers [3.5]

3.7 Current Configuration [4]

Die Objekte in diesem Abschnitt dienen lediglich der Anzeige von aktuellen Werten wichtiger Bluetooth- und IP-Parameter sowie von Versionsinformationen für das Gerät blue2net.

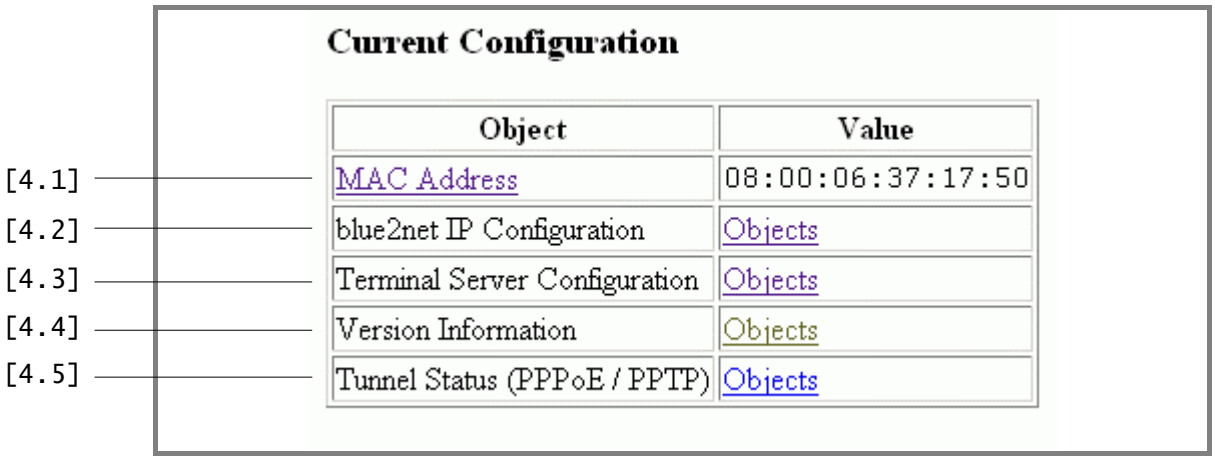

Abb. 19 Current Configuration [4]

Objekte (siehe Abb. 19)	**Hier. stufe**	**Erklärung**
MAC Address	[4.1]	Die MAC-Adresse ist eine fixe und eindeutige Adresse des Ethernet-Controllers im blue2net. Sie können diese Adresse auch auf dem Typenschild an der Gehäuseunterseite des Gerätes finden (MAC-Adr.).
blue2net IP Configuration	[4.2]	siehe Tabelle 19
Terminal Server Configuration	[4.3]	siehe Tabelle 20
Version Information	[4.4]	siehe Tabelle 21
Tunnel Status (PPPoE / PPTP)	[4.5]	siehe Tabelle 22

Tabelle 18 Current Configuration [4]

3.7.1 blue2net IP Configuration [4.2]

Diese Objekte zeigen Ihnen, welche IP-Adressen Ihrem blue2net zugewiesen wurden.

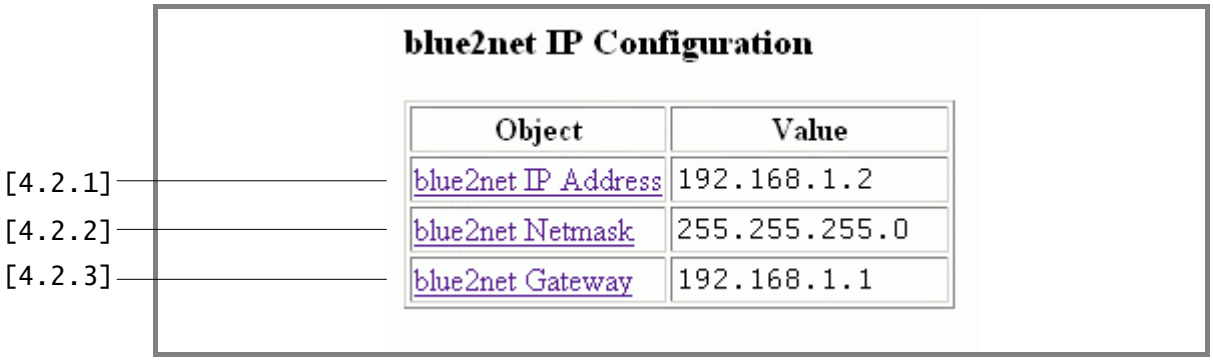

Abb. 20 blue2net IP Configuration [4.2]

Objekte (siehe Abb. 20)	**Hier. stufe**	**Erklärung**
blue2net IP Address	[4.2.1]	IP-Adresse, die blue2net zugewiesen wurde. Wenn das Verfahren 'blue2net IP Address Resolution' [2.1] auf *dhcp* gesetzt ist, wurde dieser Wert über eine DHCP-Abfrage erfasst.
blue2net Netmask	[4.2.2]	Subnetzmaske, die blue2net zugewiesen wurde. Wenn das Verfahren 'blue2net IP Address Resolution' [2.1] auf *dhcp* gesetzt ist, wurde dieser Wert über eine DHCP-Abfrage erfasst.
blue2net Gateway	[4.2.3]	Gateway, das blue2net zugewiesen wurde. Wenn das Verfahren 'blue2net IP Address Resolution' [2.1] auf *dhcp* gesetzt ist, wurde dieser Wert über eine DHCP-Abfrage erfasst.

Tabelle 19 blue2net IP Configuration [4.2]

3.7.2 Terminal Server Configuration [4.3]

Diese Objekte zeigen, welche Werte den Terminals zugewiesen wurden.

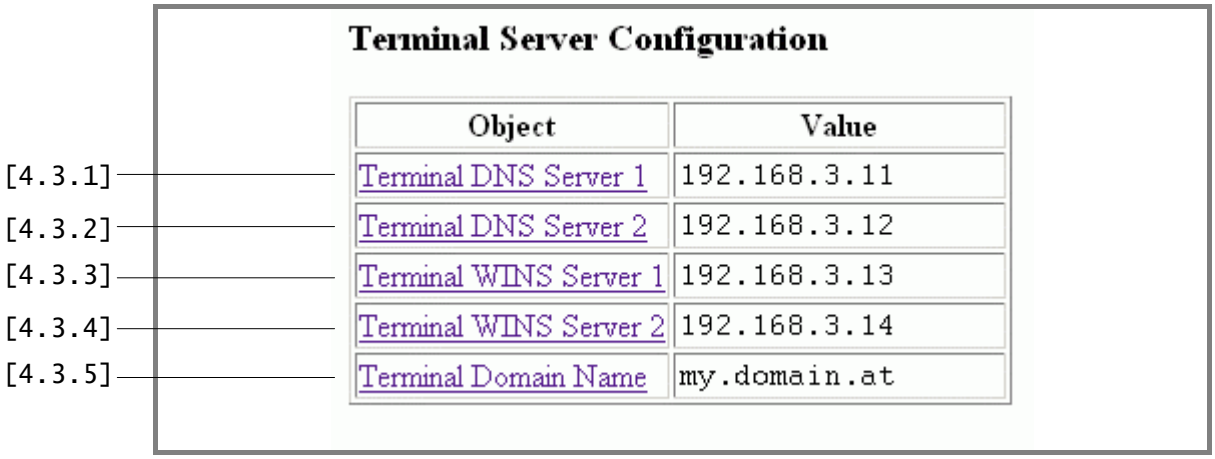

Abb. 21 Terminal Server Configuration [4.3]

Objekte (siehe Abb. 21)	**Hier. stufe**	**Erklärung**
Terminal DNS Server 1	[4.3.1]	IP-Adresse von DNS Server 1, der den Terminals zugewiesen wurde. Wenn 'Terminal IP Address Resolution' [3.1] auf *dhcp* gesetzt ist, wurde dieser Wert über eine DHCP-Abfrage erfasst.
Terminal DNS Server 2	[4.3.2]	IP-Adresse von DNS Server 2, der den Terminals zugewiesen wurde. Wenn 'Terminal IP Address Resolution' [3.1] auf *dhcp* gesetzt ist, wurde dieser Wert über eine DHCP-Abfrage erfasst.
Terminal WINS Server 1	[4.3.3]	IP-Adresse von WINS Server 1, der den Terminals zugewiesen wurde. Wenn 'Terminal IP Address Resolution' [3.1] auf *dhcp* gesetzt ist, wurde dieser Wert über eine DHCP-Abfrage erfasst.
Terminal WINS Server 2	[4.3.4]	IP-Adresse von WINS Server 1, der den Terminals zugewiesen wurde. Wenn 'Terminal IP Address Resolution' [3.1] auf *dhcp* gesetzt ist, wurde dieser Wert über eine DHCP-Abfrage erfasst.
Terminal Domain Name	[4.3.5]	Domänen-Name, der den Terminals zugewiesen wurde. Wenn 'Terminal IP Address Resolution' [3.1] auf *dhcp* gesetzt ist, wurde dieser Wert über eine DHCP-Abfrage erfasst.

Tabelle 20 Terminal Server Configuration [4.3]

3.7.3 Version Information [4.4]

Diese Objekte informieren über die in Ihrem blue2net zum Einsatz kommende Software, Hardware und Firmware. Sie könnten diese Information benötigen, wenn Sie mit einer Service-Hotline sprechen.

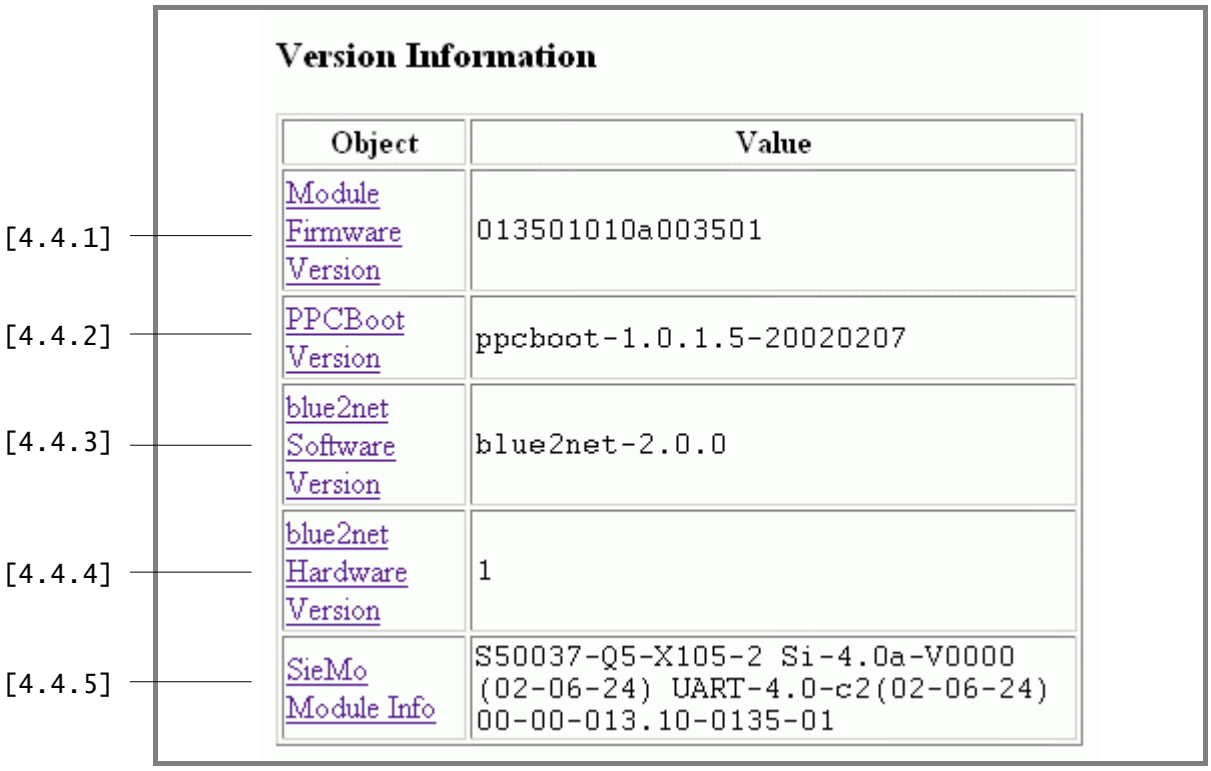

Abb. 22 Version Information [4.4]

Objekte (siehe Abb. 22)	**Hier. stufe**	**Erklärung**
Module Firmware Version	[4.4.1]	Firmware-Version des Bluetooth-Moduls.
PPCBoot Version	[4.4.2]	Version der Boot-Loader-Software.
blue2net Software Version	[4.4.3]	Version der blue2net-Anwendungs-Software.
blue2net Hardware Version	[4.4.4]	Version der blue2net-Hardware.
SieMo Module Info	[4.4.5]	Versions-Information zum Siemens Bluetooth-Modul SieMo S50037.

Tabelle 21 Version Information [4.4]

3.7.4 Tunnel Status [4.5]

Diese Objekte informieren über den aktuellen Zustand des „Tunnels“.

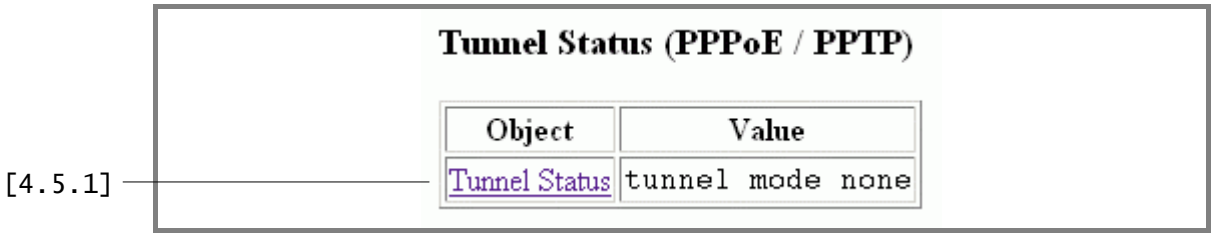

Abb. 23 Tunnel Status [4.5.1]

Objekte (siehe Abb. 23)	Hier. stufe	Erklärung
Tunnel Status	[4.5.1]	Aktueller Zustand des „Tunnels“.

Tabelle 22 Tunnel Status [4.5.1]

Hier beispielhaft einige Statusmeldungen:

Meldung	Bedeutung
... pptp process running...	Tunnel wurde erfolgreich aufgebaut
... pptp	xDSL-Mode eingestellt ohne Verbindung
... none	Es wurde kein Tunnel-Modus aufgebaut
... peer not responding	das Modem/der Server antwortet nicht, xDSL-Verbindung unterbrochen oder falsche PPTP-Server-Adresse eingestellt
... authentication failed	Passwort und/oder UserName wurde nicht anerkannt, z.B. wegen falscher Eingabe

Tabelle 23 Statusmeldungen (Beispiele)

3.8 Configuration Access [5]

Dieses Kapitel beschreibt Objekte, die den Zugang zur Konfiguration steuern.

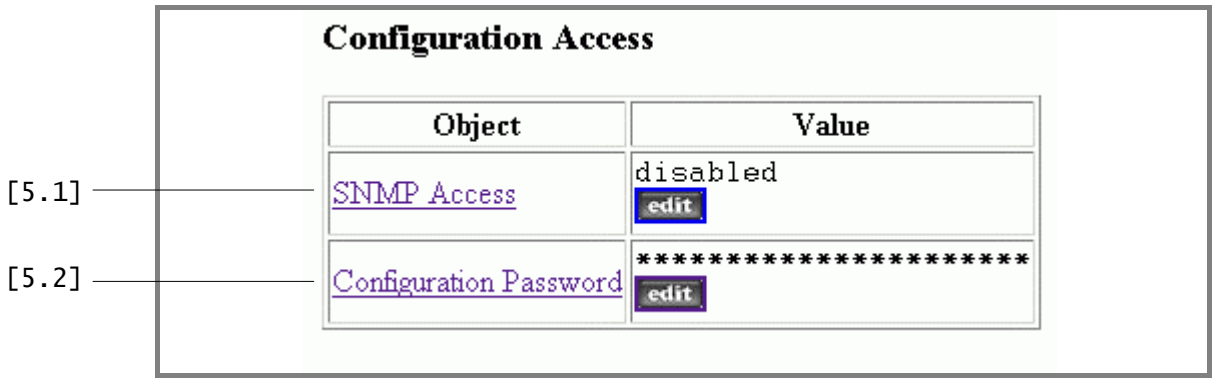

Abb. 24 Configuration Access [5]

Objekte (siehe Abb. 24)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
SNMP Access	[5.1]	disabled enabled	Dieses Objekt steuert den Zugang zu einem SNMP-Interface für die Konfiguration von blue2net.
Configuration Password	[5.2]	changeme Passwort Ihrer Wahl (4…22 Zeichen)	Dieses Passwort wird zur Authentifizierung von Personen, die zum Konfigurieren von blue2net übers Web-Interface berechtigt sind. **Sie sollten dieses Passwort nie vergessen!** **Sicherheitshinweis:** Sie sollten diesen Passwort sofort nach der Installation von blue2net ändern. **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 5)

Tabelle 24 Configuration Access [5]

3.8.1 Change of the Configuration Password [5.2]

Sie müssen das Passwort zweimal eingeben (siehe Abb. 25).

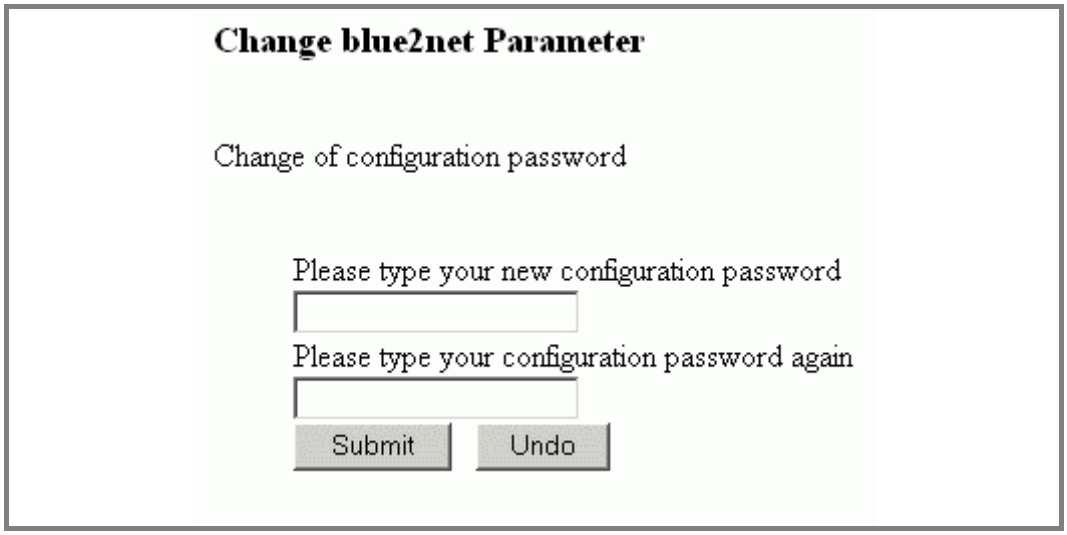

Abb. 25 Change blue2net Configuration Password [5.2.1]

Mit der Eingabe allein sind Ihre Änderungen noch nicht aktiv. Um sie zu speichern und zu aktivieren, führen Sie einen der Aktivierungsbefehle ('Activation Commands') 'Save Settings Temporarily' oder 'Save Settings Permanently' aus (siehe Kapitel 3.9.1 und 3.9.2).

3.9 Activation Commands [6]

Jede Änderung, die Sie an blue2net-Einstellungen durchführen, werden erst wirksam, nachdem Sie diese mit einem der beiden *Aktivierungsbefehle* 'Save Settings Temporarily' oder 'Save Settings Permanently' abgespeichert haben. Das bringt gewisse Vorteile, z.B. in Hinblick auf mögliche Aussperrung nach falschen Einstellungen (siehe auch Kapitel 5), darf aber besonders im Hinblick auf Sicherheitseinstellungen nicht vergessen werden.

Wenn Sie die Werkseinstellungen wiederherstellen wollen oder die Konfiguration im Permanent-Speicher aktivieren wollen, finden Sie hier die dazugehörigen Befehle.

Von der Service-Homepage heruntergeladene Software-Updates oder in das Gerät geladene Dateien für Ihre blue2net-eigene Homepage (Specific Homepage) müssen abgespeichert werden, bevor sie wirksam werden.

Beachten Sie bitte die Warnungen, um einer möglichen Aussperrung vom Zugang über Bluetooth oder LAN vorzubeugen (siehe Kapitel 5).

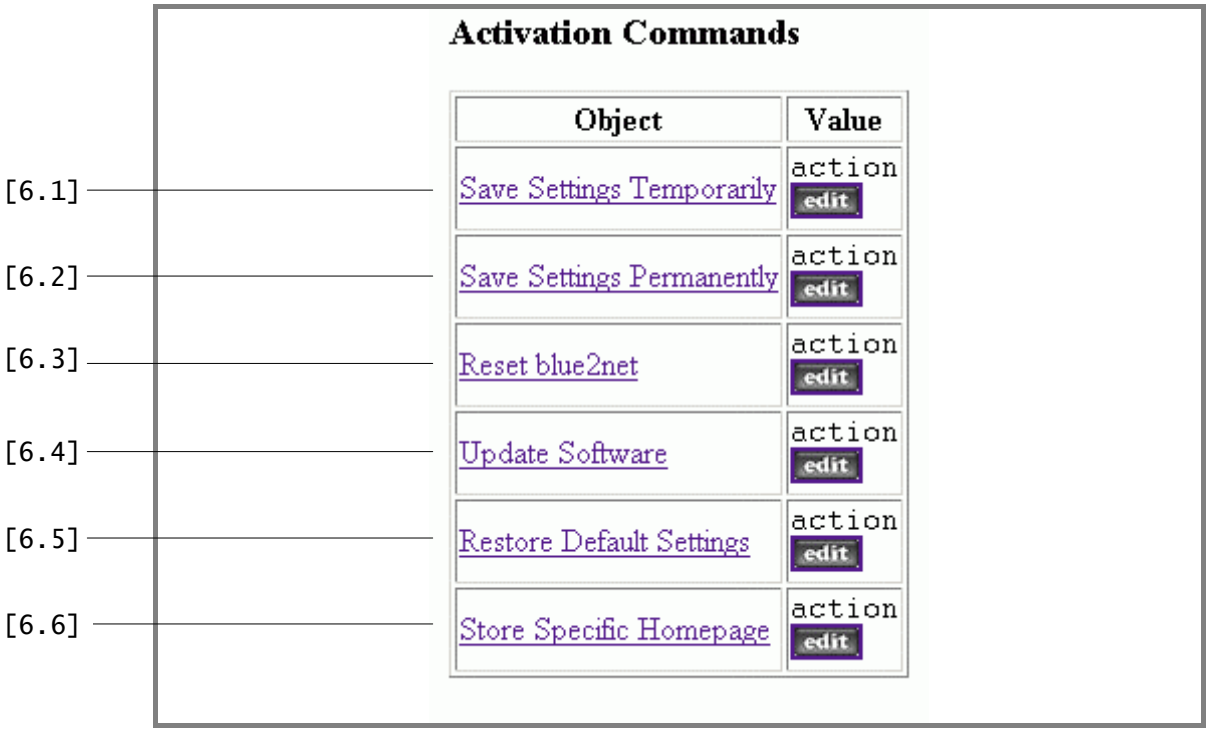

Abb. 26 Activation Commands [6]

Klicken Sie auf <edit>. Damit kommen Sie zu einer Seite, wie sie in Abb. 27 als Beispiel gezeigt ist.

Wenn Sie dort auf <Submit> klicken, werden Ihre Änderungen wirksam.

Abb. 27 Change blue2net parameter

3.9.1 Save Settings Temporarily [6.1]

Einstellungen vorübergehend abspeichern [6.1]

Änderungen, die Sie an einer oder mehreren Einstellungen durchführen, werden nicht wirksam, solange sie nicht abgespeichert sind. Beachten Sie das bitte besonders in Zusammenhang mit Sicherheitseinstellungen.

Abspeichern können Sie Änderungen entweder

- *vorübergehend* (z.B. für eine laufende Sitzung), indem Sie 'Save Settings Temporarily' [6.1] auswählen, oder
- *dauerhaft* (bis neuerliche Änderungen im Speicher vorgenommen werden), indem Sie 'Save Settings Permanently' [6.2] auswählen.

'Save Settings Temporarily' speichert geänderte Einstellungen nur in einem temporären (flüchtigen) Speicher, wodurch sie nur während der aktuellen Sitzung gültig und nicht dauerhaft abgespeichert sind.

Wenn Sie also die Stromversorgung unterbrechen oder einen Reset (z.B. [6.3]) ausführen, gehen diese Änderungen verloren. Wenn Sie nur den Konfigurationsvorgang durch Klicken auf [Close Session] oder [Home] beenden, gehen die Änderungen nicht verloren.

Vorteil: Sie können Ihre Einstellungen testen, bevor Sie diese dauerhaft abspeichern (ausgenommen alle blue2net IP-Parameter [2]). Wenn Sie sich also z.B. durch falsche Einstellungen aus dem Zugang über Bluetooth oder LAN aussperren, haben Sie immer noch die Möglichkeit, zu den vorherigen *dauerhaft gespeicherten* Einstellungen zurückzukehren, indem Sie die Stromversorgung unterbrechen oder einen Reset [6.3] über LAN (siehe weiter unten) ausführen. Damit werden die im Permanent-Speicher abgelegten Einstellungen wieder aktiv. Anschließend können Sie Ihre Einstellungen überdenken und richtige anwenden.

Wenn Sie 'Bluetooth Parameters' [1.#] und/oder 'IP Parameters for Terminals' [3.#] konfiguriert haben und dann 'Save Settings Temporarily' ausführen, während Sie über Bluetooth verbunden sind, werden Sie die Bluetooth-Verbindung zu blue2net neu herstellen müssen.

Hinweis: Sorgen Sie dafür, dass bestehende Bluetooth-Verbindungen anderer Terminals geordnet beendet werden, bevor Sie diese Funktion ausführen.

Vorsicht! Sie könnten sich durch falsche Einstellungen *aussperren!* Informieren Sie sich bitte in Kapitel 5, wie Sie das verhindern können.

Im Falle der Aussperrung haben Sie 2 Alternativen, blue2net auf zuvor im Permanent-Speicher abgespeicherte Einstellungen zurückzusetzen:

1. Unterbrechen Sie die Stromversorgung von blue2net.

2. Greifen Sie von einem Web-Browser über LAN oder Bluetooth auf blue2net zu. Loggen Sie sich in die blue2net-Konfigurationsfunktion ein (blue2net-IP-Adresse [4.2.1] erforderlich!). Klicken Sie auf <edit> neben 'Activation Commands' [6], dann auf <edit> neben 'Reset blue2net' [6.3] und aktivieren Sie die Funktion durch Klicken auf <Submit>.

Hinweis: Wenden Sie sich im Zweifelsfall an den Netzwerk-Administrator oder informieren Sie sich im entsprechenden Kapitel der Bedienungsanleitung.

3.9.2 Save Settings Permanently [6.2]

Einstellungen dauerhaft abspeichern [6.2]

Änderungen, die Sie an einer oder mehreren Einstellungen durchführen, werden nicht wirksam, solange sie nicht abgespeichert sind. Beachten Sie das bitte besonders in Zusammenhang mit Sicherheitseinstellungen.

Abspeichern können Sie Änderungen entweder

- *vorübergehend* (z.B. für eine laufende Sitzung), indem Sie 'Save Settings Temporarily' [6.1] auswählen, oder
- *dauerhaft* (bis weitere Änderungen dort gespeichert werden), indem Sie 'Save Settings Permanently' [6.2] auswählen.

'Save Settings Permanently' speichert geänderte Einstellungen in einem Permanent-Speicher, bis weitere Änderungen dort gespeichert werden.

Wenn Sie 'Bluetooth Parameters' [1.#] und/oder 'IP Parameters for Terminals' [3.#] konfiguriert haben und dann 'Save Settings Permanently' ausführen, während Sie über Bluetooth verbunden sind, wird diese Verbindung unterbrochen und muss neu hergestellt werden.

Hinweis: Sorgen Sie dafür, dass bestehende Bluetooth-Verbindungen anderer Terminals geordnet beendet werden, bevor Sie diese Funktion ausführen.

Vorsicht! Erwägen Sie, Ihre Einstellungen zuerst zu testen, wie dies unter 'Save Settings Temporarily' (Kapitel 3.9.1) beschrieben wurde, denn wenn Sie sich durch falsche Einstellungen *aussperren*, haben sie im schlimmsten Fall (siehe Kapitel 5.1) nur die Möglichkeit, das Gerät zum Kundendienst (siehe Kapitel 14) zu bringen und dort auf Werkseinstellungen zurücksetzen zu lassen. Informieren Sie sich bitte auch in Kapitel 5, wie Sie Aussperrung verhindern können.

Hinweis: Wenden Sie sich im Zweifelsfall an den Netzwerk-Administrator oder informieren Sie sich im entsprechenden Kapitel der Bedienungsanleitung.

3.9.3 Reset blue2net [6.3]

blue2net rücksetzen [6.3]

Mit dieser Funktion können Sie Einstellungen reaktivieren, die im Permanent-Speicher abgespeichert sind.blue2net wird dabei mit den Einstellungen aus dem Permanent-Speicher gestartet.

Diese Funktion hat die gleiche Wirkung wie ein Unterbrechen der Stromversorgung und ist besonders dann nützlich, wenn der Installationsort des Gerätes oder der Netzstecker nicht leicht zugänglich ist.

Zu beachten ist, dass Einstellungen, die nur temporär gespeichert wurden, verloren gehen.

Hinweis: Sorgen Sie dafür, dass bestehende Bluetooth-Verbindungen anderer Terminals geordnet beendet werden, bevor Sie diese Funktion ausführen.

Eine Bluetooth-Verbindung kann erst nach einer Wartezeit von 2 Minuten nach Aktivierung des Befehls „Reset blue2net“ neuerlich aufgebaut werden.

Hinweis: Wenden Sie sich im Zweifelsfall an den Netzwerk-Administrator oder informieren Sie sich im entsprechenden Kapitel der Bedienungsanleitung.

3.9.4 Update Software [6.4]

Software-Update [6.4]

Der Hersteller von blue2net könnte Software-Updates bereitstellen, um die Leistung des Gerätes zu verbessern oder Fehler und Mängel zu beheben.

Besuchen Sie von Zeit zu Zeit die blue2net-Homepage, um von Updates Kenntnis zu erlangen.

'Update Software' muss aktiviert werden, nachdem die neue Software von der Service-Homepage heruntergeladen und in das Dateisystem von blue2net übertragen wurde.

Details zum Ablauf sind in Kapitel 6 ersichtlich.

Hinweis: Wenden Sie sich im Zweifelsfall an den Netzwerk-Administrator oder informieren Sie sich im entsprechenden Kapitel der Bedienungsanleitung.

3.9.5 Restore Default Settings [6.5]

Werkseinstellungen wiederherstellen [6.5]

'Restore Default Settings' setzt alle Konfigurationswerte auf voreingestellte Werte (Werkseinstellung) zurück. Welche Werte das sind, ist aus der Liste in Kapitel 12 ersichtlich.

Alle benutzerdefinierten Werte werden dabei unwiderruflich zurückgesetzt. Um Ihre eigenen Werte wiederherzustellen, müssten Sie alle diese Werte neuerlich eingeben.

Verwenden Sie 'Restore Default Settings' als einen möglichen Weg, um ggf. Kontrolle über alle Parameter wiederzugewinnen, indem Sie alle eigenen Einstellungen auf Vorgabewerte zurücksetzen und danach neu konfigurieren.

Hinweis: Wenden Sie sich im Zweifelsfall an den Netzwerk-Administrator oder informieren Sie sich im entsprechenden Kapitel der Bedienungsanleitung.

3.9.6 Store Specific Homepage [6.6]

blue2net-eigene Homepage (Specific Homepage) speichern [6.6]

Verwenden Sie die Funktion 'Store Specific Homepage', um Ihre eigenen Anwendungen (z.B. HTML-Files, Spiele) in den Permanent-Speicher von blue2net zu laden. Diese können Sie danach auf der Homepage des Web-Interface aufrufen (Abb. 3).

Details zum Ladevorgang sind in Kapitel 7.1 dargestellt.

Hinweis: Wenden Sie sich im Zweifelsfall an den Netzwerk-Administrator oder informieren Sie sich im entsprechenden Kapitel der Bedienungsanleitung.

4 Einsatz-Szenarien

Dieses Kapitel soll es Ihnen erleichtern, Konfigurationseinstellungen für typische Einsatzgebiete schnell und einfach vorzunehmen, besonders zu Beginn, wenn Sie mit den Konfigurationsfunktionen noch nicht vertraut sind. Es ist nicht beabsichtigt, alle möglichen Szenarien damit abzudecken. Für Ihre speziellen Sicherheitsanforderungen und Präferenzen könnte es nötig sein, blue2net entsprechend anzupassen. Bitte beachten Sie besonders Kapitel 5 „Aussperrung verhindern“.

4.1 Business-Szenario mit kontrolliertem Zugang

Typisches Szenario: Besprechungszimmer, wo Teilnehmern ein voreingestelltes Bluetooth-Passwort [1.12] oder temporärer Zugang gewährt wird.
Charakteristik: Die Sicherheitsstufe ist hoch, nur ausgewählte Personen haben Zugang zum LAN, nur berechtigte Personen haben Zugang zur Konfiguration.

Parameter	Hier. stufe	eingestellt auf	Begründung
Bluetooth Device Name	[1.1]	Name Ihrer Wahl (1...16 Zeichen)	In einer Umgebung mit mehreren blue2net-Geräten sollte jedes einen eindeutigen Namen zur klaren Unterscheidung haben.
Terminal Table	[1.10]	Kein Terminal registriert (Bluetooth-Adresse auf 00:00:00:00:00:00 gesetzt)	Alle Benutzer sollen mit dem voreingestellten Bluetooth-Passwort 'Default Bluetooth Passkey' [1.12] Zugang haben.
Default Access Mode	[1.11]	enabled (Voreinstellung)	Jedes Terminal hat Zugang zum LAN, braucht aber den 'Default Bluetooth Passkey' [1.12], da 'Auth. Level' [1.8.4] auf *auth* oder *authandenc* gesetzt ist.
Default Bluetooth Passkey	[1.12]	Passwort Ihrer Wahl (1…16 Zeichen)	Das Passwort wird nur autorisierten Personen bekannt gegeben. Aus Sicherheitsgründen sollten Sie das Passwort öfters ändern!

Parameter	Hier. stufe	eingestellt auf	Begründung
Auth. Level	[1.8.4]	auth oder authandenc	Zugang erlangen bei dieser Einstellung nur Personen, die das Bluetooth-Passwort 'Default Bluetooth Passkey' [1.12] kennen.
Terminal IP Address Resolution	[3.1]	masquerading (Voreinstellung)	Für die Terminals sind bei dieser Einstellung keine IP-Adressen erforderlich.
Configuration Password	[5.2]	Passwort Ihrer Wahl (4…22 Zeichen)	Nur autorisierte Personen (z.B. der System-Administrator) können blue2net konfigurieren. Achtung! Vergessen Sie das neue Passwort nicht

Tabelle 25 Einstellungen für den Businessbereich bei kontrolliertem Zugang

4.2 Szenario mit öffentlichem Zugang (Hot Spot)

Typisches Szenario: Aufenthaltsräume in Flughäfen und Hotels, Internet-Cafès.
Charakteristik: Schneller und leichter Zugang ohne Berechtigung für jedermann, nur berechtigte Personen haben Zugang zur Konfiguration.

Parameter	Hier. stufe	eingestellt auf	Begründung
Bluetooth Device Name	[1.1]	Name Ihrer Wahl (1…16 Zeichen)	Erforderlich, um ein blue2net unter anderen Bluetooth-Geräten zu erkennen. In einer Umgebung mit mehreren blue2net-Geräten sollte jedes einen eindeutigen Namen zur klaren Unterscheidung haben.
Terminal Table	[1.10]	Bluetooth-Adresse [1.10.2], Bluetooth-Passwort [1.10.3] und IP-Adresse [1.10.4] der bei Ihnen am häufigsten verwendeten Terminals	Sie wollen „VIPs" eine eigene fixe Terminal-IP-Adresse zugestehen. Setzen Sie in diesem Fall 'Terminal IP Address Resolution' [3.1] auf *masqueradingpool*. .
Default Access Mode	[1.11]	enabled (Voreinstellung)	Leichter Zugang für jedermann
Auth. Level	[1.8.4]	noauth (Voreinstellung)	Bei 'Hot Spot'-Szenarien gestatten Sie jedermann den Zugang zu Ihren Einrichtungen.

Parameter	Hier. stufe	eingestellt auf	Begründung
Terminal IP Address Resolution	[3.1]	masqueradingpool	Verwenden Sie diese Einstellung, wenn Sie „VIPs" besonders betreuen wollen. Für die VIP-Terminals müssen Sie dann im 'Terminal Table' [1.10] IP-Adressen [1.10.4] eintragen.
Terminal IP Address Resolution	[3.1]	masquerading (Voreinstellung)	Für die Terminals sind bei dieser Einstellung keine IP-Adressen erforderlich.
Configuration Password	[5.2]	Passwort Ihrer Wahl (4…22 Zeichen)	Nur autorisierte Personen (z.B. der System-Administrator) können blue2net konfigurieren. Achtung! Vergessen Sie das neue Passwort nicht!

Tabelle 26 Einstellungen für Szenarien mit öffentlichem Zugang (Hot Spot)

4.3 Heimanwender-Szenario mit Kabel-Modem

Typisches Szenario: Mehrere Familienmitglieder wollen Zugang zum Internet über ein Kabel-Modem haben. DHCP ist am Server des ISP verfügbar, nur eine berechtigte Person hat Zugang zur Konfiguration.
Charakteristik: Aus Sicherheitsgründen muss blue2net gegen einen Zugriff durch Nachbarn und nicht berechtigte Personen außerhalb der Wohnung oder des Hauses geschützt werden. Eine Firewall kann zum Schutz des PC installiert werden.

Parameter	Hier. stufe	eingestellt auf	Begründung
Bluetooth Device Name	[1.1]	Name Ihrer Wahl (1...16 Zeichen)	Erforderlich, um ein blue2net unter anderen Bluetooth-Geräten zu erkennen.
Default Access Mode	[1.11]	enabled (Voreinstellung)	Sie können jedes Ihrer Bluetooth-Terminals einsetzen.
Default Bluetooth Passkey	[1.12]	Passwort Ihrer Wahl (1…16 Zeichen)	Zugang durch Nicht-Familienmitglieder vermeiden. Achtung! Vergessen Sie das neue Bluetooth-Passwort nicht.
Auth. Level	[1.8.4]	authandenc	Zugang durch Nicht-Familien-mitglieder vermeiden. Achtung! Vergessen Sie nicht das eingestellte Bluetooth-Passwort.

Parameter	Hier. stufe	eingestellt auf	Begründung
Firewall Settings	[2.6.1]	enabled	Um Angriffen von LAN-Seite her (z.B. Kabel-Modem / Internet) vorzubeugen. Details zu den Regeln siehe Kapitel 9.
Terminal IP Address Resolution	[3.1]	masquerading (Voreinstellung)	Für die Terminals sind bei dieser Einstellung keine IP-Adressen erforderlich.
Configuration Password	[5.2]	Passwort Ihrer Wahl (4…22 Zeichen)	Nur autorisierte Personen (z.B. der System-Administrator) können blue2net konfigurieren. Achtung! Vergessen Sie das neue Passwort nicht.

Tabelle 27 Einstellungen für den Heimanwender

Hinweis: Wenn Internetadressen nach der Eingabe im Browser nicht aufgelöst werden (Fehlermeldung: Die Seite wurde nicht gefunden...), könnte es daran liegen, dass die DNS-IP-Adressen 1 u. 2 durch den DHCP-Server nicht richtig übermittelt werden können. Tragen Sie diese in so einem Fall bitte manuell ein ([3.5.1] und [3.5.2]). Die Werte der DNS-IP-Adressen erhalten Sie vom ISP.

4.4 Heimanwender-Szenario mit xDSL-Modem

Typisches Szenario: Mehrere Familienmitglieder wollen Zugang zum Internet über ein xDSL-Modem haben. Nur eine berechtigte Person hat Zugang zur Konfiguration.
Charakteristik: Aus Sicherheitsgründen muss blue2net gegen einen Zugriff durch Nachbarn und nicht berechtigte Personen außerhalb der Wohnung oder des Hauses geschützt werden (Bluetooth-Verbindungen absichern!)

Parameter	Hier. stufe	eingestellt auf	Begründung / Hinweis
Bluetooth Device Name	[1.1.1]	Name Ihrer Wahl (1...16 Zeichen)	Erforderlich, um ein blue2net unter anderen Bluetooth-Geräten zu erkennen.
Default Access Mode	[1.11]	enabled (Voreinstellung)	Sie können jedes Ihrer Bluetooth-Terminals einsetzen.
Default Bluetooth Passkey	[1.12]	Passwort Ihrer Wahl (1…16 Zeichen)	Zugang durch Nicht-Familien-mitglieder vermeiden. Achtung! Vergessen Sie das neue Bluetooth-Passwort nicht.
Auth. Level	[1.8.4]	authandenc	Zugang durch Nicht-Familien-mitglieder vermeiden. Achtung! Vergessen Sie nicht das eingestellte Bluetooth-Passwort.

Parameter	Hier. stufe	eingestellt auf	Begründung / Hinweis
blue2net IP Address Resolution	[2.1]	predefined	Das xDSL-Modem kann keine DHCP-Anfragen beantworten.
PPTP Server IP Address	[2.7.4]	vorgegebene IP-Adresse (könnte z.B. lauten: 10.0.0.138)	Falls für Ihren xDSL-Zugang das PPTP-Protokoll verwendet wird, tragen Sie hier die vorgegebene IP-Adresse ein. Entnehmen sie diese IP-Adresse aus den Unterlagen ihres xDSL-Modems oder kontaktieren sie ihren xDSL-Anbieter
Fixed blue2net IP Address	[2.2.1]	Beispiel: [2.7.4]: 10.0.0.138 (vorgegebener Wert vom Provider oder aus der Beschreibung zum xDSL-Modem) [2.2.2]: 255.255.255.0 (Werkseinstellung des blue2net) [2.2.1]: 10.0.0.140 'Fixed blue2net IP Address', die im gleichen IP-Netz wie [2.7.4] liegt.	Wenn 'Tunnel Mode' [2.7.1] auf *pppoe* gestellt ist, können die Werkseinstellungen (siehe Kapitel 12) für diese Werte belassen werden. Wenn 'Tunnel Mode' [2.7.1] auf *pptp* gestellt ist, sind die Werte dieser Parameter so einzustellen, dass 'Fixed blue2net IP Address' im gleichen IP-Netz liegen, wie die vom xDSL-Modem vorgegebene IP-Adresse 'PPTP Server IP Address' [2.7.4].
Fixed blue2net Netmask	[2.2.2]		
Fixed blue2net Gateway	[2.2.3]	0.0.0.0.	Für diese Betriebsart ist dieser Wert erforderlich.
Tunnel Mode	[2.7.1]	pppoe oder /pptp	Bringen Sie bei Ihrem xDSL-Provider in Erfahrung, welches Tunnel-Protokoll für ihren xDSL-Zugang zu verwenden ist.
Tunnel User Name	[2.7.3.1]	zugewiesener User Name	Bringen Sie bei Ihrem xDSL-Provider den Ihnen zugewiesenen 'User Name' in Erfahrung.
Tunnel User Password	[2.7.3.2]	zugewiesenes User Password	Bringen Sie bei Ihrem xDSL-Provider das Ihnen zugewiesene 'User Password' in Erfahrung.
Terminal IP Address Resolution	[3.1]	masquerading (Voreinstellung)	Für die Terminals sind bei dieser Einstellung keine IP-Adressen erforderlich.

Parameter	Hier. stufe	eingestellt auf	Begründung / Hinweis
Configuration Password	[5.2]	Passwort Ihrer Wahl (4…22 Zeichen)	Nur autorisierte Personen (z.B. der System-Administrator) können blue2net konfigurieren. Achtung! Vergessen Sie das neue Passwort nicht.

Tabelle 28 Einstellungen für den Heimanwender mit xDSL-Modem

5 Aussperrung verhindern

Unter den Einstellungen gibt es einige, die besondere Beachtung verdienen. Falsche Einstellungen, Passwörter oder IP-Adressen könnten Sie vom Zugang zu blue2net über Bluetooth oder Ethernet (LAN) oder beides aussperren.

Das ist keine Fehlfunktion von blue2net. Aus Sicherheitsgründen sind einige Einstellungen unumgänglich, könnten aber unter den unten beschriebenen Umständen Aussperrung vom Zugang verursachen.

Es wird deshalb empfohlen, diese Einstellungen besonders zu beachten.

Führen Sie Aufzeichnungen zu den folgenden Einstellungen:

- 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 Kombination mit [1.10.3])
- Terminal Bluetooth Passkey [1.10.3] (in Kombination mit [1.10.2])

Bewahren Sie diese an einem sicheren Platz getrennt von blue2net, der Bedienungsanleitung, dem PC, Laptop oder PDA auf.

Bitte beachten Sie auch die Anweisungen betreffend das Abspeichern der Einstellungen wie in Kapitel 3.9.2 beschrieben und zeichnen Sie *permanent gespeicherte Einstellungen* auf.

5.1 Aussperrung vom Zugang über Bluetooth und Ethernet (LAN)

Parameter	Hier. stufe	Vor der Umstellung auf	ist zu beachten
Configuration Password	[5.2]	eigenes, neues Passwort	Wenn Sie das Konfigurations-Passwort ändern, was Sie aus Sicherheitsgründen tun sollten, sorgen Sie bitte dafür, dass Sie das neue Passwort nicht vergessen! Andernfalls würden Sie vom Konfigurationszugang ausgesperrt. Sie müssten das Gerät dann zum Kundendienst bringen oder einsenden, um es auf die Vorgabewerte rücksetzen zu lassen.

Tabelle 29 Aussperrungs-Szenarien: Aussperrung vom Zugang über Bluetooth und Ethernet (LAN)

5.2 Aussperrung vom Zugang über Bluetooth

Parameter	Hier. stufe	Vor der Um-stellung auf	ist zu beachten
Connectability Mode	[1.5]	nonconnectable	Die einzige Zugangsmöglichkeit zu Ihrem blue2net besteht über das Ethernet (LAN). Eine Bluetooth-Verbindung ist nicht mehr möglich.
Max. No. of Terminals Connected	[1.6]	0	
Auth. Level	[1.8.4]	auth oder authandenc	Wenn Sie die Authentifizierung aktivieren, was Sie aus Sicherheits-gründen tun sollten, sorgen Sie bitte dafür, dass Sie die eingetragenen Bluetooth-Passwörter [1.12] und [1.10.3] der Terminals in Erinnerung behalten.
Default Access Mode	[1.11]	disabled	Nur Terminals, die in der Tabelle 'Terminal Table' [1.10] aufscheinen, haben Zugangsrechte. Vergewissern Sie sich, dass Sie für jedes dieser Terminals die 'Terminal Bluetooth Address' [1.10.2] und das zugehörige Bluetooth-Passwort [1.10.3] kennen. Wenn keine Terminals in 'Terminal Table' [1.10], registriert sind, haben Sie keinen Zugang
Default Bluetooth Passkey	[1.12]	neues Passwort	Wenn Sie das Bluetooth-Passwort 'Default Bluetooth Passkey' ändern, was Sie aus Sicherheitsgründen tun sollten, sorgen Sie bitte dafür, dass Sie das neue Passwort nicht vergessen! Wenn Sie in 'Terminal Table' [1.10] keine Terminals registriert haben, werden Sie keinen Zugang erhalten.
Terminal IP Address Resolution	[3.1]	dhcp	Falls kein DHCP-Dienst verfügbar ist, bekommt blue2net nie eine IP-Adresse für ein Terminal, und somit ist keine Verbindung möglich.

Tabelle 30 Aussperrungs-Szenarien: Aussperrung vom Zugang über Bluetooth

5.3 Aussperrung vom Zugang über Ethernet (LAN)

Parameter	Hier. stufe	Vor der Umstellung auf	ist zu beachten
blue2net IP Address Resolution	[2.1]	predefined	Vergewissern Sie sich, dass Sie die fixen blue2net-IP-Adressen kennen; das sind die 'Fixed blue2net IP Address' [2.2.1] und die 'Fixed blue2net Netmask' [2.2.2].
blue2net IP Address Resolution	[2.1]	dhcp wenn DHCP aber nicht verfügbar ist	Vergewissern Sie sich, dass Sie die blue2net-Rückfall-IP-Adressen kennen; das sind die 'Fallback blue2net IP Address' [2.3.1] und die 'Fallback blue2net Netmask' [2.3.2].

Tabelle 31 Aussperrungs-Szenarien: Aussperrung vom Zugang über Ethernet (LAN)

6 Software-Update

Die Software-Update-Funktion ermöglicht Ihnen die Nutzung der neuesten Features und Verbesserungen.

Hinweis: Nach dem Software-Update haben Sie die gleichen Einstellungen der Parameter wie zuvor. Einstellungen, die im Permanent-Speicher abgespeichert waren, müssen nicht mehr neu eingegeben werden.

Besuchen Sie von Zeit zu Zeit die blue2net-Homepage, um über Updates sowohl an der Software als auch an der Bedienungsanleitung informiert zu sein.

Ein Software-Update wird erst wirksam, nachdem blue2net einen erneuten Systemstart (Reboot) durchgeführt hat.

6.1 Das Herunterladen neuer Software

Hinweis: Während des Update-Vorganges darf die Stromversorgung nicht unterbrochen werden. Sollte dies doch geschehen, muss blue2net an den Kundendienst eingeschickt werden.

Der Update-Vorgang über das Ethernet (LAN) ist nur möglich, wenn die Firewall *deaktiviert* ist. Siehe dazu Kapitel 2.8, 3.5 und 3.5.3.

Während des Update-Vorganges blinkt die LED sehr schnell.

Hinweis: Im Falle von Unklarheiten wenden Sie sich bitte an den Netzwerk-Administrator.

Wie erhält man eine neue Software-Version?

1. Verwenden Sie einen an das Internet angeschlossenen PC oder Laptop.
2. Besuchen Sie unsere Homepage 'http://www.siemens.at/bluetooth' von Ihrem PC oder Laptop aus.
3. Laden Sie die neueste Software-Version (b2n_image...) herunter und speichern Sie diese auf Ihrer Festplatte (z.B. unter C:\temp\).
4. Öffnen Sie Ihren Web-Browser und Ihren Datei-Manager (z.B. Windows Explorer) und richten Sie am besten beide Fenster auf dem Bildschirm nebeneinander ein (siehe Abb. 28).
5. Stellen Sie eine Verbindung zu Ihrem blue2net über LAN (Firewall muss deaktiviert sein!) oder Bluetooth her.
6. Ermitteln Sie Ihre blue2net-IP-Adresse [4.2.1] (z.B. über das blue2net Web-Interface (siehe Abb. 3): Klicken Sie auf 'Configuration' / Klicken Sie auf <edit> neben 'Current Configuration' / Klicken Sie auf 'Objects' neben

'blue2net IP Configuration' / Lesen Sie die IP-Adresse neben 'blue2net IP Address' ab).

7. Geben Sie bei Ihrem Web-Browser im Adressfeld '**ftp://config@< blue2net IP Address >/tmp/**' ein (siehe Abb. 28) und drücken Sie die'Enter'-Taste.

8. Geben Sie nach der Eingabeaufforderung in das Login-Eingabefeld den Benutzernamen „config" sowie das Konfigurations-Passwort (Voreinstellung heisst „changeme") ein.

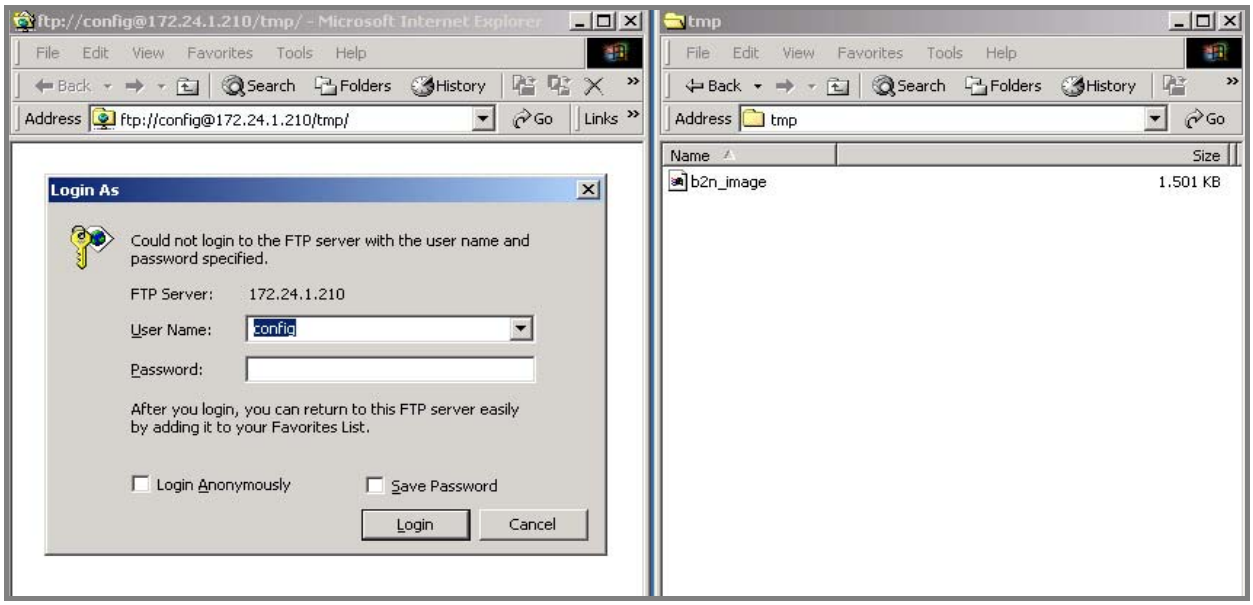

Abb. 28 Software-Update: Login auf blue2net

9. Kopieren Sie die Datei „**b2n_image...**" vom Festplattenverzeichnis (z.B. C:\temp\) in das blue2net-Dateisystem, z.B. durch „drag and drop".

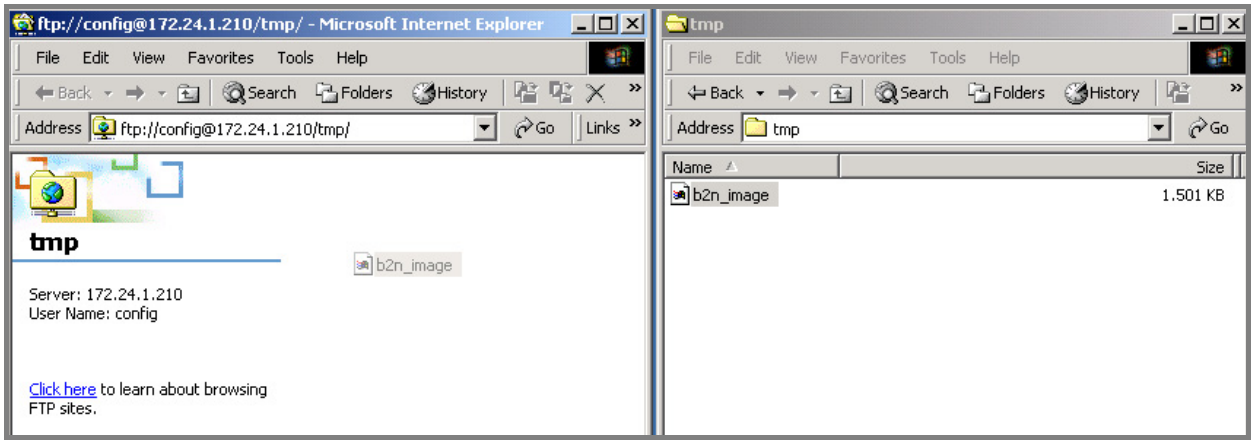

Abb. 29 Software-Update: Image-Datei auf blue2net ziehen

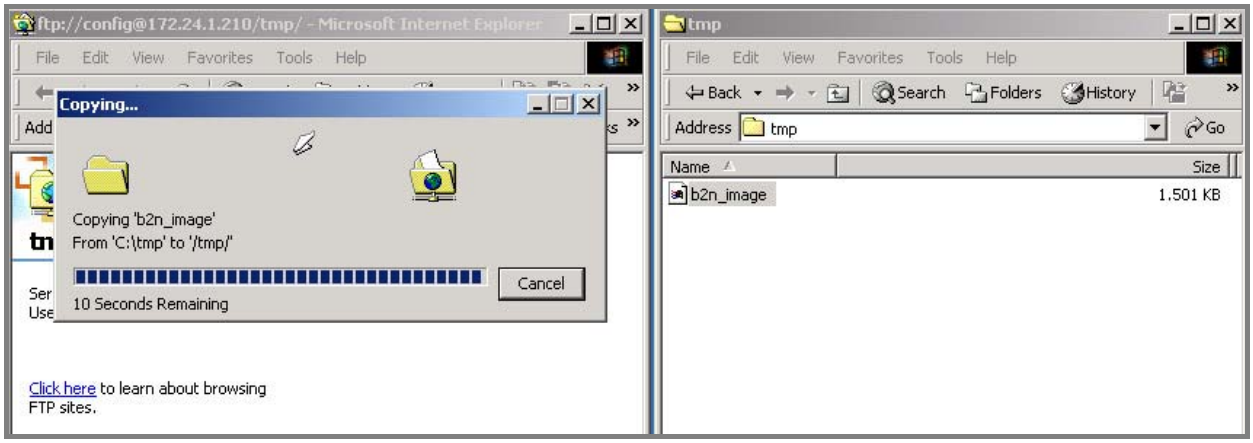

Abb. 30 Software-Update: Kopierfortschritt

Speichern der neuen Software

10. Wechseln Sie nach dem Kopieren zur blue2net-Haupt-Konfigurations-Seite (siehe Abb. 4).

11. Vergewissern Sie sich, dass alle anderen Benutzer ihre Bluetooth-Verbindungen geordnet beendet haben.

12. Klicken Sie auf <edit> neben 'Activation Commands' [6].

13. Klicken Sie auf <edit> neben 'Update Software' [6.4].

14. Klicken Sie auf <Submit>, um die neue Software abzuspeichern und wirksam werden zu lassen nach dem Reboot.

Abb. 31 Software-Update: dauerhaft speichern

Der Updatevorgang wird damit gestartet. Dies wird mittels schnellen Blinkens der Anzeige-LED signalisiert.

Sollten Sie den Updatevorgang über eine Bluetooth-Verbindung initiiert haben, wurde diese jetzt wegen des Updatevorgangs abgebrochen. Sie sollten dann aber die Anzeige-LED beobachten, um nach 2 - 10 Minuten (siehe unten: „Das Ergebnis des Updateprozesses überprüfen“) feststellen zu können, ob der Updatevorgang erfolgreich abgeschlossen wurde.

Sollten Sie den Updatevorgang über eine LAN-Verbindung initiiert haben, können Sie am Webbrowser den Fortschritt verfolgen.

Achtung! Während des Update-Prozesses dürfen Sie keine Funktion im Browser aktivieren (anklicken) oder die Spannungsversorgung unterbrechen, da sonst Schäden bis zur Unbrauchbarkeit von blue2net die Folge wären.

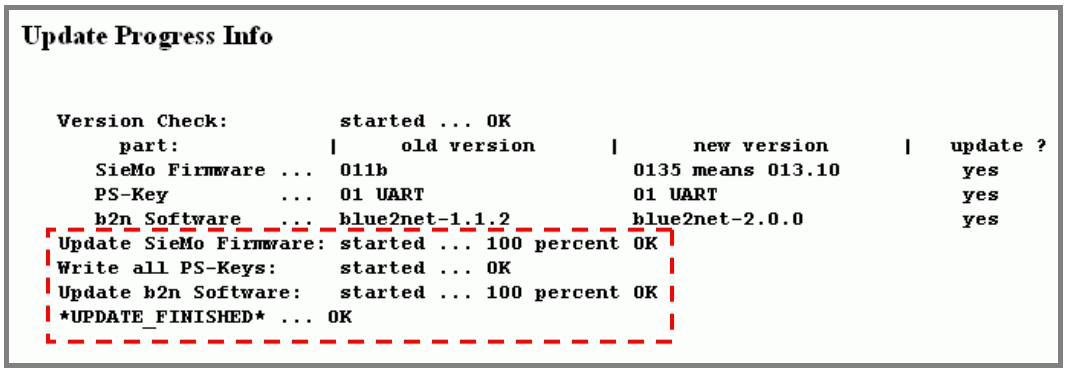

Abb. 32 Fortschritt des Software-Update-Prozesses

Fortschritt des Update-Prozesses

Beim Updateprozess wird überprüft, welche Teile (Bluetooth-Modul, blue2net-Software, Keys) upgedated werden müssen, um dann die erforderlichen Updates durchzuführen. Dies kann 2 – 10 Minuten dauern.

15. Das Ergebnis des Updateprozesses überprüfen

- **Bei erfolgreichem Update** wird die Anzeige-LED für ca. 30 sec. auf Dauerleuchten geschaltet bzw. im Webbrowser (NICHT bei Initiierung über Bluetooth!) eine entsprechende Meldung angezeigt.

  Anschließend wird blue2net mit der neuen Softwareversion erneut gestartet (Reboot), was ca. 2 Minuten dauert (normales, langsames Blinken der Anzeige-LED). Bereits im Permanent-Speicher befindliche Einstellungen bleiben unverändert.

  Die neue Software ist danach bereit zur Verwendung.

- **Bei nicht erfolgreichem Update** wird die Anzeige-LED für ca. *30 sec. auf „aus“ geschaltet*, anschließend wird der Reboot-Vorgang gestartet (normales, langsames Blinken der Anzeige-LED).

  Falls der Update-Vorgang nicht erfolgreich war, sollten Sie eine Wiederholung desselben versuchen. Bei erneutem Fehlschlagen wird empfohlen, sich an den Kundendienst (siehe Kapitel 14) zu wenden. Halten Sie dann auch die Rückmeldung der Statusinformation (nur bei Initiierung über LAN möglich) am Webbrowser bereit.

7 Speichern der spezifischen Homepage

Für die Nutzung dieser Funktion sind Kenntnisse über die Erstellung von Web-Seiten sowie über das Linux-Tool „tar" erforderlich.

Es besteht die Möglichkeit, spezifische Homepages auf blue2net zu speichern. Linux „tar" dient hier als nützliches Werkzeug, um HTML-Dateien zu bündeln und diese in der Datei **b2n_user.gz** komprimiert abzulegen. Die Größe dieser komprimierten Datei darf 60 Kbytes nicht überschreiten.

Der entsprechende Befehl beim Linux-Tool lautet:
`tar -cvzf b2n_user.gz <your HTML source directory>`.

Die spezifische Homepage ist nach dem von blue2net durchgeführten Systemstart (Reboot) verfügbar und permanent abgespeichert.

7.1 Das Laden der spezifischen Homepage

Das Laden der spezifischen Homepage auf Ihr blue2net erfolgt ähnlich wie der Vorgang beim Software-Update (siehe Kapitel 6).

Das Laden der spezifischen Homepage über Ethernet (LAN) ist nur möglich, wenn die Firewall *deaktiviert* ist. Siehe dazu die Kapitel 2.7, 3.5 and 3.5.3.

Laden der Datei für die spezifische Homepage:

1. Öffnen Sie Ihren Web-Browser und Ihren Datei-Manager (z.B. Windows Explorer) und richten Sie am besten beide Fenster auf dem Bildschirm nebeneinander ein (siehe Abb. 33).

2. Stellen Sie eine Verbindung zu Ihrem blue2net über LAN (Firewall muss deaktiviert sein!) oder Bluetooth her.

3. Erfragen Sie Ihre blue2net-IP-Adresse [4.2.1] (z.B. über das blue2net-Web-Interface (siehe Abb. 3): Klicken Sie auf 'Configuration' / Klicken Sie auf <edit> neben 'Current Configuration' / Klicken Sie auf 'Objects' neben 'blue2net IP Configuration' / Lesen Sie die IP-Adresse neben 'blue2net IP Address' ab).

4. Geben Sie bei Ihrem Web-Browser im Adressfeld **'ftp://config@< blue2net IP Address >/tmp/**' ein (siehe Abb. 33).

5. Geben Sie nach der Eingabeaufforderung in das Login-Eingabefeld den Benutzernamen „config" sowie das Konfigurations-Passwort (Voreinstellung heißt „changeme") ein.

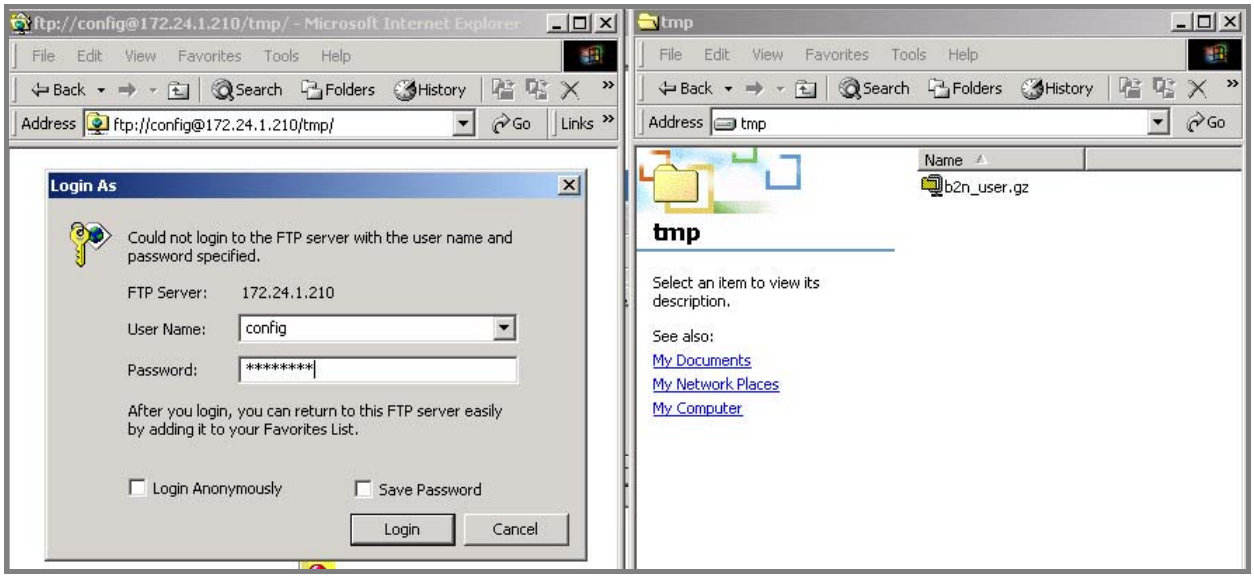

Abb. 33 Spezifische Homepage: Login auf blue2net

6. Kopieren Sie die Datei „**b2n_user.gz**" vom Festplattenverzeichnis (z.B. C:\temp\) in das blue2net-Dateisystem, z.B. durch „drag and drop".

7. Wechseln Sie nach dem Kopieren zur blue2net-Haupt-Konfigurations-Seite (siehe Abb. 4).

Temporäres Speichern der spezifischen Homepage:

8. Klicken Sie auf <edit> neben 'Activation Commands' [6].

9. Klicken Sie auf<edit> neben 'Store Specific Homepage' [6.6].

10. Durch Klicken auf <Submit> wird die Homepage in blue2net (zunächst temporär) gespeichert.

    ACHTUNG! Nach diesem Schritt ist die Homepage nicht dauerhaft abgespeichert. Es besteht hingegen die Möglichkeit zu überprüfen, ob die Homepage auf dem Bildschirm richtig dargestellt wird oder nicht. Sollten Sie diese nach der Überprüfung permanent abspeichern wollen, fahren Sie folgendermaßen fort:

Abb. 34 Spezifische Homepage: Temporäres Speichern der spezifischen Homepage

Dauerhaftes Speichern der spezifischen Homepage:

11. Vergewissern Sie sich, dass alle anderen Benutzer die von ihnen eingerichteten Bluetooth-Verbindungen geordnet beendet haben.
12. Öffnen Sie die blue2net-Haupt-Konfigurations-Seite (siehe Abb. 4).
13. Klicken Sie auf <edit> neben 'Activation Commands' [6].
14. Klicken Sie auf <edit> neben 'Save Settings Permanently' [6.2].
15. Speichern Sie Ihre spezifische Homepage durch Klicken auf <Submit>.
16. Nun wird blue2net erneut gestartet (Reboot). Dieser Vorgang kann bis zu 2 Minuten dauern.

Ihre spezifische Homepage ist somit bereit zur Verwendung.

8 Fehlerbehebung

Dieser Abschnitt bietet Hilfestellung bei der Bewältigung eventueller Schwierigkeiten.

Berücksichtigen Sie bitte auch, dass etwaige Störungen (z.B. fehlgeschlagene Herstellung oder Aufrechterhaltung einer stabilen Bluetooth-Verbindung) oder eine verminderte Datenübertragungsrate auch aus Mängeln in Ihrem Bluetooth-Terminal, gegebenenfalls auch in Verbindung mit dem Betriebssystem auf Terminal-Seite, resultieren können.

8.1 Hardware

Problem	Mögliche Ursache	Mögliche Lösung
LED-Anzeige leuchtet nicht	Fehlerhaftes Netzgerät	Überprüfen des Netzgerätes
LED-Anzeige leuchtet nicht ununterbrochen	Mangelhafte Systemeinstellungen	Unterbrechen und Wiederherstellen der Stromversorgung
Kein Zugang zum Netz	Beschädigte Netzwerkkabel, -stecker oder -steckdosen	Überprüfen der Verbindung zum Netz

Tabelle 32 Fehlerbehebung: Hardware

8.2 Bluetooth-Verbindung

Problem	Mögliche Ursache	Mögliche Lösung
blue2net vom Bluetooth-Terminal aus nicht auffindbar	Mögliche Ursachen siehe unter „Datenübertragungsrate ist sehr niedrig.“ weiter unten in der Tabelle.	Mögliche Lösungen siehe unter „Datenübertragungsrate ist sehr niedrig.“ weiter unten in der Tabelle.
	blue2net 'Discoverability Mode' [1.4] auf *nondiscoverable* gesetzt.	Einstellen des blue2net 'Discoverability Mode' [1.4] auf *discoverable*
Ein Dienst ist von blue2net nicht sichtbar.	Die größtmögliche Zahl an Terminals wurde bereits zu blue2net verbunden.	Überprüfen der Werte 'Max. No. of Terminals connected' [1.6] und 'Multipoint Mode' [1.3]
	'Connectability Mode' [1.3] ist auf *disabled* gesetzt.	'Connectability Mode' [1.3] auf *enabled* setzen

Problem	Mögliche Ursache	Mögliche Lösung
Verbindung zwischen blue2net und dem Bluetooth-Terminal nicht möglich.	Manche Terminals unterstützen das „LAN Access Profile" nicht.	Derzeit unterstützt blue2net nur das „LAN Access Profile".
	'Default Access Mode' [1.11] wurde auf *disabled* gesetzt.	'Default Access Mode' [1.11] auf *enabled* setzen oder 'Terminal BT-Address' [1.10.2] des Bluetooth-Terminals in die 'Terminal Table' [1.10]. eintragen.
	Das Bluetooth-Terminal ist in der Tabelle 'Terminal Table' [1.10] registriert.	Verwenden Sie das in der Tabelle 'Terminal Table' [1.10] vorgesehene Passwort 'Terminal Bluetooth Passkey' [1.10.3].
Datenübertragungsrate ist sehr niedrig.	Bluetooth-Funksignalstärke ist zu niedrig.	1. Überprüfen der Ausrichtung des blue2net-Gehäuses (siehe Abb. 1). 2. Verringern des Abstandes zwischen blue2net und den Bluetooth-Terminals. 3. Überprüfen, ob es zwischen blue2net und den Bluetooth-Terminals Objekte gibt, welche die Funksignale stören.
	Funksignal ist gestört (z.B. von Mikrowellenherd).	Position von blue2net ändern (siehe Kapitel 2.2).

Tabelle 33 Fehlerbehebung: Bluetooth-Verbindung

8.3 Zugang zum LAN/Internet

Problem	Mögliche Ursache	Mögliche Lösung
LAN nicht erreichbar (z.B. Internet-Zugang nicht möglich).	IP-Parameter für blue2net [2] sind nicht geeignet für Ihr LAN.	Überprüfen der IP-Parameter für blue2net [2]. Fragen Sie bei Ihrem Netzwerk-Administrator oder Internet-Service-Provider nach den richtigen IP-Parametern für blue2net [2].

Problem	Mögliche Ursache	Mögliche Lösung
Externe Computer (Internet) sind über die eigenen IP-Adressen erreichbar, jedoch nicht über deren URLs (z.B. www.siemens.at). (Fehlermeldung: Die Seite wurde nicht gefunden...)	DNS-IP-Adressen-Konfiguration ist falsch (siehe 'Terminal Fixed Servers' [3.5]).	Fragen Sie bei Ihrem Netzwerk-Administrator oder Internet-Service-Provider nach den richtigen DNS-IP-Adressen. Tragen Sie diese manuell ein ([3.5.1] und [3.5.2]).
Das Bluetooth-Terminal ist an blue2net angeschlossen, es kann jedoch extern nicht erreicht werden (z.B. Installieren eines Web-Servers auf dem Bluetooth-Terminal nicht möglich).	'Terminal IP-Address Resolution' [3.1] ist auf *masquerading* gesetzt.	Ausschluss gewisser Terminals vom „Masquerading" durch Zuweisung fixer IP-Adressen [1.10.2] und [1.10.4] in der Tabelle 'Terminal Table' [1.10]. Dann 'Terminal IP Address Resolution' [3.1] auf *masqueradingpool* setzen. Alle in der Tabelle 'Terminal Table' [1.10] aufgelisteten Terminals werden von außerhalb dann sichtbar sein.
	'Default Firewall' [2.6.1] ist auf *enabled* gesetzt.	Von außen unsichtbar zu sein ist einer der Hauptgründe für die Verwendung von Firewalls. Überlegen Sie sich genau, ob Sie die Firewall deaktivieren wollen oder nicht.

Tabelle 34 Fehlerbehebung: Zugang zum LAN

8.4 Software-Update

Problem	Mögliche Ursache	Mögliche Lösung
Image-Datei kann auf blue2net nicht gespeichert werden.	Es wurden zu viele Dateien auf das blue2net-/temp-Verzeichnis kopiert. Speicherplatz ist voll.	Neustarten von blue2net (siehe Kapitel 3.9.3). Es wird empfohlen, ausschließlich blue2net-Softwaredateien (b2n_image) auf blue2net zu kopieren.

Tabelle 35 Fehlerbehebung: Software-Update

8.5 Zugang zur Konfiguration

Problem	Mögliche Ursache	Mögliche Lösung
Es besteht eine Bluetooth-Verbindung zu blue2net, der eingebaute Web-Server ist jedoch nicht erreichbar.	IP-Adresse für den blue2net-Zugang wurde falsch eingegeben.	Überprüfen der blue2net-IP-Adresse (siehe Kapitel 2.6).
	Auf dem Web-Browser wurde ein Proxy für die PPP-Verbindung konfiguriert.	Ändern der Konfiguration am Web-Browser auf „no proxy" oder Ausschluss der blue2net-IP-Adresse.
	Eingabe von http://... statt http**s**://.... im Adressfeld des Web-Browsers.	Ändern auf http**s**://....
Konfigurations-Passwort wird permanent gefragt.	Am Web-Browser sind die „Cookies" nicht aktiviert.	Aktivieren der „Cookies" auf dem Web-Browser.

Tabelle 36 Fehlerbehebung: Zugang zur Konfiguration

9 Firewall

Die Firewall in blue2net kann aktiviert werden, um Angriffen von Ethernet-Seite (z.B. über LAN, Kabel-Modem oder xDSL-Anschluss) vorzubeugen.

Hinweis: Bei Aktivierung der Firewall kann es durch die vorprogrammierten Sicherheits-Einstellungen bei gewissen Anwendungen (z. B. Spiele über Internet) zu Einschränkungen kommen.

Es wird davon ausgegangen, dass alle über Bluetooth angeschlossenen Geräte vertrauenswürdig sind und keine Maßnahmen gegen sie ergriffen werden müssen (Ausnahme: die Konfiguration über SNMP wird nicht gestattet).

Wenn die Firewall aktiv ist, können Sie noch folgende Dienste nützen:

Dienst	Protokolle	Ports
HTTP	tcp / udp	80
HTTP webcaching	tcp / udp	8080
HTTPS	tcp / udp	443
FTP	tcp / udp	20, 21, über 1500
MS MEDIA PLAYER	tcp	1755, 7007
QUICKTIME	tcp	458, 545
REALPLAYER	tcp	1090, 554, 7070
DHCP	tcp / udp	67 (ein), 68 (aus)
DNS	tcp	53
DNS	udp	53 (nur zu Servern)
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

Tabelle 37 Dienste, die bei aktivierter Firewall genützt werden können

Transaktionen für all diese Dienste können nur von innerhalb der Firewall (von einem über Bluetooth angeschlossenen Gerät) gestartet werden.

Bei aktivierter Firewall können Sie von LAN-Seite her nur blue2net konfigurieren, da dafür https mit Passwortschutz verwendet wird. Ein Software-Update und das Laden einer spezifischen Homepage sind über Ethernet (LAN) *nicht* möglich.

Wie Sie die Firewall aktivieren bzw. deaktivieren finden Sie in den Kapiteln 2.7, 3.5 und 3.5.3.

10 Regulatory Statement / Konformitätserklärung

10.1 General

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

10.2 European Union (EU) and EFTA Member States

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

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

Tabelle 38 Conformity with standards and specifications

Note that the radio frequency band used by this equipment is not harmonized throughout the European Community. According to the R&TTE directive 1999/5/EC this equipment is a 'Class 2' equipment and marked accordingly with the assigned Class Identifier.

Abb. 35 CE Conformity Marking / CE Konformitätszeichen

10.3 United States of America (USA)

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

FCC ID: P6L-blue2net

Operation is subject to the following two conditions:

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

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

11 Bluetooth Compliance

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

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

12 Werkseinstellungen

[Hier.stufe] Parameter & Objekte	Werkseinstellung
[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	eindeutige Adresse für das BT-Gerät
[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	– (Anzeige)
[1.8] Service Table	–
[1.8.1] Service Index	– (Anzeige)
[1.8.2] Service Name	LAN ACCESS 1
[1.8.3] Service Description	LAN ACCESS via blue2net
[1.8.4] Auth. Level	noauth
[1.8.5] Service Provider	SIEMENS
[1.8.6] Service URL	http://www.siemens.at/bluetooth
[1.8.7] Service ID	1
[1.9] Number of Terminals	– (Anzeige)
[1.10] Terminal Table	–
[1.10.1] Terminal Index	– (Anzeige)
[1.10.2] Terminal Bluetooth Address	00:00:00:00:00:00
[1.10.3] Terminal Bluetooth Passkey	1234
[1.10.4] Terminal IP Address	0.0.0.0
[1.11] Default Access Mode	enabled
[1.12] Default Bluetooth Passkey	1234
[2] IP Parameters for blue2net	–
[2.1] blue2net IP Address Resolution	dhcp
[2.2] Fixed blue2net IP Configuration	–
[2.2.1] Fixed blue2net IP Address	192.168.1.2
[2.2.2] Fixed blue2net Netmask	255.255.255.0
[2.2.3] Fixed blue2net Gateway	192.168.1.1
[2.3] DHCP blue2net IP Objects	–
[2.3.1] Fallback blue2net IP Address	192.168.1.2
[2.3.2] Fallback blue2net Netmask	255.255.255.0
[2.3.3] Fallback blue2net Gateway	192.168.1.1
[2.4] Time Server IP	0.0.0.0
[2.5] IP Masquerading	192.168.2.2
[2.6] Firewall Settings	–
[2.6.1] Default Firewall	disabled
[2.7] Tunnel Configuration	–
[2.7.1] Tunnel Mode	none
[2.7.2] Tunnel Establishment Control	disabled
[2.7.3] Authentication Parameters	–
[2.7.3.1] Tunnel User Name	pppoeuser
[2.7.3.2] Tunnel User Pasword	pppoepassw
[2.7.4] PPTP Server IP Address	10.0.0.138

Tabelle 39 Werkseinstellungen (Default-Werte) (1)

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

Tabelle 40 Werkseinstellungen (Default-Werte) (2)

Um die Werkseinstellungen wiederherzustellen, verwenden Sie bitte den Aktivierungsbefehl 'Restore Default Settings' (siehe Kapitel 3.9.5).

13 Abkürzungen und Begriffe

Term	Erklärung
Authentifizierung	Ein Sicherheitsverfahren zur Identifikation berechtigter Benutzer
Autorisierung	Ein Sicherheitsverfahren, bei dem einem Gerät die Erlaubnis zum Zugriff auf einen bestimmten Dienst gegeben wird
BT	Bluetooth
CE	Conformity Europe
connectable	Ein Bluetooth-Gerät ist verbindungsbereit (connectable), wenn es auf einen Funkruf (paging) antwortet, so dass andere Geräte eine Verbindung dazu aufbauen können
DHCP	Dynamic Host Configuration Protocol
discoverable	Ein Bluetooth-Gerät ist auffindbar (discoverable), wenn es auf Anfragen anderer Bluetooth-Geräte antwortet, so dass andere Geräte in der Umgebung seine Anwesenheit feststellen können
DNS	Domain Name Server
DRAM	Dynamic Read and Write Memory
FCC	Federal Communications Commission
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
HTTPS	secure HyperText Transfer Protocol
HW	Hardware
IMAP	Internet Mail Access Protocol
IMAP SEC	Internet Mail Access Protocol secure
IP	Internet Protocol
ISP	Internet Service Provider
KPOP	Post Office Protocol Kerberos
blue2net	LAN Access Point, das hier beschriebene Gerät
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Medium Access Control
Passkey	Ein anderer Name für PIN
PCMCIA	Personal Computer Memory Card Int. Association Synonym für einen Standard für Steckkarten, wie z.B.Bluetooth- und Faxkarten
PDA	Personal Digital Assistant
PIN	Personal Identification Number

Tabelle 41 Abkürzungen und Begriffe (1)

Term	Erklärung
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 Tunneling 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
Terminal	Unter Terminal wird hier ein Bluetooth-fähiges Gerät verstanden, z.B. Laptop, PDA, PC etc.
UDP	Universal Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
WINS	Windows Internet Naming Service
xDSL	x Digital Subscriber Line (x … je nach ISP verschieden)

Tabelle 42 Abkürzungen und Begriffe (2)

14 Service / Kundendienst

Falls bei Ihrem Gerät Störungen auftreten, wenden Sie sich bitte an Ihren lokalen Händler.

Technische Informationen, Software-Updates und Antworten auf oft gestellte Fragen (FAQs) finden Sie auf der Produkt-Homepage www.siemens.at/bluetooth.

15 Garantie und Gewährleistung

Die Siemens AG bietet Händlern ab Kaufdatum eine Garantie von 12 Monaten.

Aufwendungen, die als Folge einer Aussperrung durch falsche Konfigurationseinstellungen entstehen, sind aus den Garantieansprüchen ausgenommen und werden daher nicht ersetzt. Im Falle einer Aussperrung kontaktieren Sie bitte Ihren lokalen Händler.

Das Gerät darf unter keinen Umständen geöffnet werden. Andernfalls erlöschen jegliche Garantie- und Gewährleistungsansprüche.

Neben den Bestimmungen des Produkthaftungsgesetzes haftet der Verkäufer im Rahmen der gesetzlichen Bestimmungen nur dann für ein Produkt, wenn der vorliegende Schaden nachweislich vorsätzlich verursacht wurde oder auf grobe Fahrlässigkeit seitens des Verkäufers zurückzuführen ist. Der Verkäufer haftet nicht für Schäden, die durch gewöhnliche Fahrlässigkeit entstanden sind. Ebenso wenig haftet er für Folgeschäden, entgangenen wirtschaftlichen Gewinn, den Verlust an Ersparnissen oder Zinsen oder für Schäden, die dem Käufer aufgrund von Forderungen durch Dritte erwachsen. Die Produkthaftung erstreckt sich auch nicht auf medizinische Betreuung, Krankenhausaufenthalte oder Krankenpflege. Siemens übernimmt insbesonders keine Haftung für Folgeschäden aus der Verwendung von blue2net im Bereich Gesundheitserhaltung, Lebensrettung und sicherheitskritischer Anwendungen.

Der Verkäufer ist im Falle der Nichtbefolgung der Anleitungen bezüglich Montage, Inbetriebnahme und Betrieb (so wie diese in der Bedienungsanleitung aufgeführt sind) sowie im Falle der Nichteinhaltung von Lizenzvorschriften seitens des Käufers von der Produkthaftung entbunden.

16 Technische Daten

Funktechnologie	Bluetooth V1.1, power class 2, 2 dBm
Frequenzbereich	2.402 to 2.480 GHz
Reichweite	20m
Übertragungsraten (maximal)	asymmetrisch: 723 Kbits/s downlink 57 Kbits/s uplink symmetrisch: 434 Kbits/s downlink und uplink
Multipoint	ja, Master / Slave Switch; für Anschluss von bis zu 7 Benutzern gleichzeitig
Bluetooth Profiles	LAN Access Profile Generic Access Profile Serial Port Profile PAN vorbereitet
Empfängerempfindlichkeit	besser als -80 dBm
Antenne	integrierte Patch-Antenne
Bluetooth-Modul	Siemens SieMo S50037
Bluetooth-Stack	Siemens SurfBlue
Prozessor	Power PC
Speicher DRAM / Flash	16 MB / 2 MB
Betriebssystem	Embedded Linux
Ethernet	10 Mbit/s, Stecker RJ45
Stromversorgung	4.5 V, 1 A, externes Netzteil, Stecker RJ11
Energieverbrauch	< 2,5 W
Abmessungen	150 x 140 x 32 mm (5.90 x 5.51 x 1.26 Zoll)
Gewicht	200 g (7.05 oz)
Montagebereich	nur in Innenräumen
Temperatur	0 bis +40 °C (+32 to +104 °F)
Konfiguration	eingebauter Web-Server
blue2net IP-Adressen-Zuweisung	DHCP oder predefined (fix)
Terminal IP-Adressen-Zuweisung	masquerading oder DHCP oder predefined (fix)
Sicherheit	Konfigurations-Passwort and HTTPS Bluetooth-Passwort integrierte Firewall
Software-Aktualisierungen	Software-Aktualisierungen gegebenenfalls unter http://www.siemens.at/bluetooth
Weitere Information	http://www.siemens.at/bluetooth

Tabelle 43 Technische Daten

17 Index

18 CE-Erklärung

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

We, **SIEMENS AG**
PSE PRO RCD

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

declare that the product

Type Designation: **blue2net Bluetooth™ LAN Access Point, S50037-D*-***
(Siemens Bluetooth™ Module SieMo-S50037 integrated inside)
Equipment class: **Class 2**
Product Description: **Wireless Access Point to Local Area Networks based on the Bluetooth™ Technology.**

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

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

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

Address: **CETECOM ICT Services GmbH, Untertürkheimer Strasse 6–10,**
D-66117 Saarbrücken, Germany.
Notified Body number: **0682**

The technical documentation relevant to the above equipment will be held at:
SIEMENS AG, PSE PRO RCD
Erdberger Lände 26
A-1031 Vienna, Austria
Point of contact: **Mr. Diyap Canbolant**
Tel.: +43 5 1707 36313, Fax: +43 5 1707 57679, E-Mail: diyap.canbolant@siemens.com

Head of Development
Günther Hraby
Vienna, 18.3.

Head of Quality Assurance
Herbert Haunschmid
Vienna, 15.3.02

Abb. 36 Konformitätserklärung

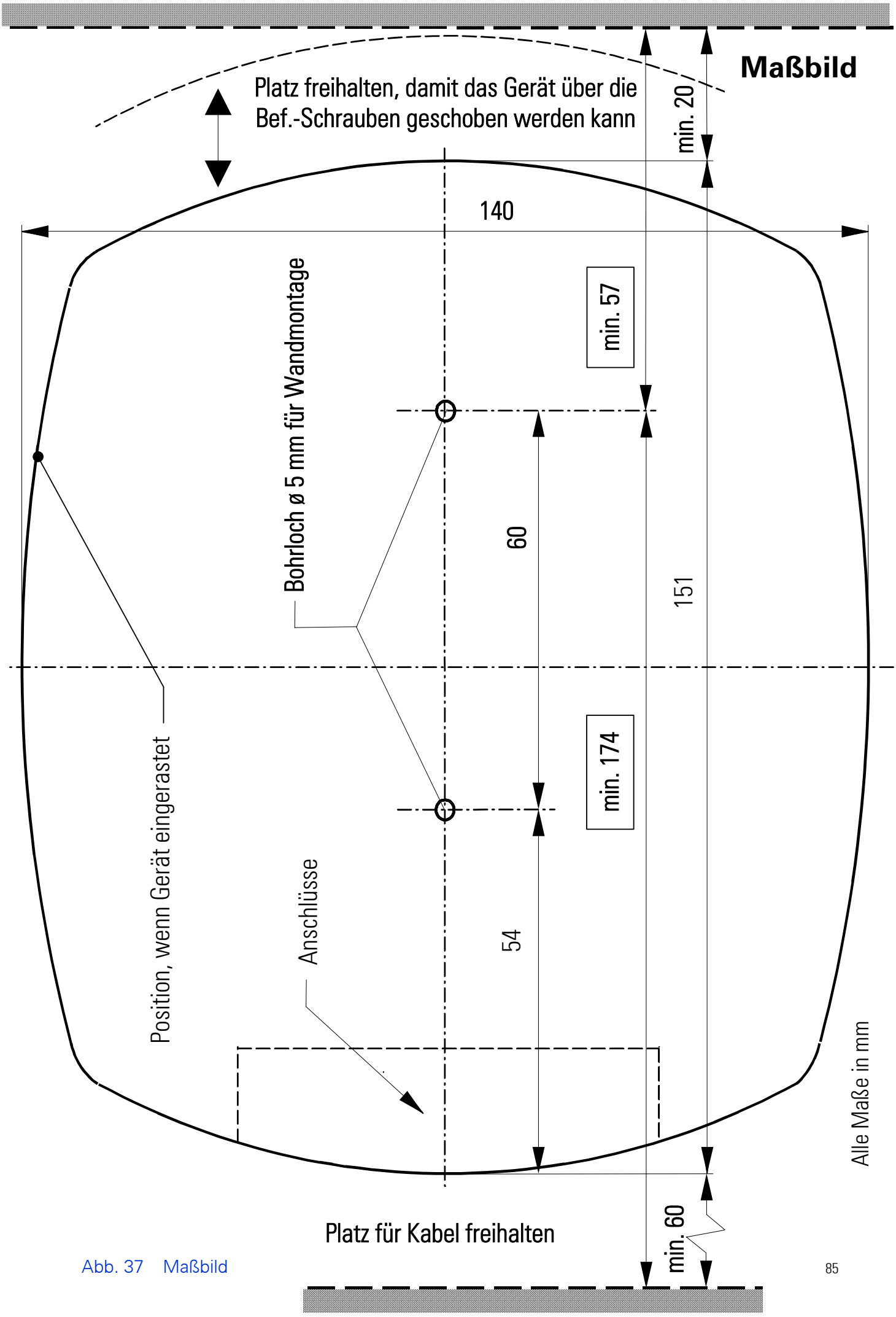

Abb. 37 Maßbild