SIEMENS

blue2net
LAN Access Point

Bedienungsanleitung

Ausgabe Januar 2003, Version 4.0

BLUETOOTH ist eine Handelsmarke von Bluetooth SIG, Inc., U.S.A, und ist lizenziert für Siemens AG.

Linux und Embedded Linux sind Handelsmarken von Linus Torvalds.

Windows, Internet Explorer und MS Media Player sind Handelsmarken der Microsoft Corporation.

Real Player™ ist eine Handelsmarke von Real Systems.

Quick Time™ ist eine Handelsmarke von Apple Corp.

Acrobat ® und Acrobar Reader ® sind Handelsmarken von Adobe Systems Inc.

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

Navigation im PDF-Dokument (v. CD-ROM oder Siemens-Homepage):

Wenn Sie z.B. Acrobat Reader ® verwenden, muß dazu das Werzeug  angeklickt sein.

Wenn Sie im PDF-Dokument auf aktive Elemente klicken, gelangen Sie direkt zu den Ansichten, auf die verwiesen wird.

Aktive Elemente sind:

- Lesezeichen (Register auf der linken Seite v. z.B. Acrobat Reader ®)
- Inhaltsverzeichnis, Abbildungsverzeichnis, Tabellenverzeichnis,
- Hierarchietabelle (Kapitel, Seiten),
- Verweise auf Kapitel, Seiten, Abbildungen und Tabellen,
- einige URLs.

Um zur Ausgangsposition zurückzugelangen, klicken Sie auf  .

Ausgabe Januar 2003, Version 4.0 (gilt für Software mit Versions-Nrn. 4.0.x)

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 „PAN Profile“ (Personal Area Networking Profile), das bedeutet eine drahtlose Ethernet-Anbindung, oder 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,welches per USB oder PCMCIA-Adapter oder als Compact-Flash-Card angeschlossen wird. Diese Geräte werden im Folgenden als „Bluetooth-Terminals“ bezeichnet. 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. Er kann zusammen mit einem Ethernet Switch auch als Access-Router für PCs/Laptops (im folgenden werden diese als Ethernet-Terminals bezeichnet) verwendet werden, die Sie fix über Ethernet-Kabel vernetzen.

2 Schnelleinstieg

Diese Orientierungshilfe soll Ihnen den Zugang zu der in der Bedienungs-anleitung enthaltenen Information erleichtern.

Es gibt Informationen, die Sie vor der ersten Inbetriebnahme unbedingt brauchen, damit Sie mit blue2net problemlos und sicher arbeiten können. Diese finden Sie unter „Unbedingt lesen".

Wenn das Gerät dann z.B. anhand eines passenden Szenarios mit ausreichenden Sicherheitseinstellungen betrieben werden kann, können Sie sich mit den einzelnen Parametern später im Detail vertraut machen und ev. individuelle Anpassungen vornehmen. Auch die Aktivierung der Firewall, die Vorgehensweise für einen Software-Update oder die Einrichtung einer gerätespezifischen Homepage müssen Sie nicht bei den ersten Schritten kennen. All das finden Sie unter „Später lesen".

Gewisse Informationen sind erst wichtig, wenn man die technischen Möglich-keiten des Gerätes für das Netzwerk in der Firma oder zu Hause voll und auf den Zweck optimiert ausschöpfen will. Unter „Für Fachleute" werden Fachleute die nötigen Informationen dazu finden, die dem Laien im Rahmen dieser Anleitung teilweise nicht umfassend verständlich gemacht werden können.

Hinweis: In der PDF-Datei (von der CD-ROM oder Siemens blue2net-Homepage) gelangen Sie durch Klicken auf die Kapitel-Nr. zum entsprechenden Kapitel.

	Information zur Orientierung	Details in Kapitel
1. Unbedingt lesen	Lesen Sie diese Kapitel unbedingt, bevor Sie blue2net in Betrieb nehmen oder konfigurieren.	
Aufstellung und Montage	• Für erste Inbetriebnahme und Vornahme der Basiskonfiguration kann das Gerät neben dem Terminal auf den Tisch gestellt werden. • Später kann die fixe Installation von blue2net vorgenommen werden (optimale Positionswahl unter Beachtung der Richtcharakteristik. Bei der Montage die Abstände für Kabelzuführung etc. beachten – dafür gibt es ein Maßbild).	4.2 letzte Seite
Betrieb am LAN oder xDSL-Modem einrichten	• Für den Betrieb an einem Firmen-LAN oder Kabel-Modem kann blue2net für den Anfang in den meisten Fällen mit den Werkseinstellungen betrieben werden. • Für Betrieb an einem xDSL-Modem müssen Sie blue2net erst konfigurieren, bevor Sie es an das xDSL-Modem anschließen. Die gewünschte Konfiguration und die besonders wichtigen Sicherheitseinstellungen werden z.B. anhand der Einsatz-Szenarien vorgenommen.	4.3.1 4.3.2

	Information zur Orientierung	Details in Kapitel
Sicherheit Technisch bedingte Sicherheit, Benutzerseitig bedingte Sicherheit (z.B. Passwortgebarung)	Technisch gesehen ist blue2net einer der sichersten LAN-Access-Points am Markt. Sie müssen sich mit den Sicherheitsfunktionen vertraut machen, damit Sie diese optimal ausschöpfen können, und einige grundlegende Regeln beachten (z.B. Umgang mit Passwörtern). Sie müssen aber die Sicherheitseinstellungen auf Ihre Bedürfnisse und Zwecke abstimmen und selbst zwischen der Erfüllung höherer Sicherheitsansprüche oder mehr Komfort abwägen.	3 6.5
Terminal anmelden	Es ist eine grundsätzliche Vorgangsweise beschrieben, wie eine Bluetooth-Verbindung zwischen Terminal (Laptop, PDA,...) und blue2net hergestellt wird (aufgrund der Vielzahl von Produkten kann hier nicht auf Details des jeweiligen Anmeldungsvorgangs eingegangen werden. Informieren Sie sich bitte über die Bedienungsanleitung des von Ihnen verwendeten Produktes). Damit haben Sie jetzt Zugang zur Konfiguration (ist sowohl über Bluetooth als auch LAN möglich)	5
Zugang zur Konfigurationsseite	Zugang zu den Parametern finden Sie über die Web-Seite in blue2net (bitte beachten: Adresse https://... **mit s** eingeben!). Prüfen Sie vorher, ob Ihr Web-Browser 128 bit Verschlüsselung (Cipher Strength) beherrscht. Wenn nicht, aktualisieren Sie den Browser)	6
Konfiguration	Für einen sicheren Betrieb müssen Sie nach dem erstmaligen Anmelden des Terminals unbedingt noch Sicherheitseinstellungen vornehmen. Ebenso verlangen verschiedene Anwendungen passende Einstellungen an den div. Parametern. Dazu können Sie entweder • aus mehreren **Szenarios** eines auswählen und die Parameter entsprechend einstellen (empfohlen, wenn Sie mit Netzwerktechnik nicht vertraut sind), oder • die Parameter einzeln einstellen und damit auf Ihre individuellen Ansprüche anpassen. Dazu müssen Sie sich über die Detailbeschreibung mit den Parametern vertraut machen. Hierarchienummern zwischen eckigen Klammern – z.B. [1.8.4] – werden Ihnen bei der Identifikation und Auffindung der Parameter helfen.	6.5 7 8 8.3

	Information zur Orientierung	Details in Kapitel
Einsatz-Szenarien	Damit kommen Sie zu schnellen Resultaten. Sie wählen eines von mehreren typischen Einsatz-Szenarien aus. Es werden in den 3 Haupt-Kategorien • Heimanwender • Business • Öffentliche Hot Spots verschiedene Szenarien dargestellt, mit Hilfe derer Sie rasch zu guten, sicheren Konfigurations-Einstellungen kommen, ohne die Detailzusammenhänge kennen zu müssen (Betrieb an LAN oder xDSL, Sicherheit, Zugang, Ausschluss, VIP's, etc.).	7.1 7.2 7.3
Aussperrung verhindern	Mit einigen Konfigurations-Parametern müssen Sie vorsichtig umgehen. Diese können bei falscher Einstellung und anschließender unbedachter Speicherung bewirken, dass blue2net über die Bluetooth-Verbindung oder sogar gänzlich unzugänglich wird, obwohl dies keine Fehlfunktion ist. Dies muss Ihnen unbedingt bewusst werden.	10 8.9
Speichern der Konfigurations-einstellungen	Konfigurationseinstellungen müssen nach einer Änderung zuerst gespeichert werden, bevor sie wirksam werden können. Dazu gibt es Optionen, die Sie kennen sollten, um Aussperrung zu verhindern und um vor Datenverlust und Sicherheitsproblemen bewahrt zu werden.	8.9 8.9.1 8.9.2

2. Später lesen	Detaillierte Information zu den Parametern und weniger oft gebrauchte Funktionen	
Erklärungen zu den einzelnen Parametern	Alle Parameter werden im Detail erklärt.	ab 8.3
Firewall	Die eingebaute Firewall kann/sollte unter bestimmten Bedingungen aktiviert werden. Sie können Regeln zur Umgehung der Firewall für die Fernwartung definieren.	14 8.5.3 8.5.4
Software Update	Diese Informationen weisen Ihnen den Weg, wenn Sie eine aktualisierte Software von der Siemens Homepage herunterladen und in blue2net hochladen wollen.	11
Specific Homepage	Es kann eine eigene Homepage in das Gerät geladen werden.	12

	Information zur Orientierung	Details in Kapitel
3. Für Fachleute	Dieses Kapitel ist für jene, die etwas über die Netzwerkstruktur beim Betrieb von blue2net erfahren wollen.	
Netzwerkstrukturen	blue2net hat Features, mit deren Hilfe Sie nicht nur Zugang für mehrere Terminals erhalten können, sondern auch kostengünstig ein kleines Netzwerk aufbauen können. Dazu ist teilweise aber auch einiges an Spezialwissen notwendig. In begrenztem Rahmen wird auch auf Details eingegangen. Wenn Sie nicht selbst bereits Netzwerke verwalten, werden Sie gelegentlich Unterstützung von einem Netzwerk-Administrator brauchen oder sich in die Literatur einarbeiten müssen, um alles zu verstehen.	9

4. Allg. Informationen	Diese Kapitel stellen allgemeine Informationen zum Gerät, zur Fehlerbehebung und zu Werkseinstellungen bereit.	
Fehlerbehebung	Entnehmen Sie diesem Teil einige Hinweise zur Fehlerbehebung als Unterstützung oder Anregung bei gängigen und bereits öfter aufgetretenen Problemen.	13
Technische Daten	Liste der technischen Daten	21
Werks- (Default-) Einstellungen	Es gibt eine Liste aller Werkseinstellungen der Konfigurations-Parameter. Diese können auch zur Gänze durch absichtliches Rücksetzen wiederhergestellt werden.	17 8.9.5
Konformität, CE, Bluetooth Compliance	Informationen zur Konformität mit Industrienormen, Gesetzen und der Bluetooth-Lizenz	15 23 16
Abkürzungen & Begriffe	Stellt die verwendeten Abkürzungen und Erklärungen zu einigen Begriffen bereit.	18
Kundendienst	Kontaktadresse für Reparatur, Service und Auskünfte.	19
Garantie und Gewährleistung	Bedingungen für Leistungen aus Garantie und Gewährleistung.	20
Index	Suchhilfe	22
Maßbild	Abmessungen und Bohrbild für die Montage	letzte Seite

3 Sicherheit

Es gibt immer wieder Diskussionen über die Sicherheit drahtloser Netzwerke.

Siemens hat sich zum Einsatz der Bluetooth-Technologie entschieden, weil diese sehr hohe Sicherheitsansprüche erfüllt.

3.1 Technisch bedingte Sicherheit

Im Folgenden werden die wichtigsten technologischen Unterschiede bezüglich Sicherheit für Bluetooth und dem gängigen Funkstandard Wireless LAN (WLAN) gegenübergestellt. WLAN steht hier für den Standard IEEE 802.11b.

Mechanismus zum Finden eines Access-Points

Bluetooth:

Bei Bluetooth ist das Terminal der aktive Teil beim Suchen nach Access Points. Das Terminal sendet eine Suchanfrage und der LAN Access Point. antwortet mit seiner Bluetooth Adresse, falls dieses Antwortverhalten aktiviert ist. Ist ein allgemeiner Zugang zum LAN Access Point nicht gewünscht, so kann dieses Antwortverhalten im LAN Access Point deaktiviert werden und es ist dem Angreifer nicht einfach möglich (durch eine einfache Suchabfrage) herauszufinden, ob ein potentieller Angriffspunkt überhaupt vorhanden ist.

WLAN:

Bei WLAN senden die Access Points in fixen Zeitintervallen eine Nachricht, um Terminals in der Umgebung mitzuteilen, dass hier ein drahtloser Zugang zu einem Netzwerk möglich ist. Diese Tatsache nutzen sog. War-Driver aus, um potentielle Angriffspunkte zu suchen.

Mechanismus zum Verschlüsseln von übertragenen Daten

Alle Daten werden auf Funkebene verschlüsselt übertragen.
Im Vergleich zu WEP (Wireless Equivalent Privacy) bei WLAN sind die Sicherheitsmechanismen bei Bluetooth wesentlich stärker.

Bluetooth:

Bluetooth verwendet zum Verschlüsseln von Daten den sogenannten E0 Algorithmus. Es wird für jede Verbindung ein neuer Key erzeugt. Das Rückrechnen des Key ist bei diesem Algorithmus nur mit erheblichen Aufwand und nach einer viel größeren Anzahl an Paketen möglich. Da aber nach jedem Verbindungsaufbau ein neuer Key zum Verschlüsseln erzeugt wird, kann davon ausgegangen werden, dass der Key praktisch nicht rückgerechnet werden kann.

WLAN:

WLAN verwendet zum Verschlüsseln von Daten den sogenannten RC4 Algorithmus, welcher für alle Verbindungen den gleichen Key zum Verschlüsseln der Daten verwendet. Durch passives Abhören von

Datenpaketen kann der Key nach ca. 1.000.000 Datenpaketen rückgerechnet werden und jeder weitere Datenverkehr passiv mitgelesen und entschlüsselt werden.

Frequenzzuteilung für die Datenübertragung

Bluetooth:

Das technische Verfahren zur Frequenzzuteilung bei „Bluetooth Frequency Hopping“ (Die Frequenz wird 1600 mal pro Sekunde geändert) erfordert für das Eindringen bzw. für das Mithören einen erheblichen technischen Aufwand. Gleichzeitig ist durch das „Frequency Hopping“ die Störsicherheit hoch, was sich günstig auf den Datendurchsatz auswirkt.

WLAN:

Bei WLAN erfolgt die Übertragung der Daten in einem fixen Frequenzband. Passives Mithören ist dadurch mit handelsüblichen WLAN-Geräten möglich.

Reichweite

Nicht unterschätzen sollte man aber auch die Tatsache, dass die geringere Reichweite von Bluetooth (ca. 20m) bezüglich Sicherheit einen Vorteil bringt. Der Erreichbarkeitsbereich ist auf „Wohnungsgröße" begrenzt. Nur „Angreifern", welche sich in diesem Bereich befinden ist es überhaupt möglich, einen Angriff zu starten. Die bei WLAN-Netzen gefürchteten War-Driver-Angriffe auf Firmennetze können durch geschicktes Anbringen der Bluetooth-LAN-Access-Points (u.a. z.B. Ausnutzen der Richtcharakteristik) im Inneren des Firmengeländes durch „physikalische“ Maßnahmen verhindert werden (siehe Kapitel 4.2).

3.2 Benutzerseitig bedingte Sicherheit

Bedenken Sie bitte, dass auch ein beträchtlicher Teil der Sicherheit in den Händen des Benutzers liegt:

a) die Entscheidung zum Einsatz von geeigneten Passwörtern,

b) die auf den Einsatzzweck abgestimmte Abwägung zwischen hohen Sicherheitsansprüchen oder mehr Komfort (z.B. kurze Passwörter, die man sich natürlich leichter merkt, als lange mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen),

c) Disziplin beim Umgang mit Passwörtern, um den Zugriff auf Passwörter zu verhindern (Geheimhaltung bei Vergabe, Aufbewahrung und Eingabe).

4 Installation von blue2net

Kurzanleitung:

1. Sicherheitshinweise beachten.
2. Packungsinhalt kontrollieren.
3. Gerät z.B. auf den Tisch neben den Laptop stellen. Fixe Platzierung erst vornehmen, wenn die Erstinstallation abgeschlossen ist.
4. Weiter mit Kap. 4.3.1 (Betrieb am LAN z.B. Firmennetzwerk, Kabelmodem eines Internet-Service-Providers) oder 4.3.2 (Betrieb an einem xDSL-Modem)

4.1 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

4.2 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 (je nach verwendetem Bluetooth-Terminal, Platzierung des blue2net und Entfernung zwischen Terminal und blue2net können sich alle angeschlossenen Terminals zusammen einen effektiv nutzbaren Datendurchsatz von bis zu 80 kByte/s aufteilen. 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

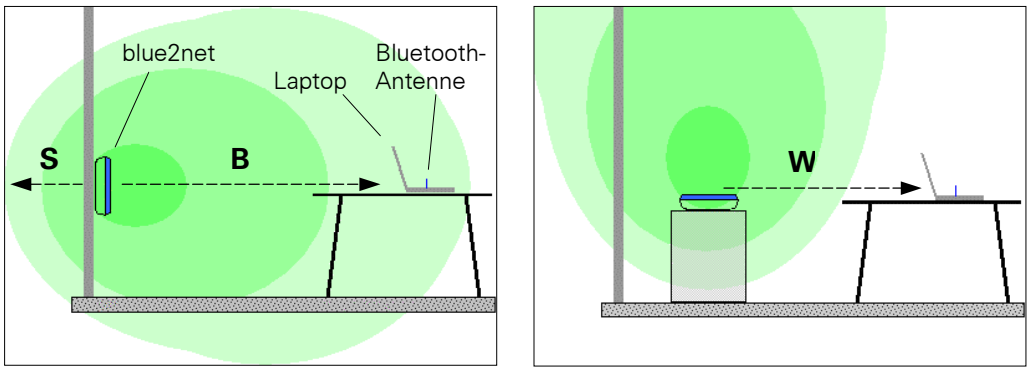


Abb. 1 Richtcharakteristik von blue2net und Erzielung guter Reichweiten

- 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 gegenüber-liegenden 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.

4.3 Anschluss von blue2net am Ethernet

Für blue2net sind grundsätzlich zwei Betriebsarten vorgesehen:

- Betrieb am LAN (z.B. Firmennetzwerk, Kabel-Modem eines Internet-Service-Providers) (siehe Kapitel 4.3.1)
- Betrieb an einem xDSL-Modem (siehe Kapitel 4.3.2)

blue2net ist im Auslieferungszustand für den Betrieb am LAN konfiguriert.

Hinweis: In beiden Betriebsarten kann blue2net als Access-Router verwendet werden, wenn Sie einen Ethernet-Switch für 10 Mbit/s verwenden.

4.3.1 Betrieb am LAN einrichten

Kurzanleitung:

Vorgehensweise:

1. Sie brauchen zunächst eine IP-Adresse.
   Heimanwender: Kontaktieren Sie den Internet-Service-Provider. Melden Sie blue2net unter Angabe der Ethernet MAC-Adresse (siehe Typenschild auf Geräte-Unterseite) in dessen Netzwerk an.
   Firmennetzwerk: blue2net erhält die IP-Adresse meistens automatisch über einen DHCP-Server zugewiesen. Wenn nicht, Netzwerkbetreuer kontaktieren (MAC-Adresse bereithalten).
2. blue2net über Ethernet-Kabel an LAN-Stecker oder Kabel-Modem anstecken (siehe Abb. 2)
3. Stromversorgung anstecken, LED beginnt zu blinken. Ca. 40 Sekunden warten, bis Anzeige-LED dauerhaft leuchtet (siehe Kap. 4.4) (bei Problemen Netzwerk-Administrator oder ISP kontaktieren).
4. Terminal über Bluetooth zu blue2net verbinden (siehe Kap. 5)
5. Browser am Terminal starten (Proxy-Einstellungen deaktivieren oder umgehen, Cookies aktivieren).
6. Web-Interface (Homepage) aufrufen über https://192.168.2.2 (siehe Kap. 6.2)
7. Konfigurationsseite aufrufen (siehe Kap. 6.4):
   „Configuration“ anklicken, Passwort „changeme“ eingeben. Passwort im nächsten Schritt sofort ändern und nicht mehr vergessen!.
8. Sicherheitseinstellungen und weitere Konfiguration vornehmen. Wählen Sie dazu z.B. ein passendes Szenario in Kap. 7 (siehe auch Kap. 6.5).
9. Konfiguration permanent abspeichern (siehe Kap. 8.9.2). Die Bluetooth-Verbindung wird dabei abgebrochen.
10. Für den Einstieg ins Internet bauen Sie nochmal die Bluetooth-Verbindung auf (Bluetooth-Passwort bereithalten) und starten anschließend – falls nicht bereits offen - den Browser am Bluetooth-Terminal.

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 an Ihren Netzwerk-Administrator oder ISP (Internet Service Provider) und fragen Sie dort, ob bei Ihrem LAN DHCP zur Verfügung steht. Wenn die IP-Adressen über DHCP zugewiesen werden, könnten Sie von Ihrem Netzwerk-Administrator oder ISP nach der Ethernet-*MAC-Adresse* gefragt 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 (siehe Kapitel 8.5.1).

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 (z.B. anhand eines der Einsatz-Szenarien in Kapitel 7). Lesen Sie dazu zunächst weiter im Kapitel 6.5.

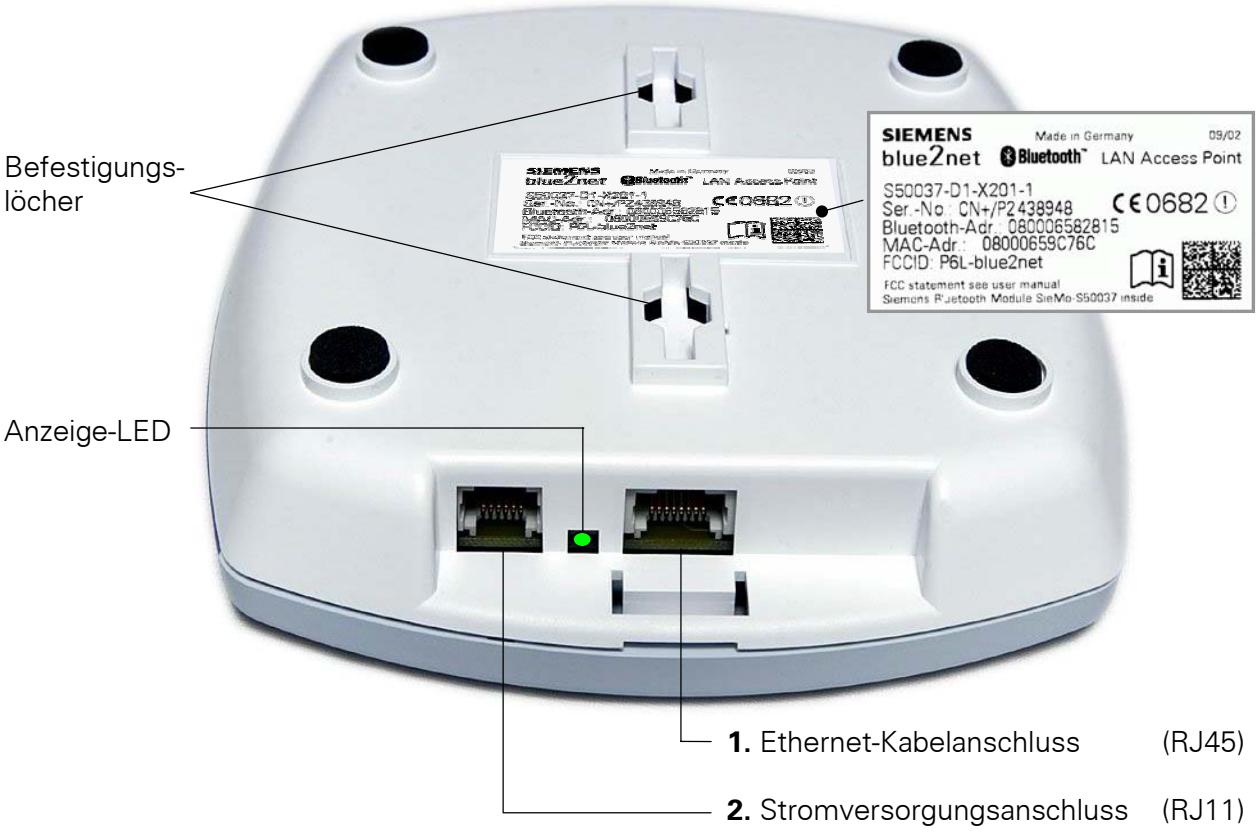


Abb. 2 Unterseite des Gerätes: Anschlüsse, Befestigungslöcher, LED und Typenschild

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 (auch dadurch erkennbar, dass diese am Bluetooth-Terminal als Suffix (Anhängsel) angezeigt wird).

   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 die blue2net-IP-Adresse manuell konfigurieren (siehe Kapitel 8.5.1).

  Ziehen Sie in diesem Fall einen Experten für Netzwerktechnik zu Rate (z.B. den Netzwerk-Administrator Ihrer Firma oder des ISP).

Nachdem die manuelle blue2net-IP-Konfiguration erfolgreich durchgeführt und eine Netzverbindung aufgebaut wurde, ist blue2net betriebsbereit. Es müssen dann aber u.a. noch die ***Sicherheitseinstellungen*** vorgenommen werden. Um die für Ihre Anforderungen geeigneten Einstellungen, besonders hinsichtlich Sicherheit, auszuwählen, gehen Sie z.B. anhand eines der Einsatz-Szenarien aus Kapitel 7 vor. Fahren Sie bitte mit Kapitel 6.5 ff fort.

4.3.2 Betrieb an einem xDSL-Modem einrichten

Kurzanleitung:

blue2net ist im Auslieferungszustand für LAN konfiguriert, muss also für xDSL zuerst von Ihnen konfiguriert werden.

Vorgehensweise:

1. Stromversorgung anstecken, aber noch nicht zum xDSL-Modem verbinden (siehe Abb. 2). Ca. 2 Minuten warten (bis Anzeige-LED auf Dauerleuchten).
2. Terminal über Bluetooth zu blue2net verbinden (siehe Kap. 5)
3. Browser starten (Proxy-Einstellungen deaktivieren, Cookies aktivieren).
4. Web-Interface (Homepage) aufrufen über https://192.168.2.2 (siehe Kap. 6.2)
5. Konfigurationsseite aufrufen (siehe Kap. 6.4): „Configuration“ anklicken, Passwort „changeme“ eingeben. Passwort im nächsten Schritt sofort ändern und nicht mehr vergessen!
6. xDSL-Konfiguration und Sicherheitseinstellungen vornehmen. Wählen Sie dazu z.B. ein passendes Szenario in Kap. 7.1.1 oder 7.3 (siehe auch Kap. 6.5 und 8.5.5)
7. Konfiguration permanent abspeichern (siehe Kap. 8.9.2). Die Bluetooth-Verbindung wird dabei abgebrochen.
8. blue2net über Kabel zum xDSL Modem verbinden (siehe Abb. 2).
9. Für den Einstieg ins Internet bauen Sie die Bluetooth-Verbindung nochmal auf (ev. Bluetooth-Passwort bereithalten) (siehe auch Kap. 5) und starten anschließend – falls nicht bereits offen - den Browser am Bluetooth-Terminal.

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) bei den Einsatz-Szenarien in Kapitel 7.1.1 und 7.3. Dort finden Sie u.a. auch geeignete Sicherheitseinstellungen, ohne sich vorher in die Beschreibung einzelner Parameter vertiefen zu müssen. Eine detaillierte Beschreibung aller Parameter für die zum xDSL-Betrieb vorgesehene Tunnel-Konfiguration finden Sie in Kapitel 8.5.5.

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, PDA) 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 Hochlaufphase durchlaufen hat, mit dem nächsten Schritt fortfahren (grüne Anzeige-LED auf Dauerleuchten).

2. Konfiguration für xDSL durchführen und Werte anschließend permanent speichern:
   - Eine Aufzählung der Parameter finden Sie bei den xDSL-Szenarien im Kapitel 7.1.1 (die **fett** gedruckten sind aus technischen Gründen unbedingt notwendig für die Herstellung der xDSL-Verbindung)
   - Den Aufbau einer Bluetooth-Verbindung und den Zugang zur Konfiguration lesen Sie in den Kapiteln 5 bis 6.2, und 6.4.
   - Anweisungen zum permanenten Abspeichern finden Sie in Kapitel 8.9.2

   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 nur dann abgesichert, wenn Sie die Sicherheitseinstellungen z.B. lt. Szenario vorgenommen haben*** (siehe Kapitel 6.5).

4.4 Bedeutung des Verhaltens der LED-Anzeige

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

Position der Anzeige-LED: siehe Abb. 2

5 Terminal über Bluetooth zu blue2net verbinden

Stellen Sie sicher, dass Ihre verwendeten Bluetooth- Terminals (z.B. Laptop, PDA oder Mobiltelefon) mindestens eines der folgenden Services nutzen kann:

- PAN-NAP (Personal Area Network – Network Access Point). Ein Bluetooth-Terminal mit drahtloser Verbindung verhält sich damit so, als ob es direkt über Kabel am Ethernet angeschlossen wäre).
- LAP (LAN Access Profile) Dieses Profil wird zunehmend durch das PAN-NAP Service abgelöst..

Nur wenn Sie das „LAN Access Profile“ verwenden: Wenn Ihr Bluetooth-Terminal nicht automatisch eine PPP-Verbindung aufbaut (z.B. DFÜ unter Windows BS, erkennbar am Symbol  in der Statuszeile), müssen Sie eine einrichten (siehe dazu die Benutzeranleitung des Bluetooth-Moduls).

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
- Wählen Sie das gewünschte Service („PAN Network Access Point“-Service oder „LAN Access Profile“).
- Verbinden Sie Ihr Terminal mit dem gewählten Gerät.
  Um Ihr blue2net bei mehreren angezeigten blue2net-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 (‚Terminal Bluetooth Passkey’ [1.10.3]) eingeben. Das voreingestellte Passwort lautet '**1234**' (siehe dazu auch Kap. 8.1 und 8.3).

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).

6.1 Erforderliche Browser-Einstellung

- **Deaktivieren** Sie die **Proxy-Einstellungen** im Web-Browser Ihres PDA oder Laptop

  oder

  umgehen Sie den Proxy-Server. Lassen Sie den Web-Browser bei Eingabe der blue2net-IP-Adresse den Proxy-Server nicht verwenden. Das erreichen Sie z.B. beim IE 6.0, indem Sie im Feld unter „Für Adressen, die wie folgt beginnen, keinen Proxy-Server verwenden“ (Proxyeinstellungen/Ausnahmen) bzw. „Do not use proxy server for addresses beginning with:“ (Proxy Settings/Exceptions) die blue2net-IP-Adresse eintragen.
- **Aktivieren** Sie die **Cookies!**
- Stellen sie sicher, dass ihr Browser SSL 3.0 unterstützt. (z.B. beim Internet Explorer unter: Extras > Internetoptionen > Erweitert > Sicherheit: „SSL 3.0 verwenden“ angeklickt)

6.2 Zugang über Bluetooth

- Für den Zugriff brauchen Sie eine bestehende Bluetooth-Verbindung zu blue2net wie in Kapitel 5 beschrieben.
- Das blue2net-Web-Interface (Abb. 3 zeigt die Homepage) erreichen Sie durch Eingabe der blue2net-IP-Adresse in der Adressleiste des Browsers am Bluetooth-Terminal:

  Beachte das „**s**“ !

  a) Gilt nur für den Auslieferungszustand: Geben Sie https://192.168.2.2 ein (beachten Sie bitte, dass blue2net nur den sicheren Zugang über https unterstützt). Bei dieser IP-Adresse handelt es sich um die voreingestellte IP-Adresse ‚IP Masquerading’ [2.5] mit der Terminals, die über Bluetooth verbunden sind, blue2net erreichen können.

  b) Ist der ‚IP Address Suffix Mode’ aktiviert (Werkseinstellung), sehen Sie die aktuelle blue2net-IP-Adresse des blue2net nach dem Bluetooth-Geräte-Namen (Bluetooth Device Name) angezeigt. Sie können somit die IP-Adresse nach einer Bluetooth-Geräte-Abfrage (Bluetooth device inquiry) am Bluetooth-Terminal direkt ablesen und damit durch Eingabe von http**s**://<abgelesene IP-Adresse> auf die Konfigurationsseiten des blue2net zugreifen.

  c) Ist der ‚IP Address Suffix Mode’ nicht aktiviert, müssten Sie die blue2net-IP-Adresse z.B. einer schriftlichen Aufzeichnung entnehmen.

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 Auslieferungszustand 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 6.2) und lesen Sie den Wert des Parameters ‘blue2net IP Address’ ab (siehe Kapitel 8.7.1).

- 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 für diesen Fall, dass die IP-Adresse des Rechners, mit dem Sie die Konfiguration durchführen (= Administrations-Rechner) und die Rückfall-IP-Adresse von blue2net im gleichen Subnetz liegen (ev. Netzwerk-Administrator kontaktieren).
- Greifen Sie auf das Web-Interface durch Eingabe von **https://< blue2net-IP-Adresse >** in die Adressleiste Ihres Web-Browsers zu (siehe Abb. 3).

6.4 Wie Sie zur Konfigurations-Seite gelangen

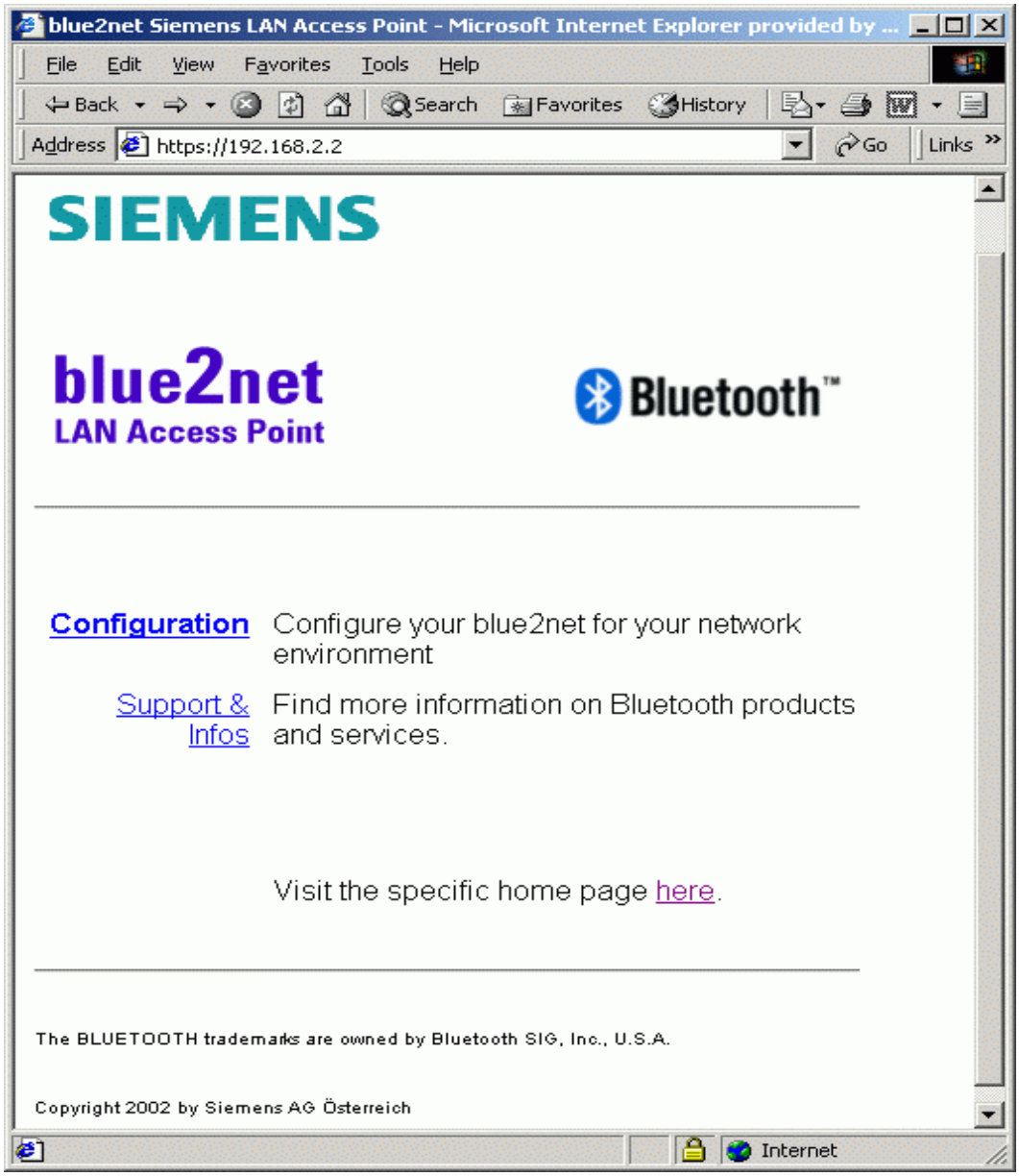


Abb. 3 blue2net-Web-Interface (Homepage)

- 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 8.8). 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 10 !!

6.5 Auswahl von Sicherheitseinstellungen

Mit den in blue2net vorgegebenen Werkseinstellungen ist es bei Kenntnis der „Default-Passwörter“ möglich, von jedem in Funkreichweite (ca. 20 m) befindlichen Bluetooth-Terminal Zugriff auf die Konfigurationsseiten und das LAN hinter blue2net zu erlangen oder von einem PC über das LAN auf die Konfigurationsseiten zuzugreifen und etwas zu ändern.

Seien Sie sich dessen bewusst, dass ihr Gerät nur dann sicher ist, wenn sie die Sicherheitseinstellungen (z.B. lt. Szenario in Kap. 7) vorgenommen und gespeichert haben.

- Den Zugriff auf die blue2net-Konfiguration verhindern Sie durch Änderung des voreingestellten Konfigurations-Passwortes auf ein geeignetes Passwort Ihrer Wahl.
- Den Zugriff über die Bluetooth-Verbindung verhindern Sie durch Autorisierung, über festgelegte Passwörter, Beschränkung auf ausgewählte Terminals, hohe Verschlüsselungsstärke (z.B. 128 bit Verschlüsselung), dadurch, dass Sie blue2net unentdeckbar machen, etc. aber z.B. auch durch Ausnützung der Richtcharakteristik.

Betrieb am LAN/Kabel-Modem:

Nachdem blue2net seine Startphase abgeschlossen hat, ist es grundsätzlich bereit zur Benützung. Der Zugriff ist jedoch *nur mit den Default-Passwörtern abgesichert*.

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

- Sie nehmen die Werte aus den Einsatz-Szenarien. Die Kapitel 7.1.2, 7.1.3 und 7.2 zeigen Einstellungen für 3 typische Anwendungsfälle für LAN/Kabel-Modem.
- Sie stellen sich die Werte anhand der Detailbeschreibungen aller Parameter selbst ein, z.B. weil Sie blue2net nach persönlichen Anforderungen einrichten wollen. Kap. 8 zeigt detailliert die Konfigurationseinstellungen.

Betrieb an einem xDSL-Modem:

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

- Bei der Konfiguration für die Herstellung der Tunnel-Verbindung nehmen Sie *nicht nur die fett gedruckten Werte* aus den Einsatz-Szenarien in Kap. 7.1.1 sondern auch die anderen Einstellungen, die auf Ihren Anwendungsfall passen (Heimanwender aus Kap. 7.1.1 und 7.1.3, Hot Spot Anwender aus Kap. 7.3).
- Bei der Konfiguration für die Herstellung der Tunnel-Verbindung nehmen Sie *nur die fett gedruckten Werte* aus den Einsatz-Szenarien in Kap. 7.1.1. Die restlichen Werte stellen Sie z.B. anhand der Detailbeschreibungen aller Parameter selbst ein, z.B. weil Sie blue2net nach persönlichen Anforderungen einrichten wollen. Kap. 8 zeigt detailliert die Konfigurationseinstellungen.

7 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. Beachten Sie besonders Kapitel 10 „Aussperrung verhindern".

Wenn Sie blue2net neu erworben haben, müssen Sie nur die im jeweiligen Szenario angeführten Einstellungen vornehmen, die restlichen Werte können Sie auf den Werkseinstellungen belassen.

Wenn Sie blue2net bereits konfiguriert haben, können Sie auf die Werkseinstellungen zurückstellen (siehe Kapitel 8.9.5) und dann entsprechend den Empfehlungen zum Szenario neu konfigurieren.

Machen Sie sich zunächst kurz damit vertraut, auf welche Weise Sie bei blue2net Einstellungen ändern können (siehe Kapitel 8.1 und 8.2).

In den Tabellen ist zu jedem Parameter eine Hierarchiestufe angegeben, z.B. [1.8.4]. Diese Hierarchienummern zwischen eckigen Klammern finden Sie wieder in den Tabellen von Kap. 8.3 ff und werden Ihnen bei vielen Gelegenheiten bei der Identifikation und Auffindung der Parameter helfen.

Hinweis: Generell ist zu empfehlen, dass beim Aufbau eines internen Netzwerkes, wo blue2net als Router arbeitet, ein Switch zum Einsatz kommt und nicht ein Hub, da es im Netzwerk zu Kollisionen von Datenpaketen und damit Einbrüchen in der Datenrate kommen kann.

7.1 Heimanwender-Szenarien

7.1.1 Heimanwender-Szenario mit xDSL-Modem (kein Access-Router vorhanden)

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!).

Dieses Szenario trifft dann auf Sie zu, wenn Sie noch keinen Access-Router besitzen (Sie hatten bis jetzt nur über einen PC Zugang zum Internet oder haben einen neuen Internet-Zugang).

Wenn Sie bisher einen PC als Access-Router für andere PCs verwendet haben, können Sie statt dessen blue2net verwenden. blue2net ist geräuschlos (keine beweglichen Teile) und verbraucht weniger Energie als ein PC im Standby-

Modus (<3,6 W). Da ein kleiner Switch billiger als ein Access-Router ist, verwenden Sie blue2net als Access-Router.

Wenn Sie nur drahtlos ins WWW-Internet gelangen möchten, können Sie die in Abb. 4 hellgrün hinterlegten Geräte weglassen. In diesem Fall ist blue2net direkt an das xDSL-Modem anzuschließen. In der Konfiguration in Tabelle 1 und Tabelle 3 können Sie ebenfalls die hellgrün hinterlegten Schritte weglassen.

Bringen Sie zuerst in Erfahrung, ob Ihr xDSL-Dienst-Anbieter PPPoE oder PPtP als Zugangsprotokoll verwendet.

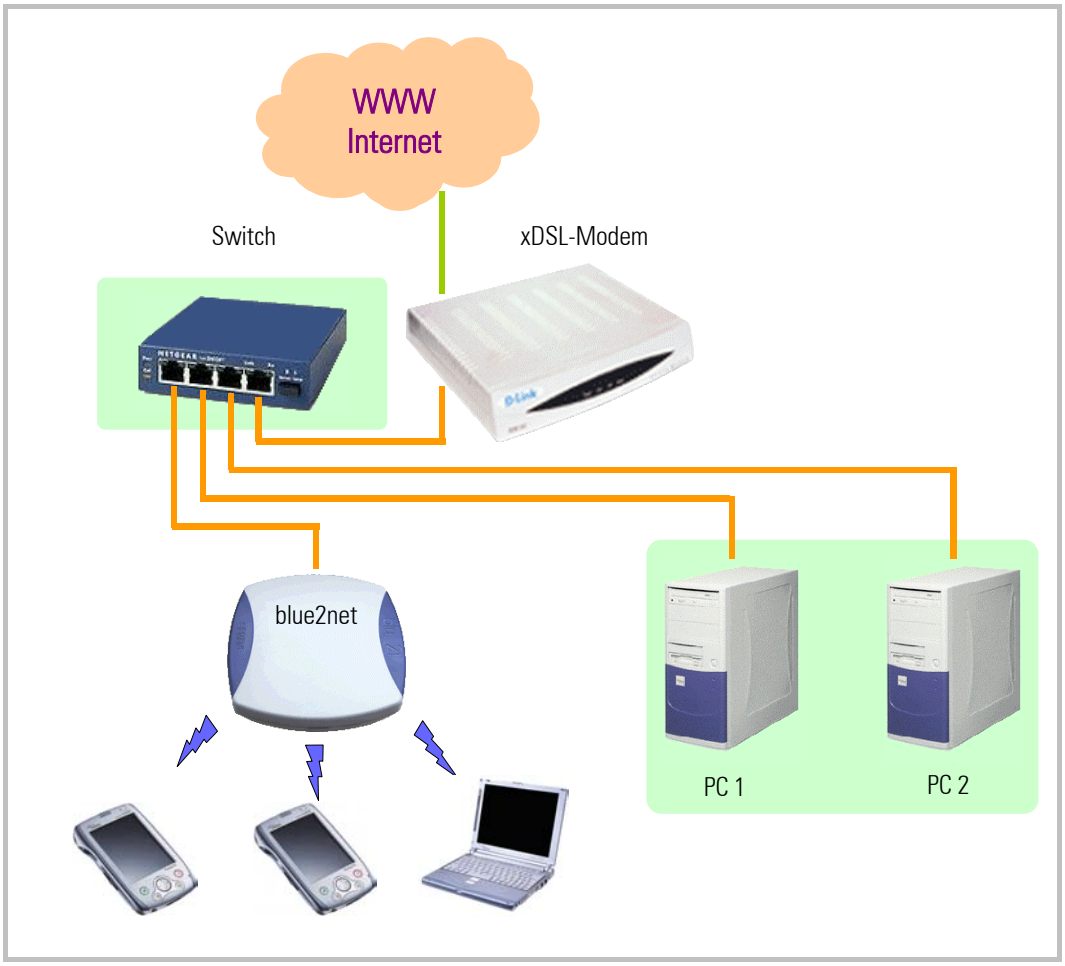


Abb. 4 Szenario „Heimanwender mit xDSL-Modem“

xDSL-Modem mit PPtP Protokoll (z.B. ADSL in Österreich)

Vergewissern Sie sich nochmals, dass Ihr xDSL-Dienst-Anbieter PPtP als Zugangsprotokoll verwendet. Nur dann sind die Einstellungen in der folgenden Tabelle für Sie geeignet.

Hinweis: Die fett gedruckten Parameter sind jene, die unbedingt konfiguriert sein müssen, bevor Sie blue2net das erste mal mit einem xDSL-Modem verbinden können (siehe Kapitel 4.3.2).

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. Sie können natürlich auch den voreingestellten Namen beibehalten
Default Access Mode	[1.11]	disabled	Kein Zugang für jedermann. Achtung! Vergessen Sie nicht die Einstellungen in Tabelle [1.10] vorzunehmen!
Terminal Table	[1.10]	Bluetooth-Adresse [1.10.2], Bluetooth-Passwort [1.10.3] und Terminal-IP-Adresse [1.10.4] der bei Ihnen am häufigsten verwendeten Terminals. 'Allow Bluetooth Bonding' [1.10.5] ist *enabled*	Sie können hier die Bluetooth-Adressen der Bluetooth-Geräte aller Familienmitglieder eintragen, Jedes Gerät besitzt einen eigenen Bluetooth-Passkey. Wenn ein Gerät immer die gleiche IP-Adresse bekommen soll, tragen Sie auch diese ein (im Bereich 192.168.2.71 bis 192.168.2.253).
blue2net IP Address Resolution	[2.1]	predefined	Das xDSL-Modem kann keine DHCP-Anfragen beantworten.
Fixed blue2net IP Address	[2.2.1]	Beispiel: [2.7.4] ist 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.	Diese Parameter sind so einzustellen, dass 'Fixed blue2net IP Address' im gleichen IP-Netz liegt, wie die vom xDSL-Modem vorgegebene IP-Adresse 'PPTP Server IP Address' [2.7.4]. Wenn also z.B. die Netzmaske 255.255.255.0 lautet, müssen [2.2.1] und [2.7.4] in den ersten 3 Blöcken übereinstimmen, im letzten Block müssen sie sich unterscheiden (höher oder niederer, min. 1, max 254).
Fixed blue2net Netmask	[2.2.2]		
Fixed blue2net Gateway	[2.2.3]	0.0.0.0.	Für diese Betriebsart ist dieser Wert erforderlich.

Parameter	Hier. stufe	eingestellt auf	Begründung / Hinweis
Default Firewall	[2.6.1]	enabled	Obwohl Ihre Geräte (hinter blue2net) durch Masquerading vom WWW-Internet aus nicht mehr erreichbar sind, schalten Sie noch die Firewall ein, um andere neugierige Teilnehmern im WWW vom Heimnetz sicher auszusperren.
Tunnel Mode	[2.7.1]	pptp	Diese Tabelle von Einstellungen ist nur dann für Sie geeignet, wenn Ihr xDSL-Anbieter PPtP als Zugangs-Protokoll verwendet.
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.
PPTP Server IP Address	[2.7.4]	vorgegebene IP-Adresse (könnte z.B. lauten: 10.0.0.138)	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.
Additional IP Interface	[2.8.1]	enabled	Zweite IP-Schnittstelle für lokales Heimnetz einschalten. **Wenn Sie kein Heimnetzwerk betreiben, können Sie diesen Konfigurations-Schritt auslassen**.
Terminal IP Address Resolution	[3.1]	masquerading (Voreinstellung)	Für die Terminals sind bei dieser Einstellung keine offiziellen IP-Adressen erforderlich. Die Geräte Ihrer Familien-Mitglieder haben Sie bereits in die Tabelle ‚Terminal Table' [1.10] eingetragen.
Local DHCP Server for Ethernet	[3.6.2]	enabled	Schalten Sie den blue2net-internen DHCP-Server für Ethernet ein. **Wenn Sie kein Heimnetzwerk betreiben, können Sie diesen Konfigurations-Schritt auslassen**.

Parameter	Hier. stufe	eingestellt auf	Begründung / Hinweis
Fixed IP Addresses for Local Wired Network	[3.9]	[3.9.1] MAC-Adressen der Netzwerkkarten [3.9.2] IP-Adressen für die Netzwerkkarten	Sie sollten hier die Ethernet-MAC-Adressen der PCs/Laptops eintragen, die an Ihrem Heim-Netz über Ethernet (drahtgebunden) teilnehmen. (Adressbereich 192.168.3.3 bis 192.168.3.19). **Wenn Sie kein Heimnetzwerk betreiben, können Sie diesen Konfigurations-Schritt auslassen.**
Configuration Password	[5.2]	Passwort Ihrer Wahl (4…22 Zeichen)	Nur autorisierte Personen (z.B. jenes Familienmitglied, das sich am besten auskennt) können blue2net konfigurieren. Achtung! Vergessen Sie das neue Passwort nicht.

Tabelle 1 Szenario „Heimanwender mit xDSL-Modem und PPtP“, Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

Optionale Einstellungen:

Wenn Sie öfter Probleme haben, Internetseiten zu erreichen (Fehlermeldung: z.B. „Die Seite kann nicht angezeigt werden. ...Fehler: Server oder DNS kann nicht gefunden werden“), könnte es daran liegen, dass der (externe) DHCP-Server nicht zuverlässig arbeitet (siehe auch Kap. 13.3). Für diesen Fall können Sie zusätzlich folgende Werte einstellen:

Parameter	Hier. stufe	eingestellt auf	Begründung
Terminal DNS Server 1/2	[3.5.1] [3.5.2]	DNS-Server-Werte, die Ihr Dienst-Anbieter empfiehlt Unter ‚Current Configuration' [4] >> ‚Terminal Server Configuration' [4.3] finden Sie die Werte für die DNS-Server ([4.3.1] u. [4.3.2]). (während der DHCP-Server des Internet-Anbieters funktioniert)	Nur von Bedeutung, wenn der DHCP-Server Ihres Internet-Anbieters nicht zuverlässig funktioniert.

Tabelle 2 Szenario „Heimanwender mit xDSL-Modem und PPtP“, Optionale Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

xDSL-Modem mit PPPoE Protokoll (z.B. TDSL bei der Deutschen Telekom)

Vergewissern Sie sich nochmals, dass Ihr xDSL-Dienst-Anbieter PPPoE als Zugangsprotokoll verwendet. Nur dann sind die Einstellungen in der folgenden Tabelle für Sie geeignet.

Hinweis: Die fett gedruckten Parameter sind jene, die unbedingt konfiguriert sein müssen, bevor Sie blue2net das erste mal mit einem xDSL-Modem verbinden können (siehe Kapitel 4.3.2).

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. Sie können natürlich auch den voreingestellten Namen beibehalten
Default Access Mode	[1.11]	disabled	Kein Zugang für jedermann. Achtung! Vergessen Sie nicht die Einstellungen in Tabelle [1.10] vorzunehmen!
Terminal Table	[1.10]	Bluetooth-Adresse [1.10.2], Bluetooth-Passwort [1.10.3] und Terminal-IP-Adresse [1.10.4] der bei Ihnen am häufigsten verwendeten Terminals. 'Allow Bluetooth Bonding' [1.10.5] ist *enabled*	Sie können hier die Bluetooth-Adressen der Bluetooth-Geräte aller Familienmitglieder eintragen, Jedes Gerät besitzt einen eigen Bluetooth-Passkey. Wenn ein Gerät immer die gleiche IP-Adresse bekommen soll, tragen Sie auch diese ein (im Bereich 192.168.2.71 bis 192.168.2.253).
blue2net IP Address Resolution	[2.1]	predefined	Das xDSL-Modem kann keine DHCP-Anfragen beantworten.
Fixed blue2net IP Address	[2.2.1]	192.168.3.2	Das ist die IP-Addresse von blue2net in Ihrem Heimnetzwerk. **Wenn Sie kein Heimnetzwerk betreiben, können Sie diesen Konfigurations-Schritt auslassen**.

Parameter	Hier. stufe	eingestellt auf	Begründung / Hinweis
Fixed blue2net Gateway	[2.2.3]	0.0.0.0.	Für diese Betriebsart ist dieser Wert erforderlich.
Default Firewall	[2.6.1]	enabled	Obwohl Ihre Geräte (hinter blue2net) durch Masquerading vom WWW-Internet aus nicht mehr erreichbar sind, schalten Sie noch die Firewall ein, um andere neugierige Teilnehmer im WWW vom Heimnetz sicher auszusperren.
Tunnel Mode	[2.7.1]	pppoe	Diese Tabelle von Einstellungen ist nur dann für Sie geeignet, wenn Ihr xDSL-Anbieter PPPoE als Zugangs-Protokoll verwendet.
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]	masqueradingpool	Für die Terminals sind bei dieser Einstellung keine offiziellen IP-Adressen erforderlich.
Local DHCP Server for Ethernet	[3.6.2]	enabled	Schalten Sie den blue2net-internen DHCP-Server für Ethernet ein. **Wenn Sie kein Heimnetzwerk betreiben, können Sie diesen Konfigurations-Schritt auslassen**.
Fixed IP Addresses for Local Wired Network	[3.9]	[3.9.1] MAC-Adressen der Netzwerk-Karten [3.9.2] IP-Adressen für die Netzwerk-Karten	Sie sollten hier die Ethernet-MAC-Adressen der PCs/Laptops eintragen, die an Ihrem Heim-Netz über Ethernet (drahtgebunden) teilnehmen. (Adressbereich 192.168.3.3 bis 192.168.3.19). **Wenn Sie kein Heimnetzwerk betreiben, können Sie diesen Konfigurations-Schritt auslassen.**

Parameter	Hier. stufe	eingestellt auf	Begründung / Hinweis
Configuration Password	[5.2]	Passwort Ihrer Wahl (4…22 Zeichen)	Nur autorisierte Personen (z.B. jenes Familienmitglied, das sich am besten auskennt) können blue2net konfigurieren. Achtung! Vergessen Sie das neue Passwort nicht.

Tabelle 3 Szenario „Heimanwender mit xDSL-Modem und PPPoE“, Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

Optionale Einstellungen:

Wenn Sie öfter Probleme haben, Internetseiten zu erreichen (Fehlermeldung: z.B. „Die Seite kann nicht angezeigt werden. ...Fehler: Server oder DNS kann nicht gefunden werden“), könnte es daran liegen, dass der (externe) DHCP-Server nicht zuverlässig arbeitet (siehe auch Kap. 13.3). Für diesen Fall können Sie zusätzlich folgende Werte einstellen:

Parameter	Hier. stufe	eingestellt auf	Begründung
Terminal DNS Server 1/2	[3.5.1] [3.5.2]	DNS-Server-Werte, die Ihr Dienst-Anbieter empfiehlt Unter ‚Current Configuration' [4] >> ‚Terminal Server Configuration' [4.3] finden Sie die Werte für die DNS-Server ([4.3.1] u. [4.3.2]). (während der DHCP-Server des Internet-Anbieters funktioniert)	Nur von Bedeutung, wenn der DHCP-Server Ihres Internet-Anbieters nicht zuverlässig funktioniert.

Tabelle 4 Szenario „Heimanwender mit xDSL-Modem und PPPoE“, Optionale Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

7.1.2 Heimanwender-Szenario mit Kabel-Modem (kein Access-Router vorhanden)

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 der PCs/Laptops aktiviert werden.

Dieses Szenario trifft dann auf Sie zu, wenn Sie noch keinen Access-Router besitzen (Sie hatten bis jetzt nur über einen PC Zugang zum Internet oder haben einen neuen Internet-Zugang).

Wenn Sie bisher einen PC als Access-Router für andere PCs verwendet haben, können Sie statt dessen blue2net verwenden. blue2net ist geräuschlos (keine beweglichen Teile) und verbraucht weniger Energie als ein PC im Standby-Modus (<3,6 W). Da ein kleiner Switch billiger als ein Access-Router ist, verwenden Sie blue2net als Access-Router.

Wenn Sie nur drahtlos ins WWW-Internet gelangen möchten, können Sie die in Abb. 5 hellgrün hinterlegten Geräte weglassen. In diesem Fall ist blue2net direkt an das Kabel-Modem anzuschließen. In der Konfiguration in Tabelle 5 können Sie ebenfalls die hellgrün hinterlegten Schritte weglassen.

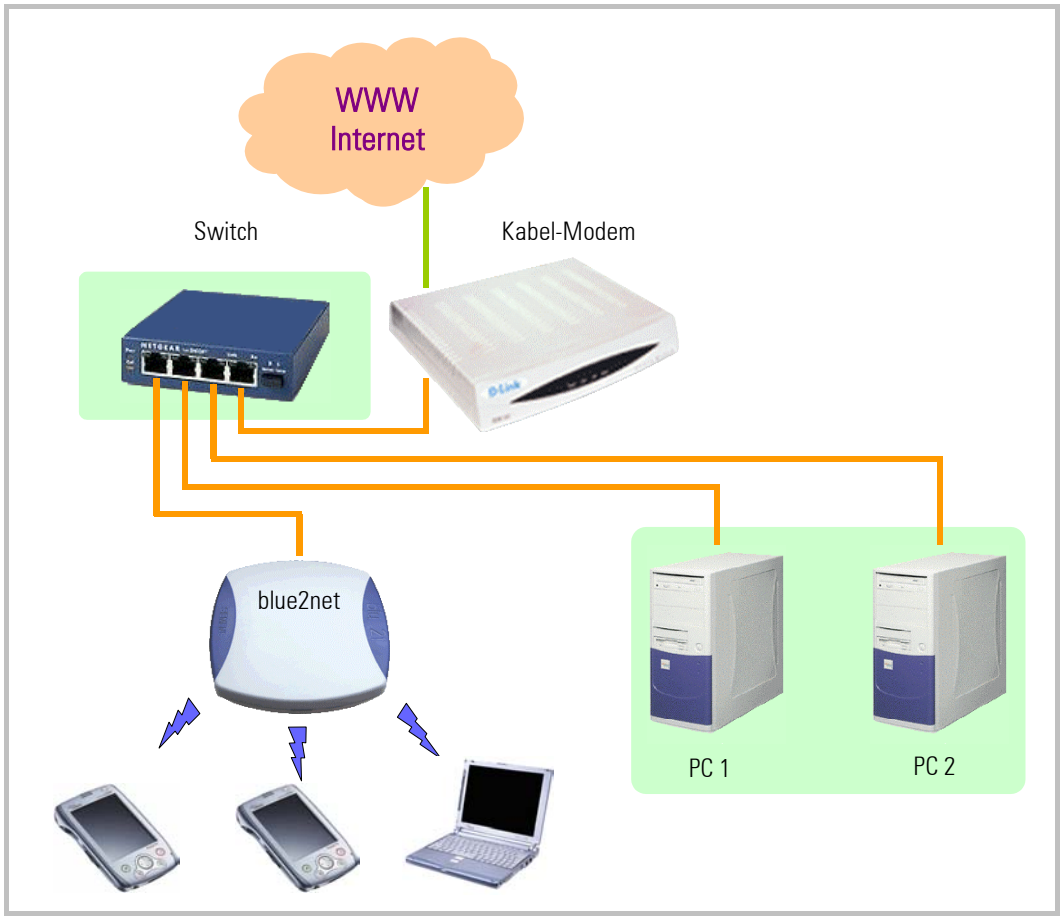


Abb. 5 Szenario „Heimanwender mit Kabel-Modem“

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. Sie können natürlich auch den voreingestellten Namen beibehalten
Terminal Table	[1.10]	Bluetooth-Adresse [1.10.2], Bluetooth-Passwort [1.10.3] und Terminal-IP-Adresse [1.10.4] der bei Ihnen am häufigsten verwendeten Terminals. 'Allow Bluetooth Bonding' [1.10.5] ist *enabled*	Sie können hier die Bluetooth-Adressen der Bluetooth-Geräte aller Familienmitglieder eintragen. Jedes Gerät besitzt einen eigenen Bluetooth-Passkey. Wenn ein Gerät immer die gleiche IP-Adresse bekommen soll, tragen Sie auch diese ein (im Bereich 192.168.2.71 bis 192.168.2.253).
Default Access Mode	[1.11]	disabled	Kein Zugang für jedermann. Achtung! Vergessen Sie nicht die Einstellungen in Tabelle [1.10] vorzunehmen!
blue2net IP Address Resolution	[2.1]	dhcp (Voreinstellung)	Ihr Internet-Anbieter weist über DHCP eine offizielle IP-Adresse zu.
Default Firewall	[2.6.1]	enabled	Obwohl Ihre Geräte (hinter blue2net) durch Masquerading vom WWW-Internet aus nicht mehr erreichbar sind, schalten Sie noch die Firewall ein, um andere neugierige Teilnehmern im WWW vom Heimnetz sicher auszusperren.
Additional IP Interface	[2.8.1]	enabled	Zweite IP-Schnittstelle für lokales Heimnetz einschalten. **Wenn Sie kein Heimnetzwerk betreiben, können Sie diesen Konfigurations-Schritt auslassen**.

Parameter	Hier. stufe	eingestellt auf	Begründung / Hinweis
Local DHCP Server for Ethernet	[3.6.2]	enabled	Schalten Sie den blue2net-internen DHCP-Server für Ethernet ein. **Wenn Sie kein Heimnetzwerk betreiben, können Sie diesen Konfigurations-Schritt auslassen**.
Fixed IP Addresses for Local Wired Network	[3.9]	[3.9.1] MAC-Adressen der Netzwerkkarten [3.9.2] IP-Adressen für die Netzwerkkarten	Sie sollten hier die Ethernet-MAC-Addressen der PCs/Laptops eintragen, die an Ihrem Heim-Netz über Ethernet (drahtgebunden) teilnehmen. (Adressbereich 192.168.3.3 bis 192.168.3.19). **Wenn Sie kein Heimnetzwerk betreiben, können Sie diesen Konfigurations-Schritt auslassen.**
Configuration Password	[5.2]	Passwort Ihrer Wahl (4…22 Zeichen)	Nur autorisierte Personen (z.B. jenes Familienmitglied, das sich am besten auskennt) können blue2net konfigurieren. Achtung! Vergessen Sie das neue Passwort nicht.

Tabelle 5 Szenario „Heimanwender mit Kabel-Modem“, Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

Optionale Einstellungen:

Wenn Sie öfter Probleme haben, Internetseiten zu erreichen (Fehlermeldung: z.B. „Die Seite kann nicht angezeigt werden. ...Fehler: Server oder DNS kann nicht gefunden werden“), könnte es daran liegen, dass der (externe) DHCP-Server nicht zuverlässig arbeitet (siehe auch Kap. 13.3). Für diesen Fall können Sie zusätzlich folgende Werte einstellen:

Parameter	Hier. stufe	eingestellt auf	Begründung
Fallback blue2net IP Address Fallback blue2net Netmask Fallback blue2net Gateway	[2.3.1] [2.3.2] [2.3.3]	IP-Parameter vom Dienst-Anbieter (Unter ‚Current Configuration’ [4] >> ‚blue2net IP Configuration’ [4.2] finden Sie die Werte für die blue2net-IP-Adresse [4.2.1, Netzmaske [4.2.2] und Gateway [4.2.3].	Die meisten Internet-Anbieter für Dienste über Kabel-Modem weisen immer die gleichen IP-Parameter zu Wenn Sie diese als Rückfall-Werte hier eintragen, stört Sie auch ein kurzer Server-Ausfall beim Anbieter nicht, wenn blue2net gerade in dieser Zeit neu startet.
Terminal DNS Server 1/2 Terminal WINS Server 1/2 Terminal Domain Name	[3.5.1] [3.5.2] [3.5.3] [3.5.4] [3.5.5]	DNS-Server-Werte, die Ihr Dienst-Anbieter empfiehlt (Unter ‚Current Configuration’ [4] >> ‚Terminal Server Configuration’ [4.3] finden Sie die Werte für die DNS-Server ([4.3.1] u. [4.3.2]), die WINS-Server ([4.3.3] und [4.3.4]) sowie Domain-Name [4.3.5]. (während der DHCP-Server des Internet-Anbieters funktioniert)	Nur von Bedeutung, wenn der DHCP-Server Ihres Internet-Anbieters nicht zuverlässig funktioniert. (während der DHCP-Server des Internet-Anbieters funktioniert)

Tabelle 6 Szenario „Heimanwender mit Kabel-Modem“, Optionale Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently’ [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

7.1.3 Heimanwender Szenario mit Access-Router

Typisches Szenario: Mehrere Familienmitglieder wollen Zugang zum Internet über ein Kabel-Modem oder xDSL-Modem haben. Nur eine berechtigte Person hat Zugang zur Konfiguration von blue2net.
Zusätzliche Annahmen: Es ist ein Access-Router vorhanden, der das Kabel-Modem oder xDSL-Modem bedient und die Funktionalitäten Masquerading, Firewall und DHCP zur Verfügung stellt (eventuell sind Access-Router und Kabel-Modem/xDSL-Modem in einem Gerät vereint).
Charakteristik: Aus Sicherheitsgründen muss blue2net gegen einen Zugriff durch Nachbarn und nicht berechtigte Personen außerhalb der Wohnung oder des Hauses geschützt werden.

Sie haben zum Beispiel schon ein kleines Heimnetzwerk, über das die ganze Familie Zugang zum Internet hat. Nun wollen Sie zusätzlich mit blue2net auch drahtlos mit PDA oder Laptop bequem vom Sofa surfen oder E-Mails abfragen können. In Abb. 6 ist die Situation dargestellt. Die Geräte mit weißem Hintergrund sind bereits vorhanden, die Geräte im blauen Feld sollen zusätzlich Zugang zum Internet und zum Heimnetz erhalten.

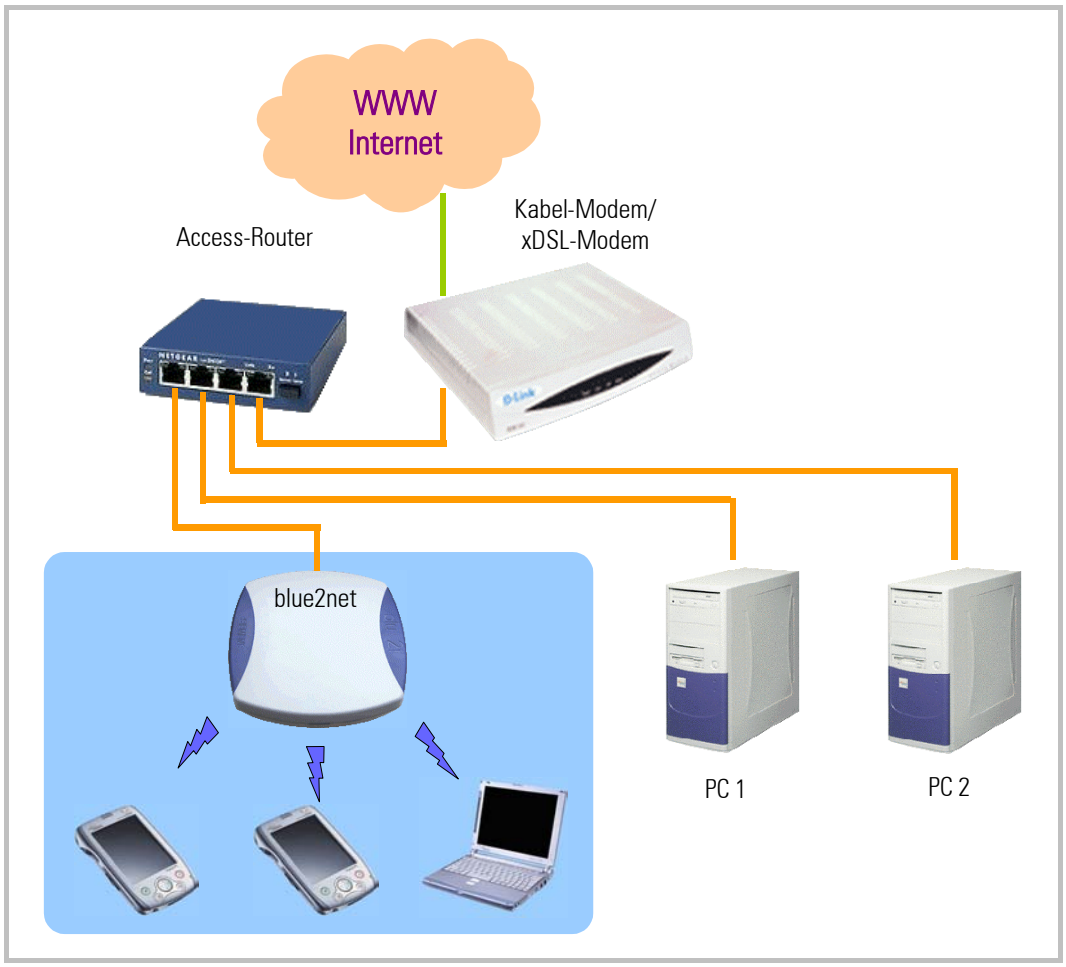


Abb. 6 Szenario „Heimanwender mit Access-Router“

Parameter	Hier. stufe	eingestellt auf	Begründung
Bluetooth Device Name	[1.1.1]	Name Ihrer Wahl (1...16 Zeichen)	In einer Umgebung mit mehreren blue2net-Geräten sollte jedes einen eindeutigen Namen zur klaren Unterscheidung haben. Sie können natürlich auch den voreingestellten Namen beibehalten.
Terminal Table	[1.10]	Alle Terminals sind registriert. Für Sie ist die Bluetooth-Adresse [1.10.2) und der jeweilige Bluetooth-Passkey [1.10.3] (**16-stellig!!**) eingetragen. Die IP-Adresse [1.10.3] ist auf *0.0.0.0* gesetzt 'Allow Bluetooth Bonding' [1.10.5] ist *enabled*	Alle Benutzer haben ein eigenes Bluetooth Passwort, das nur in Zusammenhang mit Ihrem Bluetooth-Gerät Zugang gewährt. Verwenden Sie alle 16 Stellen des Bluetooth-Passkeys für höchste Sicherheit.
Default Access Mode	[1.11]	disabled	Nur Geräte, deren Bluetooth-Adresse in [1.10] eingetragen sind, und die den Bluetooth-Passkey kennen, bekommen Zugang.
Minimum Length of Key for Encryption	[1.13]	16	Verschlüsselungsstärke auf Maximum (128 bit). Mit dieser Einstellung erhalten nur Geräte Zugang, die diese Verschlüsselungsstärke auch unterstützen. **Vorsicht!** Gefahr einer Aussperrung! Überprüfen Sie zuerst, ob Ihr Terminal 128 bit Verschlüsselung beherrscht (siehe Kap. 10.2 und 13.2).
Terminal IP Address Resolution	[3.1]	dhcp	Alle Bluetooth-Geräte bekommen von Ihrem blue2net-internen DHCP-Server die IP-Adressen und sonstige Information zugewiesen

Parameter	Hier. stufe	eingestellt auf	Begründung
Local DHCP Server for NAP	[3.6.1]	disabled	Da Sie einen eigenen DHCP-Server am Access-Router haben, schalten Sie den DHCP-Server für NAP-Terminals auf blue2net aus
IP Connection Mode for NAP Terminals	[3.7]	bridging	Bluetooth Geräte, die NAP Service benutzen, sind direkt am Ethernet angebunden.
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 7 Szenario „Heimanwender mit Access-Router“, Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

Optionale Einstellungen:

Wenn Sie öfter Probleme haben, Internetseiten zu erreichen (Fehlermeldung: z.B. „Die Seite kann nicht angezeigt werden. ...Fehler: Server oder DNS kann nicht gefunden werden“), könnte es daran liegen, dass der (externe) DHCP-Server nicht zuverlässig arbeitet (siehe auch Kap. 13.3). Für diesen Fall können Sie zusätzlich folgende Werte einstellen:

Parameter gruppe	Hier. stufe	eingestellt auf	Begründung
Fallback blue2net IP Address Fallback blue2net Netmask Fallback blue2net Gateway	[2.3.1] [2.3.2] [2.3.3]	Werte, die blue2net normalerweise über DHCP am Access-Router bekommt. Tragen Sie hier jene Werte ein, die Sie für blue2net auf Ihrem DHCP-Server am Access-Router vorgesehen haben (auch zu finden unter ‚Current Configuration' [4] >> ‚blue2net IP Configuration' [4.2] >> blue2net IP-Adresse [4.2.1], Netzmaske [4.2.2] und Gateway [4.2.3].	blue2net verwendet diese Werte, falls Ihr (externer) DHCP-Server kurzfristig ausfällt während blue2net neu startet.

Parameter gruppe	Hier. stufe	eingestellt auf	Begründung
Terminal DNS Server 1/2 Terminal WINS Server 1/2 Terminal Domain Name	[3.5.1] [3.5.2] [3.5.3] [3.5.4] [3.5.5]	Werte, die normalerweise über DHCP verteilt werden (DNS). Tragen Sie hier jene Werte ein, die Ihr DHCP-Server am Access-Router normalerweise an blue2net bei einer DHCP-Anfrage senden würde (auch zu finden unter ‚Current Configuration' [4] >> ‚Terminal Server Configuration' [4.3] >> DNS-Server [4.3.1] u. [4.3.2], WINS-Server [4.3.3] und [4.3.4] sowie Domain-Name [4.3.5]. (während der DHCP-Server des Internet-Anbieters funktioniert)	blue2net verwendet diese Werte, falls Ihr (externer) DHCP-Server kurzfristig ausfällt während blue2net neu startet.

Tabelle 8 Szenario „Heimanwender mit Access-Router", Optionale Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

7.2 Business-Szenarien

7.2.1 Business-Szenario mit kontrolliertem, allgemeinem Zugang

Typisches Szenario: Besprechungszimmer, wo Teilnehmern (Kunden, Besuchern) über ein voreingestelltes Bluetooth-Passwort [1.12] temporärer Zugang gewährt wird.
Charakteristik: Die Sicherheitsstufe ist mittel, alle Personen mit Kenntnis des Bluetooth-Passwortes haben Zugang zum LAN, nur berechtigte Personen haben Zugang zur Konfiguration.
Aus Sicherheitsgründen sollte blue2net in diesem Einsatz-Szenario auf ein eigenes Netzsegment außerhalb der Firmen-Firewall gelegt sein.
Anschluß: blue2net wird an ein Firmen-Netzsegment angeschlossen und über den DHCP-Server dieses eigenen Netzsegements mit einer IP-Adresse versorgt.

Parameter	Hier. stufe	eingestellt auf	Begründung
Bluetooth Device Name	[1.1.1]	Name Ihrer Wahl (1...16 Zeichen)	In einer Umgebung mit mehreren blue2net-Geräten sollte jedes einen eindeutigen Namen zur klaren Unterscheidung haben.
Auth. Level	[1.8.4]	noauth	Sie erlauben jedermann, der Ihr blue2net Gerät entdecken kann, Zugriff auf das Netzwerk, an dem blue2net angeschlossen ist. **Sicherheitshinweis:** Da jedermann Zugang erhält, ist es wichtig, dass blue2net auf ein eigenes Netzsegment außerhalb der Firmen-Firewall gelegt wird.
Terminal Table	[1.10]	Kein Terminal registriert (Bluetooth-Adresse auf *00:00:00:00:00:00* gesetzt). (Voreinstellung)	Alle Benutzer sollen mit dem voreingestellten Bluetooth-Passwort 'Default Bluetooth Passkey' [1.12] Zugang haben.
Default Bluetooth Passkey	[1.12]	Passwort Ihrer Wahl (1…16 Zeichen)	Das Passwort sollte für den Benutzer leicht in Erfahrung zu bringen sein.
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 9 Szenario „Businessbereich, kontrollierter allgemeiner Zugang“, Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

Optionale Einstellungen:

Wenn Sie öfter Probleme haben, Internetseiten zu erreichen (Fehlermeldung: z.B. „Die Seite kann nicht angezeigt werden. ...Fehler: Server oder DNS kann nicht gefunden werden"), könnte es daran liegen, dass der (externe) DHCP-Server nicht zuverlässig arbeitet (siehe auch Kap. 13.3). Für diesen Fall können Sie zusätzlich folgende Werte einstellen:

Parameter gruppe	Hier. stufe	eingestellt auf	Begründung
Fallback blue2net IP Address Fallback blue2net Netmask Fallback blue2net Gateway	[2.3.1] [2.3.2] [2.3.3]	Werte, die blue2net normalerweise über DHCP bekommt. Tragen Sie hier jene Werte ein, die Sie für blue2net auf Ihrem Firmen-DHCP-Server vorgesehen haben (auch zu finden unter ‚Current Configuration' [4] >> ‚blue2net IP Configuration' [4.2] >> blue2net IP-Adresse [4.2.1], Netzmaske [4.2.2] und Gateway [4.2.3].	blue2net verwendet diese Werte, falls Ihr Firmen-DHCP-Server kurzfristig ausfällt.
Terminal DNS Server 1/2 Terminal WINS Server 1/2 Terminal Domain Name	[3.5.1] [3.5.2] [3.5.3] [3.5.4] [3.5.5]	Werte, die normalerweise über DHCP verteilt werden (DNS). Tragen Sie hier jene Werte ein, die Ihr Firmen-DHCP-Server normalerweise an blue2net bei einer DHCP-Anfrage senden würde (auch zu finden unter ‚Current Configuration' [4] >> ‚Terminal Server Configuration' [4.3] >> DNS-Server [4.3.1] u. [4.3.2], WINS Server [4.3.3] und [4.3.4] sowie Domain-Name [4.3.5]. (während der DHCP-Server funktioniert)	blue2net verwendet diese Werte, falls Ihr Firmen-DHCP-Server kurzfristig ausfällt.

Tabelle 10 Szenario „Businessbereich, kontrollierter allgemeiner Zugang", Optionale Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

7.2.2 Business Szenario mit sicherem Zugang für Mitarbeiter ins Firmen-Netz

Typisches Szenario: Außendienst-Mitarbeiter sind gelegentlich in der Firma, um Berichte abzuliefern, Mails zu lesen und zu versenden, neue Daten auf Ihre Laptops oder PDAs zu laden.

Charakteristik: Die Sicherheitsstufe ist hoch, nur Bluetooth Geräte, die in der Tabelle [1.10] eingetragen sind, und die mittels pro Gerät eigenem Passkey authentifiziert sind, erhalten Zugang zum lokalen LAN (und eventuell Internet), Alle Daten werden auf Funkebene verschlüsselt übertragen. Im Gegensatz zu WEP bei WLAN sind die Sicherheitsmechanismen bei Bluetooth so stark, dass Sie sich damit wirklich sicher fühlen können.

Zusätzliche Annahmen: Es wird davon ausgegangen, dass Sie auf einem anderen Gerät einen DHCP-Server in Betrieb haben, und auch den WWW-Internet-Anschluss Ihres Firmen-Netzes über ein anderes Gerät abwickeln.
blue2net ist innerhalb Ihrer Firewall in Ihr Firmen-Netzwerk integriert.

Parameter	Hier. stufe	eingestellt auf	Begründung
Bluetooth Device Name	[1.1.1]	Name Ihrer Wahl (1...16 Zeichen)	In einer Umgebung mit mehreren blue2net-Geräten sollte jedes einen eindeutigen Namen zur klaren Unterscheidung haben.
Discoverability Mode	[1.4]	nondiscoverable	Diese Einstellung erschwert potentiellen Angreifern, blue2net überhaupt zu finden. Nur wenn ein neues Bluetooth-Terminal dazukommt, wird kurzfristig auf „sichtbar“ umgestellt.
Terminal Table	[1.10]	Alle Terminals sind registriert. Für die Terminals ist die Bluetooth-Adresse [1.10.2] und der jeweilige Bluetooth-Passkey [1.10.3] (**16-stellig**!!) eingetragen. Die IP-Adresse [1.10.4] ist auf *0.0.0.0* gesetzt. ‘Allow Bluetooth Bonding’ [1.10.5] ist *enabled*	Alle Benutzer haben ein eigenes Bluetooth-Passwort, das nur in Zusammenhang mit Ihrem Bluetooth-Gerät Zugang gewährt. Benutzen Sie alle 16 Stellen des Bluetooth-Passworts.

Parameter	Hier. stufe	eingestellt auf	Begründung
Default Access Mode	[1.11]	disabled	Nur Geräte, deren Bluetooth-Adresse in [1.10] eingetragen sind, und die den entsprechenden Bluetooth-Passkey kennen, erhalten Zugang.
Minimum Length of Key for Encryption	[1.13]	16	Verschlüsselungsstärke auf Maximum (128 bit). Mit dieser Einstellung erhalten nur Geräte Zugang, die diese Verschlüsselungsstärke auch unterstützen. **Vorsicht!** Gefahr einer Aussperrung! Überprüfen Sie zuerst, ob Ihr Terminal 128 bit Verschlüsselung beherrscht (siehe Kap. 10.2 und 13.2).
Terminal IP Address Resolution	[3.1]	dhcp (Voreinstellung)	Alle Bluetooth-Geräte bekommen vom Firmen-DHCP-Server die IP-Adressen und sonstige Information zugewiesen
Local DHCP Server for NAP	[3.6.1]	disabled	Da die Firma einen eigenen DHCP-Server hat, schalten Sie den DHCP-Server für NAP Terminals auf blue2net aus
IP Connection Mode for NAP Terminals	[3.7]	bridging	Bluetooth-Geräte, die das „NAP Service“ benutzen, sind direkt am Ethernet angebunden.
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 11 Szenario „Businessbereich, sicherer Zugang für Mitarbeiter“, Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently’ [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

Optionale Einstellungen:

Wenn Sie öfter Probleme haben, Internetseiten zu erreichen (Fehlermeldung: z.B. „Die Seite kann nicht angezeigt werden. ...Fehler: Server oder DNS kann nicht gefunden werden“), könnte es daran liegen, dass der (externe) DHCP-Server nicht zuverlässig arbeitet (siehe auch Kap. 13.3). Für diesen Fall können Sie zusätzlich folgende Werte einstellen:

Parameter gruppe	Hier. stufe	eingestellt auf	Begründung
Fallback blue2net IP Address Fallback blue2net Netmask Fallback blue2net Gateway	[2.3.1] [2.3.2] [2.3.3]	Werte, die blue2net normalerweise über DHCP bekommt. Tragen Sie hier jene Werte ein, die Sie für blue2net auf Ihrem Firmen-DHCP-Server vorgesehen haben (auch zu finden unter ‚Current Configuration’ [4] >> ‚blue2net IP Configuration’ [4.2] >> blue2net IP-Adresse [4.2.1], Netzmaske [4.2.2] und Gateway [4.2.3].	blue2net verwendet diese Werte, falls Ihr Firmen-DHCP-Server kurzfristig ausfällt.
Terminal DNS Server 1/2 Terminal WINS Server 1/2 Terminal Domain Name	[3.5.1] [3.5.2] [3.5.3] [3.5.4] [3.5.5]	Werte, die normalerweise über DHCP verteilt werden (DNS). Tragen Sie hier jene Werte ein, die Ihr Firmen-DHCP-Server normalerweise an blue2net bei einer DHCP-Anfrage senden würde (auch zu finden unter ‚Current Configuration’ [4] >> ‚Terminal Server Configuration’ [4.3] >> DNS-Server [4.3.1] u. [4.3.2], WINS-Server [4.3.3] und [4.3.4] sowie Domain-Name [4.3.5]. (während der DHCP-Server funktioniert)	blue2net verwendet diese Werte, falls Ihr Firmen-DHCP-Server kurzfristig ausfällt.

Tabelle 12 Szenario „Businessbereich, sicherer Zugang für Mitarbeiter“, Optionale Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently’ [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

7.3 Szenarien für öffentlichen Zugang (Public Hot Spot)

7.3.1 Szenario mit öffentlichem Zugang für wenige Benutzer (kleiner Hot Spot, xDSL)

Typisches Szenario: Lounges in Flughäfen und Aufenthaltsräume in kleinen Hotels, kleine (Internet-)Cafès.
Charakteristik: Schneller und leichter Zugang mit Berechtigung für jedermann, nur berechtigte Personen haben Zugang zur Konfiguration, maximal 7 User gleichzeitig.
Zusätzliche Annahmen: Es wird im Beispiel davon ausgegangen, dass Sie zusätzlich zu blue2net ein xDSL-Modem mit Ethernet-Anschluss zur Verfügung haben und einen Vertrag mit einen xDSL-Internet-Service-Anbieter abgeschlossen haben.

Parameter	Hier. stufe	eingestellt auf	Begründung
Bluetooth Device Name	[1.1.1]	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. Sie können für den Namen z.B. den Namen Ihres Internet-Cafés o.ä. verwenden.
Terminal Table	[1.10]	Bluetooth-Adresse [1.10.2], Bluetooth-Passwort [1.10.3] und Terminal-IP-Adresse [1.10.4] der bei Ihnen am häufigsten verwendeten Terminals ‚Allow Bluetooth Bonding' [1.10.5] ist *enabled*	Sie wollen „VIPs" eine eigene fixe Terminal-IP-Adresse zugestehen. Setzen Sie in diesem Fall 'Terminal IP Address Resolution' [3.1] auf *masqueradingpool*. .
Default Bluetooth Passkey	[1.12]	Allgemeiner Bluetooth Passkey	Der Bluetooth Passkey kann z.B. einen Bezug zum Namen Ihres Internet-Cafés haben, damit er von Ihren Kunden leicht im Gedächtnis behalten werden kann.
blue2net IP Address Resolution	[2.1]	predefined	Diese Einstellung ist erforderlich, um die Protokolle PPtP und PPPoE verwenden zu können.

Parameter	Hier. stufe	eingestellt auf	Begründung
Fixed blue2net IP Configuration	[2.2]	Werte laut xDSL Dienst-Anbieter	Wenn Ihr xDSL Dienst-Anbieter PPtP als Protokoll verwendet, tragen Sie hier jene Werte ein, die er fordert. Falls Ihr xDSL-Anbieter PPPoE verwendet, können Sie die Standard-Einstellungen beibehalten. In beiden Fällen setzen Sie ‚Fixed Blue2net Gateway' [2.2.3] auf *0.0.0.0*
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 Establishment Control	[2.7.2]	enabled oder disabled	Wenn Ihr xDSL Anbieter die Online-Zeit verrechnet, sollten Sie Tunnel-Establishment Control auf enabled stellen, um nur Online zu sein, wenn jemand Ihren Hot Spot auch nützt.
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.
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
Terminal Fixed Servers	[3.5]	DNS-Server 1 u. 2 [3.5.1] u. [3.5.2] Tragen Sie die Werte ein, die Ihr xDSL-Anbieter empfiehlt.	

Parameter	Hier. stufe	eingestellt auf	Begründung
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 13 Szenario „Öffentlicher Zugang (kleiner Hot Spot)“, Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

Optionale Einstellungen:

Wenn Sie öfter Probleme haben, Internetseiten zu erreichen (Fehlermeldung: z.B. „Die Seite kann nicht angezeigt werden. ...Fehler: Server oder DNS kann nicht gefunden werden“), könnte es daran liegen, dass der (externe) DHCP-Server nicht zuverlässig arbeitet (siehe auch Kap. 13.3). Für diesen Fall können Sie zusätzlich folgende Werte einstellen:

Parameter	Hier. stufe	eingestellt auf	Begründung
Terminal DNS Server 1/2	[3.5.1] [3.5.2]	DNS-Server-Werte, die Ihr Dienst-Anbieter empfiehlt Unter ‚Current Configuration' [4] >> ‚Terminal Server Configuration' [4.3] finden Sie die Werte für die DNS-Server ([4.3.1] u. [4.3.2]). (während der DHCP-Server des Internet-Anbieters funktioniert)	Nur von Bedeutung, wenn der DHCP-Server Ihres Internet-Anbieters nicht zuverlässig funktioniert.

Tabelle 14 Szenario „Öffentlicher Zugang (kleiner Hot Spot)“, Optionale Einstellungen

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

7.3.2 Szenario mit öffentlichem Zugang für viele Benutzer (großer Hot Spot, xDSL)

Typisches Szenario: Lounges in Flughäfen und Aufenthaltsräume in großen Hotels, größere (Internet-)Cafès.
Charakteristik: Schneller und leichter Zugang mit Berechtigung für jedermann, nur berechtigte Personen haben Zugang zur Konfiguration, bis zu 28 User gleichzeitig.
Zusätzliche Annahmen: Es wird im Beispiel davon ausgegangen, dass Sie zusätzlich zu mehreren blue2net ein xDSL-Modem mit Ethernet-Anschluss zur Verfügung haben und einen Vertrag mit einen xDSL-Internet-Service Anbieter abgeschlossen haben. Sie benötigen für je 7 User, die gleichzeitig über Bluetooth einen Internet Zugang nutzen, 1 blue2net Gerät.

Sie können mehr als 7 Benutzern gleichzeitig Internet Zugang gewähren, wenn Sie mehrere blue2net Geräte kaskadieren.

Dabei gibt es 2 Rollen:

- Master-blue2net ist jenes Gerät, welches das xDSL-Modem bedient und über DHCP die Bluetooth-Terminals (Laptops, PDAs) der Kunden mit einer IP-Adresse versorgt.
- Die restlichen blue2net Geräte sind in der Slave-Rolle konfiguriert.

Der Master arbeitet als Access-Router, da seine Netto-Nutzbandbreite auf der Ethernet-Schnittstelle etwa 300 kBps (Kilobyte pro Sekunde) oder 2,4 Mbps (Megabit pro Sekunde) beträgt. Einem blue2net steht etwa eine Netto-Funkbandbreite von 80 kBps zur Verfügung, daher können Sie 1 Master und 3 Slaves ohne Einschränkung betreiben.

Beachten Sie, dass Sie auch über xDSL 300 kBps Bandbreite zur Verfügung haben sollten, wenn es durch gleichzeitige Aktivität aller Teilnehmer keine Einschränkungen geben soll.

Technischer Hinweis: Da Bluetooth ein schnelles Frequenz-Sprung-Verfahren benutzt (1600 Frequenzwechsel pro Sekunde) und 79 Frequenzen zur Verfügung stehen, die „zufällig“ benutzt werden, kommt es beim Betrieb vieler Access-Points (bis zu 10 und mehr) nicht zu merkbaren Leistungseinbußen.

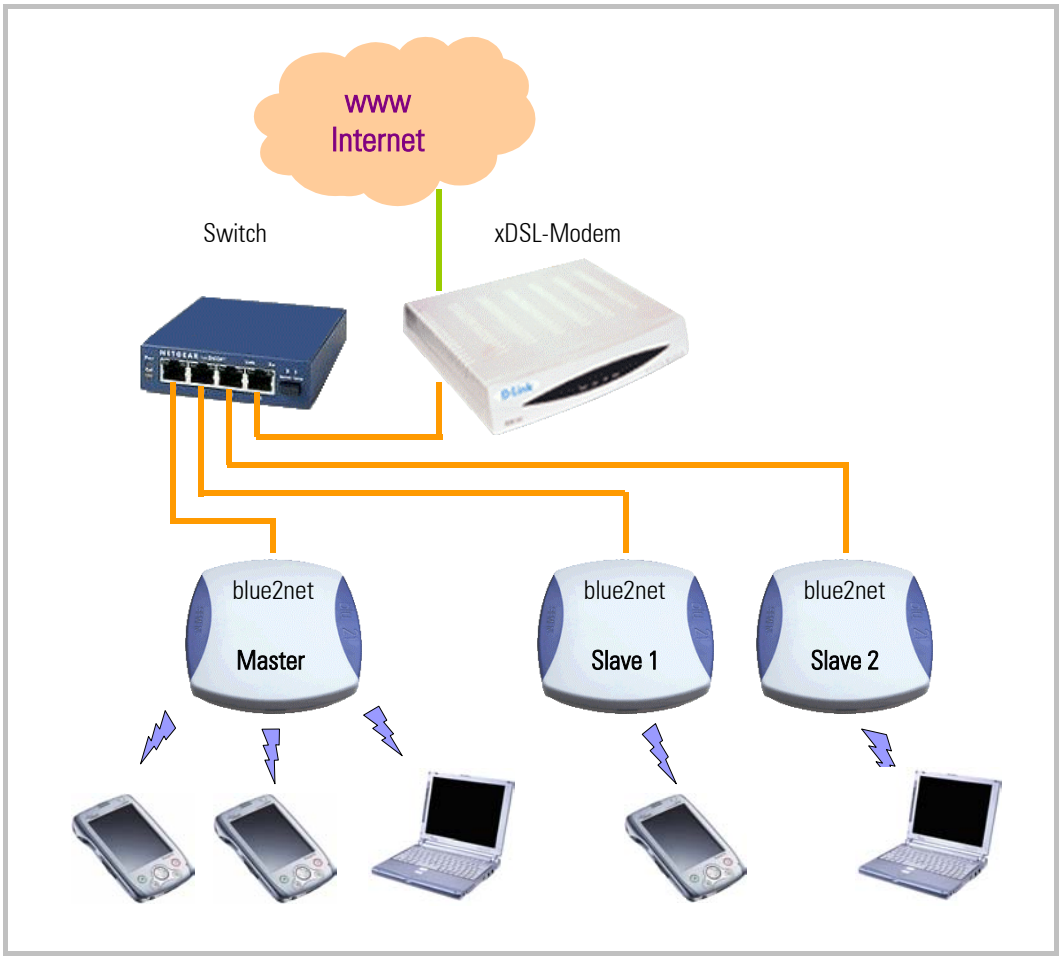


Abb. 7 Szenario „Öffentlicher Zugang (großer Hot Spot)“ mit Master/Slave-Konfiguration

Einstellungen am Master blue2net:

Hinweis zur Inbetriebnahme des Master-blue2net: Da der Master-blue2net die Slave-blue2net mit IP-Adressen versorgt, soll dieser betriebsbereit sein, bevor die Slaves eingeschaltet werden.

Parameter	Hier. stufe	eingestellt auf	Begründung
Bluetooth Device Name	[1.1.1]	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. Sie können für den Namen z.B.: den Namen Ihres Kaffeehauses o.ä. verwenden.

Parameter	Hier. stufe	eingestellt auf	Begründung
Terminal Table	[1.10]	Bluetooth-Adresse [1.10.2], Bluetooth-Passwort [1.10.3] und Terminal-IP-Adresse [1.10.4] der bei Ihnen am häufigsten verwendeten Terminals 'Allow Bluetooth Bonding' [1.10.5] ist *enabled*	Sie wollen „VIPs" eine eigene fixe Terminal-IP-Adresse zugestehen.. . Außerdem sollten Sie hier die Ethernet-MAC-Adressen der Slave-blue2net-Geräte und die für Sie vorgesehenen Internet-Adressen im Netz 192.16.8.2.x eintragen. (im Bereich 192.168.2.71-192.168.2.253)
Default Bluetooth Passkey	[1.12]	Allgemeiner Bluetooth Passkey	Der Bluetooth-Passkey kann z.B. einen Bezug zum Namen Ihres Internet-Cafes haben, damit er von Ihren Kunden leicht im Gedächtnis behalten werden kann.
blue2net IP Address Resolution	[2.1]	predefined	Über PPtP und PPPoE wird nicht DHCP unterstützt.
Fixed blue2net IP Configuration	[2.2]	Werte laut xDSL Dienst-Anbieter	Wenn Ihr xDSL Dienst-Anbieter PPtP als Protokoll verwendet, tragen Sie hier jene Werte ein, die er fordert. Falls Ihr xDSL-Anbieter PPPoE verwendet, tragen Sie hier jene Adresse ein, die in ‚IP Masquerading' [2.5] steht, also z.B. 192.168.2.2 . In beiden Fällen setzen Sie ‚Fixed blue2net Gateway' [2.2.3] auf *0.0.0.0*
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.

Parameter	Hier. stufe	eingestellt auf	Begründung
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
Additional IP Interface for blue2net	[2.8.1]	enabled/disabled zweites IP-Interface	Wenn Ihr xDSL-Anbieter PPtP verwendet, schalten Sie hier auf enabled. Wenn Ihr xDSL-Dienstanbieter PPPoE verwendet, belassen Sie hier die Einstellung *disabled*
Local DHCP Server for Ethernet	[2.6.2]	enabled	Schalten Sie den blue2net-internen DHCP-Server für Ethernet ein.
IP Connection Mode for NAP Terminals	[3.7]	bridging	Schalten Sie den Modus für die Network-Access-Profile Benutzer auf *bridging*
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 15 Szenario „Öffentlicher Zugang (großer Hot Spot)“, Einstellungen am Master-blue2net

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently’ [6.2] abzuspeichern (siehe Kapitel 8.9.2)! und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

Optionale Einstellungen:

Wenn Sie öfter Probleme haben, Internetseiten zu erreichen (Fehlermeldung: z.B. „Die Seite kann nicht angezeigt werden. ...Fehler: Server oder DNS kann nicht gefunden werden“), könnte es daran liegen, dass der (externe) DHCP-Server nicht zuverlässig arbeitet (siehe auch Kap. 13.3). Für diesen Fall können Sie zusätzlich folgende Werte einstellen:

Parameter	Hier. stufe	eingestellt auf	Begründung
Terminal DNS Server 1/2	[3.5.1] [3.5.2]	DNS-Server-Werte, die Ihr Dienst-Anbieter empfiehlt Unter ‚Current Configuration' [4] >> ‚Terminal Server Configuration' [4.3] finden Sie die Werte für die DNS-Server ([4.3.1] u. [4.3.2]). (während der DHCP-Server des Internet-Anbieters funktioniert)	Nur von Bedeutung, wenn der DHCP-Server Ihres Internet-Anbieters nicht zuverlässig funktioniert.

Tabelle 16 Szenario „Öffentlicher Zugang (großer Hot Spot)“, Optionale Einstellungen am Master-blue2net

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

Einstellungen an den Slave-blu2net-Geräten:

Parameter	Hier. stufe	eingestellt auf	Begründung
Bluetooth Device Name	[1.1.1]	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. Sie können für den Namen z.B.: den Namen Ihres Kaffeehauses o.ä. verwenden.
Terminal Table	[1.10]	Bluetooth-Adresse [1.10.2], Bluetooth-Passwort [1.10.3] der bei Ihnen am häufigsten verwendeten Terminals 'Allow Bluetooth Bonding' [1.10.5] ist *enabled*	Sie wollen „VIPs" eine eigene fixe Terminal-IP-Adresse zugestehen. Die IP-Adresse der VIP-Terminals belassen Sie auf 0.0.0.0, da sie über DHCP vom Master-blue2net zugewiesen wird. Hinweis: Die Bluetooth-Adresse [1.10.2] und das Bluetooth-Passwort [1.10.3] sollen hier ident zum Master-blue2net gewählt werden (gleiche Tabelle bis auf IP-Adresse).
Default Access Mode	[1.11]	enabled (Voreinstellung)	Leichter Zugang für jedermann
Default Bluetooth Passkey	[1.12]	Allgemeiner Bluetooth-Passkey	Der Bluetooth-Passkey kann z.B. einen Bezug zum Namen Ihres Internet-Cafes haben, damit er von Ihren Kunden leicht im Gedächtnis behalten werden kann.
blue2net IP Address Resolution	[2.1]	dhcp (Voreinstellung)	Die Slave-blue2net-Geräte bekommen Ihre IP-Adresse vom Master-blue2net-Gerät.
Terminal IP Address Resolution	[3.1]	dhcp	Die IP-Adressen aller Terminals werden vom Master-blue2net-Gerät verwaltet und über DHCP verteilt.
Local DHCP Server for NAP	[3.6.1]	disabled	Schalten Sie den blue2net-internen DHCP-Server für NAP aus, das übernimmt das Master-blue2net-Gerät.
IP Connection Mode for NAP Terminals	[3.7]	bridging	Schalten Sie den Modus für die Network-Access-Profile Benutzer auf *bridging.*

Parameter	Hier. stufe	eingestellt auf	Begründung
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 17 Szenario „Öffentlicher Zugang (großer Hot Spot)“, Einstellungen am Slave-blue2net

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

Optionale Einstellungen:

Parameter	Hier. stufe	eingestellt auf	Begründung
Fallback blue2net IP Address	[2.3.1]	[2.3.1]: Tragen Sie hier die gleichen IP-Parameter ein, die Sie am Master für dieses Slave-Gerät unter [1.10.4] eingetragen haben.	Diese Werte dienen nur als Rückfall-Werte, falls das Master-blue2net während des Neustarts des Slave-Geätes ausgefallen ist.
Fallback blue2net Netmask	[2.3.2]	[2.3.2]: ‚Terminal Netmask' [3.4] des Master-blue2net-Gerätes, also z.B. 255.255.255.0.	
Fallback blue2net Gateway	[2.3.3]	[2.3.3]: Masquerading-IP ‚IP Masquerading' [2.5] des Master-blue2net-Gerätes, also z.B. 192.168.2.2 .	
Terminal DNS Server 1/2	[3.5.1] [3.5.2]	DNS-Server-Werte, die Ihr Dienst-Anbieter empfiehlt Unter ‚Current Configuration' [4] >> ‚Terminal Server Configuration' [4.3] finden Sie die Werte für die DNS-Server ([4.3.1] u. [4.3.2]). (während der DHCP-Server des Internet-Anbieters funktioniert)	Nur als Rückfall-Werte, wenn das Master-blue2net-Gerät während eines Neustarts des Slave-blue2net-Gerätes ausgefallen ist.

Tabelle 18 Szenario „Öffentlicher Zugang (großer Hot Spot)“, Optionale Einstellungen am Slave-blue2net

Vergessen Sie nicht, die Einstellungen mit ‚Save Settings Permanently' [6.2] abzuspeichern (siehe Kapitel 8.9.2) und warten Sie anschließend ca. 2 min. Danach ist das Gerät wieder zur Benützung bereit.

8 Konfiguration

8.1 Haupt-Konfigurations-Seite

Klicken Sie auf **Configuration** im Web-Interface (Abb. 3), um zu der folgenden Übersicht (Abb. 8) zu gelangen. Die Nummern in den eckigen Klammern zeigen den Platz eines Parameters in der Hierarchie des Web-Interface an (Details dazu in Kapitel 8.3).

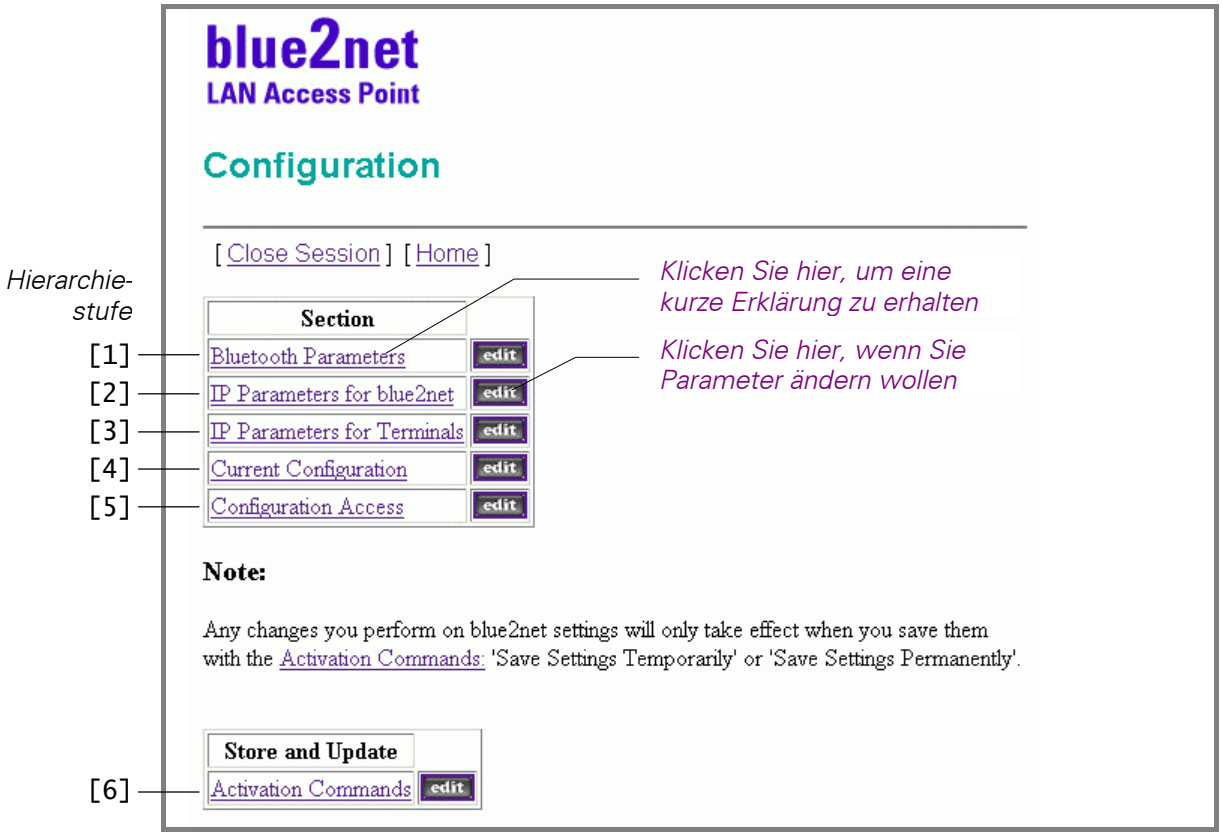


Abb. 8 Haupt-Konfigurations-Seite [0]

Klicken Sie auf eine der <edit>-Schaltflächen und geben Sie das Konfigurations-Passwort ein (Abb. 9). Das voreingestellte Passwort lautet „**changeme**".

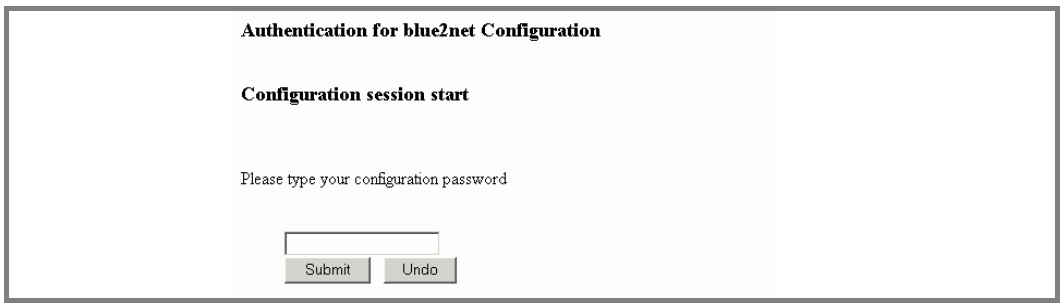


Abb. 9 Authentifizierung (Authentication)

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

Aus Sicherheitsgründen sollten Sie das Passwort sofort ändern. Vergessen Sie nicht, dass Sie die Änderung anschließend abspeichern müssen. Verwenden Sie dazu die '*Activation Commands*' (siehe Kapitel 8.9)!

Hinweis: Merken Sie sich 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 Kap. 10.1

Objekte (siehe Abb. 8)	**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 und eine zweite IP-Schnittstelle aktiviert und konfiguriert werden für den Einsatz von blue2net als Access-Router.
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 Range). Ferner können hier die 2 blue2net-internen DHCP-Server für Bluetooth PAN NAP und Ethernet kontrolliert werden.
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.

Objekte (siehe Abb. 8)	Hierarchie stufe	Erklärung
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 19 Parametergruppen auf der Haupt-Konfigurations-Seite [0]

8.2 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 8.9)!

Bluetooth-Verbindungen (auch die anderer Terminals) werden abgebrochen, wenn Sie mit einem der Aktivierungsbefehle abspeichern (siehe Kapitel 8.9)!

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.

8.3 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 8.1)	Aktion / Anzeige	Seite
[1] **Bluetooth Parameters** (Kapitel 8.4)		**56**
[1.1] Bluetooth Device Name	➡ Objects	57
[1.1.1] Bluetooth Device Name	edit, ▸ Submit	61
[1.1.2] IP Address Suffix Mode	edit, ▸ Submit	61
[1.2] Bluetooth Device Address	eindeutige, fixe Adresse	57
[1.3] Multipoint Mode	edit, ▸ Submit,	57
[1.4] Discoverability Mode	edit, ▸ Submit	57
[1.5] Connectability Mode	edit, ▸ Submit	58
[1.6] Max. No. of Terminals Connected	edit, ▸ Submit	58
[1.7] Number of Services	Nummer	58
[1.8] Service Table	➡ Table (3 Reihen)	58 & 61
[1.8.1] Service Index	Nummer	62
[1.8.2] Service Name	edit, ▸ Submit	62
[1.8.3] Service Description	edit, ▸ Submit	62
[1.8.4] Auth. Level	edit, ▸ Submit	** 63
[1.8.5] Service Provider	edit, ▸ Submit	63
[1.8.6] Service URL	edit, ▸ Submit	63
[1.8.7] Service ID	Nummer	63
[1.8.8] Bluetooth Service Class	Service Class	64
[1.8.9] Activation	edit, ▸ Submit	64
[1.9] Number of Terminals	Nummer	58
[1.10] Terminal Table	➡ Table (40 Reihen)	58
[1.10.1] Terminal Index	Nummer	67
[1.10.2] Terminal Bluetooth Address	edit, ▸ Submit	67
[1.10.3] Terminal Bluetooth Passkey	edit, ▸ Submit	67
[1.10.4] Terminal IP Address	edit, ▸ Submit	68
[1.10.5] Allow Bluetooth Bonding	edit, ▸ Submit	* 68
[1.11] Default Access Mode	edit, ▸ Submit	59
[1.12] Default Bluetooth Passkey	edit, ▸ Submit	59
[1.13] Minimum Length of Key for Encryption	edit, ▸ Submit	* 60
[2] **IP Parameters for blue2net** (Kapitel 8.5)		**69**
[2.1] blue2net IP Address Resolution	edit, ▸ Submit	70
[2.2] Fixed blue2net IP Configuration	➡ Objects	70
[2.2.1] Fixed blue2net IP Address	edit, ▸ Submit	72
[2.2.2] Fixed blue2net Netmask	edit, ▸ Submit	72
[2.2.3] Fixed blue2net Gateway	edit, ▸ Submit	72

Tabelle 20 Hierarchie in den Seiten für die Konfigurationseinstellungen (1)

		Aktion / Anzeige	Seite
[2]	**IP Parameters for blue2net** (Kapitel 8.5)		**69**
[2.3]	DHCP blue2net IP Objects	➡ Objects	70
[2.3.1]	Fallback blue2net IP Address	edit, ▸ Submit	73
[2.3.2]	Fallback blue2net Netmask	edit, ▸ Submit	73
[2.3.3]	Fallback blue2net Gateway	edit, ▸ Submit	73
[2.4]	Time Server IP	edit, ▸ Submit	70
[2.5]	IP Masquerading	edit, ▸ Submit	71
[2.6]	Firewall Settings	➡ Objects	71
[2.6.1]	Default Firewall	edit, ▸ Submit	74
[2.6.2]	Port Forwarding Rules	➡ Table (10 Reihen)	* 74
[2.6.2.1]	Index	Nummer	* 75
[2.6.2.2]	Enable Rule	edit, ▸ Submit	* 76
[2.6.2.3]	Protocol	edit, ▸ Submit	* 76
[2.6.2.4]	Lower Port Number	edit, ▸ Submit	* 76
[2.6.2.5]	Enable Port Range	edit, ▸ Submit	* 77
[2.6.2.6]	Higher Port Number	edit, ▸ Submit	* 77
[2.6.2.7]	Fwd. Destination IP Addr.	edit, ▸ Submit	* 77
[2.6.2.8]	Fwd. Source IP Address	edit, ▸ Submit	* 77
[2.6.2.9]	Fwd. Source IP Add. Netm.	edit, ▸ Submit	* 77
[2.6.3]	Number of Port Forwarding Rules	Nummer	* 74
[2.7]	Tunnel Configuration (PPPoE / PPTP)	➡ Objects	71
[2.7.1]	Tunnel Mode	edit, ▸ Submit	79
[2.7.2]	Tunnel Establishment Control	edit, ▸ Submit	80
[2.7.3]	Authentication Parameters	➡ Objects	80
[2.7.3.1]	Tunnel User Name	edit, ▸ Submit	81
[2.7.3.2]	Tunnel User Password	edit, ▸ Submit	81
[2.7.4]	PPTP Server IP Address	edit, ▸ Submit	80
[2.8]	Access Router	➡ Objects	* 71
[2.8.1]	Additional IP Interface	edit, ▸ Submit	* 83
[2.8.2]	Fixed Additional IP Interface	➡ Objects	* 83
[2.8.2.1]	Fixed b2n Addl. IP Address	edit, ▸ Submit	* 83
[2.8.2.2]	Fixed b2n Addl. IP Netmask	edit, ▸ Submit	* 83
[3]	**IP Parameters for Terminals** (Kapitel 8.5.7)		**82**
[3.1]	Terminal IP Address Resolution	edit, ▸ Submit	84
[3.2]	Start of Terminal IP Address Pool Range	edit, ▸ Submit	*** 86
[3.3]	End of Terminal IP Address Pool Range	edit, ▸ Submit	*** 86
[3.4]	Terminal Net Mask	edit, ▸ Submit	86
[3.5]	Terminal Fixed Servers	➡ Objects	86
[3.5.1]	Terminal DNS Server 1	edit, ▸ Submit	88
[3.5.2]	Terminal DNS Server 2	edit, ▸ Submit	88
[3.5.3]	Terminal WINS Server 1	edit, ▸ Submit	89
[3.5.4]	Terminal WINS Server 2	edit, ▸ Submit	89
[3.5.5]	Terminal Domain Name	edit, ▸ Submit	89
[3.6]	Local DHCP Server Objects	➡ Objects	* 86
[3.6.1]	Local DHCP Server for NAP	edit, ▸ Submit	* 90
[3.6.2]	Local DHCP Server for Ethernet	edit, ▸ Submit	* 90
[3.7]	IP Connection Mode for NAP Terminals	edit, ▸ Submit	* 87
[3.8]	Available IP Addresses for Local Wired Network	➡ Objects	* 87
[3.8.1]	Lowest IP Address of Range	edit, ▸ Submit	* 91
[3.8.2]	Highest IP Address of Range	edit, ▸ Submit	* 91
[3.9]	Fixed IP Addresses for Local Wired Network	➡ Table (40 Reihen)	* 87
[3.9.1]	Index	Nummer	* 93
[3.9.2]	MAC Address	edit, ▸ Submit	* 93
[3.9.3]	IP Address	edit, ▸ Submit	* 93
[3.10]	Number of Fixed IP Addresses	Nummer	* 87

Tabelle 21 Hierarchie in den Seiten für die Konfigurationseinstellungen (2)

		Aktion / Anzeige	Seite
[4]	**Current Configuration** (Kapitel 8.7)		**94**
[4.1]	MAC Address	eindeutige, fixe Adresse	94
[4.2]	blue2net IP Configuration	➡ Objects	95
[4.2.1]	blue2net IP Address	Adresse	95
[4.2.2]	blue2net Netmask	Adresse	95
[4.2.3]	blue2net Gateway	Adresse	95
[4.3]	Terminal Server Configuration	➡ Objects	96
[4.3.1]	Terminal DNS Server 1	Adresse	96
[4.3.2]	Terminal DNS Server 2	Adresse	96
[4.3.3]	Terminal WINS Server 1	Adresse	96
[4.3.4]	Terminal WINS Server 2	Adresse	96
[4.3.5]	Terminal Domain Name	Domäne	96
[4.4]	Version Information	➡ Objects	97
[4.4.1]	Module Firmware Version	Version	97
[4.4.2]	PPCBoot Version	Version	97
[4.4.3]	blue2net Software Version	Version	97
[4.4.4]	blue2net Hardware Version	Version	97
[4.4.5]	SieMo Module Info	Version	97
[4.5]	Tunnel Status (PPPoE/PPTP)	➡ Objects	94
[4.5.1]	Tunnel Status	Status d.Tunnel-Verbind.	98
[4.5.2]	IP Address of Tunnel Endpoint on b2n	Adresse	* 98
[5]	**Configuration Access** (Kapitel 8.8)		**99**
[5.1]	SNMP Access	edit, ▶ Submit	99
[5.2]	Configuration Password	edit, ▶ Submit	99
[6]	**Activation Commands** (Kapitel 8.9)		**100**
[6.1]	Save Settings Temporarily	edit, ▶ Submit	101
[6.2]	Save Settings Permanently	edit, ▶ Submit	102
[6.3]	Reset blue2net	edit, ▶ Submit	103
[6.4]	Update Software	edit, ▶ Submit	104
[6.5]	Restore Default Settings	edit, ▶ Submit	104
[6.6]	Store Specific Homepage	edit, ▶ Submit	104

Tabelle 22 Hierarchie in den Seiten für die Konfigurationseinstellungen (3)

Änderungshinweise:

gegenüber der Vorgänger-SW v 3.0.0 / Bedienungsanleitung v 3.0 wurde folgendes geändert (siehe auch Kap. 11.3):

*) neuer Parameter

**) Werkseinstellung (Default-Wert) wurde geändert!

***) Funktionsänderung

[3.2] und [3.3] wurden umbenannt und haben neue Funktion

[3.3.1] und [3.3.2] sind entfallen

[5.2.1] wird ab jetzt mit [5.2] bezeichnet

8.4 Bluetooth Parameters [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.

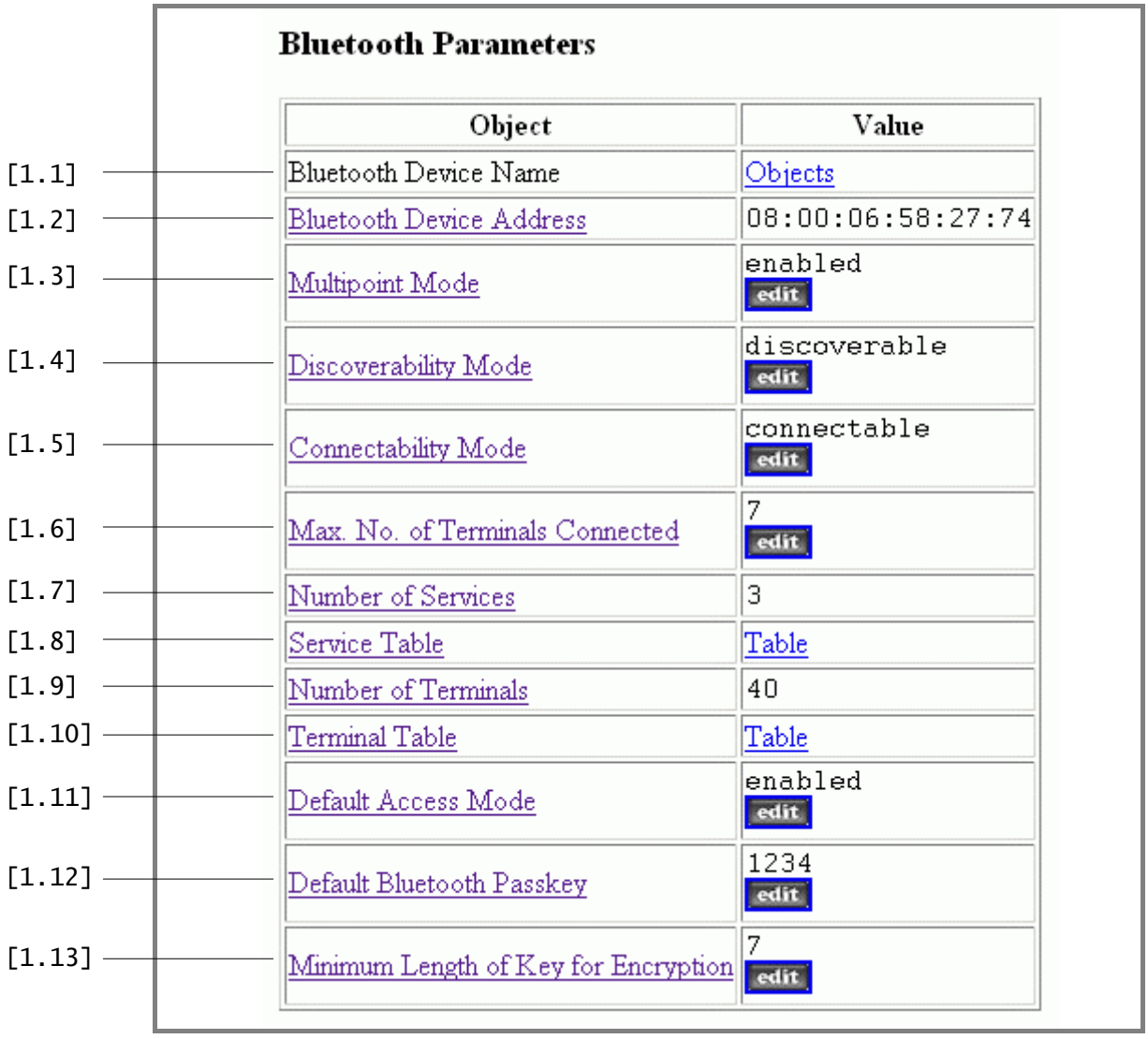


Abb. 10 Bluetooth Parameters [1]

Objekte (siehe Abb. 10)	**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”. **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 10) Terminals, deren Software keine direkte Eingabe einer BT-Adresse zum Verbindungsaufbau erlaubt, müssen blue2net einmal „gesehen“ und die Daten gespeichert haben, bevor Sie eine Verbindung aufbauen können.

Objekte (siehe Abb. 10)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
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 10)
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 10)
Number of Services	[1.7]	3 (drei) (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 8.4.1).
Number of Terminals	[1.9]	40 (vierzig) (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 8.4.3).

Objekte (siehe Abb. 10)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
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 10)
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. Das Passwort sollte möglichst 16 Stellen lang sein und aus Groß- u. Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 10)

Objekte (siehe Abb. 10)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Minimum Length of Key for Encryption	[1.13]	7 anderer Wert Ihrer Wahl (1...16) 16 = 128 bit 7 = 56 bit 5 = 40 bit	Mit diesem Objekt bestimmen Sie die minimal erforderliche Schlüssellänge für Bluetooth-Dienste deren Auth. Level auf 'authandenc' eingestellt ist. Der Wert repräsentiert die Anzahl von Oktetten (Achtbitzeichen), die beim Verschlüsseln verwendet wird. Ein Wert von 7 entspricht 7 mal 8 = 56 bit Die Schlüssellänge wird für Services zwischen blue2net und Terminals ausgehandelt. Maximaler Schutz gegen Mithören ist bei einer Schlüssellänge von 16 (= 128 Bit) gegeben. Achtung! Gefahr einer Aussperrung! Überprüfen Sie zuerst, ob Ihr Terminal 128 bit Verschlüsselung beherrscht (siehe Kap. 10.2, 13.2). Terminals, welche die volle Schlüssellänge von 128 bit nicht beherrschen (z.B. wenn 16 eingestellt ist, was 128 bit entspricht), können die Dienste nicht benützen (sind dann von der Datenübertragung ausgeschlossen). Es kann aber durch geeignete Wahl von 'Minimum Length of Key for Encryption' auch eine Verschlüsselung mit geringerer Schlüssellänge ermöglicht werden. Die Gefahr des „Mithörens“ wird dadurch aber erhöht.

Tabelle 23 Bluetooth Parameters [1]

8.4.1 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 werden.

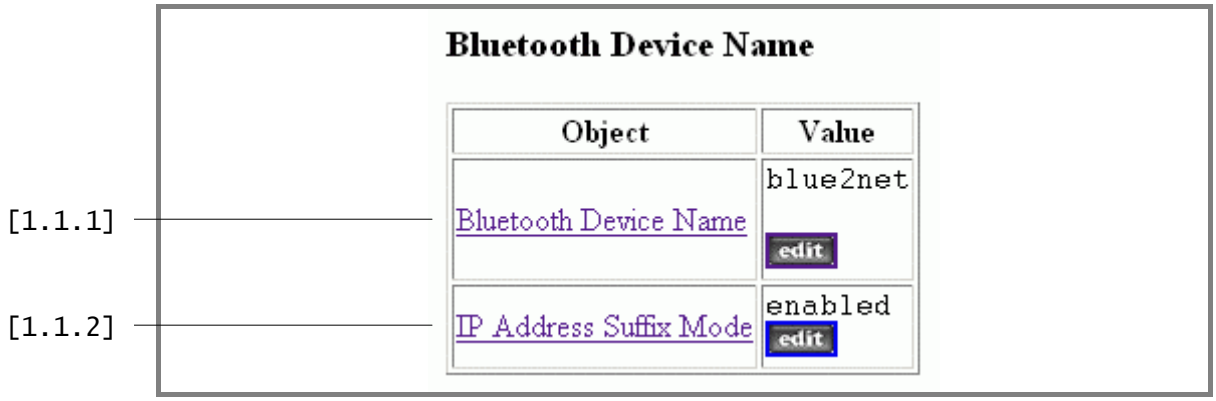


Abb. 11 Bluetooth Device Name [1.1]

Objekte (siehe Abb. 11)	**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 24 Bluetooth Device Name [1.1]

8.4.2 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.

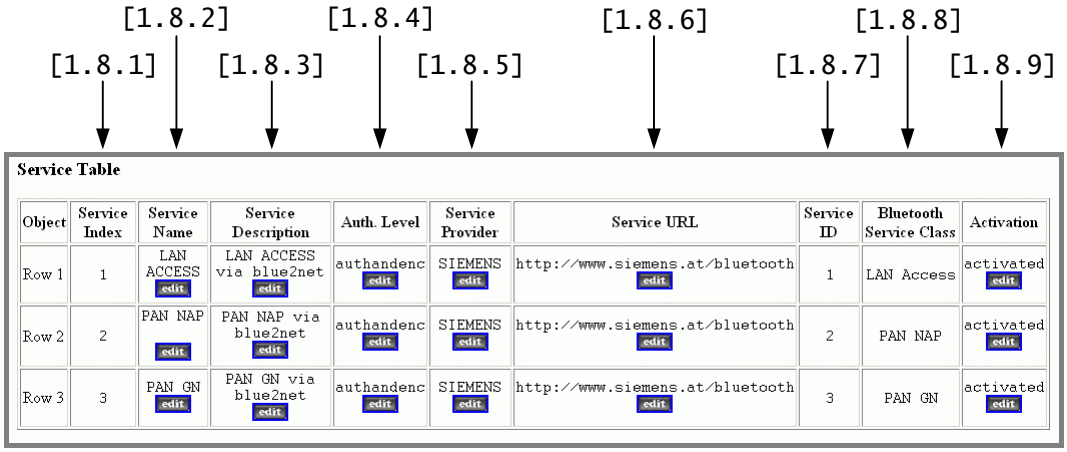


Abb. 12 Service Table [1.8]

Objekte (siehe Abb. 12)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Service Index	[1.8.1]	1 / 2 / 3 (nur Anzeige)	Ein eindeutiger Wert für jeden Dienst
Service Name	[1.8.2]	LAN ACCESS 1/ PAN NAP/ PAN GN 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/ PAN NAP/ PAN GN/ via blue2net andere Beschreibung Ihrer Wahl (1...31 Zeichen)	Anzeige der Dienste-Beschreibung. Beeinflusst nicht die Funktionalität.

Objekte (siehe Abb. 12)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Auth. Level	[1.8.4]	authandenc noauth auth	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 [1.12] bzw. [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 [1.12] bzw. [1.10.3] gefragt, bevor der Benutzer irgendeinen verschlüsselten Datentransfer durchführen kann. **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 10)
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 / 2 / 3 (nur Anzeige)	Wert (Service Record Handle Subfield), der einem Client übermittelt wird, der SDP verwendet

Objekte (siehe Abb. 12)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Bluetooth Service Class	[1.8.8]	LAN Access / PAN NAP / PAN GN (nur Anzeige)	Beschreibung der Service Class (Bluetooth Profile) die blue2net anbietet.
Activation	[1.8.9]	activated deactivated	Wenn die entsprechende Bluetooth Service Class auf *activated* gesetzt ist, kann diese von einem Client (Bluetooth-Terminal / Bluetooth-Gerät) benutzt werden. **Vorsicht!** Gefahr einer Aussperrung, falls **alle 3** Einträge auf *deactivated* gesetzt sind! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 10)

Tabelle 25 Service Table [1.8]

8.4.3 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 für ‚LAN Access Profile' zu erhalten, muss 'Terminal IP Address Resolution' [3.1] auf *predefined* oder *masqueradingpool* gesetzt sein.

Um dem Terminal bei Benutzung des PAN NAP-Service die IP-Adresse zuweisen zu können, muss der DHCP-Server für NAP-Terminals [3.6.1] auf *enabled* gesetzt sein (siehe Kap. 8.6.2).

Wenn Sie wollen, dass sich alle Bluetooth Terminals mit eigenem Bluetooth-Passwort authentifizieren müssen, aber IP-Adressen aus dem Pool zugewiesen bekommen sollen, setzen Sie ‚Default Access Mode' [1.11] auf *disabled*. In der Terminal-Tabelle tragen Sie nur Bluetooth-Adressen [1.10.2] und Bluetooth-Passkeys [1.10.3] ein, die IP-Adressen [1.10.4] lassen Sie aber auf *0.0.0.0* gestellt.

Wenn der ‚IP Connection Mode for NAP Terminals' [3.7] (siehe Kap. 8.6, Seite 87) auf *bridging* gesetzt ist, kann die Terminal-Tabelle auch für Rechner benutzt werden, die über Ethernet mit blue2net verbunden sind. Diese werden dann mit DHCP konfiguriert, wenn ‚Local DHCP Server for Ethernet' [3.6.2] auf *enabled* gesetzt wurde.

Als Terminal-Bluetooth-Adresse [1.10.2] ist dann die Ethernet-Adresse der Netzwerkkarte des entsprechenden Rechners einzutragen. Der ‚Terminal Bluetooth Passkey' [1.10.3] ist in diesem Fall ohne Bedeutung. Wenn ‚IP Connection Mode for NAP Terminals' [3.7] auf *routing* gesetzt ist, verwenden Sie die Werte-Tabelle zu ‚Fixed IP Addresses for Local Wired Network' [3.9] (siehe Abb. 27) für die Zuweisung von IP-Adressen an Rechner-Netzwerkarten.

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 (zwischen 'Start/End of Terminal IP Address Pool Range' [3.2] u. [3.3]) .

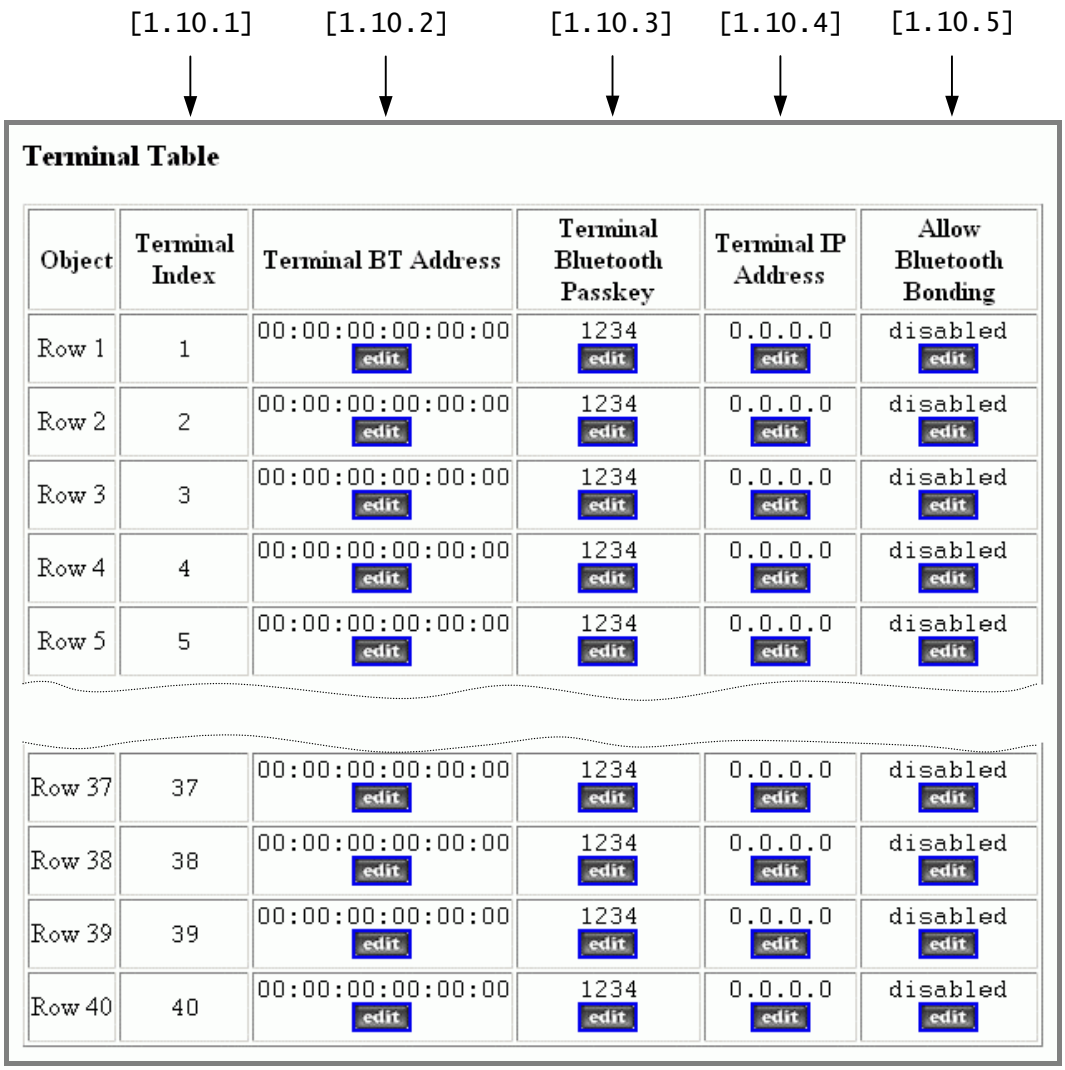


Abb. 13 Terminal Table [1.10]

Objekte (siehe Abb.13)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Terminal Index	[1.10.1]	1-40 (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 oder die Ethernet-Adresse einer Rechner-Netzwerkkarte, wenn ‚IP Connection Mode for NAP Term.'[3.7] auf *bridging* gesetzt ist und ein Rechner mit DHCP konfiguriert werden soll. 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 10und 10.1)
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 10)

Objekte (siehe Abb.13)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
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, sofern es „LAN Access Profile“ benutzt. Bei „PAN NAP-Service“ wird die Terminal-IP-Adresse zugewiesen, wenn ‚Local DHCP Server for NAP’ [3.6.1] auf *enabled* gesetzt ist. Wenn es sich um eine Ethernet-Adresse handelt, wird die ‚Terminal IP Address‘ per DHCP dem Rechner zugewiesen, wenn ‚Local DHCP Server for NAP’ [3.6.1] auf *enabled* gesetzt ist und ‚IP Connection Mode for NAP Terminals’ [3.7] auf *bridging* gesetzt ist. Wenn aber bei 'Terminal IP Address' *0.0.0.0* eingetragen ist, wird dem Terminal ein Wert aus dem Vorrat von Terminal-IP-Adressen zwischen 'Start/End of Terminal IP Address Pool Range' [3.2] u. [3.3] zugewiesen.
Allow Bluetooth Bonding	[1.10.5]	disabled enabled	Wenn 'Allow Bluetooth Bonding' auf *enabled* eingestellt ist, wird die interne Information zur Authentifikation für dieses Bluetooth-Gerät im permanenten Speicher von blue2net abgelegt. Die Eingabe des Bluetooth-Passkey [1.10.3] ist nur einmalig beim ersten Verbindungsaufbau notwendig. Danach "kennen" sich die Geräte und eine Eingabe des Bluetooth-Passkeys [1.10.3] ist daher nicht mehr erforderlich.

Tabelle 26 Terminal Table [1.10]

8.5 IP Parameters for blue2net [2]

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

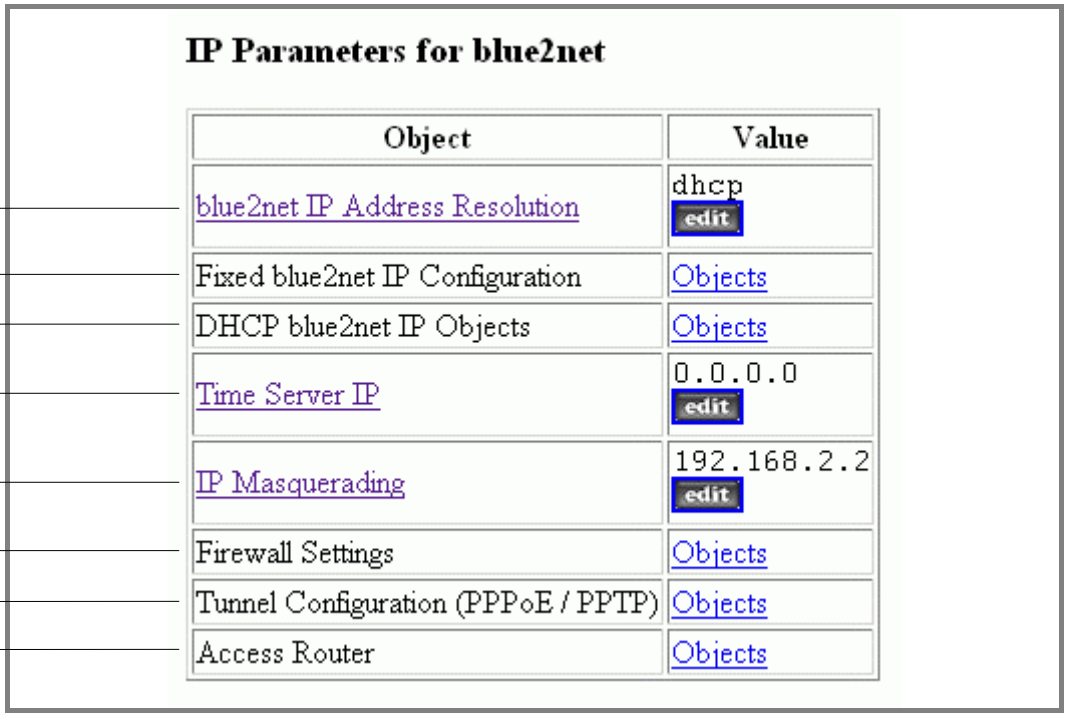


Abb. 14 IP Parameters for blue2net [2]

Objekte (siehe Abb. 14)	**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 10)
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).

Objekte (siehe Abb. 14)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
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. Wenn Sie ‚IP Connection Mode for NAP Terminals' auf *routing* gestellt haben, sollte dieser Wert auch verschieden von ‚Fixed blue2net Additional IP Address' [2.8.2.1] sein, falls ‚Additional IP Interface' [2.8.1] auf *enabled* gesetzt ist.
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. 17). Auch „Port Forwarding" ist hier konfigurierbar.
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).
Access Router	[2.8]		Konfiguration einer zweiten IP-Schnittstelle am Ethernet-Anschluss, um blue2net als Access-Router betreiben zu können.

Tabelle 27 IP Parameters for blue2net [2]

8.5.1 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 .

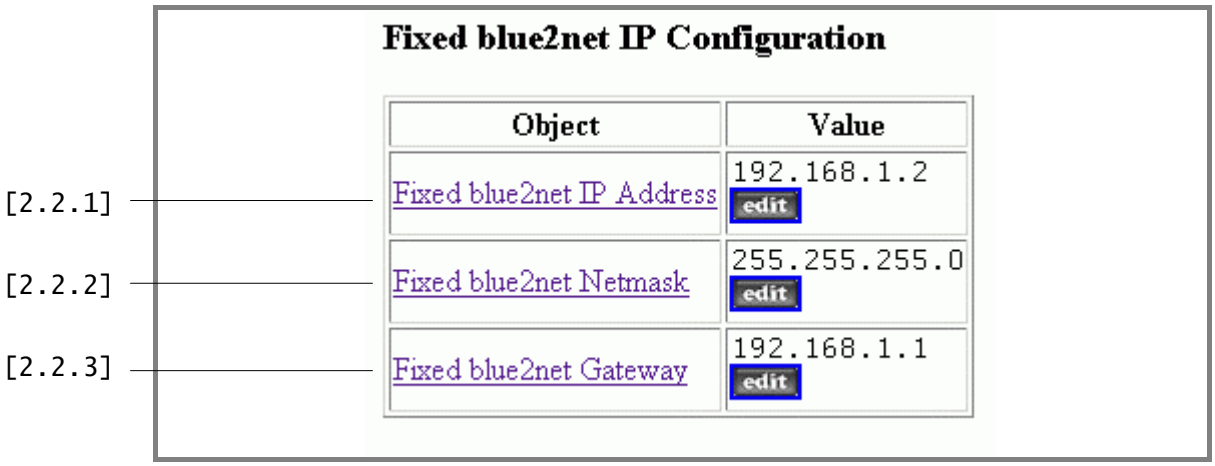


Abb. 15 Fixed blue2net IP Configuration [2.2]

Objekte (siehe Abb. 15)	**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 28 Fixed blue2net IP Configuration [2.2]

8.5.2 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 Kapitel 4.3.

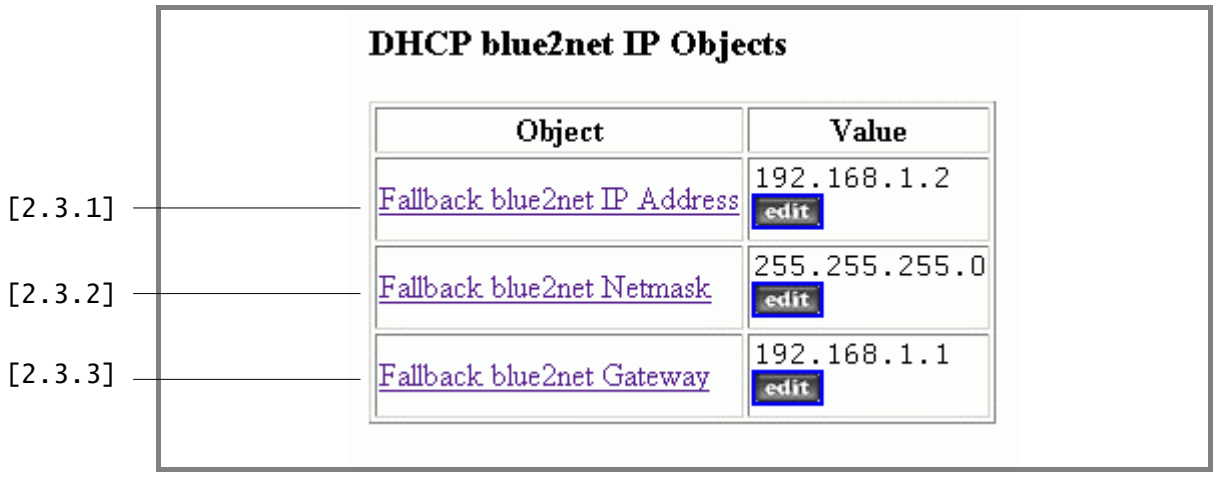


Abb. 16 DHCP blue2net IP Objects [2.3]

Objekte (siehe Abb. 16)	**Hierarchie 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 29 DHCP blue2net IP Objects [2.3]

8.5.3 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. Es können aber definierte Zugänge durch die Firewall zu Rechnern im lokalen Netz hinter blue2net ermöglicht werden (z.B.: Fernwartung von Rechnern). Die Definition der Regeln für diese definierten Zugänge wird unter 8.5.4 näher beschrieben.

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

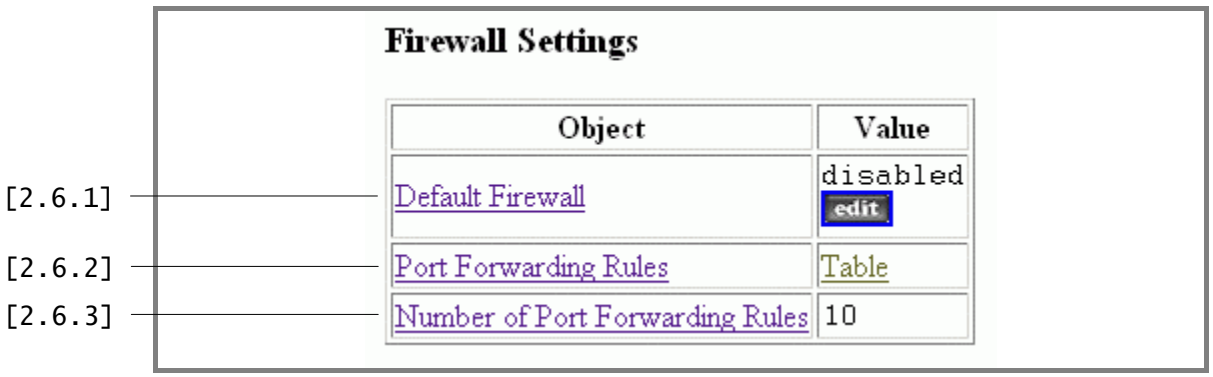


Abb. 17 Firewall Settings [2.6]

Objekte (siehe Abb. 17)	**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 14).
Port Forwarding Rules	[2.6.2]		Tabelle von Port-Forwarding-Regeln (Port Weiterleitung), wichtig z.B. für Fernwartung von Servern
Number of Port Forwarding Rules	[2.6.3]	10 (nur Anzeige)	Maximale Anzahl an aktiven Port-Forwarding-Regeln [2.6.2]

Tabelle 30 Firewall Settings [2.6]

8.5.4 Port Forwarding Rules [2.6.2]

„Port Forwarding“ wird verwendet, wenn Sie blue2net als Access-Router mit „Masquerading“ verwenden und auf einem lokalen Rechner (der über Ethernet oder Bluetooth angeschlossen ist) ein Service zur Verfügung stellen wollen, das vom Internet aus erreichbar sein soll.

Das ist zum Beispiel der Fall, wenn Sie auf einem Rechner einen PPTP oder PPPoE Server bereitstellen, so dass vom Internet sicheres VPN in Ihr Netzwerk möglich ist.

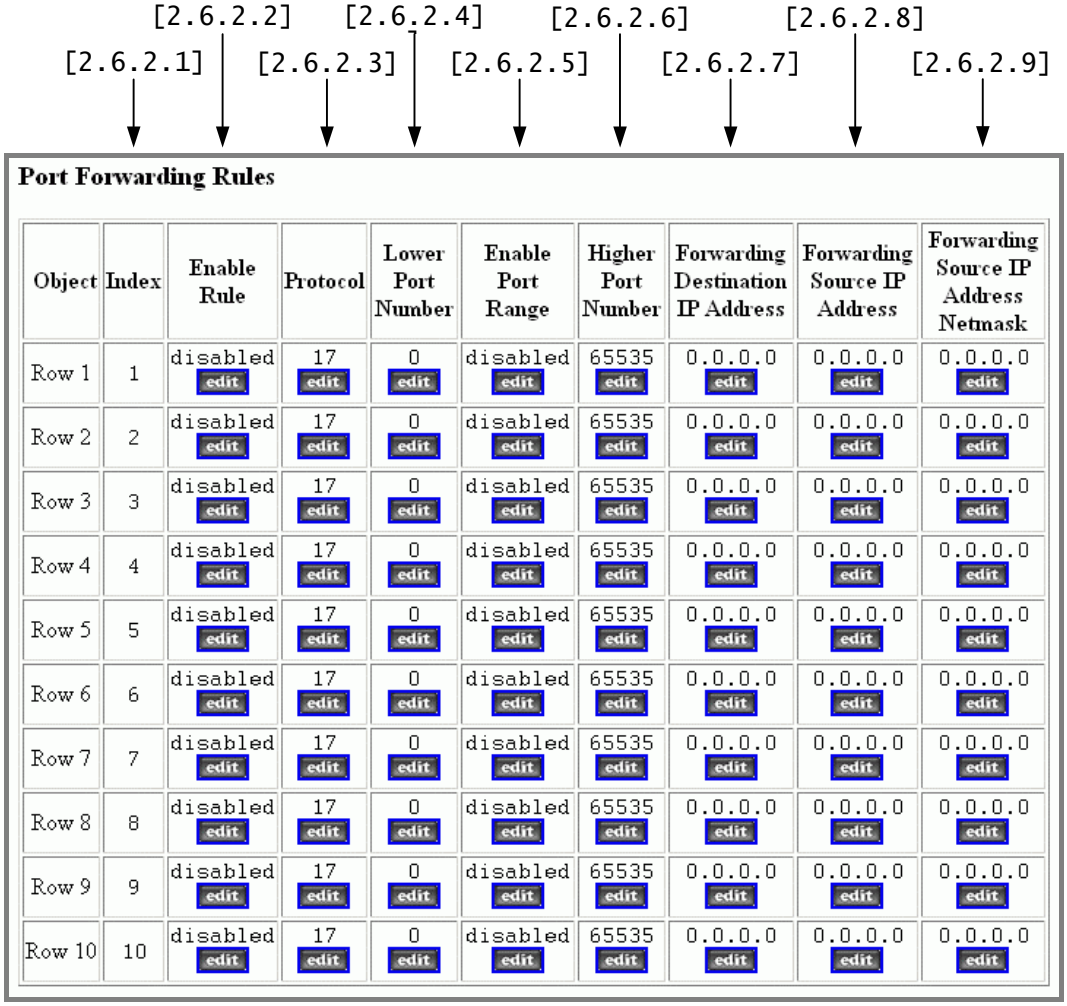


Abb. 18 Port Forwarding Rules [2.6.2]

Objekte (siehe Abb. 18)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Index	[2.6.2.1]	1-10 (Nur Anzeige)	Eindeutiger Wert für jede Regel. Es wird von blue2net für jede Regel nach der Reihe geprüft, ob sie zutrifft. Wenn ja, wird sie angewandt und die restlichen nicht mehr durchsucht.

Objekte (siehe Abb. 18)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Enable Rule	[2.6.2.2]	disabled enabled	Schaltet diese eine Regel ein (enabled) oder aus (disabled). Die Regel selbst bleibt im ausgeschalteten Zustand erhalten und kann bei Bedarf durch setzen dieses Schalters auf *enabled* wieder aktiviert werden.
Protocol	[2.6.2.3]	17 andere Protokoll-Nummer (0 ... 255)	Nummer des IP-Protokolls, das weitergeleitet werden soll: 6.....tcp, 17.....udp, 47.....gre, 255.....alle Protokolle **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 10) Wenn Sie alle Protokolle (=Wert 255) und damit tcp port 443 weiterleiten und kein zweites IP-Interface aktiviert haben(‚Additional IP Interface' [2.8.1] auf *enabled*), ist blue2net vom Ethernet-Anschluss aus nicht mehr konfigurierbar.
Lower Port Number	[2.6.2.4]	0 andere Port-Nummer (0 ... 65535), die aber nicht höher sein sollte, als [2.6.2.6])	Wenn ‚Enable Port Range' [2.6.2.5] *disabled* ist, ist das die Nummer eines einzelnen Ports, der weitergeleitet werden soll (nur von Bedeutung, wenn in ‚Protocol' [2.6.2.3] Wert 6 (tcp) oder 17 (udp) eingestellt ist). Wenn ‚Enable Port Range' [2.6.2.5] *enabled* ist, ist das die niedrigste Nummer eines Portbereiches (inklusive), **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 10) Wenn Sie einen tcp-Port-Bereich (Range), der 443 enthält, weiterleiten und kein zweites IP-Interface aktiviert haben (‚Additional IP Interface' [2.8.1] auf *enabled*), ist blue2net vom Ethernet-Anschluss aus nicht mehr konfigurierbar.

Objekte (siehe Abb. 18)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Enable Port Range	[2.6.2.5]	disabled enabled	Stellen Sie diesen Schalter auf *enabled*, wenn Sie einen zusammenhängenden Bereich von Ports weiterleiten wollen. Der Bereich ist durch ‚Lower Port Number' [2.6.2.4] und ‚Higher Port Number' [2.6.2.6] festgelegt. Nur für tcp und udp (6 oder 17 in ‚Protocol' [2.6.2.3] gültig.
Higher Port Number	[2.6.2.6]	65535 andere Port-Nummer (0 ... 65535), die aber nicht niedriger sein sollte, als [2.6.2.4])	Wenn ‚Enable Port Range' [2.6.2.5] *enabled* ist, ist das die Nummer des höchsten Ports (inklusive) aus dem weiterzuleitenden Bereich. Wenn ‚Enable Port Range' [2.6.2.5] *disabled* ist, ist dieser Parameter unwirksam. **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 10) Wenn Sie einen tcp-Port-Bereich (Range), der 443 enthält, weiterleiten und kein zweites IP-Interface aktiviert haben (‚Additional IP Interface' [2.8.1] auf *enabled*), ist blue2net vom Ethernet-Anschluss aus nicht mehr konfigurierbar.
Forwarding Destination IP Address	[2.6.2.7]	0.0.0.0	Das ist die Ziel-IP-Adresse der Weiterleitung, d.h. die IP-Adresse des Rechners, auf dem das (die) Service(s) tatsächlich laufen.
Forwarding Source IP Address	[2.6.2.8]	0.0.0.0	IP-Adresse des Rechners oder Rechner-Netzwerkes, die das (die) Service (s) benutzen dürfen.
Forwarding Source IP Address Netmask	[2.6.2.9]	0.0.0.0	Maske für die Source-Adresse (alle Adress-Teile, wo in der Maske 1(in binär) steht, müssen mit der in ‚Forwarding Source IP Address' [2.3.6.8] angegeben übereinstimmen).

Tabelle 31 Port Forwarding Rules [2.6.2]

Beispiele:

Wenn Sie einen Server betreiben, den Sie vom Internet aus fernwarten wollen, können Sie auf diesem ein PPTP Server-Programm installieren und auf blue2net die beiden folgenden Regeln eintragen, um PPTP zu diesem Server weiterzuleiten (interessant für kleine Firmen, die Ihre EDV-Infrastruktur von einer anderen Firma betreuen lassen).

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

Tabelle 32 Beispiel Port-Forwarding-Regel für PPTP-Tunnel

Das gleiche können Sie auch mit l2tp erreichen, wenn Sie also auf Ihrem Server einen L2TP-Server-Programm (LNS) laufen haben und folgende Regel aktivieren:

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

Tabelle 33 Beispiel Port-Forwarding-Regel für L2TP-Tunnel

Wenn Sie einen Rechner im lokalen Netzwerk mit SSH vom WWW-Internet aus erreichen können wollen, müssen Sie auf diesem Rechner ein SSH-Service laufen lassen und die Regeln in Tabelle 33 aktivieren.

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

Tabelle 34 Beispiel Port-Forwarding-Regel für SSH-Tunnel

8.5.5 Tunnel Configuration (PPPoE / PPTP) [2.7]

Bei der Anbindung von einem xDSL-Modem an ein Endgerät läuft „über“ das Ethernet-Protokoll noch ein sogenanntes Tunnel-Protokoll. 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).

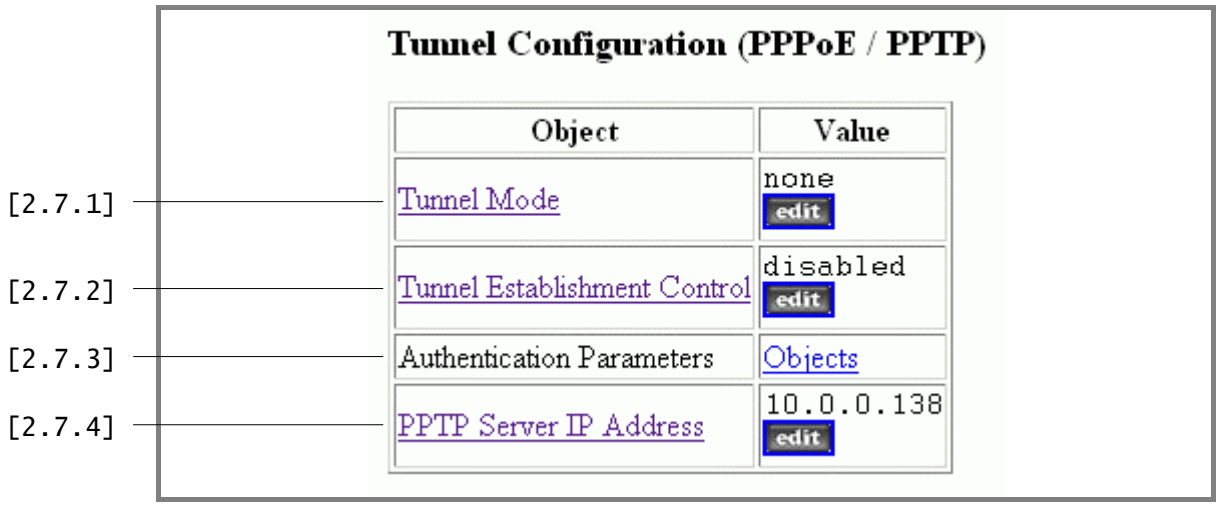


Abb. 19 Tunnel Configuration (PPPoE / PPTP) [2.7]

Objekte (siehe Abb. 19)	**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. 19)	**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 das Tarifmodell Ihres xDSL-Anbieters die Online-Zeit nicht in Rechnung stellt (z.B. ‚Flat-Rate'. 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 die Online-Zeit im Tarifmodell Ihres xDSL-Anbieters maßgebend ist. Achtung! Wenn blue2net als Access-Router arbeitet und [2.7.2] auf *enabled* gestellt ist, wird für PCs am drahtgebundenen Ethernet der Tunnel nicht automatisch aufgebaut! D.h. in diesem Fall dürfen Sie nicht auf *enabled* stellen.
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 35 Tunnel Configuration (PPPoE / PPTP) [2.7]

8.5.6 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.

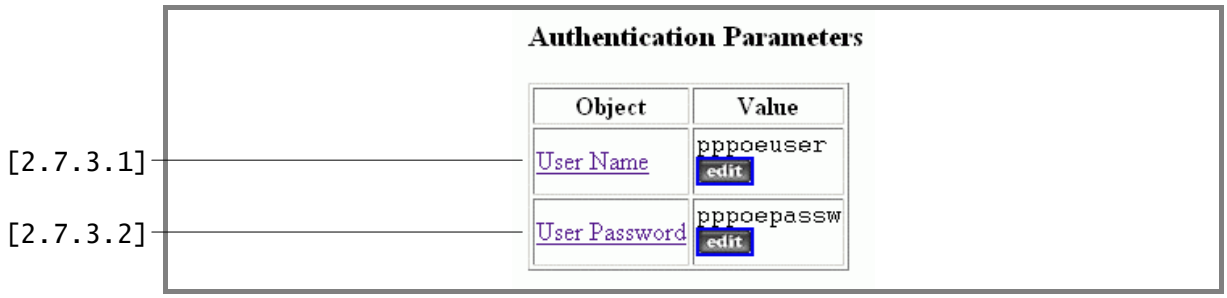


Abb. 20 Authentication Parameters [2.7.3]

Objekte (siehe Abb. 20)	**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 36 Authentication Parameters [2.7.3]

8.5.7 Access Router [2.8]

Sie können blue2net als Access-Router nutzen. Dazu müssen Sie die Werkseinstellungen der Parameter unter ‚Access Router' [2.8] ändern (es sei denn, Sie stellen die Verbindung zum WWW über ein xDSL-Modem, das PPPoE benutzt, her (siehe ‚Authentication Parameters' [2.7.3] in Kapitel 8.5.6).

Stellen Sie dazu ‚Additional IP Interface' [2.8.1] auf *enabled*, um ein zweites IP-Interface für ein kleines Heim-Netzwerk einzuschalten.

Wenn ‚IP Connection Mode for NAP Terminals' [3.7] auf *bridging* gesetzt ist und ‚Terminal IP Address Resolution' auf *masquerading* oder *masqueradingpool* gesetzt ist, wird für das zweite IP-Interface gleich die in ‚IP Masquerading' [2.5] angegebene IP-Adresse und die in ‚Terminal Netmask' [3.4] angegebene Netzmaske benützt. Ansonsten werden im „Bridging-Mode" die unter ‚Fixed Additional IP Interface' [2.8.2] eingetragenen Werte verwendet.

Wenn ‚IP Connection mode for NAP Terminals' [3.7]auf *routing* gesetzt ist, sollten Sie für das zweite IP-Interface eine IP-Addresse benutzen, die nicht im gleichen Subnetz wie die Bluetooth-Terminals mit PAN NAP-Service liegt. Das ist bei ‚Terminal IP Address Resolution' [3.1] auf *masquerading* oder *masqueradingpool* die IP-Addresse von ‚IP Masquerading' [2.5] und die Netzmaske von [3.4].

Hinweis: Die Nutz-Bandbreite von blue2net als Access-Router ist etwa 300 kBps (kiloByte pro Sekunde). Setzen Sie blue2net mit aktivierter Access-Router-Funktionalität nicht direkt hinter einem zusätzlichen Hardware-Router zusammen mit einem HUB ein, da solch ein Router schnelle Bursts erzeugen kann, die zum Einbruch des Datendurchsatzes für Ethernet-Terminals führen können. Der Grund sind Datenpaket-Kollisionen zwischen Paketen vom WWW-Internet zu blue2net und Paketen, die blue2net zu Rechnern am Heim-LAN weiterschickt. In diesem Fall können Sie ja direkt Ihren Hardware-Router für PCs am Ethernet benützten.

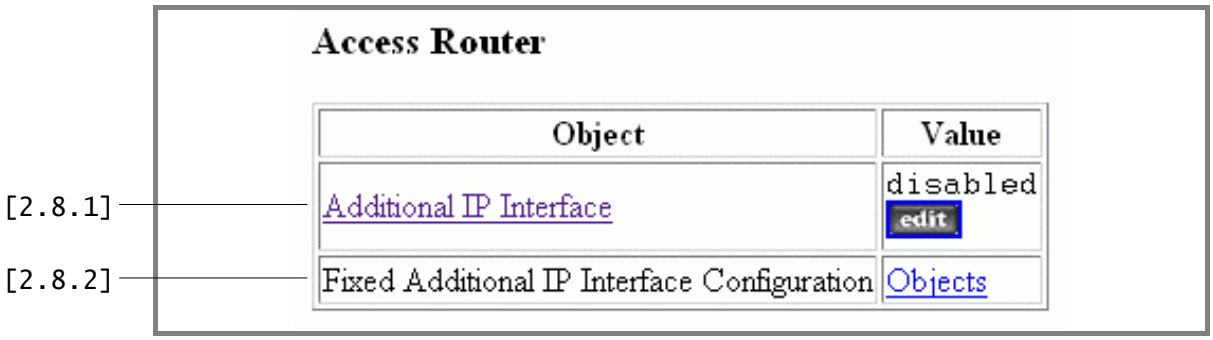


Abb. 21 Access-Router [2.8]

Objekte (siehe Abb. 21)	Hier. stufe	Werkseinstellung, weitere Werte, Wertebereich	Erklärung
Additional IP Interface	[2.8.1]	disabled enabled	Einschalten/Ausschalten einer zweiten IP-Schnittstelle an blue2net.
Fixed Additional IP Interface Configuration	[2.8.2]		Menü zum Konfigurieren der zweiten IP-Schnittstelle.

Tabelle 37 Access Router [2.8]

8.5.8 Fixed Additional IP Interface Configuration [2.8.2]

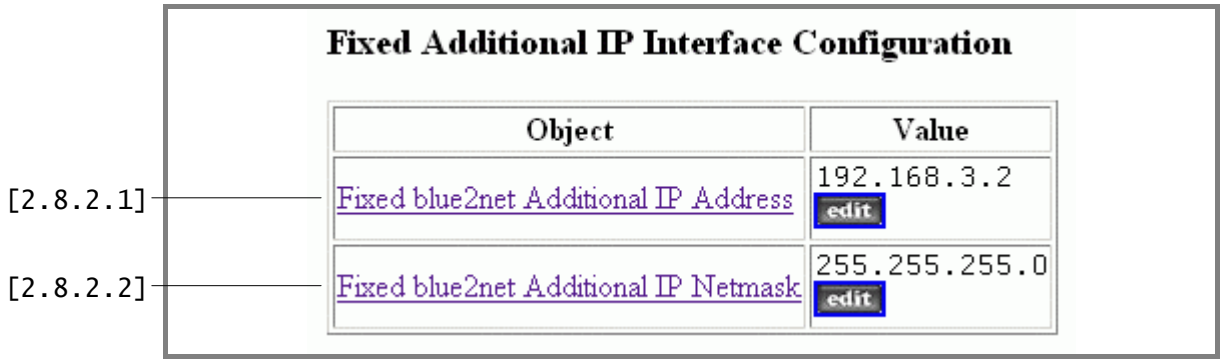


Abb. 22 Fixed Additional IP Interface Configuration [2.8.2]

Objekte (siehe Abb. 22)	Hier. stufe	Werkseinstellung, weitere Werte, Wertebereich	Erklärung
Fixed blue2net Additional IP Address	[2.8.3.1]	192.168.3.2 andere IP-Adresse	IP-Adresse der zweiten IP-Schnittstelle (wird nur benützt, wenn ‚IP Connection Mode for NAP Terminals' [3.7] auf *routing* gesetzt ist). Wenn Sie „masquerading" benützen, d.h. ‚Terminal IP Address Resolution' [3.1] auf *masquerading* eingestellt haben, muss diese IP-Adresse verschieden von ‚IP Masquerading' [2.5] sein!
Fixed blue2net Additional IP Netmask	[2.8.3.2]	255.255.255.0 andere Netzmaske	Subnetzmaske für die zweite IP-Schnittstelle (wird nur benützt, wenn ‚IP Connection Mode for NAP Terminals' [3.7] auf *routing* gesetzt ist).

Tabelle 38 Fixed Additional IP Interface Configuration [2.8.2]

8.6 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.

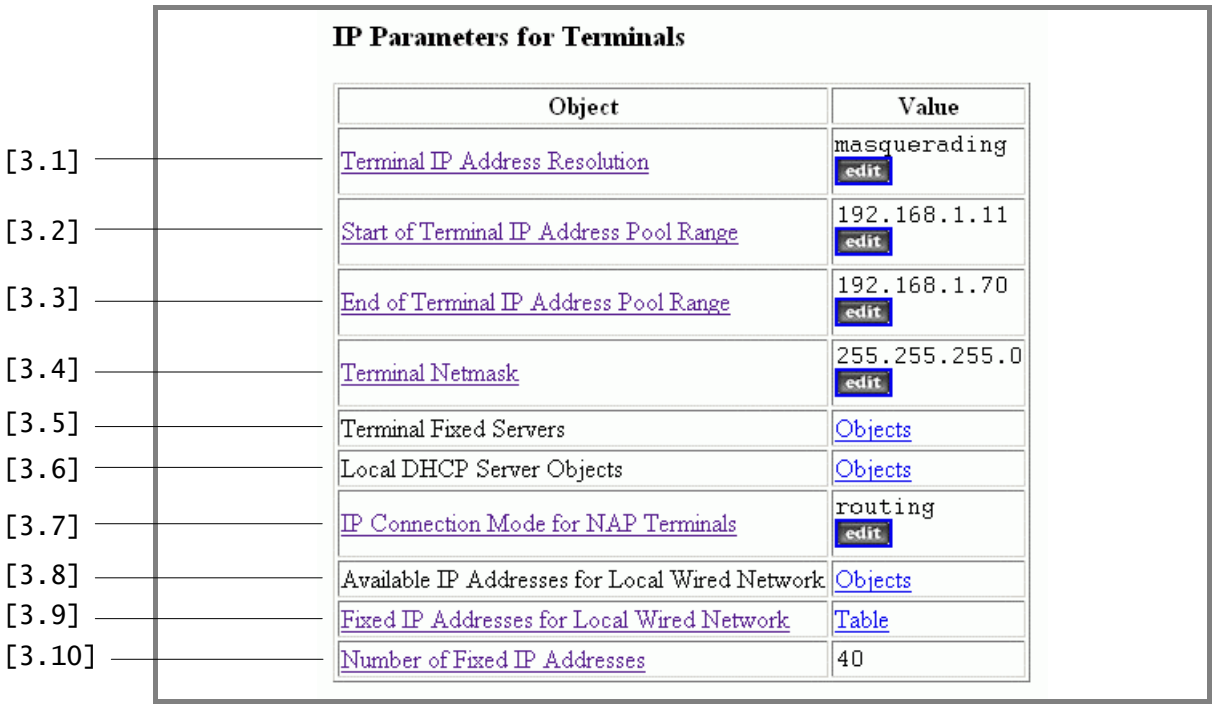


Abb. 23 IP Parameters for Terminals [3]

Objekte (siehe Abb. 23)	**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 Bluetooth-Terminals mit LAP-Profile erforderlich (empfohlene Einstellung für Heimanwender mit Kabel-Modem oder xDSL-Modem). Zu Ihrem ISP ist nur die offizielle IP vom blue2net sichtbar. Für PAN NAP sollten Sie in diesem Fall den DHCP-Server aktivieren ([3.6.1] ‚Local DHCP Server for NAP' auf *enabled*) ... Fortsetzung →

Objekte (siehe Abb. 23)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Terminal IP Address Resolution (Fortsetzung)	[3.1]	masquerading dhcp predefined masqueradingpool	Wenn als Verfahren *dhcp* eingestellt ist, wird blue2net während des Verbindungsaufbaus eine DHCP-Anfrage aussenden, welche die Bluetooth-Adresse des Terminals enthält. Um PAN NAP-Terminals gleich zu behandeln, sollten Sie ‚IP Connection Mode for NAP Terminals' [3.7] auf *bridging* setzten und den DHCP-Server für NAP-Terminals deaktivieren (‚Local DHCP Server for NAP' [3.6.1] auf *disabled*). Wenn als Verfahren *predefined* eingestellt ist, wird blue2net eine IP-Adresse aus einem Vorrat von fixen IP-Adressen verwenden (siehe ‚Start/End of Terminal IP Address Pool Range' [3.2] u. [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 8.4.3) Für PAN NAP sollten Sie in diesem Fall den DHCP-Server aktivieren ([3.6.1] „Local DHCP Server for NAP" auf *enabled*) 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 8.4.3). **Vorsicht!** Gefahr einer Aussperrung! Verwenden Sie diesen Parameter sorgfältig! (siehe Kapitel 10)

Objekte (siehe Abb. 23)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Start of Terminal IP Address Pool Range (Achtung! Änderung des Namens und der Funktion gegenüber v 3.0 !)	[3.2]	192.168.2.11	Niedrigste IP-Adresse des Bereiches für „LAN Access Profile"-Teminals und PAN-Terminals (bei ‚Local DHCP Server for NAP' [3.6.1] *enabled*). Wenn ‚IP Connection Mode for NAP Terminals' [3.7] auf *bridging* und ‚Access Router' [2.8] eingestellt– ‚Additional IP Interface' [2.8.1] *enabled* und ‚Local DHCP Server for Ethernet' [3.6.2] *enabled* – wird der Bereich auch für Adresszuweisungen an Rechner am lokalen Ethernet verwendet.
End of Terminal IP Address Pool Range (Achtung! Änderung des Namens und der Funktion gegenüber v 3.0 ! Auch [3.3.1] und [3.3.2] sind entfallen)	[3.3]	192.168.2.70	Höchste Adresse des IP-Adress-Bereiches. Wenn Sie nur IP-Adressen an Terminals mit eingetragener MAC-Adresse vergeben wollen (siehe Tabelle zu ‚Fixed IP Address for Local Wired Network' [3.9]), setzen Sie [3.2] und [3.3] auf *0.0.0.0*
Terminal Netmask	[3.4]	255.255.255.0 anderer Wert	Subnetzmaske, welche zu den IP-Adressen aus dem „Terminal IP Address Pool Range" [3.2]-[3.3] gehört.
Terminal Fixed Servers	[3.5]		Während die PPP-Verbindung aufgebaut wird, werden diese Parameter an das Bluetooth-Terminal gesendet. Diese Werte werden auch beim lokalen DHCP-Server an PAN NAP- und Ethernet-Terminals übermittelt.
Local DHCP Server Objects	[3.6]		Hier können Sie DHCP-Server für Bluetooth-PAN-Terminals oder Ethernet-Terminals starten und stoppen.

Objekte (siehe Abb. 23)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
IP Connection Mode for NAP Terminals	[3.7]	routing bridging	Anbindung von Bluetooth Terminals bei PAN NAP-Service an die Ethernet-Schnittstelle. *routing* – keine Verbindung zur Ethernet-Schnittstelle, IP-Daten werden geroutet. *bridging* – direkte Verbindung der PAN NAP-Terminals zur Ethernetschnittstelle (auf Ethernet-Protokoll-Ebene).
Available IP Addresses for Local Wired Network	[3.8]		Pool von IP-Adressen, die über DHCP an Ethernet-Terminals (PCs/Laptops) vergeben werden, sofern ‚IP Connection Mode for NAP Terminals' [3.7] auf *routing* gesetzt ist, und ‚Local DHCP Server for Ethernet' [3.6.2] auf *enabled* gesetzt ist.
Fixed IP Addresses for Local Wired Network	[3.9]		Tabelle von Ethernet-Adressen und zugehörigen IP-Adressen, die über DHCP an die entsprechenden Ethernet-Terminals (PCs/Laptops) vergeben werden, sofern ‚IP Connection Mode for NAP Terminals' [3.7] auf *routing* gesetzt ist und ‚Local DHCP Server for Ethernet' [3.6.2] auf *enabled* gesetzt ist.
Number of Fixed IP Addresses	[3.10]	40 (nur Anzeige)	Anzahl der maximal möglichen Einträge in Tabelle ‚Fixed IP Address for Local Wired Network' [3.9].

Tabelle 39 IP Parameters for Terminals [3]

Beachten Sie, dass ‚IP Connection Mode for NAP Terminals' [3.7] auch darauf Einfluss hat, welche Bereiche für die Ethernet-Terminals bei Adresszuweisung über DHCP verwendet werden (siehe [3.6], [3.9] und [3.10]).

Der Grund dafür liegt darin, dass im „Bridging-Mode" für ‚IP Connection Mode for NAP Terminals' [3.7] Ethernet und PAN NAP auf Ethernet-Protokoll-Ebene verbunden sind. Zwischen einem Bluetooth Terminal, das mit „PAN NAP-Profil" verbunden ist und einem PC/Laptop im lokalen LAN werden dann die Informations-Pakete direkt mit Ethernet-Protokoll weitergeleitet. Da kein Routing auf IP-Ebene stattfinden muss, dürfen die PCs/Laptops und Bluetooth-PAN NAP-Terminals im gleichen IP-Subnetz liegen.

Wenn dagegen ‚IP Connection Mode for NAP Terminals' [3.7] auf *routing* gesetzt ist, müssen die Informations-Pakete zwischen PCs/Laptops am lokalen LAN und Bluetooth PAN NAP-Terminals auf IP-Ebenen geroutet werden - dafür müssen diese Terminals dann in verschiedenen IP-Subnetzen liegen.

8.6.1 Terminal Fixed Servers [3.5]

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

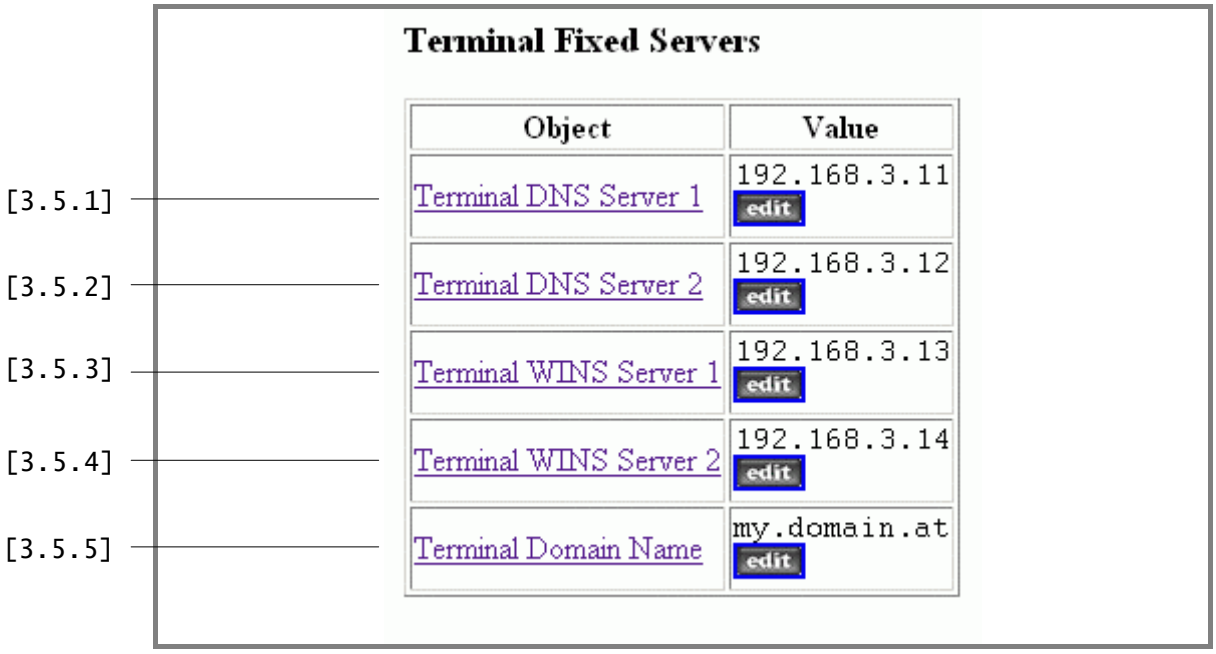


Abb. 24 Terminal Fixed Servers [3.5]

Objekte (siehe Abb. 24)	**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. 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 13.3).
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. 24)	**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 40 Terminal Fixed Servers [3.5]

8.6.2 Local DHCP Server Objects [3.6]

Hier ist es möglich, Bluetooth-Terminals, die sich über das „PAN NAP-Service“ verbinden, und Rechnern, die drahtgebunden am lokalen Ethernet angeschlossen sind, mit DHCP IP-Adressen zuzuweisen.

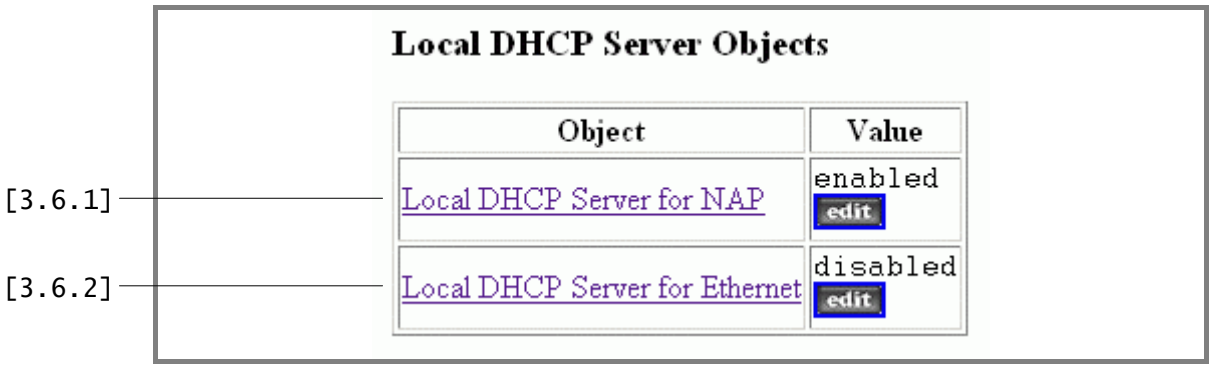


Abb. 25 Local DHCP Server Objects [3.6]

Objekte (siehe Abb. 25)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Local DHCP Server for NAP	[3.6.1]	enabled disabled	Hier kann man den DHCP-Server für Bluetooth-Terminals, die sich über „PAN NAP-Service“ verbinden aktivieren.
Local DHCP Server for Ethernet	[3.6.2]	disabled enabled	Hier kann man den DHCP-Server für Ethernet-Terminals (PCs/Laptops) aktivieren. Im „Bridging-Mode“ ist diese Einstellung nicht wirksam.

Tabelle 41 Local DHCP Server Objects [3.6]

Für den Fall, dass ‚IP Connection Mode for NAP Terminals” [3.7] auf *bridging* gesetzt ist, können [3.6.1] und [3.6.2] nicht unabhängig voneinander eingeschaltet werden. In diesem Fall bedient der DHCP-Server sowohl Bluetooth-Terminals über „PAN NAP-Service“ als auch Ethernet-Terminals (PCs/Laptops am lokalen LAN), sobald der Schalter [3.6.1] auf *enabled* gesetzt ist.

8.6.3 Available IP Addresses for Local Wired Network [3.8]

Die in dem angeführten Bereich liegenden IP-Adressen werden vom DHCP-Server den Ethernet-Terminals (PCs/Laptops am lokalen LAN) zugewiesen. Natürlich geschieht das nur dann, wenn ‚Local DHCP Server for Ethernet" [3.6.2] auf *enabled* gesetzt ist. Außerdem wird dieser Bereich von IP-Adressen nur dann benützt, wenn ‚IP Connection Mode for NAP Terminals' auf *routing* gesetzt ist.

Ist ‚IP Connection Mode for NAP Terminals" auf *bridging* gesetzt, wird dagegen der Bereich von [3.2]-[3.3] auch für die Ethernet-Terminals (PCs/Laptops am lokalen LAN) benützt, wenn der DHCP-Server in [3.6.1] oder [3.6.2] auf *enabled* gesetzt ist.

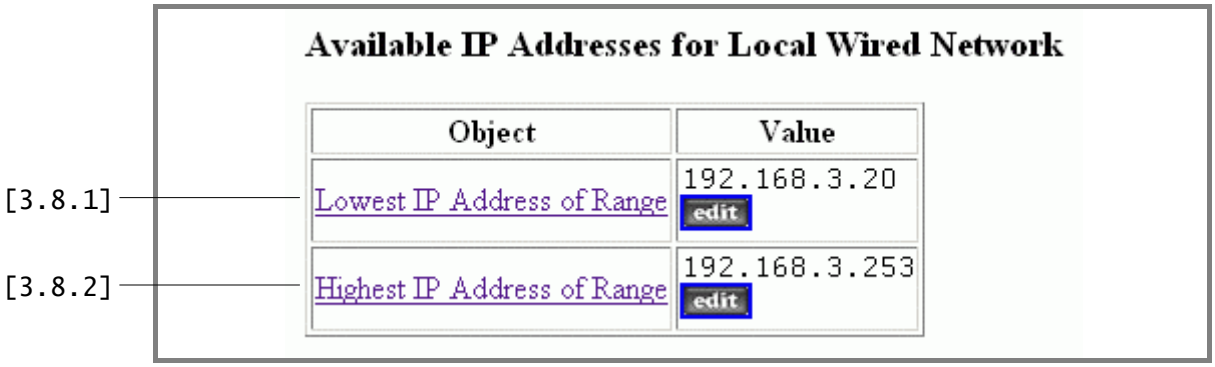


Abb. 26 Available IP Addresses for Local Wired Network [3.8]

Objekte (siehe Abb. 26)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Lowest IP Address of Range	[3.8.1]	192.168.3.20	Die niedrigste IP-Adresse (inklusive) des Bereiches, der vom DHCP-Server für Ethernet-Terminals (PCs/Laptops am lokalen LAN) zur IP-Adress-zuweisung verwendet wird, wenn die Ethernet-Adresse nicht explizit in ‚Fixed IP Addresses for Local Wired Network' [3.9] angeführt ist.
Highest IP Address of Range	[3.8.2]	192.168.3.253	Die höchste (inklusive) IP-Adresse des Bereiches. Wenn Sie nur IP-Adressen an Terminals mit eingetragener MAC-Adresse vergeben wollen (siehe Tabelle zu ‚Fixed IP Address for Local Wired Network' [3.9]), setzen Sie [3.8.1] und [3.8.2] auf *0.0.0.0* .

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

Dieser Bereich von IP-Adressen wird vom DHCP-Server für die Adresszuweisung an PCs/Laptops am lokalen LAN verwendet, wenn die Ethernet-Adresse des PCs/Laptops nicht in Tabelle [3.9] angeführt ist und ‚IP Connection Mode for NAP Terminals' [3.7] auf *routing* gesetzt ist.

Die IP-Adressen im Bereich (Range) sollten im gleichen Subnetz liegen wie die IP-Adressen des zweiten IP-Interfaces unter [2.8.2].

Wenn Sie ein xDSL-Modem benützen und als Zugangsprotokoll PPPoE verwenden, sollten die IP-Adressen im Bereich im gleichen Subnetz liegen wie die IP-Adressen des ersten IP-Interface von blue2net unter [2.2].

8.6.4 Fixed IP Addresses for Local Wired Network [3.9]

Hier können Sie Rechnern am lokalen Ethernet via DHCP fixe IP-Adressen zuweisen. Diese Tabelle wird nur benützt, wenn ‚IP Connection Mode for NAP Terminals' [3.7] auf *routing* gesetzt ist und der DHCP-Server in [3.6] aktiviert ist.

Falls das zweite IP-Interface eingeschaltet ist, sollten diese IP-Adressen im gleichen Subnetz liegen wie die IP-Adresse des zweiten IP-Interfaces von blue2net unter [2.8.2].
Sonst sollten diese IP-Adressen im Subnetz der IP-Adresse des ersten IP-Interfaces von blue2net unter [2.2] liegen.

Wenn Sie ein xDSL-Modem benützen und als Zugangsprotokoll PPPoE verwenden, sollten die IP-Adressen im Subnetz der IP-Adresse des ersten IP-Interfaces von blue2net unter [2.2] liegen.

Hinweis: Stellen Sie sicher, dass sich keine ‚Fixed IP Address for Local Wired Network' [3.9.3] mit dem IP-Adressen-Bereich [3.8.1] bis [3.8.2] (‚Available IP Addresses for Local Wired Network') überlappen.

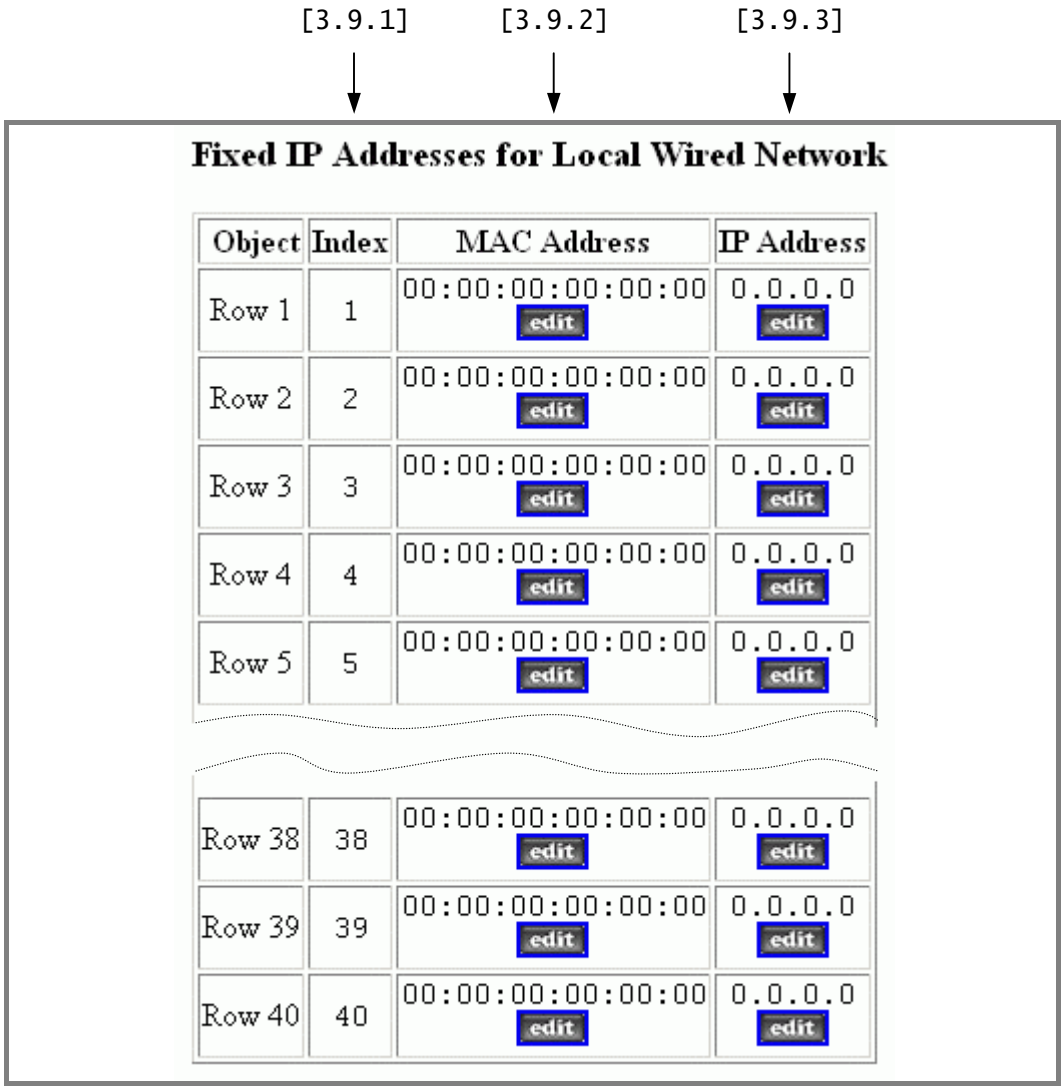


Abb. 27 Fixed IP Addresses for Local Wired Network [3.9]

Objekte (siehe Abb. 27)	**Hier. stufe**	**Werkseinstellung, weitere Werte, Wertebereich**	**Erklärung**
Index	[3.9.1]	1-40 Nummer des Eintrages (nur Anzeige)	ohne Bedeutung
MAC Address	[3.9.2]	XX:XX:XX:XX:XX X ... 0-9 und A-F	Ethernet-Adresse der Netzwerkkarte des Ethernet-Terminals (PCs/Laptops) (in Hexadezimal-Format)
IP Address	[3.9.2]	AAA.BBB.CCC.DDD Internet-Adresse	IP-Addresse, die mittels DHCP auf der Netzwerkkarte des Ethernet-Terminals (PCs/Laptops am Heim-Netzwerk) eingestellt werden soll.

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

8.7 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.

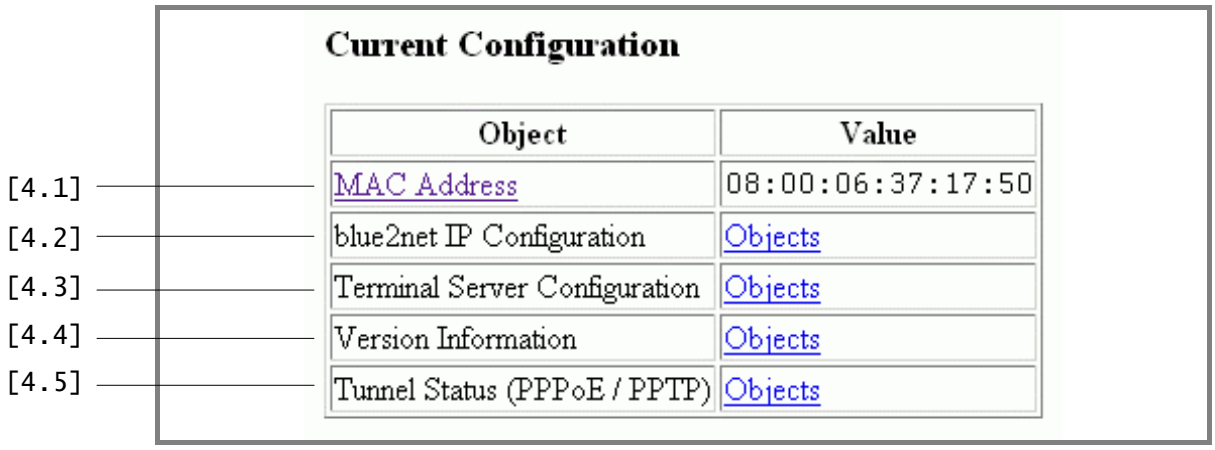


Abb. 28 Current Configuration [4]

Objekte (siehe Abb. 28)	**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 45
Terminal Server Configuration	[4.3]	siehe Tabelle 46
Version Information	[4.4]	siehe Tabelle 47
Tunnel Status (PPPoE / PPTP)	[4.5]	siehe Tabelle 48 und Tabelle 49

Tabelle 44 Current Configuration [4]

8.7.1 blue2net IP Configuration [4.2]

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

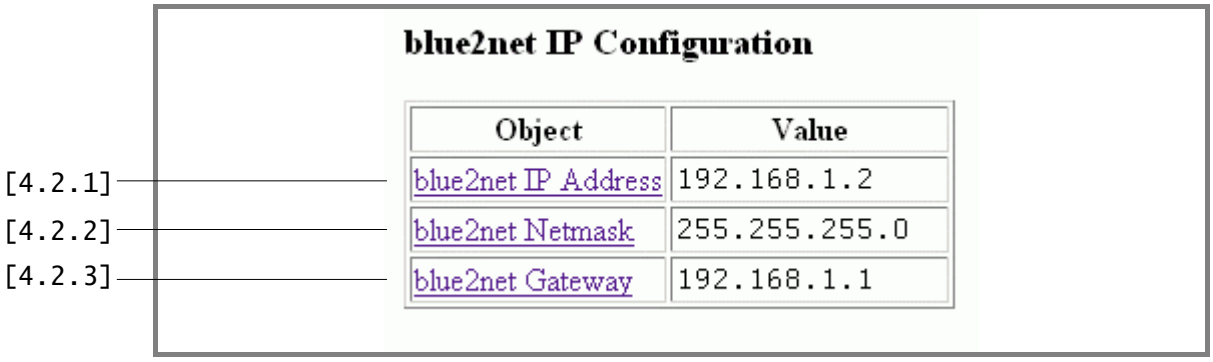


Abb. 29 blue2net IP Configuration [4.2]

Objekte (siehe Abb. 29)	**Hier. stufe**	**Erklärung**
blue2net IP Address	[4.2.1]	IP-Adresse, die blue2net zugewiesen wird. 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 wird. 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 wird. Wenn das Verfahren 'blue2net IP Address Resolution' [2.1] auf *dhcp* gesetzt ist, wurde dieser Wert über eine DHCP-Abfrage erfasst.

Tabelle 45 blue2net IP Configuration [4.2]

8.7.2 Terminal Server Configuration [4.3]

Diese Objekte zeigen, welche Werte den Terminals zugewiesen wurden.

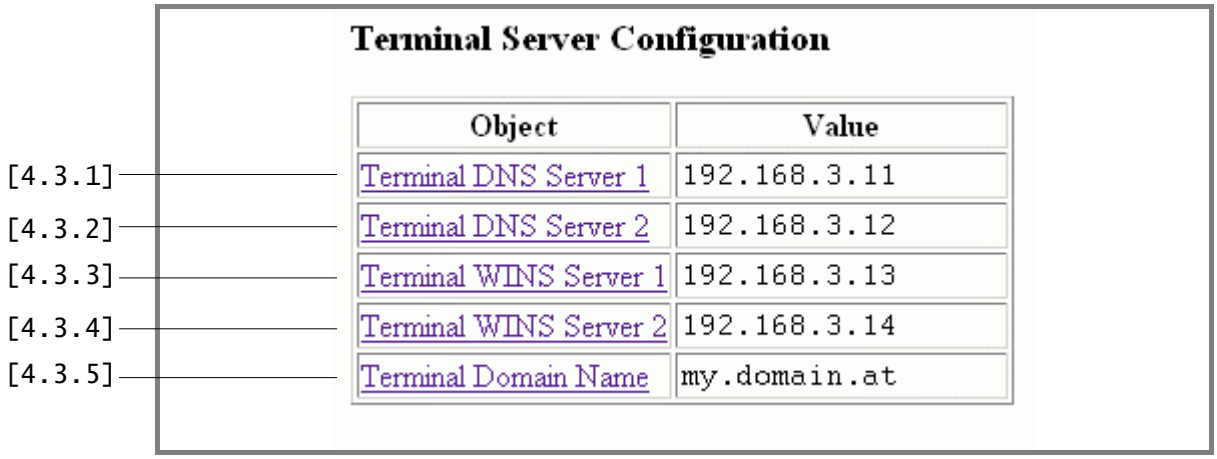


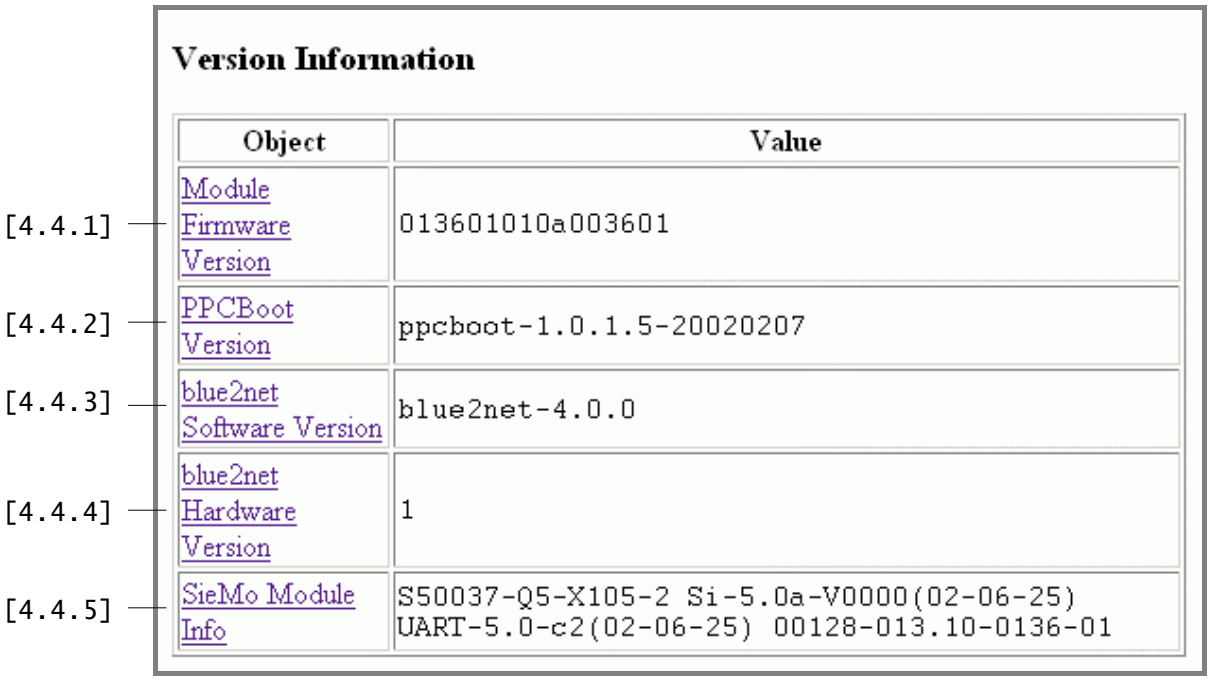
Abb. 30 Terminal Server Configuration [4.3]

Objekte (siehe Abb. 30)	**Hier. stufe**	**Erklärung**
Terminal DNS Server 1	[4.3.1]	IP-Adresse von DNS-Server 1, der den Terminals zugewiesen wird. 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 wird. 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 wird. 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 wird. 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 wird. Wenn 'Terminal IP Address Resolution' [3.1] auf *dhcp* gesetzt ist, wurde dieser Wert über eine DHCP-Abfrage erfasst.

Tabelle 46 Terminal Server Configuration [4.3]

8.7.3 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.



Version Information

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

Abb. 31 Version Information [4.4] (Beispiel)

Objekte (siehe Abb. 31)	**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 47 Version Information [4.4]

8.7.4 Tunnel Status (PPPoE / PPTP) [4.5]

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

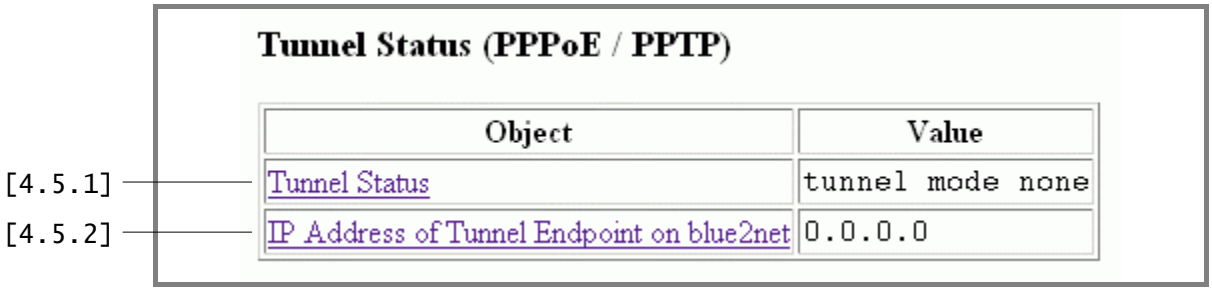


Abb. 32 Tunnel Status (PPPoE / PPTP) [4.5]

Objekte (siehe Abb. 32)	Hier. stufe	Erklärung
Tunnel Status	[4.5.1]	Aktueller Zustand des „Tunnels“.
IP Address of Tunnel Endpoint on blue2net	[4.5.2]	Aktueller Wert für die IP-Adresse des Tunnel-Endpunkts auf blue2net.

Tabelle 48 Tunnel Status [4.5]

Hier beispielhaft einige Statusmeldungen zu [4.5.1] :

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 User Name wurde nicht anerkannt, z.B. wegen falscher Eingabe

Tabelle 49 Statusmeldungen (Beispiele)

8.8 Configuration Access [5]

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

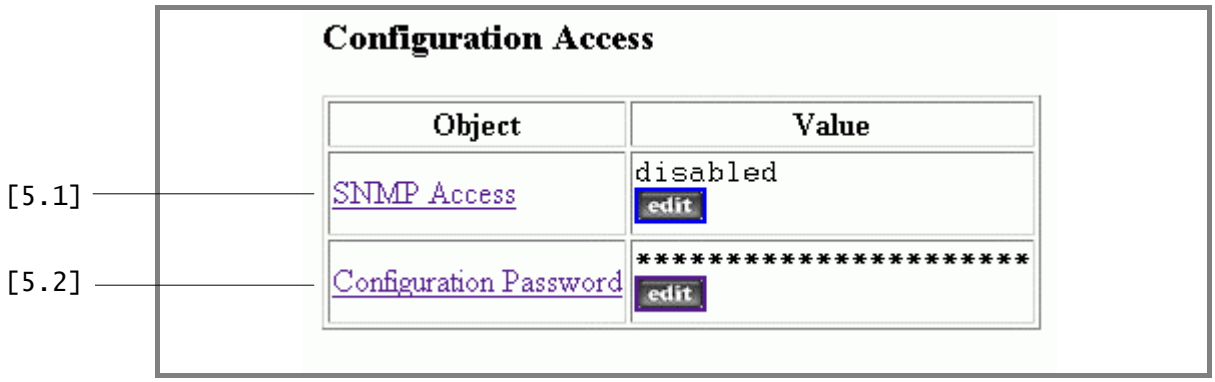


Abb. 33 Configuration Access [5]

Objekte (siehe Abb. 33)	**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. Eine Änderung an dieser Einstellung wird erst wirksam, nachdem sie permanent gespeichert wurde (siehe 8.9.2) und ein Reset von blue2net durchgeführt wurde (siehe 8.9.3). Die Konfiguration von blue2net über das Web-Interface ist auch dann möglich, wenn der SNMP Zugriff aktiviert ist.
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 10)

Tabelle 50 Configuration Access [5]

8.8.1 Change of Configuration Password [5.2]

Sie müssen das Passwort zweimal eingeben (siehe Abb. 34).

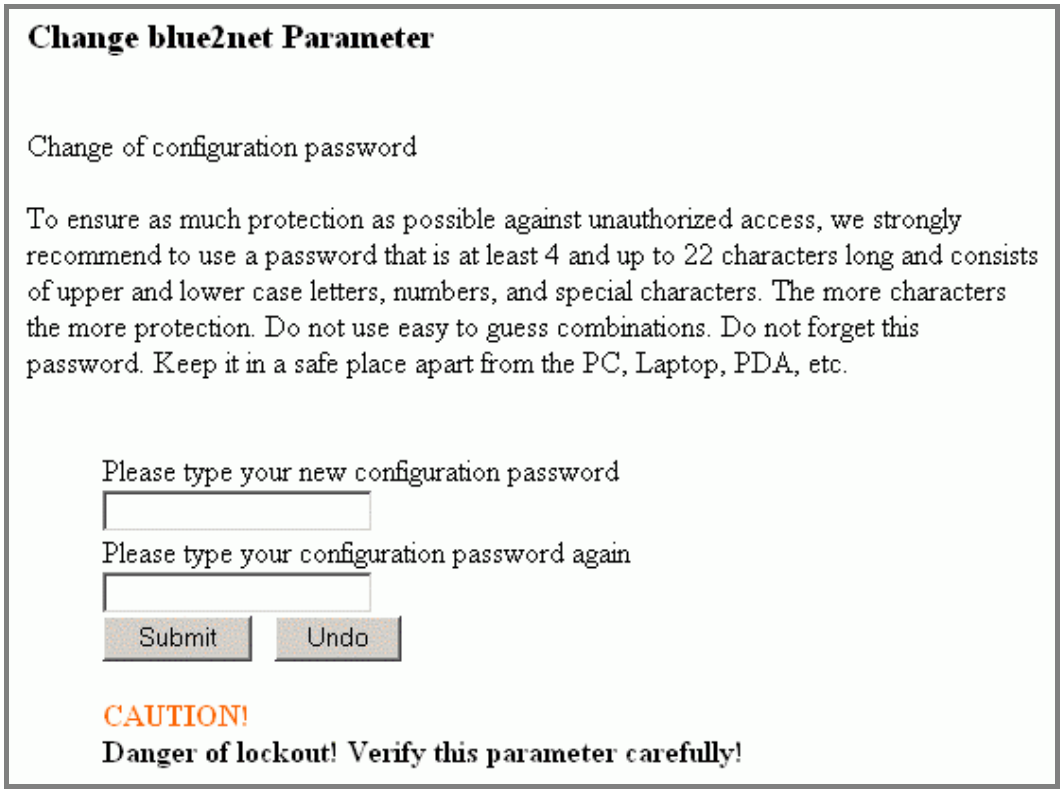


Abb. 34 Change of Configuration Password [5.2]

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 8.9.1 und 8.9.2).

8.9 Activation Commands [6]

Jede Änderung, die Sie an blue2net-Einstellungen durchführen, wird 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 10), 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 die Warnungen, um einer möglichen Aussperrung vom Zugang über Bluetooth oder LAN vorzubeugen (siehe Kapitel 10).

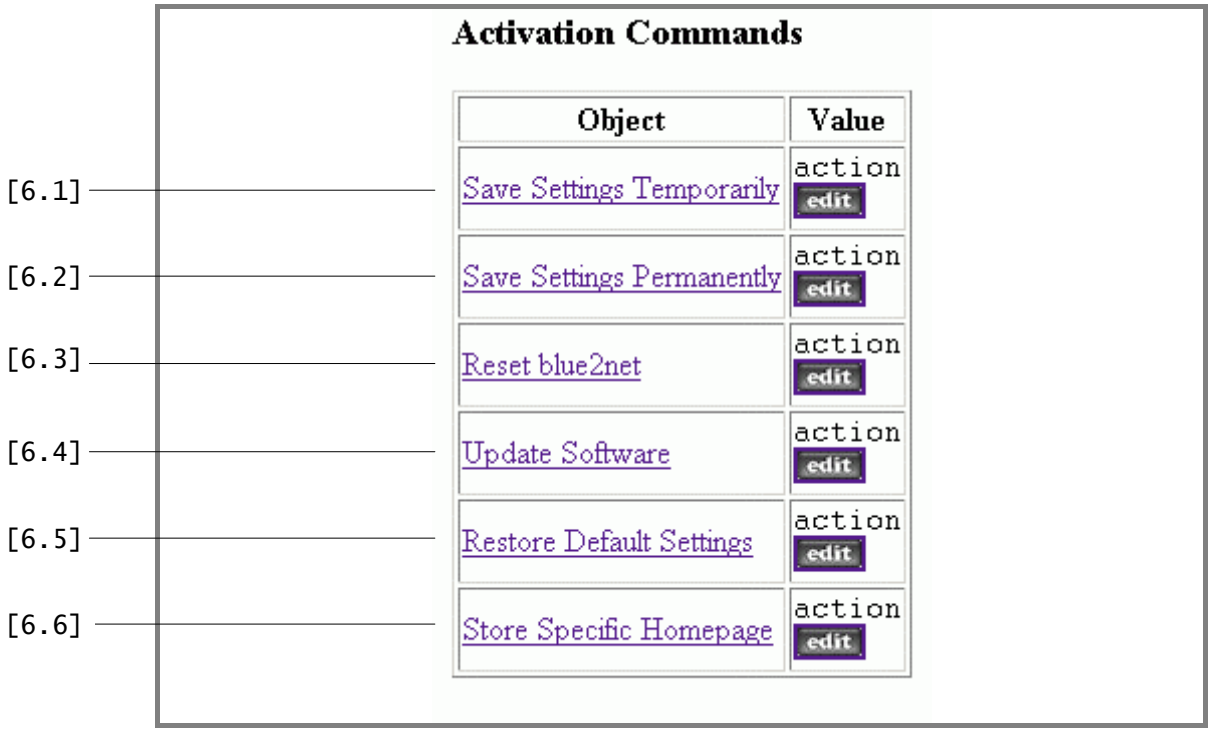


Abb. 35 Activation Commands [6]

Klicken Sie auf <edit>. Damit kommen Sie zu einer Seite, wie sie in Abb. 36 als Beispiel gezeigt ist.

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

Abb. 36 Activation Command (Save Settings Temporarily [6.1])

8.9.1 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 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 in Kapitel 10, 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.

8.9.2 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 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 8.9.1) beschrieben wurde, denn wenn Sie sich durch falsche Einstellungen *aussperren*, haben Sie im schlimmsten Fall (siehe Kapitel 10.1) nur die Möglichkeit, das Gerät zum Kundendienst (siehe Kapitel 19) zu bringen und dort auf Werkseinstellungen zurücksetzen zu lassen. Informieren Sie sich auch in Kapitel 10, wie Sie Aussperrung verhindern können.

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

8.9.3 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.

8.9.4 Update Software [6.4]

Software-Update [6.4]

Der Hersteller von blue2net stellt Software-Updates bereit, 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 wurde.

Details zum Ablauf sind in Kapitel 11 ersichtlich.

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

8.9.5 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 17 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.

8.9.6 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 12.1 dargestellt.

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

9 Übersicht Netzwerkstrukturen

Dieses Kapitel ist für jene, die etwas über die Netzwerkstruktur beim Betrieb von blue2net erfahren wollen.

Wenn Ihnen Begriffe wie Internet Protokoll, Ethernet Protokoll und Routing nichts sagen, überspringen Sie dieses Kapitel einfach und benützen Sie das Ihrem Einsatzzweck entsprechende Einsatz-Szenario in Kapitel 7

- Wenn ‚IP Connection Mode for NAP Terminals' [3.7] auf *bridging* eingestellt ist, sind die Geräte, die dieses Service benützen, so an das lokale Netz auf der Ethernetstelle des blue2net angebunden, als wären sie direkt mit einer Netzwerkkarte dort angesteckt. Sie können damit alle Protokolle ab Schicht 2 (Ethernet Standard IEEE 802.3) nutzen.

  Bluetooth-Geräte, die „LAN Access Profile" als Zugangsprofil benützen, können alle Protokolle ab Schicht 3 Internet Protokoll benützen. blue2net kann stellvertretend für Sie Konfigurations-Information mittels DHCP unter Benützung der Bluetooth-Adresse als MAC-Adresse von einem externen DHCP-Server besorgen. Mittels der „proxy_arp" Technik erscheinen die LAP-Terminals für andere Teilnehmer am Ethernet für IP-Verkehr so, als wären Sie direkt am Ethernet-Kabel angeschlossen.

- Wenn ‚IP Connection Mode for NAP Terminals' [3.7] auf *routing* eingestellt ist, arbeitet blue2net als Router für jene Bluetooth-Geräte, die NAP als Zugangsservice benützen. Alle Bluetooth-Geräte liegen am besten im gleichen Subnetz, DHCP Anfragen der Bluetooth-NAP-Terminals gelangen nicht ins lokale Ethernet, am besten aktiviert man den „Local DHCP Server for NAP Terminals". Bluetooth-Geräte sind jetzt anhand des IP-Subnetzes, in dem sie arbeiten, von Geräten am lokalen Ethernet unterscheidbar. Da blue2net kein Router-Informationsprotokoll unterstützt (RIP, IGP), können Router, die am lokalen Ethernet arbeiten, Datenpakete nicht direkt an die Bluetooth-Geräte senden. Daher müssen Sie in diesem Fall Masquerading und/oder Port-Forwarding benützen. Nur wenn Sie eine reine „Insel-Lösung" ohne Router oder Anbindung ans Internet betreiben, können Sie auf Masquerading verzichten.

9.1 Netz-Struktur bei ‚IP Connection Mode for NAP Terminals' [3.7] auf „routing"

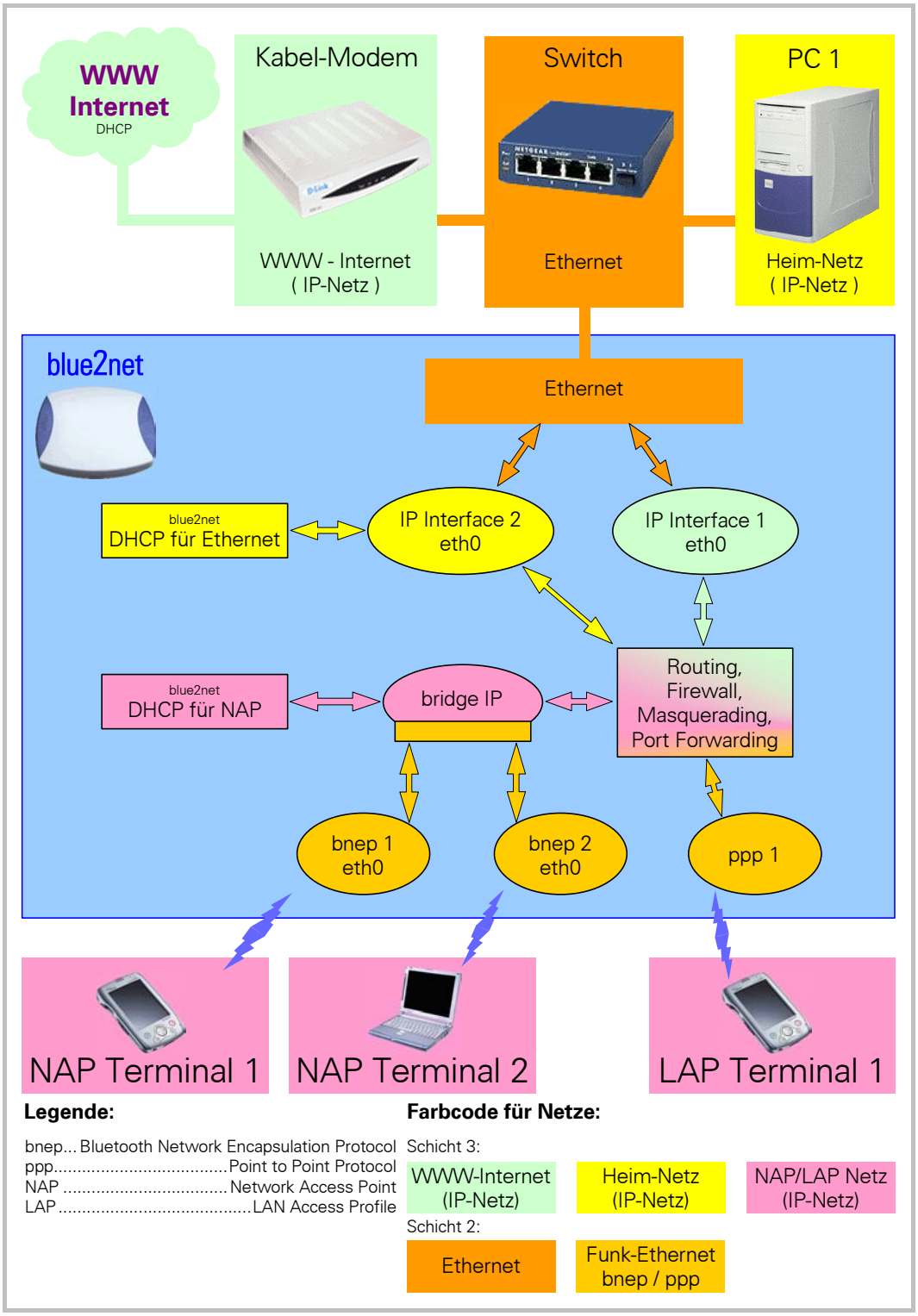


Abb. 37 Netzwerkstruktur bei blue2net im Mode ‚IP Connection Mode for NAP Terminals' auf „routing"

Abb. 37 zeigt die Netzwerkstruktur von blue2net als Router für Bluetooth-NAP-Terminals.

Dies ist der typische Anwendungsfall, wenn Sie zu Hause blue2net über ein Kabel-Modem mit dem Internet verbinden wollen.

Bluetooth LAN-Access-Profile-Teminals und Bluetooth-NAP-Terminals liegen im gleichen IP-Subnetz und werden mittels des blue2net-internen DHCP-Servers für NAP konfiguriert, blue2net zeigt in diesem Fall (Masquerading aktiviert) die Masquerading IP [2.5] auf der „bridge". Die NAP-Terminals sind am blue2net auf Ethernet-Ebene miteinander verbunden (z.B. ARP).

Der PC 1 liegt in einem lokalen IP-Subnetz, blue2net hat ein eigenes zweites IP-Interface in diesem Subnetz. Der PC 1 wird ebenfalls von blue2net mittels eines blue2net-internen DHCP-Servers für Ethernet-Terminals konfiguriert.

Da nicht geroutet werden kann, wenn IP-Interface 2 und „Bridge"-IP (‚IP Masquerading' aus [2.5]) im selben Subnetz liegen, vergewissern Sie sich bitte, dass ‚Fixed blue2net Additional IP Address' [2.8.3.1] nicht im selben Subnetz wie ‚IP Masquerading' [2.5] mit Netzmaske aus ‚Terminal Netmask' [3.4] liegt.

Die Verbindung zum Internet-Service-Provider erfolgt über das erste IP-Interface von blue2net, blue2net bekommt die IP-Daten für dieses Interface z.B. über einen DHCP-Server des ISP.

Alle IP-Pakete vom und zum Internet müssen durch den Block „Routing, Firewall, Masquerading, Port Forwarding" hindurchgehen, da beim ISP nur die IP-Adresse von IP-Interface 1 anerkannt wird. Auch der lokale PC 1 schickt seine für das Internet bestimmten Datenpakete zuerst zu blue2net, wo sie maskiert (d.h. wo die Absender IP-Adresse durch die IP-Adresse von blue2net am 1.Interface ersetzt wird) und ins Internet weitergeroutet werden. Die für PC 1 bestimmten Pakete aus dem Internet kommen über IP-Interface 1 zu blue2net, werden im Routing-Block demaskiert (d.h. als Zieladresse wird statt der IP-Adresse am ersten IP-Interface von blue2net wieder die oben ausgetauschte Absender-IP-Adresse des PC 1 ins IP-Paket geschrieben) und gehen über IP-Interface 2 zum PC 1.

9.2 Netz-Struktur bei ‚IP Connection Mode for NAP Terminals' [3.7] auf „bridging"

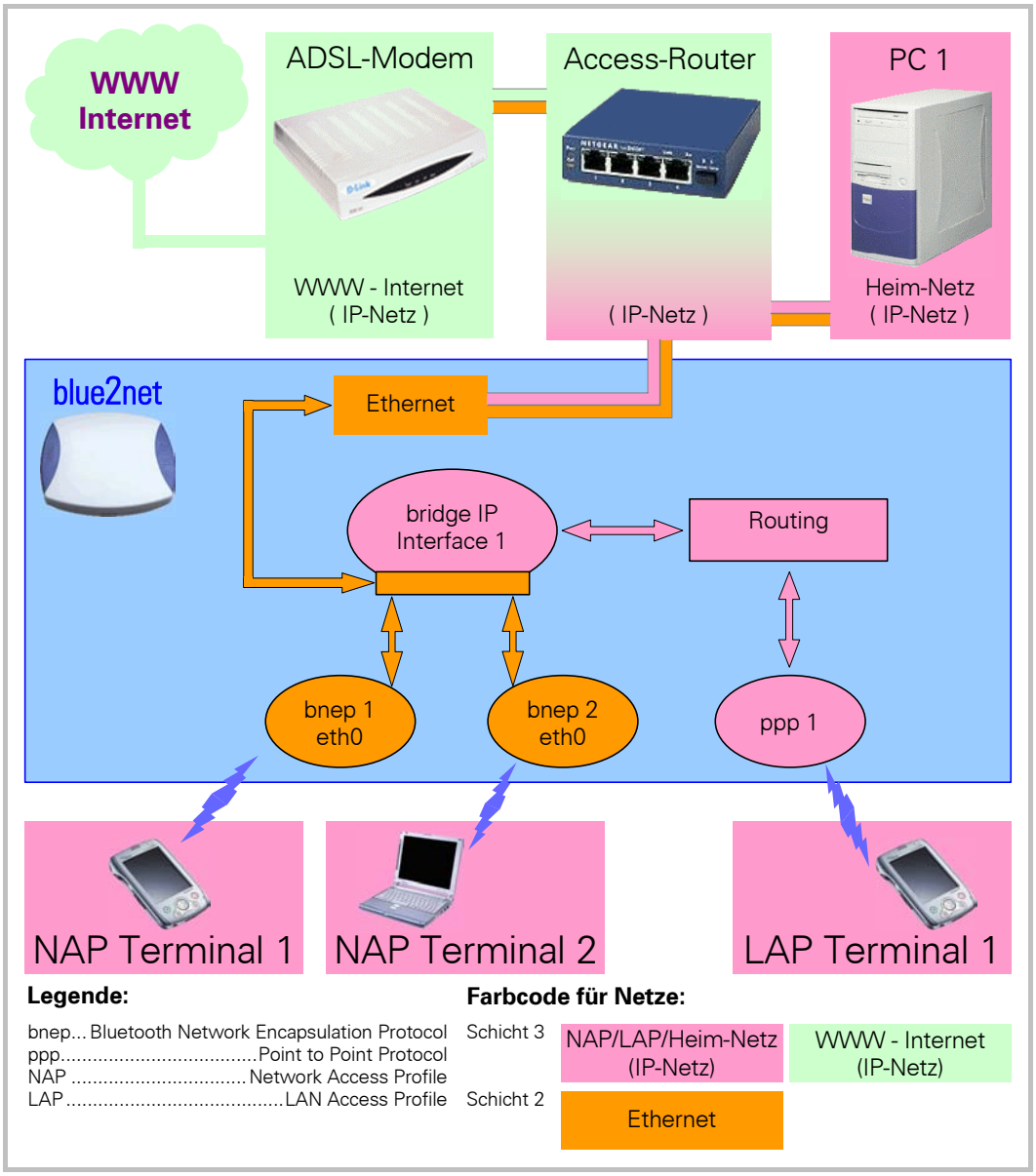


Abb. 38 Netzwerkstruktur bei blue2net im Mode ‚IP Connection Mode for NAP Terminals' auf „bridging"

In Abb. 38 sehen Sie eine typische Netzstruktur bei Einsatz von blue2net im ‚IP Connection Mode for NAP Terminals' [3.7] auf *bridging*. Die Abbildung zeigt speziell die Situation, wo Sie bereits ein anderes Gerät als Access-Router im Einsatz haben, das Ihnen die Funktionen

- Bedienung des ADSL Modems
- Konfiguration der Geräte mit DHCP
- Firewall gegen WWW Internet

zur Verfügung stellt. Dies kann natürlich auch wieder ein blue2net zusammen mit einem preisgünstigen Switch sein. Im „Bridging-Mode“ sind alle Ethernet Geräte auf blue2net miteinander verbunden, als ob sie direkt am Ethernet angeschlossen wären. Auch der PDA „NAP Terminal 1“ und der Laptop „NAP Terminal 2“ sind über die Schnittstellen „bnep1“ und „bnep2“ und die „bridge“ direkt mit dem lokalen Ethernet am Access-Router verbunden. Daher kann PC1 z.B. das „NAP Terminal 1“ ohne Umweg über Routing erreichen. blue2net erscheint im lokalen Netz mit der IP-Adresse, die Sie in [2.1] bis [2.3] eingestellt haben, z.B.192.168.2.2 .

Die Bluetooth-NAP-Terminals, die Bluetooth-Terminals, die LAP benützen und die anderen Geräte am lokalen Ethernet erhalten alle vom Access-Router über dessen DHCP-Server die Informationen für Ihre IP-Schnittstellen. Dazu ist es für die Bluetooth-NAP-Terminals notwendig, dass sie durch den „Bridging-Mode“ direkt auf das lokale Ethernet zugreifen können, da DHCP Ethernet Broadcast benützt. (Siehe User-Szenario 7.1.3). Für die LAP-Terminals kann blue2net stellvertretend das DHCP-Protokoll (mit deren Bluetooth-Adresse als Hardware-Adresse) ausführen und die dabei erhaltenen Konfigurationsdaten dann mittels PPP an die Bluetooth-LAP-Terminals weitergeben.

Wenn Sie im ‚IP Connection Mode for NAP Terminals’ [3.7] auf *bridging* das zweite IP-Interface einschalten, erscheint es als zweite IP-Schnittstelle auf der „bridge“. Da angenommen werden kann, dass Sie das zweite IP-Interface für das lokale Netz nutzen wollen und die IP-Pakete aus dem lokalen Netz maskiert (Englisch: masqueraded) werden sollen, wenn ‚Terminal IP Address Resolution’ [3.1] auf *masquerading* oder *masqueradingpool* gestellt ist, erhält das zweite IP-Interface automatisch die IP-Adresse aus ‚IP Masquerading’ [2.5]. Nur wenn Sie ‚Terminal IP Address Resolution’ [3.1] auf *dhcp* oder *predefined* gestellt haben, werden die IPs aus [2.8.2] wirksam.

9.3 IP-Adressen für Terminals

Tabelle 51 bis Tabelle 58 sollen Ihnen bei der Eintragung der richtigen Werte für IP-Adressen von Terminals in der Konfigurations-Oberfläche helfen.

2 nachfolgende Tabellen gehören immer zusammen:
eine Parameter-Tabelle und eine Lösungstabelle.

Suchen Sie in der ersten Tabelle (Parameter-Tabelle) jene Zeile mit der von Ihnen gewählter Parameter-Einstellung (blau und grau hinterlegt). Dann wählen Sie in dieser Zeile in den grünen Spalten die für Sie interessante Art von Terminal aus und gehen mit der darin stehenden Index-Zahl in die nachfolgende Lösungstabelle.

Dort sehen Sie, woher die IP-Adresse des Terminals kommt. Ist die Zelle in der Parameter-Tabelle bzw. die Zeile in der Lösungstabelle rosa hinterlegt, stellt blue2net nicht automatisch sicher, dass die IP-Adresse des Terminals im richtigen Subnetz liegt. Dafür muss dann der Systemverwalter sorgen. Die Inhalte von grau hinterlegten Zellen ändern sich in einer Parameter-Tabelle nicht, die Inhalte von blau hinterlegten dagegen schon.

Ein Beispiel:
‚IP Connection Mode for NAP Terminals’ [3.7] ist auf *bridging*, ‚Additional IP Interface’ [2.8.1] ist auf *enabled* ‚Terminal IP Address Resolution’ [3.1] ist auf

masquerading, ‚Local DHCP Server for NAP' [3.6.1] ist auf *enabled*, ‚Local DHCP Server for Ethernet' [3.6.2] ist auf *enabled*, und MAC-Adresse + IP-Adresse in Terminal Table [1.10] für ein Terminal, das LAP benutzen möchte, ist nicht vorhanden.

Diese Einstellung entspricht der 3. Zeile in Tabelle 51, die Zelle für LAP-Terminal enthält den Index 3. Da die Zelle nicht rot hinterlegt ist, stellt blue2net automatisch sicher, dass die IP-Adresse des Terminals im richtigen Subnetz zu liegen kommt, indem der Subnetz-Teil der IP-Adresse von blue2net erzeugt wird.

In der Lösungs-Tabelle 52 finden Sie in der 3. Zeile, dass das LAP-Terminal seine IP-Adresse aus dem „Terminal IP Address Pool Range" [3.2]-[3.3] bezieht. Außerdem sehen Sie dort, dass die Terminal-IP-Adresse automatisch in das Subnetz gelegt wird, das durch ‚IP Masquerading' [2.5] und ‚Terminal Netmask' [3.4] definiert ist.

IP Connection Mode for NAP Terminals [3.7]	Additional IP Interface [2.8.1]	Terminal IP Address Resolution [3.1]	Local DHCP Server for NAP [3.6.1]	Local DHCP Server for Ethernet [3.6.2]	MAC-Adresse + IP-Adresse in ‚Terminal Table' [1.10] vorhanden	Terminal Type -> Index in Tabelle 52		
						Bluetooth LAP	Bluetooth NAP	Ethernet
bridging	enabled	masquerading	enabled	egal	ja	1	1	1
bridging	enabled	masquerading	disabled	egal	ja	1	6	6
bridging	enabled	masquerading	enabled	egal	nein	3	3	3
bridging	enabled	masquerading	disabled	egal	nein	3	6	6
bridging	enabled	masqueradingpool	enabled	egal	ja	7	7	7
bridging	enabled	masqueradingpool	disabled	egal	ja	7	6	6
bridging	enabled	masqueradingpool	enabled	egal	nein	1	1	1
bridging	enabled	masqueradingpool	disabled	egal	nein	1	6	6
bridging	enabled	predefined	enabled	egal	ja	4	4	4
bridging	enabled	predefined	disabled	egal	ja	4	2	2
bridging	enabled	predefined	enabled	egal	nein	5	5	5
bridging	enabled	predefined	disabled	egal	nein	2	2	2
bridging	enabled	dhcp	egal	egal	egal	2	2	2
bridging	disabled	masquerading	enabled	egal	ja	1	1	1
bridging	disabled	masquerading	disabled	egal	ja	1	6	6
bridging	disabled	masquerading	enabled	egal	nein	3	3	3
bridging	disabled	masquerading	disabled	egal	nein	3	6	6
bridging	disabled	masqueradingpool	enabled	egal	ja	7	7	7
bridging	disabled	masqueradingpool	disabled	egal	ja	7	6	6
bridging	disabled	masqueradingpool	enabled	egal	nein	3	3	3
bridging	disabled	masqueradingpool	disabled	egal	nein	3	6	6
bridging	disabled	predefined	enabled	egal	ja	10	10	10
bridging	disabled	predefined	disabled	egal	ja	10	12	12
bridging	disabled	predefined	enabled	egal	nein	11	11	11
bridging	disabled	predefined	disabled	egal	nein	11	12	12
bridging	disabled	dhcp	egal	egal	egal	12	12	12

Tabelle 51 Parameter-Tabelle: Auswirkungen der Einstellungen auf Terminal-IP und Terminal-Netzmasken, wenn ‚IP Connection Mode for NAP Terminals' auf *bridging* gesetzt ist

Index	Subnetz für Terminal IP	Subnetzmaske für Terminal	automatisch im richtigen Subnetz ?	IP-Adresse für Terminal von ? Dieser Eintrag muss im richtigen Subnetz sein
1	Masquerading IP [2.5]	Terminal Netmask [3.4]	ja	Eintrag in Terminal Table [1.10]
2	Fixed blue2net Additional IP Addr. [2.8.2.1]	Terminal Netmask [3.4]	nein	externer DHCP-Server
3	Masquerading IP [2.5]	Terminal Netmask [3.4]	ja	Terminal IP Address Pool Range [3.2]-[3.3]
4	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	nein	Eintrag in Terminal Table [1.10]
5	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	nein	Terminal IP Address Pool Range [3.2]-[3.3]
6	Masquerading IP aus [2.5]	Terminal Netmask [3.4]	nein	externer DHCP-Server
7	Masquerading IP aus [2.5]	Terminal Netmask [3.4]	nein	Eintrag in Terminal Table [1.10]
10	blue2net IP aus [2.1]-[2.3]	blue2net Netmask [2.1]-[2.3]	nein	Eintrag in Terminal Table [1.10]
11	blue2net IP aus [2.1]-[2.3]	blue2net Netmask [2.1]-[2.3]	nein	Terminal IP Address Pool Range [3.2]-[3.3]
12	blue2net IP aus [2.1]-[2.3]	blue2net Netmask [2.1]-[2.3]	nein	externer DHCP-Server

Tabelle 52 Lösungstabelle zu Tabelle 51

IP Connection Mode for NAP Terminals [3.7]	Additional IP Interface [2.8.1]	Terminal IP Address Resolution [3.1]	Local DHCP Server for NAP [3.6.1]	Local DHCP Server for Ethernet [3.6.2]	MAC-Adresse + IP-Adresse in ‚Terminal Table' [1.10] vorhanden	Terminal Type -> Index in Tabelle 54	
						Bluetooth LAP	Bluetooth NAP
routing	egal	masquerading	enabled	egal	ja	1	1
routing	egal	masquerading	disabled	egal	ja	1	2
routing	egal	masquerading	enabled	egal	nein	3	3
routing	egal	masquerading	disabled	egal	nein	3	2
routing	egal	masqueradingpool	enabled	egal	ja	4	4
routing	egal	masqueradingpool	disabled	egal	ja	4	2
routing	egal	masqueradingpool	enabled	egal	nein	3	3
routing	egal	masqueradingpool	disabled	egal	nein	3	2
routing	egal	predefined	enabled	egal	ja	4	4
routing	egal	predefined	disabled	egal	ja	4	2
routing	egal	predefined	enabled	egal	nein	5	5
routing	egal	predefined	disabled	egal	nein	5	2
routing	egal	dhcp	egal	egal	egal	6	2

Tabelle 53 Paramter-Tabelle: Auswirkungen der Einstellungen auf Terminal-IP und Terminal-Netzmasken für Bluetooth-Terminals, wenn ‚IP Connection Mode for NAP Terminals' auf *routing* gesetzt ist

Index	Subnetz für Terminal-IP	Subnetzmaske für Terminal	automatisch im richtigen Subnetz ?	IP-Adresse für Terminal von ? Dieser Eintrag muss im richtigen Subnetz sein
1	Masquerading IP [2.5]	Terminal Netmask [3.4]	ja	Eintrag in Terminal Table [1.10]
2	Masquerading IP [2.5]	Terminal Netmask [3.4]	nein	fixed configuration at terminal
3	Masquerading IP [2.5]	Terminal Netmask [3.4]	ja	Terminal IP Address Pool Range [3.2]-[3.3]
4	Masquerading IP [2.5]	Terminal Netmask [3.4]	nein	Eintrag in Terminal Table [1.10]
5	Masquerading IP [2.5]	Terminal Netmask [3.4]	nein	Terminal IP Address Pool Range [3.2]-[3.3]
6	Masquerading IP [2.5]	Terminal Netmask [3.4]	nein	externer DHCP-Server

Tabelle 54 Lösungstabelle zu Tabelle 53

IP Connection Mode for NAP Terminals [3.7]	Additional IP Interface [2.8.1]	Terminal IP Address Resolution [3.1]	Local DHCP Server for NAP [3.6.1]	Local DHCP Server for Ethernet [3.6.2]	MAC-Adresse + IP-Adresse in ‚Fixed IP Address for Local Wired Network' [3.9] vorhanden	Terminal-Type -> Index in Tabelle 56 Ethernet
routing	enabled	masquerading	egal	enabled	ja	1
routing	enabled	masquerading	egal	disabled	ja	2
routing	enabled	masquerading	egal	enabled	nein	3
routing	enabled	masquerading	egal	disabled	nein	2
routing	enabled	masqueradingpool	egal	enabled	ja	4
routing	enabled	masqueradingpool	egal	disabled	ja	2
routing	enabled	masqueradingpool	egal	enabled	nein	3
routing	enabled	masqueradingpool	egal	disabled	nein	2
routing	enabled	predefined	egal	enabled	ja	4
routing	enabled	predefined	egal	disabled	ja	2
routing	enabled	predefined	egal	enabled	nein	5
routing	enabled	predefined	egal	disabled	nein	2
routing	enabled	dhcp	egal	egal	egal	2

Tabelle 55 Parameter-Tabelle: Auswirkungen der Einstellungen auf Terminal-IP und Terminal-Netzmasken für Ethernet-Terminals, wenn ‚IP Connection Mode for NAP Terminals' auf *routing* gesetzt ist und die zweite IP-Schnittstelle aktiviert wurde

Index	Subnetz für Terminal IP	Subnetzmaske für Terminal	automatisch im richtigen Subnetz ?	IP-Adresse für Terminal von ? Dieser Eintrag muss im richtigen Subnetz sein
1	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	ja	Eintrag in ‚Fixed IP Address for Local Wired Network' [3.9]
2	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	nein	Fest eingestellt am Terminal oder externer DHCP-Server
3	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	ja	Available IP Addresses for Local Wired Network [3.8]
4	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	nein	Eintrag in 'Fixed IP Address for Local Wired Network' [3.9]
5	Fixed blue2net Additional IP Addr. [2.8.2.1]	Fixed blue2net Additional IP Netmask [2.8.2.2]	nein	Available IP Addresses for Local Wired Network [3.8]

Tabelle 56 Lösungstabelle zu Tabelle 55

IP Connection Mode for NAP Terminals [3.7]	Additional IP Interface [2.8.1]	Terminal IP Address Resolution [3.1]	Local DHCP Server for NAP [3.6.1]	Local DHCP Server for Ethernet [3.6.2]	MAC-Adresse + IP-Adresse in ‚Fxed IP Address for Local Wired Network' [3.9] vorhanden	Terminal Type -> Index in Tabelle 58
						Ethernet
routing	disabled	nicht dhcp	egal	enabled	ja	1
routing	disabled	nicht dhcp	egal	enabled	nein	2
routing	disabled	dhcp	egal	egal	egal	3

Tabelle 57 Parameter-Tabelle: Auswirkungen der Einstellungen auf Terminal-IP und Terminal-Netzmasken für Ethernet-Terminals, wenn ‚IP Connection Mode for NAP Terminals' auf *routing* gesetzt ist und die zweite IP-Schnittstelle nicht aktiviert ist

Index	Subnetz für Terminal IP	Subnetzmaske für Terminal	automatisch im richtigen Subnetz ?	IP-Adresse für Terminal von ? Dieser Eintrag muss im richtigen Subnetz sein
1	blue2net IP aus [2.1]-[2.3]	blue2net Netmask [2.1]-[2.3]	nein	Eintrag in 'Fixed IP Address for Local Wired Network' [3.9]
2	blue2net IP aus [2.1]-[2.3]	blue2net Netmask [2.1]-[2.3]	nein	Available IP Addresses for Local Wired Network [3.8]
3	blue2net IP aus [2.1]-[2.3]	blue2net Netmask [2.1]-[2.3]	nein	externem DHCP oder fest am Terminal eingestellt

Tabelle 58 Lösungstabelle zu Tabelle 57

10 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.

Beachten Sie auch die Anweisungen betreffend das Abspeichern der Einstellungen wie in Kapitel 8.9.2 beschrieben und zeichnen Sie *permanent gespeicherte Einstellungen* auf.

10.1 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 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 59 Aussperrungs-Szenarien: Aussperrung vom Zugang über Bluetooth und Ethernet (LAN)

10.2 Aussperrung vom Zugang über Bluetooth

Parameter	Hier. stufe	Vor der Umstellung auf	ist zu beachten
Discoverability Mode	[1.4]	nondiscoverable	Manche Terminals müssen blue2net einmal „gesehen“ und die Daten gespeichert haben, bevor Sie eine Verbindung aufbauen können. Lassen Sie deshalb jedes Terminal mindestens einmal blue2net „entdecken“ (Bluetooth-Inquiry + Service Browsing machen), wenn blue2net ‚discoverable’ ist.
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]	authandenc oder auth	Wenn Sie die Authentifizierung aktivieren, was Sie aus Sicherheitsgründen tun sollten, sorgen Sie dafür, dass Sie die eingetragenen Bluetooth-Passwörter [1.12] und [1.10.3] der Terminals in Erinnerung behalten.
Activation	[1.8.9]	deactivated	Wenn Sie für alle 3 Einträge (LAN Access, PAN NAP, PAN GN) der Bluetooth Service Class den Wert auf *deactivated* setzen, ist eine Bluetooth Verbindung nicht mehr möglich. Die einzige Zugangsmöglichkeit zu Ihrem blue2net besteht über das Ethernet (LAN).
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

Parameter	Hier. stufe	Vor der Um-stellung auf	ist zu beachten
Default Bluetooth Passkey	[1.12]	neues Passwort	Wenn Sie das Bluetooth-Passwort 'Default Bluetooth Passkey' ändern, was Sie aus Sicherheitsgründen tun sollten, sorgen Sie dafür, dass Sie das neue Passwort nicht vergessen! Wenn Sie in 'Terminal Table' [1.10] keine Terminals registriert haben, werden Sie keinen Zugang erhalten.
Minimum Length of Key for Encryption	[1.13]	16	Es könnte sein, dass ein älteres Bluetooth-Terminal nicht mehr als 56 bit Verschlüsselung beherrscht. Es kann dann keine Verbindung hergestellt werden.
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 60 Aussperrungs-Szenarien: Aussperrung vom Zugang über Bluetooth

10.3 Aussperrung vom Zugang über Ethernet (LAN)

Parameter	Hier. stufe	Vor der Um-stellung 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].
Protocol Lower Port Number Enable Port Range Higher Port Number (Port Forwarding Rules)	Kombination [2.6.2.3] [2.6.2.4] [2.6.2.5] oder [2.6.2.3] [2.6.2.4] [2.6.2.5] [2.6.2.6]	 6 443 disabled 6 ≤ 443 enabled ≥ 443	Wenn Sie tcp-Port 443 weiterleiten und kein zweites IP-Interface aktiviert haben (d.h. ‚Additional IP Interface' [2.8.1] auf *disabled* gestellt ist), ist blue2net vom Ethernet-Anschluss aus nicht mehr konfigurierbar. Achtung! tcp-Port 443 darf auch nicht im ‚Port Range' zwischen [2.6.2.4] und [2.6.2.6] enthalten sein.

Parameter	Hier. stufe	Vor der Um-stellung auf	ist zu beachten
Lower/Higher Port Number + Enable Port Range (Port Forwarding Rules)	Kombination [2.6.2.4] [2.6.2.5] [2.6.2.6]	0 enabled 65535 (tcp-Port 443 ist damit inkludiert)	Wenn Sie alle Ports (Bereich zwischen [2.6.2.4] / [2.6.2.6]) weiterleiten und kein zweites IP-Interface aktiviert haben (d.h. ‚Additional IP Interface' [2.8.1] auf *disabled* gestellt ist), ist blue2net vom Ethernet-Anschluss aus nicht mehr konfigurierbar.
Protocol (Port Forwarding Rules)	[2.6.2.3]	255 (tcp-Port 443 ist damit inkludiert)	Wenn Sie „alle Protokolle" weiterleiten (= Wert 255 bei [2.6.2.3]) und kein zweites IP-Interface aktiviert haben (d.h. ‚Additional IP Interface' [2.8.1] auf *disabled* gestellt ist), ist blue2net vom Ethernet-Anschluss aus nicht mehr konfigurierbar.

Tabelle 61 Aussperrungs-Szenarien: Aussperrung vom Zugang über Ethernet (LAN)

11 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, bleiben erhalten (beachten Sie dazu aber Kapitel 11.1).

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.

11.1 Für Umsteiger aus früheren SW-Versionen

Einstellungen, welche vor einem Software-Update permanent abgespeichert waren, gehen durch den SW-Update nicht verloren, sondern bleiben unverändert erhalten. Es können bei jeder neuen SW-Version durch Erweiterungen oder Änderungen des Funktionsumfanges neue Parameter dazukommen, einige wegfallen oder Werkseinstellungen z.B. aus Sicherheitsüberlegungen hinsichtlich der Einsatz-Szenarien auf andere Werte gestellt werden, als in der Vorgängerversion.

Damit nicht Werte aus der früheren Software-Version unkontrolliert die Funktion von blue2net beeinflussen können, wird folgende Vorgangsweise empfohlen:

- VOR dem SW-Update:
  - neue Software von der Homepage herunterladen und speichern.
  - die Werte aller Parameter notieren,
  - Wenn Sie xDSL nutzen:
    - xDSL-Verbindung abschalten (‚Tunnel Mode' [2.7.1] auf *none* stellen),
    - Werte abspeichern mit ‚Save Settings Permanently' [6.2],
  - Reset durchführen mit ‚Reset blue2net' [6.3] (bestehende BT-Verbindungen werden abgebrochen!),
- erst DANACH:
  - Software-Update durchführen,
  - alle Werte auf Werkseinstellungen zurücksetzen (siehe Kap. 8.9.5),
  - die Werte aller blue2net-Parameter wieder einstellen, Notizen aus Sicherheitsgründen anschließend vernichten.

Sie könnten natürlich auch zuerst in den Tabellen der Bedienungsanleitung der Folgeversion (z.B. wie hier in Kap. 8.3 „Hierarchie der Parameter für die Konfiguration" und Kap. 17 „Werkseinstellungen") herausfinden, welche Werte sich geändert haben (siehe Änderungshinweis), diese einzeln kontrollieren und

ggf. auf die richtigen Werte (z.B. neue Werkseinstellung) ändern. Dann gehen Sie folgendermaßen vor:

- VOR dem SW-Update:
  - neue Software von der Homepage herunterladen und speichern.
  - die Werte aller geänderten und entfallenden Parameter notieren,
  - Wenn Sie xDSL nutzen:
    - xDSL abschalten (‚Tunnel Mode' [2.7.1] auf *none* setzen),
    - Werte permanent abspeichern mit 'Save Settings Permanently' [6.2],
  - Reset durchführen mit ‚Reset blue2net' [6.3] (bestehende BT-Verbindungen werden abgebrochen!),
- erst DANACH:
  - Software-Update durchführen,
  - die Werte aller geänderten und neuen blue2net-Parameter wieder einstellen, Notizen aus Sicherheitsgründen anschließend vernichten.

11.2 Das Herunterladen neuer Software

ACHTUNG! Die im Folgenden beschriebene Vorgangsweise gilt nicht mehr für Vorgänger-Versionen!
Wenn Sie aus früheren SW-Versionen (siehe ‚Current Configuration' [4] > [4.4.3]) heraus updaten wollen, folgen Sie der Bedienungsanleitung der Vorgänger-version, die auf blue2net installiert ist (Die Bedienungsanleitung mit der Version x.y gehört jeweils zu der Software-Version x.y.z also z.B. 4.0 zu 4.0.z). Grund: die Vorgangsweise, die Sie in der Bedienungsanleitung zu dieser Version finden hat sich geändert gegenüber derjenigen, die bis zur vorhergehenden Version gegolten hat).

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

Während des Update-Vorganges blinkt die LED sehr schnell.

Hinweis: Im Falle von Unklarheiten wenden Sie sich 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. Vergewissern Sie sich, dass alle anderen Benutzer ihre Bluetooth-Verbindungen geordnet beendet haben.

5. Notieren Sie die Werte aller blue2net-Parameter,

6. Wenn Sie xDSL nutzen:
   - xDSL-Verbindung abschalten (‚Tunnel Mode' [2.7.1] auf *none* stellen),
   - Werte permanent abspeichern mit ‚Save Settings Permanently' [6.2],

7. Führen Sie einen Reset durch mit ‚Reset blue2net' [6.3] oder einfach durch kurze Unterbrechung der Stromversorgung (bestehende BT-Verbindungen werden abgebrochen!).

8. Stellen Sie eine Verbindung zu Ihrem blue2net über LAN oder Bluetooth her und verbinden Sie sich mit der Konfigurations-Seite von blue2net (siehe auch 6.4 „Wie Sie zur Konfigurations-Seite gelangen").

   Klicken Sie auf <edit> neben 'Activation Commands' [6], danach auf <edit> neben 'Update Software' [6.4]. Es wird folgende Seite angezeigt:

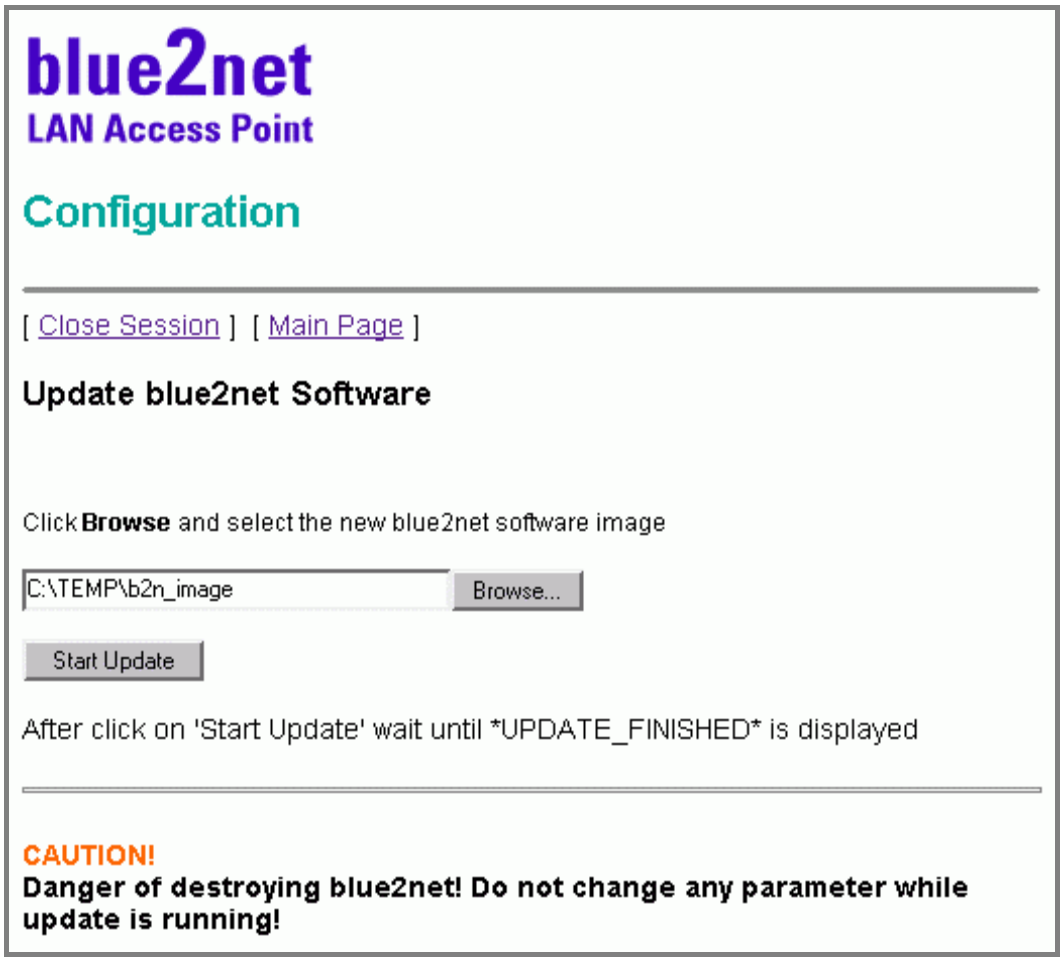


Abb. 39 Software-Update: Auswahl der neuen blue2net Software

9. Wählen Sie die zuvor aus dem Internet heruntergeladene Software-Version für blue2net mit <Browse>. Klicken Sie danach auf <Start Update>, um die

neue Software abzuspeichern und nach dem Reboot wirksam werden zu lassen.

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 (siehe Abb. 40).

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.

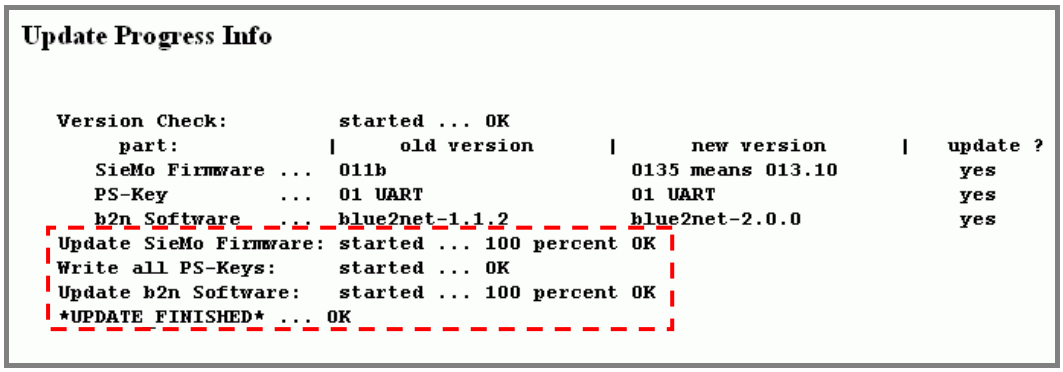


Abb. 40 Fortschritt des Software-Update-Prozesses (Beispiel)

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.

10. 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 (beachte dazu auch Kap. 11.1 und 11.3).

- **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 19) zu wenden. Halten Sie dann auch die Rückmeldung der Statusinformation (nur bei Initiierung über LAN möglich) am Webbrowser bereit.

11. alle Werte auf Werkseinstellungen zurücksetzen mit ‚Restore Default Settings' [6.5] (siehe Kap. 8.9.5),

12. die Werte aller blue2net-Parameter neu einstellen, Notizen aus Sicherheitsgründen anschließend vernichten.

    Die neue Software ist danach bereit zur Verwendung.

11.3 Zukünftige Software-Updates

Zukünftige SW-Versionen können ebenso Änderungen an den Parametern, sowohl hinsichtlich der Anzahl als auch der Werkseinstellung aufweisen.

Für zukünftige Software-Updates ist daher die gleiche Vorgangsweise empfohlen, wie dies für diese Version unter Kapitel 11.1 „Für Umsteiger aus früheren SW-Versionen" beschrieben ist.

Als Änderungshinweise dienen dann die in der Bedienungsanleitung der Folgeversion gemachten Angaben.

12 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.

12.1 Das Laden der spezifischen Homepage

Das Laden der spezifischen Homepage auf Ihr blue2net erfolgt ähnlich wie der Vorgang beim Software-Update (siehe Kapitel 11).

Laden der Datei für die spezifische Homepage:

1. Vergewissern Sie sich, dass alle anderen Benutzer die von ihnen eingerichteten Bluetooth-Verbindungen geordnet beendet haben.

2. Stellen Sie eine Verbindung zu Ihrem blue2net über LAN oder Bluetooth her und verbinden Sie sich mit der Konfigurations-Seite von blue2net (siehe auch 6.4 „Wie Sie zur Konfigurations-Seite gelangen").

   Klicken Sie auf <edit> neben 'Activation Commands', danach auf <edit> neben 'Store Specific Homepage'. Es wird folgende Seite angezeigt:

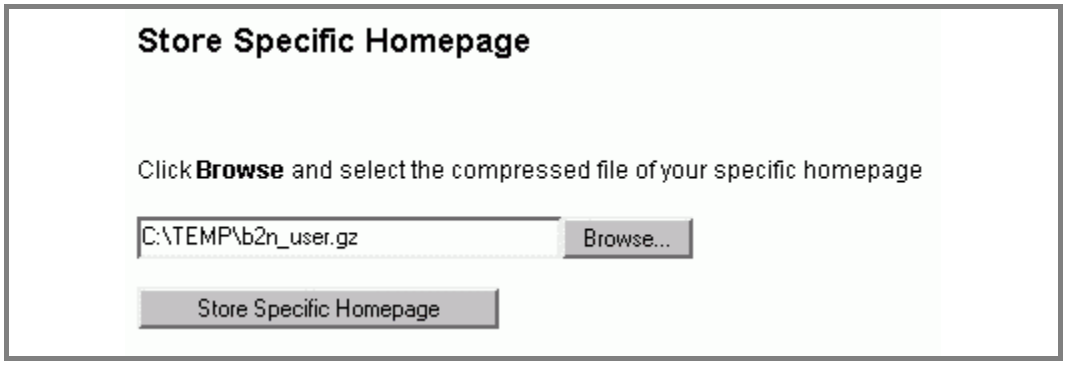


Abb. 41 Spezifische Homepage: Auswahl der neuen spezifischen Homepage

3. Wählen Sie die zuvor mit dem Linux „tar" erstellte Datei mit <Browse> aus. Klicken Sie danach auf <Store Specific Homepage>, um die neue spezifische Homepage temporär zu speichern.

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.

Nach der Überprüfung können Sie die Homepage permanent abspeichern.

Dauerhaftes Speichern der spezifischen Homepage:

4. Vergewissern Sie sich, dass alle anderen Benutzer die von ihnen eingerichteten Bluetooth-Verbindungen geordnet beendet haben.
5. Öffnen Sie die blue2net-Haupt-Konfigurations-Seite (siehe Abb. 8).
6. Klicken Sie auf <edit> neben 'Activation Commands' [6].
7. Klicken Sie auf <edit> neben 'Save Settings Permanently' [6.2].
8. Speichern Sie Ihre spezifische Homepage durch Klicken auf <Submit>.
9. Nun wird blue2net erneut gestartet (Reboot). Dieser Vorgang kann bis zu 2 Minuten dauern.

Ihre spezifische Homepage ist somit bereit zur Verwendung.

13 Fehlerbehebung

Dieser Abschnitt bietet Hilfestellung bei der Bewältigung eventueller Schwierigkeiten.

Berücksichtigen Sie 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.

13.1 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 62 Fehlerbehebung: Hardware

13.2 Bluetooth-Verbindung

Problem	Mögliche Ursache	Mögliche Lösung
blue2net vom Bluetooth-Terminal aus nicht auffindbar	siehe unter „Datenübertragungsrate ist sehr niedrig.“ weiter unten in der Tabelle.	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*
	Terminal wurde nie zuvor im ‚Discoverability Mode’ [1.4] bei Einstellung ‚discoverable’ angemeldet.	Manche Terminals müssen blue2net einmal „gesehen“ und die Daten gespeichert haben, bevor Sie eine Verbindung aufbauen können. Lassen Sie das (jedes) Terminal mindestens einmal anmelden, wenn blue2net ‚discoverable’ ist.

Problem	Mögliche Ursache	Mögliche Lösung
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
Verbindung zwischen blue2net und dem Bluetooth-Terminal nicht möglich.	Manche Terminals unterstützen weder das „LAN Access Profile" noch PAN Services z.B. Mobiltelefone unterstützen nur das Bluetooth Headset.	z.B. zukünftige Mobiltelefone werden die in blue2net angebotenen Profile/Services („LAN Access Profile"/"PAN Services", „Network Access Point" und „Group Networking") zunehmend unterstützen.
	'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].
	In der Tabelle 'Service Table' [1.8] wurden alle 3 Services deaktiviert.	über LAN auf die Konfiguration zugreifen und bei 'Activation' [1.8.9] mindestens 1 Service aktivieren.

Problem	Mögliche Ursache	Mögliche Lösung
	‚Minimum Length of Key for Encryption' [1.13] zu hoch eingestellt [1.13]. Es könnte sein, dass ein älteres Bluetooth-Terminal nicht mehr als 56 bit Verschlüsselung beherrscht. Sie können das überprüfen, indem Sie a) in der Anleitung des Bluetooth-Terminals nachschauen, b) den Hersteller kontaktieren bzw. im Internet Info einholen, c) es ausprobieren, wenn Sie sich im Fall eines Fehlschlags als zweite Möglichkeit Zugang über Ethernet/LAN oder ein anderes BT-Terminal verschaffen können.	Reduzieren Sie [1.13] auf 7 oder 5 oder Aktualisieren Sie – wenn möglich – die Firmware Ihres Bluetooth-Terminals, damit es 128 bit Verschlüsselung beherrscht oder Verwenden Sie ein Bluetooth-Terminal, das 128 bit beherrscht.
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 4.2).

Tabelle 63 Fehlerbehebung: Bluetooth-Verbindung

13.3 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. bzw. blue2net bekommt keine IP-Adresse vom DHCP-Server zugewiesen	Überprüfen der IP-Parameter für blue2net [2]. Fragen Sie bei Ihrem Netzwerk-Administrator oder Internet-Service-Provider nach den richtigen IP-Parametern. Fallback blue2net IP-Parameter [2.3.x] eintragen wie z.B. in Kap. 7.1.2 unter „Optionale Einstellungen:“ beschrieben
Externe Computer (Internet) sind über die eigenen IP-Adressen erreichbar, jedoch nicht über deren URLs (z.B. www.siemens.at). (Fehlermeldung: z.B. „Die Seite kann nicht angezeigt werden. ...Fehler: Server oder DNS kann nicht gefunden werden“)	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 von 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.

Problem	Mögliche Ursache	Mögliche Lösung
	'Default Firewall' [2.6.1] ist auf *enabled* gesetzt.	Von außen unsichtbar und vor Zugriffen geschützt zu sein ist einer der Hauptgründe für die Verwendung von Firewalls. Sie können aber einzelne Services mit „Port Forwarding“ nach außen sichtbar einblenden (siehe Kapitel 8.5.4) Wenn aber ‚Terminal Address Resolution’ [3.1] auf *masquerading* eingestellt ist, ist das Bluetooth-Terminal vom Internet aus trotzdem nicht erreichbar..

Tabelle 64 Fehlerbehebung: Zugang zum LAN

13.4 Software-Update

Problem	Mögliche Ursache	Mögliche Lösung
Image-Datei kann auf blue2net nicht gespeichert werden.	Falsche (zu große) Image-Datei wurde auf blue2net gespeichert.	Neustarten von blue2net (siehe Kapitel 8.9.3). Es wird empfohlen, ausschließlich blue2net-Softwaredateien (b2n_image) auf blue2net zu kopieren.

Tabelle 65 Fehlerbehebung: Software-Update

13.5 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 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**://....
	Etwas ältere Geräte, die Browserversionen installiert haben, die 128 bit-Verschlüsselung noch nicht beherrschen können nicht auf die Konfigurationsseite zugreifen.	Prüfen Sie, ob der Browser am Terminal die 128 bit Verschlüsselung beherrscht. Klicken Sie dazu auf „Info" in der Menüleiste des Browsers. Für Internet Explorer 5.00 gibt es ein update unter http://www.microsoft.com/windows/ie/downloads/recommended/128bit/default.asp
Konfigurations-Passwort wird permanent gefragt.	Am Web-Browser sind die „Cookies" nicht aktiviert.	Aktivieren der „Cookies" auf dem Web-Browser.

Tabelle 66 Fehlerbehebung: Zugang zur Konfiguration

14 Firewall

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

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).

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

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
DHCP (nur von Quellport 68)	tcp / udp	67
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/aus), 68 (aus/ein)
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 67 Dienste, die bei aktivierter Firewall genützt werden können

Zusätzlich werden noch Dienste durchgelassen, die Sie mit den ‚Port Forwarding Rules' [2.6.2] an Ethernet-Terminals (PCs/Laptops im Heim-LAN) weiterleiten. Sie müssen an den Zielgeräten dafür sorgen, dass Missbrauch ausgeschlossen ist. Transaktionen für alle Dienste aus Tabelle 67 können nur von innerhalb der Firewall (von einem über Bluetooth angeschlossenen Gerät oder Ethernet-Terminals (PCs/Laptop im Heim-LAN) gestartet werden.

Auch bei aktivierter Firewall können Sie von LAN-Seite her blue2net konfigurieren, da dafür https mit Passwortschutz verwendet wird. Auch Software-Update und das Laden einer spezifischen Homepage sind über Ethernet (LAN) möglich. Bei früheren SW-Versionen war das nicht möglich. blue2net ist also jetzt voll tauglich für Fernwartung.

Wie Sie die Firewall aktivieren bzw. deaktivieren finden Sie in den Kapiteln 6.4, 8.5 und 8.5.3.

15 Regulatory Statement / Konformitätserklärung

15.1 General

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

15.2 European Union (EU) and EFTA Member States

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

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

Tabelle 68 Conformity with standards and specifications

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

Abb. 42 CE Conformity Marking / CE Konformitätszeichen

15.3 United States of America (USA)

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

FCC ID: P6L-blue2net

Operation is subject to the following two conditions:

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

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

16 Bluetooth Compliance

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

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

17 Werkseinstellungen

Um die Werkseinstellungen wiederherzustellen, verwenden Sie den Aktivierungsbefehl 'Restore Default Settings' (siehe Kapitel 8.9.5).

[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	(1)	LAN ACCESS 1	
		(2)	PAN NAP	
		(3)	PAN GN	
[1.8.3]	Service Description	(1)	LAN ACCESS via blue2net	
		(2)	PAN NAP via blue2net	
		(3)	PAN GN via blue2net	
[1.8.4]	Auth. Level		authandenc (geändert!)	**
[1.8.5]	Service Provider		SIEMENS	
[1.8.6]	Service URL		http://www.siemens.at/bluetooth	
[1.8.7]	Service ID		– (Anzeige)	
[1.8.8]	Bluetooth Service Class		– (Anzeige)	
[1.8.9]	Activation	(alle 3)	activated	
[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	
[1.10.5]	Allow Bluetooth Bonding		disabled	*
[1.11]	Default Access Mode		enabled	
[1.12]	Default Bluetooth Passkey		1234	
[1.13]	Minimum Length of Key for Encryption		7	*
[2]	**IP Parameters for blue2net**		–	
[2.1]	blue2net IP Address Resolution		dhcp	
[2.2]	Fixed blue2net IP Configuration		–	
[2.2.1]	Fixed blue2net IP Address		192.168.1.2	
[2.2.2]	Fixed blue2net Netmask		255.255.255.0	
[2.2.3]	Fixed blue2net Gateway		192.168.1.1	
[2.3]	DHCP blue2net IP Objects		–	
[2.3.1]	Fallback blue2net IP Address		192.168.1.2	
[2.3.2]	Fallback blue2net Netmask		255.255.255.0	
[2.3.3]	Fallback blue2net Gateway		192.168.1.1	
[2.4]	Time Server IP		0.0.0.0	
[2.5]	IP Masquerading		192.168.2.2	

Tabelle 69 Werkseinstellungen (Default-Werte) (1)

[Hier.ebene] Parameter & Objekte	Werkseinstellung	
[2] **IP Parameters for blue2net**	–	
[2.6] Firewall Settings	–	
[2.6.1] Default Firewall	disabled	
[2.6.2] Port Forwarding Rules	–	*
[2.6.2.1] Index	– (Anzeige)	*
[2.6.2.2] Enable Rule	disabled	*
[2.6.2.3] Protocol	17	*
[2.6.2.4] Lower Port Number	0	*
[2.6.2.5] Enable Port Range	disabled	*
[2.6.2.6] Higher Port Number	65535	*
[2.6.2.7] Fwd. Destination IP Addr.	0.0.0.0	*
[2.6.2.8] Fwd. Source IP Address	0.0.0.0	*
[2.6.2.9] Fwd. Source IP Add. Netm.	0.0.0.0	*
[2.6.3] Number of Port Forwarding Rules	– (Anzeige)	*
[2.7] Tunnel Configuration	–	
[2.7.1] Tunnel Mode	none	
[2.7.2] Tunnel Establishment Control	disabled	
[2.7.3] Authentication Parameters	–	
[2.7.3.1] Tunnel User Name	pppoeuser	
[2.7.3.2] Tunnel User Password	pppoepassw	
[2.7.4] PPTP Server IP Address	10.0.0.138	
[2.8] Access Router	–	*
[2.8.1] Additional IP Interface	disabled	*
[2.8.2] Fixed Additional IP Interface	–	*
[2.8.2.1] Fixed b2n Addl. IP Address	192.168.3.2	*
[2.8.2.2] Fixed b2n Addl. IP Netmask	255.255.255.0	*
[3] **IP Parameters for Terminals**	–	
[3.1] Terminal IP Address Resolution	masquerading	
[3.2] Start of Terminal IP Addr. Pool Range	192.168.1.11	***
[3.3] End of Terminal IP Address Pool Range	192.168.1.70	***
[3.4] Terminal Net Mask	255.255.255.0	
[3.5] Terminal Fixed Servers	–	
[3.5.1] Terminal DNS Server 1	192.168.3.11	
[3.5.2] Terminal DNS Server 2	192.168.3.12	
[3.5.3] Terminal WINS Server 1	192.168.3.13	
[3.5.4] Terminal WINS Server 2	192.168.3.14	
[3.5.5] Terminal Domain Name	my.domain.at	
[3.6] Local DHCP Server Objects	–	*
[3.6.1] Local DHCP Server for NAP	enabled	*
[3.6.2] Local DHCP Server for Ethernet	disabled	*
[3.7] IP Connection Mode for NAP Terminals	routing	*
[3.8] Available IP Addresses for Local Wired Network	–	*
[3.8.1] Lowest IP Address of Range	192.168.3.20	*
[3.8.2] Highest IP Address of Range	192.168.3.253	*
[3.9] Fixed IP Addresses for Local Wired Network	–	*
[3.9.1] Index	– (Anzeige)	*
[3.9.2] MAC Address	00:00:00:00:00:00	*
[3.9.3] IP Address	0.0.0.0	*
[3.10] Number of Fixed IP Addresses	– (Anzeige)	*

Tabelle 70 Werkseinstellungen (Default-Werte) (2)

[Hier.ebene] Parameter & Objekte			Werkseinstellung
[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)
		[4.5.2] IP Address of Tunnel Endpoint on b2n	– (Anzeige) *
[5]	**Configuration Access**		–
	[5.1]	SNMP Access	disabled
	[5.2]	Configuration Password	changeme
[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 71 Werkseinstellungen (Default-Werte) (3)

Änderungshinweise:

gegenüber der Vorgänger-SW v 3.0.0 / Bedienungsanleitung v 3.0 wurde folgendes geändert (siehe auch Kap. 11.3):

*) neuer Parameter

**) Werkseinstellung (Default-Wert) wurde geändert!

***) Funktionsänderung

[3.2] und [3.3] wurden umbenannt und haben neue Funktion

[3.3.1] und [3.3.2] sind entfallen

[5.2.1] wird ab jetzt mit [5.2] bezeichnet

18 Abkürzungen und Begriffe

Term	Erklärung
ARP	Address Resolution Protocol (wird benutzt, um die zu einer IP-Addresse zugehörige Ethernet-Adresse zu finden)
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
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
IMAP	Internet Mail Access Protocol
IMAP SEC	Internet Mail Access Protocol secure
IP	Internet Protocol
ISP	Internet Service Provider
KPOP	Post Office Protocol Kerberos
LAN	Local Area Network
LAP	LAN Access Profile
LED	Light Emitting Diode
MAC	Medium Access Control
PAN	Personal Area Networking
PAN GN	Personal Area Networking Group Network
PAN NAP	Personal Area Networking Network Access Point
Passkey	Ein anderer Name für PIN
PCMCIA	Personal Computer Memory Card Int. Association Synonym für einen Standard für Steckkarten, wie z.B. Bluetooth- und Faxkarten

Tabelle 72 Abkürzungen und Begriffe (1)

Term	Erklärung
PDA	Personal Digital Assistant
PIN	Personal Identification Number
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 73 Abkürzungen und Begriffe (2)

19 Service / Kundendienst

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

Technische Informationen, Software-Updates und Antworten auf oft gestellte Fragen (FAQs) finden Sie auf der Produkt-Homepage http://www.siemens.at/bluetooth > Produkte > blue2net ...

20 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.

21 Technische Daten

Funktechnologie	Bluetooth V1.1, power class 2,2 dBm
Frequenzbereich	2.402 bis 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 bis zu 7 Benutzer gleichzeitig
Bluetooth Profiles	LAN Access Profile, Generic Access Profile, Serial Port Profile, PAN Profile
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	4.4 V, 600 mA, ext. 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	über eingebauten Web-Server
blue2net IP-Adressen-Zuweisung	DHCP oder predefined (fix)
Terminal IP-Adressen-Zuweisung	masquerading oder DHCP (extern/intern) oder predefined (fix)
xDSL Protokolle	PPPoE (RFC 2516) PPtP (RFC 2637)
Access-Router-Funktionalität	zweite IP-Schnittstelle mit internem DHCP-Server Bridging-/Routing-Möglichkeit für PAN
Kaskadierbarkeit von blue2net	Ein Master-Gerät, mehrere Slave-Geräte (für Hot Spots)
Port-Forwarding	alle IP-Protokolle, alle Ports
Sicherheit	Konfigurations-Passwort und HTTPS, Bluetooth-Passwort, integrierte Firewall
Ladbare Homepage auf blue2net	bis zu 60 kBbyte gezippt auf blue2net speicherbar
Software-Aktualisierungen mit https (Fernwartungsmöglichkeit)	unter http://www.siemens.at/bluetooth
Weitere Information	http://www.siemens.at/bluetooth

Tabelle 74 Technische Daten

22 Index

D

E

F

G

H

T

U

V

W

X

Z

23 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, 18.3.02

Head of Quality Assurance
Herbert Haunschmid
Vienna, 15.3.02

Abb. 43 Konformitätserklärung (CE-Erklärung)

Notizen:

Notizen:

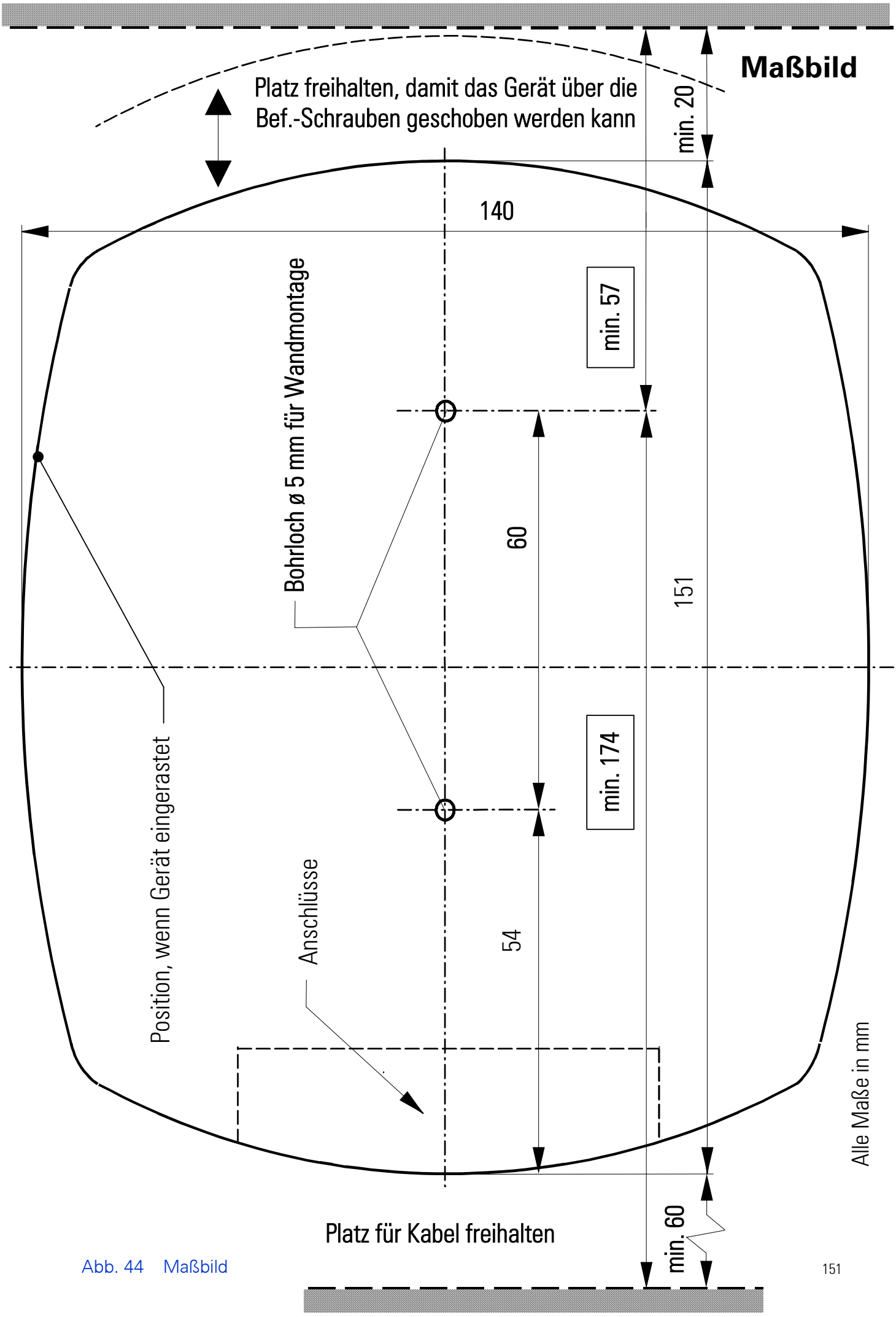


Abb. 44 Maßbild