Benutzerhandbuch

INSYS icom

Industrielle Datenkommunikation

EBW-H100

Herausgeber:
INSYS MICROELECTRONICS GmbH
Hermann-Köhl-Str. 22
93049 Regensburg
Telefon: +49 941 58692 0
Telefax: +49 941 58692 45
E-Mail: info@insys-icom.de
Internet: http://www.insys-icom.de

Datum: Dec-20
Artikelnummer: 10014939
Version: 1.11
Sprache: DE

1 Allgemeines

Diese Anleitung ermöglicht den sicheren und effizienten Umgang mit dem Produkt. Die Anleitung ist Bestandteil des Produkts und muss für Installations-, Inbetriebnahme- und Bedienpersonal jederzeit zugänglich aufbewahrt werden.

1.1 Gewährleistungsbestimmungen

Eine nicht bestimmungsgemäße Verwendung, ein Nichtbeachten dieser Dokumentation, der Einsatz von unzureichend qualifiziertem Personal sowie eigenmächtige Veränderungen schließen die Haftung des Herstellers für daraus resultierende Schäden aus. Die Gewährleistung des Herstellers erlischt.

Es gelten die Bestimmungen unserer Liefer- und Einkaufsbedingungen (AGB). Diese finden Sie auf unserer Webseite (www.insys-icom.de/impressum/) unter „AGB“.

1.2 Feedback

Wir verbessern unsere Produkte und die zugehörige Technische Dokumentation ständig. Dazu sind Ihre Rückmeldungen sehr hilfreich. Bitte teilen Sie uns mit, was Ihnen an unseren Produkten und Publikationen besonders gefallen hat und was wir Ihrer Meinung nach noch verbessern können. Wir schätzen Ihre Anregungen sehr und werden diese in unsere Arbeit einfließen lassen, um Ihnen und all unseren Kunden zu helfen. Wir freuen uns über jede Ihrer Rückmeldungen.

Schreiben Sie uns eine E-Mail an support@insys-tec.de.

Gerne erfahren wir, welche Anwendungen Sie haben. Schreiben Sie uns bitte ein paar Stichpunkte, damit wir wissen, welche Anforderungen Sie mit Produkten von INSYS icom lösen.

1.3 Kennzeichnung von Warnungen und Hinweisen

Symbole und Signalwörter

Gefahr!

Schwere gesundheitliche Schäden / Lebensgefahr

Eines dieser Symbole in Verbindung mit dem Signalwort Gefahr kennzeichnet eine unmittelbare drohende Gefahr. Bei Missachtung sind Tod oder schwerste Verletzungen die Folge.

Warnung!

Schwere gesundheitliche Schäden / Lebensgefahr möglich

Dieses Symbol in Verbindung mit dem Signalwort Warnung kennzeichnet eine möglicherweise gefährliche Situation. Bei Missachtung können Tod oder schwerste Verletzungen die Folge sein.

Vorsicht!

Leichte Verletzungen und / oder Sachschäden

Dieses Symbol in Verbindung mit dem Signalwort Vorsicht kennzeichnet eine möglicherweise gefährliche oder schädliche Situation. Bei Missachtung können leichte oder geringfügige Verletzungen die Folge sein oder das Produkt oder etwas in seiner Umgebung beschädigt werden.

Hinweis

Optimierung der Anwendung

Dieses Symbol in Verbindung mit dem Signalwort Hinweis kennzeichnet Anwendungstipps oder besonders nützliche Informationen. Diese Informationen helfen bei Installation, Einrichtung und Betrieb des Produkts zur Sicherstellung eines störungsfreien Betriebs.

1.4 Symbole und Formatierungen dieser Anleitung

Im Folgenden werden die Festlegungen, Formatierungen und Symbole erklärt, die in diesem Handbuch verwendet werden. Die unterschiedlichen Symbole sollen Ihnen das Lesen und Auffinden der für Sie wichtigen Information erleichtern. Der folgende Text entspricht in seiner Struktur den Handlungsanweisungen dieses Handbuchs.

Fett gedruckt: Das Handlungsziel. Hier erfahren Sie, was Sie mit den folgenden Schritten erreichen

Nach der Nennung des Handlungsziels wird detaillierter erklärt, was mit der Handlungsanweisung erreicht werden soll. So können Sie entscheiden, ob der Abschnitt überhaupt für Sie relevant ist.

⇢ Vorbedingungen, die erfüllt sein müssen, damit die nachfolgenden Schritte sinnvoll abgearbeitet werden können, sind mit einem Pfeil gekennzeichnet. Hier erfahren Sie zum Beispiel, welche Software oder welches Zubehör Sie benötigen.

1. Ein einzelner Handlungsschritt: Dieser sagt Ihnen, was Sie an dieser Stelle tun müssen. Zur besseren Orientierung sind die Schritte nummeriert.

✓ Ein Ergebnis, das Sie nach Ausführen eines Schrittes bekommen, ist mit einem Häkchen gekennzeichnet. Hier können Sie kontrollieren, ob die zuvor gemachten Schritte erfolgreich waren.

ⓘ Zusätzliche Informationen, die an dieser Stelle Ihre Beachtung finden sollten, sind mit einem eingekreisten „i“ gekennzeichnet. Hier werden Sie auf mögliche Fehlerquellen und deren Vermeidung hingewiesen.

➢ *Alternative Ergebnisse und Handlungsschritte sind mit einem Pfeil gekennzeichnet. Hier erfahren Sie, wie Sie auf einem anderen Weg zum gleichen Ergebnis kommen, oder was Sie tun können, falls Sie an dieser Stelle nicht das erwartete Ergebnis bekommen haben.*

2 Sicherheit

Der Abschnitt Sicherheit verschafft einen Überblick über die für den Betrieb des Produkts zu beachtenden Sicherheitshinweise.

Das Produkt ist nach den derzeit gültigen Regeln der Technik gebaut und betriebssicher. Es wurde geprüft und hat das Werk in sicherheitstechnisch einwandfreiem Zustand verlassen. Um diesen Zustand über die Betriebszeit zu erhalten, sind die Angaben der geltenden Publikationen und Zertifikate zu beachten und zu befolgen.

Die grundlegenden Sicherheitshinweise sind beim Betrieb des Produkts unbedingt einzuhalten. Über die grundlegenden Sicherheitshinweise hinaus sind in den einzelnen Abschnitten der Dokumentation die Beschreibungen von Vorgängen und Handlungsanweisungen mit konkreten Sicherheitshinweisen versehen.

Darüber hinaus gelten die örtlichen Unfallverhütungsvorschriften und allgemeine Sicherheitsbestimmungen für den Einsatzbereich des Geräts.

Erst die Beachtung aller Sicherheitshinweise ermöglicht den optimalen Schutz des Personals und der Umwelt vor Gefährdungen sowie den sicheren und störungsfreien Betrieb des Produkts.

2.1 Bestimmungsgemäße Verwendung

Das Produkt dient ausschließlich zu den aus der Funktionsübersicht hervorgehenden Einsatzzwecken. Zusätzlich darf das Gerät für die folgenden Zwecke eingesetzt werden:

- Einsatz und Montage in einem industriellen Schaltschrank
- Übernahme von Schalt- sowie Datenübertragungsfunktionen in Maschinen, die der Maschinenrichtlinie 2006/42/EG entsprechen
- Einsatz als Datenübertragungsgerät an einer speicherprogrammierbaren Steuerung

Das Produkt darf **nicht** zu den folgenden Zwecken und unter diesen Bedingungen verwendet oder betrieben werden:

- Steuerung oder Schaltung von Maschinen und Anlagen, die nicht der Richtlinie 2006/42/EG entsprechen
- Einsatz, Steuerung, Schaltung und Datenübertragung in Maschinen oder Anlagen, die in explosionsfähigen Atmosphären betrieben werden
- Steuerung, Schaltung und Datenübertragung von Maschinen, deren Funktionen oder deren Funktionsausfall eine Gefahr für Leib und Leben darstellen können

2.2 Technische Grenzwerte

Das Produkt ist ausschließlich für die Verwendung innerhalb der in den Datenblättern angegebenen technischen Grenzwerte bestimmt.

Folgende Grenzwerte sind einzuhalten:

- Die Umgebungstemperaturgrenzen dürfen nicht unter- bzw. überschritten werden.
- Der Versorgungsspannungsbereich darf nicht unter- bzw. überschritten werden.
- Die maximale Luftfeuchtigkeit darf nicht überschritten werden und Kondensatbildung muss vermieden werden.
- Die maximale Schaltspannung und die maximale Schaltstrombelastung dürfen nicht überschritten werden.
- Die maximale Eingangsspannung und der maximale Eingangsstrom dürfen nicht überschritten werden.

2.3 Pflichten des Betreibers

Der Betreiber muss grundsätzlich die in seinem Land geltenden nationalen Vorschriften bezüglich Betrieb, Funktionsprüfung, Reparatur und Wartung von elektronischen Geräten beachten.

2.4 Qualifikation des Personals

Die Installation, Inbetriebnahme und Wartung des Produkts darf nur durch ausgebildetes Fachpersonal erfolgen, das vom Anlagenbetreiber dazu autorisiert wurde. Das Fachpersonal muss diese Dokumentation gelesen und verstanden haben und die Anweisungen befolgen.

Der elektrische Anschluss und die Inbetriebnahme des Produkts darf nur durch eine Person erfolgen, die aufgrund ihrer fachlichen Ausbildung, Kenntnisse und Erfahrungen sowie Kenntnis der einschlägigen Normen und Bestimmungen in der Lage ist, Arbeiten an elektrischen Anlagen auszuführen und mögliche Gefahren selbständig zu erkennen und zu vermeiden.

2.5 Hinweise zu Transport und Lagerung

Die folgenden Hinweise sind zu beachten:

- Das Produkt während des Transports und der Lagerung keiner Feuchtigkeit und keinen anderen möglicherweise schädlichen Umweltbedingungen (Einstrahlung, Gase, usw.) aussetzen. Produkt entsprechend verpacken.
- Das Produkt so verpacken, dass es vor Erschütterungen beim Transport und bei der Lagerung geschützt ist, z.B. durch luftgepolsterte Verpackung.

Produkt vor Installation auf mögliche Beschädigungen überprüfen, die durch unsachgemäßen Transport oder unsachgemäße Lagerung entstanden sein könnten. Transportschäden müssen auf den Frachtpapieren festgehalten werden. Alle Schadensersatzansprüche unverzüglich und vor der Installation gegenüber dem Spediteur / dem für die Lagerung verantwortlichen Unternehmen geltend machen.

2.6 Kennzeichnungen auf dem Produkt

Das Typenschild des Produkts befindet sich entweder als Aufdruck oder Aufkleber auf einer Fläche des Produkts. Es kann unter anderem folgende Kennzeichnungen enthalten, die hier näher erläutert sind.

Handbuch beachten

Dieses Symbol weist darauf hin, dass das Handbuch des Produkts essentielle Sicherheitshinweise enthält, die unbedingt zu beachten sind.

Altgeräte umweltgerecht entsorgen

Dieses Symbol weist darauf hin, dass Altgeräte getrennt vom Restmüll über geeignete Sammelstellen zu entsorgen sind. Siehe auch Abschnitt Entsorgung in diesem Handbuch.

CE-Kennzeichnung

Durch die Anbringung der CE-Kennzeichnung bestätigt der Hersteller, dass das Produkt den produktspezifisch geltenden europäischen Richtlinien entspricht.

UL-Kennzeichnung

Durch die Anbringung der UL-Kennzeichnung bestätigt der Hersteller, dass das Produkt die vorgegebenen Sicherheitsanforderungen einhält.

Schutzklasse II - Schutzisolierung

Dieses Symbol weist darauf hin, dass das Produkt der Schutzklasse II entspricht.

2.7 Umweltschutz

Entsorgen Sie das Produkt sowie die Verpackung gemäß den entsprechenden Umweltschutzvorschriften. Im Abschnitt Entsorgung dieses Handbuchs finden Sie Hinweise zur Entsorgung des Produkts. Trennen Sie die Verpackungsbestandteile aus Karton und Papier sowie Kunststoff und führen Sie sie über die entsprechenden Sammelsysteme dem Recycling zu.

2.8 Sicherheitshinweise zur elektrischen Installation

Der elektrische Anschluss darf nur von autorisiertem Fachpersonal gemäß den Elektroplänen vorgenommen werden.

Die Hinweise zum elektrischen Anschluss in der Anleitung beachten, ansonsten kann die elektrische Schutzart beeinträchtigt werden.

Die sichere Trennung von berührungsgefährlichen Stromkreisen ist nur gewährleistet, wenn die angeschlossenen Geräte die Anforderungen der VDE 0106 T.101 (Grundanforderungen für sichere Trennung) erfüllen.

Für die sichere Trennung die Zuleitungen getrennt von berührungsgefährlichen Stromkreisen führen oder zusätzlich isolieren.

Vor Inbetriebnahme des Geräts ist eine leicht zugängliche, allpolige Trennvorrichtung zu installieren, um das Gerät allpolig von der Stromversorgung trennen zu können.

2.9 Grundlegende Sicherheitshinweise

Vorsicht!

Nässe und Flüssigkeiten aus der Umgebung können ins Innere des Produkts gelangen!

Brandgefahr und Beschädigung des Produkts.

Das Produkt darf nicht in nassen oder feuchten Umgebungen oder direkt in der Nähe von Gewässern eingesetzt werden. Installieren Sie das Produkt an einem trockenen, vor Spritzwasser geschützten Ort. Schalten Sie die Spannung ab, bevor Sie Arbeiten an einem Gerät durchführen, das mit Feuchtigkeit in Berührung kam.

Vorsicht!

Kurzschlüsse und Beschädigung durch unsachgemäße Reparaturen und Modifikationen sowie Öffnen von Wartungsbereichen!

Brandgefahr und Beschädigung des Produkts.

Das Öffnen des Produkts für Reparaturarbeiten oder Modifikationen ist nicht erlaubt.

Vorsicht!

Überstrom in der Geräteversorgung!

Brandgefahr und Beschädigung des Produkts durch Überstrom.

Sichern Sie das Produkt mit einer geeigneten Sicherung gegen Ströme höher als 1,6 A ab.

Vorsicht!

Überspannung und Spannungsspitzen aus dem Stromnetz!

Brandgefahr und Beschädigung des Gerätes durch Überspannung.

Installieren Sie einen geeigneten Überspannungsschutz.

Vorsicht!

Beschädigung durch Chemikalien!

Ketone und chlorierte Kohlenwasserstoffe lösen den Kunststoff des Gehäuses und beschädigen die Oberfläche des Geräts.

Bringen Sie das Gerät auf keinen Fall mit Ketonen (z.B. Aceton) und chlorierten Kohlenwasserstoffen (z.B. Dichlormethan) in Berührung.

Vorsicht!

Abstand von Antennen zu Personen!

Ein zu geringer Abstand von Mobilfunkantennen zu Personen kann die Gesundheit beeinträchtigen.

Bitte beachten Sie, dass die Mobilfunkantenne während des Betriebs mindestens 20 cm von Personen entfernt sein muss.

3 Verwendung von Open-Source-Software

3.1 Allgemeines

Unser Produkt EBW-H100 beinhaltet unter anderem auch sogenannte Open-Source-Software, die von Dritten hergestellt und für die freie Verwendung durch jedermann veröffentlicht wurde. Die Open-Source-Software steht unter besonderen Open-Source-Softwarelizenzen und dem Urheberrecht Dritter. Jeder Kunde kann die Open-Source-Software nach den Lizenzbestimmungen der jeweiligen Hersteller grundsätzlich frei verwenden. Die Rechte des Kunden, die Open-Source-Software über den Zweck unseres Produktes hinaus zu verwenden, werden im Detail von dem jeweils betroffenen Open-Source-Softwarelizenzen geregelt. Der Kunde kann die Open-Source-Software, so wie in der jeweiligen gültigen Lizenz vorgesehen, über die Zweckbestimmung, die die Open-Source-Software in unserem Produkt erfährt, hinaus frei verwenden. Für den Fall, dass zwischen unseren Lizenzbestimmungen für unser Produkt und der jeweiligen Open-Source-Softwarelizenz ein Widerspruch besteht, geht die jeweils einschlägige Open-Source-Softwarelizenz unseren Lizenzbedingungen vor, soweit die jeweilige Open-Source-Software hiervon betroffen ist.

Die Nutzung der verwendeten Open-Source-Software ist unentgeltlich möglich. Wir erheben für die Benutzung der Open-Source-Software, die in unserem Produkt enthalten ist, keine Nutzungsgebühren oder vergleichbare Gebühren. Die Benutzung der Open-Source-Software durch den Kunden in unserem Produkt ist nicht Bestandteil des Gewinns, den wir mit der vertraglichen Vergütung erzielen.

Aus der erhältlichen Liste ergeben sich alle Open-Source-Softwareprogramme, die in unserem Produkt enthalten sind. Die wichtigsten Open-Source-Softwarelizenzen sind im Abschnitt Lizenzen am Ende dieser Publikation aufgeführt.

Soweit Programme, die in unserem Produkt enthalten sind, unter der GNU General Public License (GPL), GNU Lesser General Public License (LGPL), der Clarified Artistic License oder einer anderen Open-Source-Softwarelizenz stehen, die vorschreibt, dass der Quellcode zur Verfügung zu stellen ist, und sollte diese Software nicht bereits mit unserem Produkt auf einem Datenträger im Quellcode mitgeliefert worden sein, so übersenden wir diesen jederzeit auf Nachfrage. Sollte hierbei die Zusendung auf einem Datenträger verlangt werden, so erfolgt die Übersendung gegen Zahlung einer Unkostenpauschale in Höhe von € 10,00. Unser Angebot, den Quellcode auf Nachfrage zu versenden, endet automatisch mit Ablauf von 3 Jahren nach Lieferung unseres Produkts an den Kunden. Anfragen sind insoweit möglichst unter Angabe der Seriennummer unseres Produktes an folgende Adresse zu senden:

INSYS MICROELECTRONICS GmbH

Hermann-Köhl-Str. 22

93049 Regensburg

Telefon +49 941 58692 0

Telefax +49 941 58692 45

E-Mail: support@insys-icom.de

3.2 Besondere Haftungsbestimmungen

Wir übernehmen keine Gewährleistung und Haftung, wenn die Open-Source-Softwareprogramme, die in unserem Produkt enthalten sind, vom Kunden in einer Art und Weise verwendet werden, die nicht mehr dem Zweck des Vertrages, der dem Erwerb unseres Produktes zu Grunde liegt, entspricht. Dies betrifft insbesondere jede Verwendung der Open-Source-Softwareprogramme außerhalb unseres Produktes. Für die Verwendung der Open-Source-Software jenseits des Vertragszwecks gelten die Gewährleistungs- und Haftungsbestimmungen, die die jeweils gültige Open-Source-Softwarelizenz für die entsprechende Open-Source-Software, wie nachstehend aufgeführt, vorsieht. Wir haften insbesondere auch nicht, wenn die Open-Source-Software in unserem Produkt oder die gesamte Softwarekonfiguration in unserem Produkt geändert wird. Die mit dem Vertrag, der dem Erwerb unseres Produkt zugrunde liegt, gegebene Gewährleistung gilt nur für die unveränderte Open-Source-Software und die unveränderte Softwarekonfiguration in unserem Produkt.

3.3 Verwendete Open-Source-Software

Wenden Sie sich bitte an unsere Support-Abteilung (support@insys-icom.de) für eine Liste der in diesem Produkt verwendeten Open-Source-Software.

4 Lieferumfang

Der Lieferumfang umfasst die im Folgenden aufgeführten Zubehörteile. Bitte kontrollieren Sie, ob alle angegebenen Zubehörteile in Ihrem Karton enthalten sind. Sollte ein Teil fehlen oder beschädigt sein, so wenden Sie sich bitte an Ihren Distributor.

- 1 EBW-H100
- 1 Quick Installation Guide
- 1 Monitoring App

Optionales Zubehör ist nicht im Lieferumfang enthalten. Folgende Teile sind bei Ihrem Distributor oder INSYS icom erhältlich:

- Mobilfunkantennen
- Antennenverlängerungen und Zubehör
- Hutschienennetzteile
- Monitoring-Pakete zur Überwachung externer Geräte

Folgende weiterführenden Dokumente finden Sie im Downloadbereich und auf der Produktseite des EBW-H100 unter www.insys-icom.de:

- Zusatzhandbuch ASCII-Konfigurationsdatei
- Zusatzhandbuch Automatisches Update
- Zusatzhandbuch CLI
- Zusatzhandbuch Monitoring App

5 Technische Daten

5.1 Physikalische Merkmale

Die angegebenen Daten wurden bei nominaler Eingangsspannung, unter Volllast und einer Umgebungstemperatur von 25 °C gemessen. Die Grenzwerttoleranzen unterliegen den üblichen Schwankungen.

Physikalische Eigenschaft	Wert
Betriebsspannung	10 ... 48 V DC (±20%)
Leistungsaufnahme Ruhe (eingebucht)	ca. 2 W
Leistungsaufnahme Verbindung	max. 5 W
Abgestrahlte Leistung: UMTS 850: Class 3 UMTS 1900: Class 3 UMTS 2100: Class 3 EGSM 850 und 900: Class 4 GSM 1800 und 1900: Class 1 EGSM 850 und 900: Class E2 GSM 1800 und 1900: Class E2	 0,25 W 0,25 W 0,25 W 2 W 1 W 0,5 W 0,5 W
Pegel Reset-Eingang	HIGH-Pegel = 3-12 V (Kontakt offen bzw. Spannungsfestigkeit bei Fremdspeisung) LOW-Pegel = 0-1 V
Gewicht	135 g
Abmessungen (Breite x Tiefe x Höhe)	45 mm x 110 mm x 75 mm
Temperaturbereich	-30 °C … 60 °C (max. 75 °C, s. unten)
Maximale zulässige Luftfeuchtigkeit	95% nicht kondensierend
Schutzart	Gehäuse IP40, Schraubklemmen IP20

Tabelle 1: Physikalische Eigenschaften

ⓘ Max.-Angabe gilt für gelegentliche Datenübertragung und Verwendung von nicht mehr als 2 LAN-Ports. Dabei können Funktionseinschränkungen (insbesondere bei der Datenübertragung) auftreten.

5.2 Technologische Merkmale

Technologische Eigenschaft	Beschreibung
Ethernet-Schnittstelle	10/100 Mbit/s Voll-/Halbduplex Autosense; Automatische Erkennung der Verdrahtung „Crossover" oder „Patch".
LAN ext-Schnittstelle	10/100 Mbit/s Voll-/Halbduplex Autosense; Automatische Erkennung der Verdrahtung „Crossover" oder „Patch".
GSM/GPRS-Frequenzen (2G)	850, 900, 1800, 1900 MHz
UMTS/HSPA-Frequenzen (3G)	800, 850, 900, 1900, 2100 MHz
SIM-Kartenleser	Unterstützung für 1,8 V- und 3,0 V-SIM-Karten Format: Mini-SIM (2FF), arretiert
SMS	SMS-Versand, eingehende SMS können empfangen werden, sind aber nicht über das Web-Interface zugänglich.
GPRS	GPRS Multislot Class 12, Coding scheme 1 bis 4, PBCCH, Mobile Station Class B
EDGE (EGPRS)	EDGE Multislot Class 12, Modulation and Coding Scheme MCS 1-9
HSPA	Uplink bis 5,76 MBit/s / Downlink bis 7,2 MBit/s UE CAT. [1-8]. 11. 12 supported Compressed mode (3GPP TS25.212)

Tabelle 2: Technologische Merkmale

6 Anzeige- und Bedienelemente

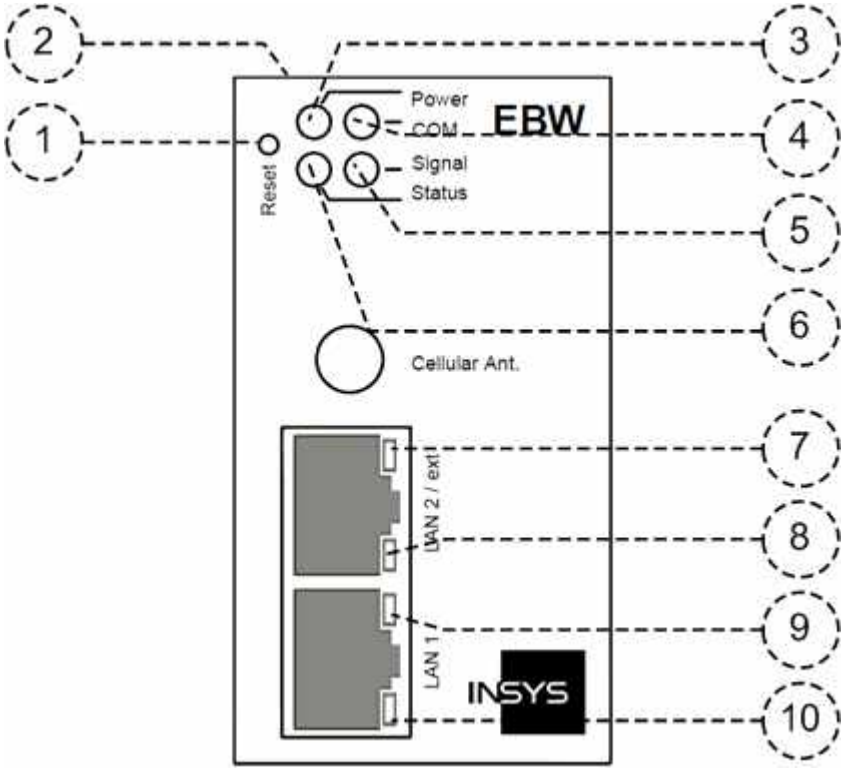


Abbildung 1: Anzeige- und Bedienelemente auf der Gerätevorderseite

Position	Bezeichnung
1	Reset-Taster
2	SIM-Karten-Slot
3	Power LED
4	COM LED
5	Signal LED
6	Status LED
7	Activity LED für LAN 2 / ext
8	Link LED für LAN 2 / ext
9	Activity LED für LAN 1
10	Link LED für LAN 1

Tabelle 3: Beschreibung der Anzeige- und Bedienelemente auf der Gerätevorderseite

6.1 Bedeutung der Anzeigeelemente

LED	Farbe	Funktion	aus	blitzt	blinkt	an
Link LAN 1/2	grün	10/100 MBit/s	10 MBit/s			100 MBit/s
Activity LAN 1/2	orange	Activity	nicht verb.		Daten-verkehr	verbunden
Power	grün	Versorgung	fehlt			vorhanden
COM	grün	WWAN-Link	offline			im Aufbau
	orange	WWAN-Link				aufgebaut
Signal	grün	SIM-Karte	kein Sig-nal o. ausge-bucht	WWAN Daten-verkehr	Feldstärke (siehe Ta-belle 5)	
Status	grün	VPN				VPN-Verbindung aufgebaut
	rot	Status				Initialisier-ung, FW-Up-date, Störung

Tabelle 4: Bedeutung Anzeigeelemente

Blinktakt LED Signal	Wertigkeit	Qualität des Signals
900 ms an, 100 ms aus	20 .. 31	sehr gut
200 ms an, 200 ms aus	13 .. 19	gut
100 ms an, 900 ms aus	0 .. 12	schlecht
aus	99 (nicht feststellbar)	ungenügend

Tabelle 5: Blinkcode der Data/Signal LED

6.2 Funktion der Bedienelemente

Bezeichnung	Bedienung	Bedeutung
Reset-Taster	Einmal kurz drücken.	Setzt die Software zurück und startet sie neu. (Soft-Reset)
	Mindestens 3 Sekunden lang drücken.	Setzt die Hardware zurück und startet sie neu. (Hard-Reset)
	Innerhalb von 2 Sekunden dreimal hintereinander kurz drücken.	Löscht alle Einstellungen und setzt das Gerät auf Werkseinstellungen zurück
SIM-Karten-Slot	Kurz auf die SIM-Karte drücken	Wirft die SIM-Karte aus.

Tabelle 6: Funktionsbeschreibung und Bedeutung der Bedienelemente

7 Anschlüsse

7.1 Anschlüsse Vorderseite

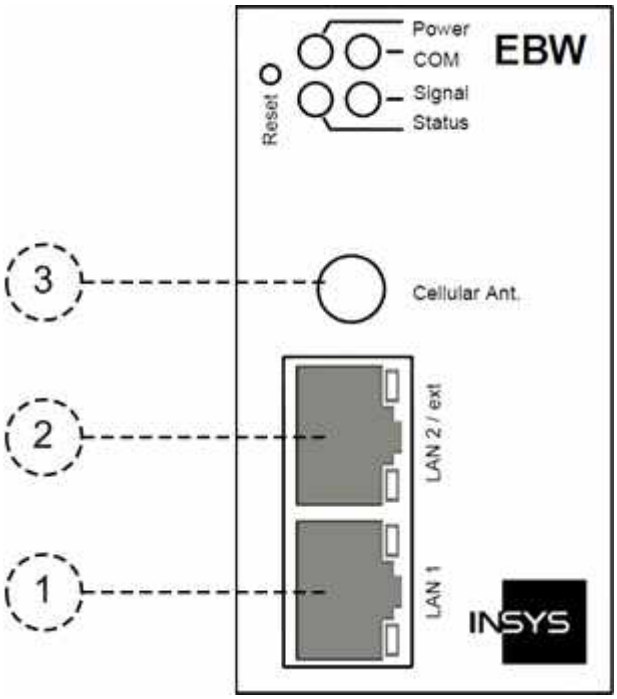


Abbildung 2: Anschlüsse auf der Gerätevorderseite

Position	Bezeichnung
1	Ethernet-Port LAN 1 (RJ45, 10/100 BT)
2	Ethernet-Port LAN 2 / ext (RJ45, 10/100 BT)
3	Mobilfunkantennenanschluss (SMA-Buchse)

Tabelle 7: Beschreibung der Anschlüsse auf der Gerätevorderseite

Bei Verwendung einer Außenantenne muss die Abschirmung des Antennensystems mit dem Schutzleiter verbunden werden.

7.2 Klemmanschlüsse Oberseite

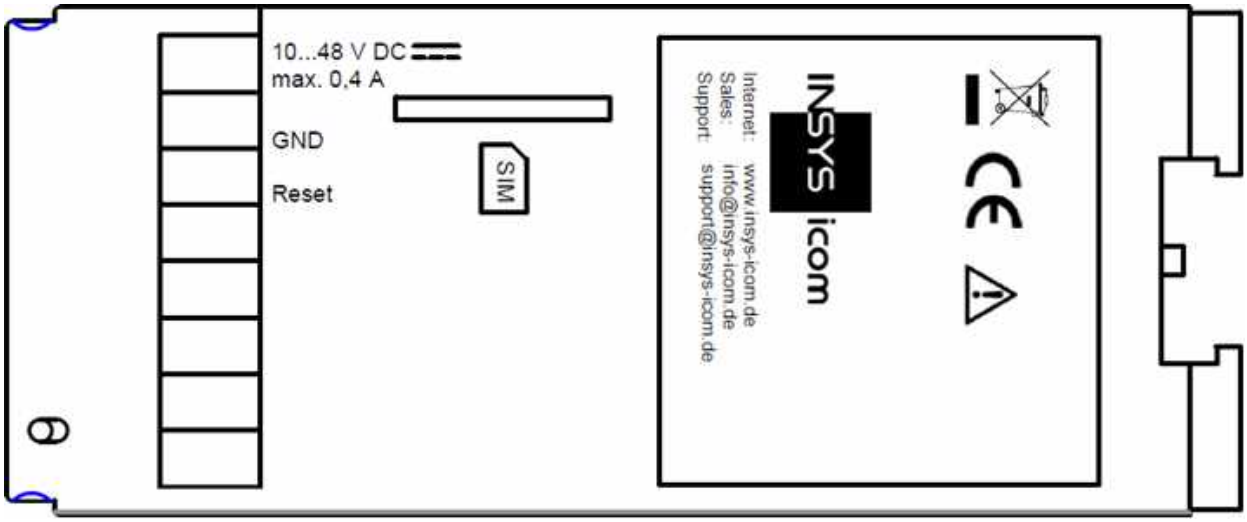


Abbildung 3: Anschlüsse auf der Geräteoberseite

Klemme	Bezeichnung	Beschreibung
1	10 ... 48 VDC	Spannungsversorgung 10 V – 48 V DC
2	GND	Ground (Masse)
3	Reset	Reset-Eingang

Tabelle 8: Beschreibung der Anschlüsse auf der Geräteoberseite

ⓘ Zum Zurücksetzen des Geräts muss der Reset-Eingang mit Masse (GND) verbunden werden. Die Funktionalität ist identisch mit dem Reset-Taster. Wird der Reset-Eingang mit einem Signalausgang verbunden, darf dessen HIGH-Pegel 12 V nicht überschreiten.

Hinweis

Anforderung an das externe Netzteil

- PS2-klassifiziert nach IEC62368-1
- Kurzschlussstrom < 8 A

8 Funktionsübersicht

Der EBW-H100 bietet Ihnen die folgenden Funktionen:

- **Konfiguration über Web-Interface, Befehlszeile (CLI) oder Konfigurationsdatei**

  Alle Funktionen können über ein Web-Interface oder eine Befehlszeilen-Schnittstelle (CLI, Command Line Interface) konfiguriert und eingestellt werden. Der Zugriff ist dabei mit einer Benutzername- und Kennwortabfrage geschützt. Der dafür erforderliche Port kann frei eingestellt werden. Alternativ kann auch eine Datei (ASCII oder binär) hochgeladen werden, welche die Konfiguration enthält.

- **Zugangskontrolle über Radius-Server**

  Der Zugang zum Web-Interface oder der Befehlszeilen-Schnittstelle (CLI) kann optional über einen Radius-Server gegen unbefugte Zugriffe geschützt werden.

- **IPv6-Routing**

  Zusätzlich zu den IPv4-Adressen verfügen die Schnittstellen über Adressen nach dem IPv6-Protokoll. Mit SLAAC (StateLess Address Auto Configuration) konfiguriert sich der Router selbständig eine oder mehrere IPv6-Adressen. Wenn im LAN ein Router mit Router Advertisement IPv6-Adressprefixe verkündet, konfiguriert sich der Router zusätzlich zu seinen bereits konfigurierten IPv6-Adressen eine Weitere mit dem verkündeten Prefix. Zusätzlich kann der Router sein Prefix an lokale Geräte verteilen (Router Advertisement).

- **DHCP-Server**

  Angeschlossene Ethernet-Geräte können automatisch ihre IP-Adresse beziehen.

- **DHCP-Client**

  An der Schnittstelle LAN ext können optional automatisch IP-Adressen aus dem Netzwerk bezogen werden.

- **Statische IP-Adresse**

  Eine statische IP-Adresse kann für die Schnittstelle LAN ext konfiguriert werden.

- **DSL-Standleitungsbetrieb**

  Eine dauerhafte Verbindung über eine DSL („PPP-over-Ethernet“)-Verbindung kann hergestellt und aufrecht erhalten werden. Dazu kann über die LAN ext-Schnittstelle ein DSL-Modem angeschlossen werden. So ist es möglich, mit einem externen Netzwerk über eine „Standleitung“ zu kommunizieren.

- **Periodischer DSL-Verbindungsaufbau**

  Eine DSL (PPPoE) -Verbindung kann zeitgesteuert aufgebaut und auch geschlossen werden. Für den Verbindungsaufbau und den Verbindungsabbau können Sie Uhrzeiten festlegen.

- **Dynamischer DSL-Verbindungsaufbau**

  Bei Bedarf kann selbständig eine DSL (PPPoE)-Verbindung aufgebaut werden. Nach einer definierbaren Idle-Time oder einer definierbaren maximalen Verbindungszeit wird die Verbindung wieder abgebaut.

- **Wählfilter für DSL-Verbindungsaufbau**

  Mit Hilfe der Wählfilter kann definiert werden, welche Datenpakete zu einem PPPoE-Verbindungsaufbau führen. Unnötige Verbindungen können so vermieden werden, Kosten werden eingespart.

- **NAT und Port-Forwarding**

  Der Router kann Datenpakete auch durch NAT und Port-Forwarding weiterleiten. Nach festlegbaren Regeln werden eingehende IP-Pakete an definierbare Ports und Port-Bereiche zu IP-Adressen und Ports im LAN weitergeleitet.

- **IP-Forwarding**

  Mit IP-Forwarding-Regeln können zusätzliche IP-Adressen an der Schnittstelle LAN ext angelegt werden. Pakete an eine dieser IP-Adressen werden an die mit ihr verknüpfte IP-Adresse im lokalen LAN weitergeleitet.

- **Einwahl-PPP-Server (Dial-In)**

  Eine Verwendung als PPP-Einwahlserver ist möglich. Wie bei einem Internet Service Provider kann ein Anrufer eine PPP-Verbindung aufbauen, um auf das dahinterliegende Netzwerk zuzugreifen.

- **Aufbau einer PPP-Verbindung durch eingehenden Anruf (Callback)**

  Es ist möglich, einen Anrufer zu identifizieren und automatisch eine PPP-Verbindung zu einer zuvor bestimmten Gegenstelle (z.B. einem Internet Service Provider) aufzubauen. Dabei kann sich der Anrufer, der den Verbindungsaufbau auslöst, über eine PPP-Authentifizierungsmethode identifizieren.

- **Automatische Anwahl einer PPP-Gegenstelle (Dial-Out)**

  Aufbau einer Verbindung zu einer PPP-Gegenstelle (z.B. Internet Service Provider), sobald ausgehender Netzwerkverkehr registriert wird.

- **Wählfilter für das Auslösen eines Verbindungaufbaus**

  Über Regeln können Sie festgelegen, welcher Netzwerkverkehr oder Netzwerkteilnehmer einen Verbindungsaufbau auslösen darf.

- **PPP-Standleitungsbetrieb**

  Herstellung und Aufrechterhaltung einer dauerhaften Verbindung über eine „Wählleitung“. So ist es möglich, mit einem Netzwerk über eine Wählverbindung wie über eine „Standleitung“ zu kommunizieren.

- **Periodischer PPP-Verbindungsaufbau**

  Es ist möglich, eine PPP-Verbindung zeitgesteuert aufzubauen zu schließen. Für den Verbindungsaufbau und den Verbindungsabbau können feste Uhrzeiten eingestellt werden.

- **OpenVPN**

  Der Router kann als OpenVPN-Server oder -Client fungieren. So können Maschinen von außen über unsichere Netzwerke eine sichere Verbindung zum LAN hinter dem Router herstellen. Es kann auch ein ganzes LAN über eine unsichere Internet-Verbindung abhör- und störungssicher durch einen VPN-Tunnel mit einem anderen Netzwerk (z.B. dem Firmennetzwerk) verbunden werden. Dabei wird die Authentifizierung bei Verbindung zu einem OpenVPN-Server über einen statischen Schlüssel, über ein Zertifikat mit Benutzernamen und Kennwort oder über ein Zertifikat alleine unterstützt. Weiterhin kann auch eine OpenVPN-Verbindung ohne Authentifizierung aufgebaut werden.

- **PPTP**

  Der Router kann als PPTP-Server oder Client fungieren. So können Maschinen von außen über unsichere Netzwerke eine sichere Verbindung zum LAN hinter dem Router herstellen. Es kann auch ein ganzes LAN über eine unsichere Internet-Verbindung abhör- und störungssicher durch einen VPN-Tunnel mit einem anderen Netzwerk (z.B. dem Firmennetzwerk) verbunden werden.

- **IPsec-Protokoll**

  Zwei Subnetze können über eine unsichere Internet-Verbindung abhör- und störungssicher durch einen IPsec-Tunnel miteinander verbunden werden. Dabei wird die Authentifizierung bei Verbindung zu einem IPsec-Endgerät über Zertifikate oder eine Passphrase (PSK) unterstützt. Insgesamt können bis zu 10 Tunnel gleichzeitig aufgebaut werden.

- **GRE-Tunnel**

  GRE-Tunnel ermöglichen die transparente Übertragung von Daten durch eine bestehende Verbindung, ohne dass die Originalpakete verändert werden.

- **IPT-Protokoll**

  Unterstützung der Kommunikation über IPT (Internet-Protokoll Telemetrie). Der Router kann sich als IPT-Slave zu einem IPT-Master verbinden und Nutzdaten des Seriell-Ethernet-Gateway an einen anderen IPT-Slave tunneln.

- **Dynamisches DNS-Update**

  Nach dem Aufbau einer PPP-Verbindung zu einem Internet Service Provider kann die zugewiesene IP-Adresse bei einem dynamischen DNS-Service (z.B. DynDNS) hinterlegt werden. Der Router kann aus dem Internet heraus erreicht werden.

- **DNS-Relay-Server**

  DNS-Anfragen können an vorher konfigurierte DNS-Server im Internet oder die beim PPP-Verbindungsaufbau übergebenen DNS-Server weitergeleitet werden.

- **Firewall (Stateful Firewall)**

  Die Firewall ermöglicht es, ein- und ausgehende IP-Verbindungen zu beschränken. Für jede Verbindung und für jeden gespeicherten Benutzer kann eine flexible Regel angelegt werden. Entspricht eine Verbindung durch den Router einer dieser Firewall-Regeln, so wird die Verbindung zugelassen, andernfalls wird die Verbindung unterbunden. Die „Stateful Firewall“ erlaubt Verbindungen auch für Protokolle mit speziellen Anforderungen, z.B. FTP.

- **MAC-Filter**

  Der MAC-Filter ermöglicht es, dass nur noch Pakete an der lokalen Ethernet-Schnittstelle akzeptiert werden, die von explizit zugelassenen Netzwerkgeräten stammen.

- **E-Mail- und SMS-Versand sowie SNMP-Trap-Auslösung bei verschiedenen Ereignissen**

  Es ist möglich, bei verschiedenen Ereignissen eine E-Mail oder eine SMS an beliebige Empfänger zu versenden oder einen SNMP-Trap auszulösen. Dazu stehen eine Reihe vordefinierter Ereignisse zur Verfügung, wie zum Beispiel der Aufbau von Verbindungen oder Tunnels, Empfang von SMS, Änderungen der Link-Zustände, fehlerhafte Authentifizierung am Web-Interface, Zurückweisungen durch die Firewall, Konfigurationsänderungen und andere interne Vorgänge im Gerät.

- **SMS-Empfang**

  Es besteht die Möglichkeit, SMS zu empfangen. Damit können verschiedene Befehle übermittelt werden, optional auch kennwortgeschützt. Nicht auswertbare SMS können an die Sandbox weitergeleitet und dort ausgewertet werden.

- **SNMP-Agent für die Bearbeitung von SNMP-Anfragen**

  Beantwortung eingehender SNMP-Anfragen (SNMP-Get-Requests) bei aktiviertem SNMP-Agent. Damit können fast alle Konfigurationsparameter ausgelesen werden.

- **Zeitsynchronisation über NTP**

  Synchronisierung der Systemzeit über das Network Time Protocol mit einem NTP-Server im Internet. So ist die Systemzeit immer aktuell und die interne Uhr muss nicht manuell eingestellt werden.

- **NTP-Server**

  Ein NTP-Server kann NTP-Anfragen im lokalen Netz beantworten.

- **HTTP und HTTPS Proxy mit URL-Filter**

  Der Proxy dient dazu, um den Zugriff auf Webadressen für Applikationen im lokalen Netz des Routers zu beschränken sowie um Verbindungs-Timeouts zu vermeiden. Es werden die Protokolle HTTP und HTTPS unterstützt. Der Proxy hält Verbindungen während dem Verbindungsaufbaus des Kommunikationsgerätes geöffnet, um einem vorzeitigen Timeout vorzubeugen. Der Proxy arbeitet nicht als Cache für häufig aufgerufene Webseiten.

- **Log-Dateien**

  Verschiedene Log-Dateien können als Textdatei über das Web-Interface heruntergeladen werden.

- **Herunterladbare Konfigurationsdateien**

  Die Konfiguration kann als binäre oder als ASCII-Datei heruntergeladen werden. Die Datei kann als Sicherheitskopie zur Konfiguration nach einer Zurückstellung auf Werkseinstellungen verwendet werden oder zum bequemen Laden einer gleichen Konfiguration in verschiedene Router. Die ASCII-Konfigurationsdatei kann bearbeitet werden und bietet eine bequeme Möglichkeit zur alternativen Konfiguration.

- **Firmware-Update über Web-Interface**

  Die Firmware kann über das Web-Interface aktualisiert werden. Ein Update kann lokal oder aus der Ferne durchgeführt werden.

- **Automatisches tägliches Update**

  Eine tägliche automatische Aktualisierung von Firmware-Dateien, Konfigurationsdateien (binär und ASCII) oder Sandbox-Image-Dateien, die auf einem Server entsprechend bereitgestellt werden, ist möglich.

- **Redundante WAN-Schnittstelle**

  Es ist möglich, das integrierte Kommunikationsgerät als redundante WAN-Schnittstelle bei Verbindungsproblemen über die LAN ext-Schnittstelle zu verwenden.

- **Frei programmierbare Sandbox**

  Es steht eine frei programmierbare Sandbox zur Verfügung. Die Sandbox ist eine Art virtueller Maschine, die auf dem Router läuft und in der man Programme starten, Daten sammeln und Dienste anbieten kann, die im eigentlichen System nicht vorhanden sind.

- **Debugging-Werkzeuge zur Analyse von Netzwerkverbindungen**

  Es stehen verschiedene Werkzeuge zur Verfügung, um Probleme mit Netzwerkverbindungen analysieren zu können. Dabei können Ping-Pakete gesendet, Routen von IP-Paketen verfolgt, DNS-Informationen abgefragt und Netzwerkpakete aufgezeichnet werden.

- **Abfragen und Setzen von Objekten über MCIP-Protokoll**

  Ein Teil der LEDs kann über das MCIP-Protokoll abgefragt oder gesetzt werden. Das MCIP-Protokoll ist sowohl in der Sandbox als auch von externen Geräten über TCP/IP verfügbar.

- **Vorinstallierte Monitoring App**

  Die vorinstallierte Monitoring App (Überwachungsapplikation) ermöglicht die Überwachung von Timern, eingehenden SMS (Mobilfunkgeräte) oder Objekten einer Siemens-Steuerung der Typen LOGO!™ bzw. S7 (jeweils lizenzpflichtig) sowie das Absetzen von Alarmmeldungen.

9 Montage

Dieser Abschnitt erklärt, wie Sie den EBW-H100 auf einer Hutschiene montieren, die Spannungsversorgung anklemmen und wie Sie ihn wieder demontieren können. Beachten Sie dazu unbedingt die Anweisungen im Abschnitt „Sicherheit“ dieses Handbuchs, insbesondere die „Sicherheitshinweise zur elektrischen Installation“.

Vorsicht!

Nässe und Flüssigkeiten aus der Umgebung können ins Innere des Geräts gelangen!

Brandgefahr und Beschädigung des Produkts.

Das Gerät darf nicht in nassen oder feuchten Umgebungen oder direkt in der Nähe von Gewässern eingesetzt werden. Installieren Sie das Gerät an einem trockenen, vor Spritzwasser geschützten Ort. Schalten Sie die Spannung ab, bevor Sie Arbeiten an einem Gerät durchführen, das mit Feuchtigkeit in Berührung kam.

Vorsicht!

Gerätezerstörung durch falsche Spannungsquelle!

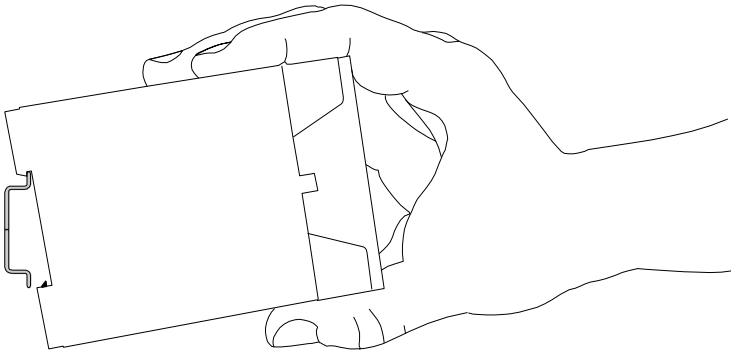
Wenn das Gerät mit einer Spannungsquelle betrieben wird, die eine größere Spannung als die zulässige Betriebsspannung liefert, wird es zerstört.

Sorgen Sie für eine geeignete Spannungsversorgung. Den richtigen Spannungsbereich finden Sie im Abschnitt Technische Daten.

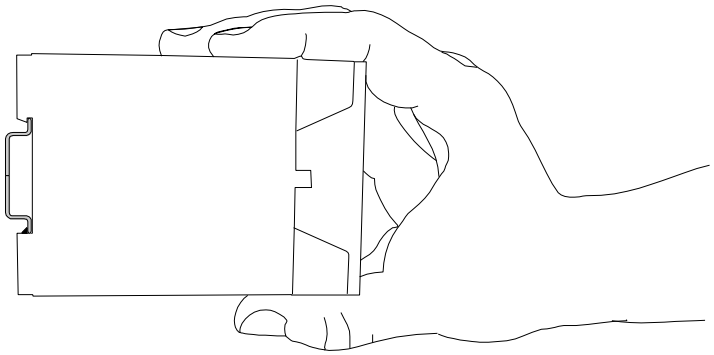
Gerät auf Hutschiene montieren

So montieren Sie den EBW-H100 auf einer DIN-Hutschiene:

1. ***Setzen Sie das Gerät, wie in der folgenden Abbildung gezeigt, an der Hutschiene an. An der oberen und der unteren Außenkante der Hutschienennut befinden sich jeweils zwei Rasthaken. Haken Sie die oberen beim Ansetzen hinter der Oberkante der Hutschiene ein.***



2. ***Klappen Sie das Gerät senkrecht zur Hutschiene, bis die zwei unteren, beweglichen Rasthaken unten in der Hutschiene einrasten.***



✓ Der EBW-H100 ist nun fertig montiert.

Spannungsversorgung anklemmen

⇢ Das Gerät ist bereits auf der Hutschiene montiert.

⇢ Die Spannungsversorgung steht bereit und ist abgeschaltet.

1. ***Klemmen Sie das Massekabel der Spannungsversorgung an der Klemme „GND“ an.***

2. ***Klemmen Sie den Pluspol der Spannungsversorgung an der Klemme für die Spannungsversorgung an.***

✓ Der EBW-H100 ist nun mit der Spannungsversorgung verbunden.

Spannungsversorgung trennen

⇢ Das Gerät ist auf der Hutschiene montiert.

⇢ Die Spannungsversorgung ist angeschlossen und abgeschaltet.

1. ***Trennen Sie das Massekabel der Spannungsversorgung von der Klemme „GND“.***

2. ***Trennen Sie den Pluspol der Spannungsversorgung von der Klemme für die Spannungsversorgung.***

   ✓ Der EBW-H100 ist von der Spannungsversorgung getrennt.

Gerät von Hutschiene demontieren

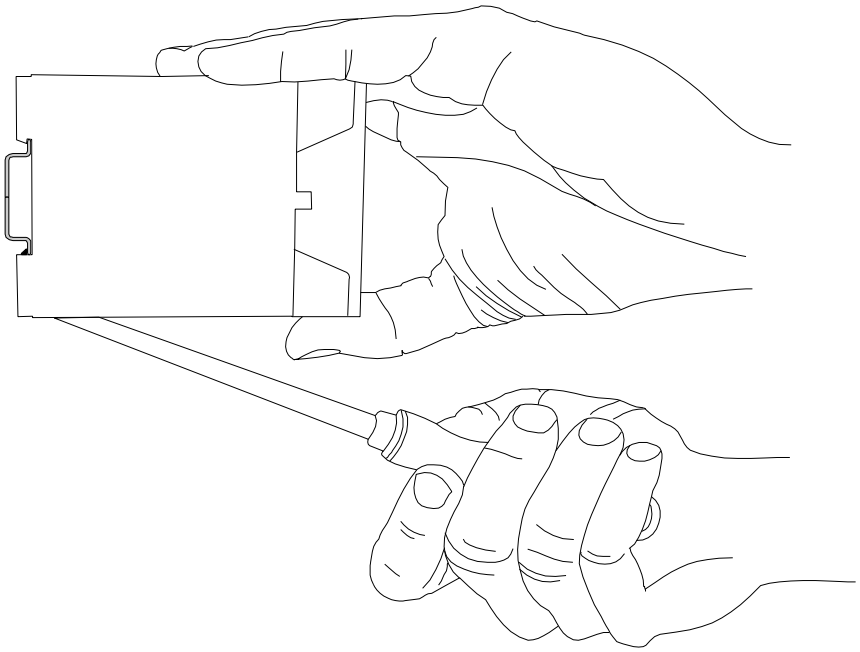
So demontieren Sie den EBW-H100 von einer DIN-Hutschiene in einem Schaltschrank:

⇢ Sie benötigen einen kleinen Schlitzschraubendreher.

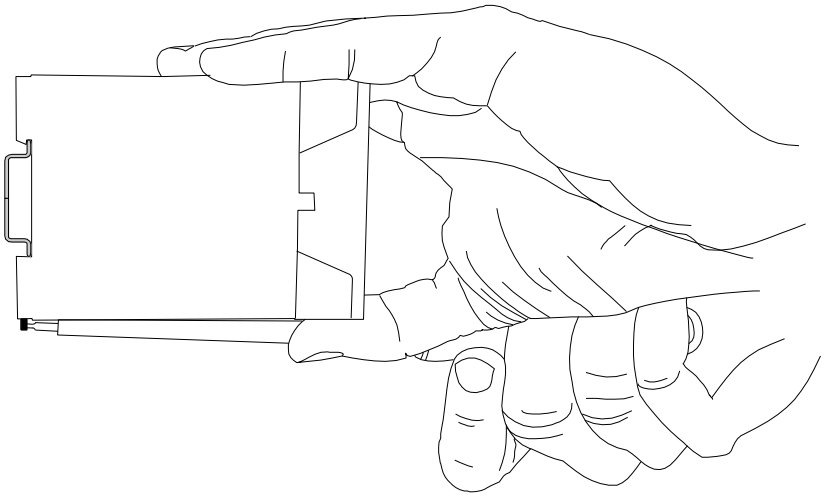
⇢ Die Spannungsversorgung des Schaltschranks ist abgestellt und gegen versehentliches Wiedereinschalten gesichert.

⇢ Alle Kabel am Gerät sind abgeklemmt.

1. ***Führen Sie den Schlitzschraubendreher wie in der folgenden Abbildung gezeigt in die Rille hinten im Boden ein.***



2. ***Bewegen Sie den Schlitzschraubendreher wie in der folgenden Abbildung gezeigt zum Gerät hin.***



✓ Die Kunststofffeder mit den unteren Rasthaken wird auseinandergezogen.

3. ***Während Sie die Kunststofffeder mit den unteren Rasthaken gespannt halten, klappen Sie das Gerät von der Hutschiene weg.***

4. ***Haken Sie das Gerät aus und nehmen Sie ihn senkrecht zur Hutschiene ab.***

✓ Der EBW-H100 ist nun demontiert.

10 Inbetriebnahme

Dieses Kapitel erklärt, wie Sie den EBW-H100 in Betrieb nehmen; d.h. mit einem PC verbinden und zur Konfiguration vorbereiten.

SIM-Karte einsetzen.

So setzen Sie die SIM-Karte ein.

⇢ Die Stromversorgung des Geräts ist abgestellt.

⇢ Sie benötigen eine funktionierende Mini-SIM-Karte Ihres Mobilfunkproviders.

⇢ Sie benötigen die dazugehörige PIN.

1. ***Schieben Sie die SIM-Karte mit den Kontakten nach außen und der Fase nach hinten zeigend in den SIM-Karten-Slot bis sie einrastet.***

   ⓘ Um die SIM-Karte zu entfernen, drücken Sie kurz auf die Karte. Die Karte wird dann ein Stück weit herausgeschoben und kann entnommen werden.

2. ***Schalten Sie die Stromversorgung wieder ein.***

Anschließen einer Mobilfunkantenne und eines PC

So verbinden Sie den EBW-H100 mit einer GSM-Antenne und über ein Netzwerkkabel mit einem PC.

⇢ Die Stromversorgung des Geräts ist abgestellt.

⇢ Sie benötigen ein Cat 5 Netzwerk-Patchkabel.

⇢ Sie benötigen eine Netzwerkkarte am PC.

⇢ Sie benötigen eine passende Mobilfunkantenne (bei INSYS icom erhältlich.)

ⓘ Für die USA gilt die Vorschrift der Federal Communications Commission (FCC), nach der die Antenne in mindestens 20 cm Abstand zu Personen, nicht am gleichen Ort mit anderen Antennen oder Sendern installiert und betrieben werden sowie einen Antennengewinn von nicht mehr als 8,4 dBi (GSM 1900) beziehungsweise 2,9.dBi (GSM 850) aufweisen soll.

1. ***Suchen Sie die RJ-45-Buchse der Netzwerkkarte am PC.***
2. ***Stecken Sie das eine Ende des Netzwerkkabels in die RJ-45-Buchse am PC und das andere Ende in eine der LAN-Buchsen des EBW-H100.***
3. ***Schließen Sie die Mobilfunkantenne an die Antennenbuchse an.***

Den EBW-H100 konfigurieren

⇢ Das Gerät ist an den PC angeschlossen.

⇢ Die Spannungsversorgung des Geräts ist eingeschaltet.

⇢ Sie haben die nötigen Zugriffsrechte, die IP-Adresse der Netzwerkkarte zu verändern, an die der EBW-H100 angeschlossen ist.

1. ***Ändern Sie die IP-Adresse der Netzwerkkarte, an die das Gerät angeschlossen ist, auf eine Adresse die mit 192.168.1. beginnt.***

   ➢ *Alternativ können Sie Ihre Netzwerkkarte auf „automatische Adresszuweisung“ konfigurieren. Der integrierte DHCP Server des EBW-H100 weist Ihrer Netzwerkkarte dann beim Anstecken eine Adresse aus dem passenden Adressbereich zu.*

   ⓘ Verwenden Sie nicht die Adresse 192.168.1.1. Das ist die ab Werk eingestellte IP-Adresse des Geräts. Verwenden Sie z.B. 192.168.1.2. als IP-Adresse für die Netzwerkkarte in Ihrem PC.

2. ***Öffnen Sie einen Webbrowser und geben Sie die URL „http://192.168.1.1“ ein.***

   ✓ Der Webbrowser lädt die Startseite des EBW-H100.

   ➢ *Falls Sie im Browserfenster die Meldung sehen, dass die Seite mit der Adresse nicht gefunden werden kann: Prüfen Sie, ob das Gerät mit Spannung versorgt ist. Falls ja, ist vermutlich die falsche IP-Adresse im Gerät eingestellt. Drücken Sie dafür dreimal innerhalb von 2 Sekunden auf den Reset-Taster und wiederholen Sie diese Anleitung ab Schritt 2.*

   ✓ Sie werden durch einen Dialog zur Authentifizierung mit Benutzernamen und Kennwort aufgefordert.

3. ***Geben Sie als Benutzernamen „insys“ und als Kennwort „icom“ ein.***

   ⓘ Benutzername und Kennwort sind als Werkeinstellung gesetzt. Funktioniert die Anmeldung am Web-Interface mit diesen Daten nicht, setzen Sie das Gerät einfach auf die Werkseinstellungen zurück. Drücken Sie dafür dreimal innerhalb von 2 Sekunden auf den Reset-Taster und wiederholen Sie diese Anleitung ab Schritt 2.

   ✓ Sie sehen die Startseite des Web-Interface.

   ✓ Der EBW-H100 ist erfolgreich installiert und bereit zur Konfiguration.

11 Bedienprinzip

Dieses Kapitel erklärt Ihnen, wie Sie bei Bedienung und Konfiguration eines EBW-H100 vorgehen.

Konfiguration und Bedienung erfolgen mit Hilfe einer web-basierten Schnittstelle (Web-Interface). Das Web-Interface selbst wird mit Hilfe eines Webbrowsers angezeigt und bedient.

11.1 Bedienung mit Web-Interface

Das Web-Interface ermöglicht eine komfortable Konfiguration mit Hilfe eines Webbrowsers. Über das Web-Interface ist es möglich, alle Funktionen zu konfigurieren. Die Bedienung ist weitgehend selbsterklärend. Das Web-Interface bietet zusätzlich eine Online-Hilfe, in der die Bedeutung möglicher Einstellungen erklärt ist. Die Online-Hilfe wird angezeigt, indem in der Titelleiste unter der Sprachauswahl die Option „Hilfetexte anzeigen“ gewählt wird.

ⓘ Wir empfehlen bei den ersten Konfigurationsvorgängen unbedingt, die Online-Hilfe zu aktivieren, um eine schnelle und fehlerfreie Konfiguration zu ermöglichen.

Konfigurieren und Einstellen mit dem Web-Interface

Hier erfahren Sie, wie Sie prinzipiell vorgehen, um mit dem Web-Interface zu konfigurieren.

⇢ Das Gerät ist betriebsbereit und Sie haben darauf Zugriff (siehe Abschnitt Inbetriebnahme).

1. ***Starten Sie den Web-Browser und geben Sie die IP-Adresse in die Adresszeile ein.***

   ⓘ Die ab Werk voreingestellte IP-Adresse ist **192.168.1.1**.

   ✓ Ein Dialog zur Authentifizierung erscheint und fordert Sie auf, Benutzernamen und Kennwort einzugeben.

2. ***Geben Sie den Benutzernamen und Kennwort ein und klicken Sie danach auf OK.***

   ⓘ Die Werkseinstellung des Web-Interface sind wie folgt: der **Benutzername** ist **„insys“**, das **Kennwort** ist **„icom“**.

   ✓ Die Startseite des Web-Interface wird angezeigt.

3. ***Wählen Sie über das Menü links den Menüpunkt aus, in dem Sie Einstellungen vornehmen möchten.***

4. ***Nehmen Sie die gewünschten Einstellungen vor.***

5. ***Klicken Sie abschließend auf die Schaltfläche OK auf der jeweiligen Konfigurationsseite, um die Einstellungen zu speichern.***

   ⓘ Bitte klicken Sie nach einer Änderung der Konfiguration stets die auf die Schaltfläche OK, da ansonsten bei einem Wechsel der Seite oder beim Schließen des Browsers die Einstellungen nicht übernommen werden.

11.2 Zugang über das HTTPS-Protokoll

Das Web-Interface ermöglicht auch eine sichere Konfiguration unter Verwendung des HTTPS-Protokolls. Das HTTPS-Protokoll ermöglicht eine Authentifizierung des Servers (d.h. des EBW-H100) sowie eine Verschlüsselung der Datenübertragung.

Bei einem ersten Zugriff über das HTTPS-Protokoll zeigt der Browser an, dass der EBW-H100 ein ungültiges Sicherheitszertifikat verwendet. Dem Zertifikat wird nicht vertraut, weil das Aussteller-Zertifikat (CA-Zertifikat) unbekannt ist.

Sie können diese Warnmeldung ignorieren und (je nach Browser und Betriebssystem) eine Ausnahme für diesen Server hinzufügen oder die sichere Verbindung zu diesem Server trotzdem aufbauen.

Wir empfehlen, das CA-Zertifikat CA_MoRoS.crt von der Zertifikats-Seite (http://www.insys-icom.de/zertifikat/) herunterzuladen und in Ihren Browser zu importieren, um INSYS MICROELECTRONICS als Zertifizierungsstelle anzuerkennen. Gehen Sie dazu vor, wie in der Dokumentation Ihres Browsers beschrieben.

Wenn INSYS MICROELECTRONICS als Zertifizierungsstelle in Ihrem Browser hinterlegt ist und sie erneut auf das Gerät über das HTTPS-Protokoll zugreifen, zeigt der Browser erneut an, dass ein ungültiges Sicherheitszertifikat verwendet wird. Dem Zertifikat wird nicht vertraut, weil sich der Common Name des Zertifikates von Ihrer Eingabe in der Adressleiste des Browsers unterscheidet. Der Browser meldet, dass sich ein anderes Gerät unter dieser URL meldet. Der Common Name des Zertifikates besteht aus der MAC-Adresse des EBW-H100, wobei die Doppelpunkte durch Unterstriche ersetzt sind.

Sie können diese Warnmeldung ignorieren und (je nach Browser und Betriebssystem) eine Ausnahme für diesen Server hinzufügen oder die sichere Verbindung zu diesem Server trotzdem aufbauen.

Um auch diese Browser-Warnung zu vermeiden, müssen Sie den Common Name des zu erreichenden EBW-H100 in die Adressleiste Ihres Browsers eingeben. Damit die URL zum richtigen Gerät führt, muss der Common Name mit der IP-Adresse des Geräts verknüpft werden. Den Allgemeinen Namen (Common Name) können Sie herausfinden, indem Sie das Zertifikat vom Gerät herunterladen und dies ansehen. Die Vorgehensweise hierzu ist von Ihrem Browser abhängig. Die Vorgehensweise für das Einrichten der Verknüpfung ist abhängig von Ihrem Betriebssystem:

- Editieren von /etc/hosts (Linux/Unix)
- Editieren von C:\WINDOWS\system32\drivers\etc\hosts (Windows XP)
- Konfigurieren Ihres eigenen DNS-Servers

Sehen Sie für weitere Informationen dazu in der Dokumentation Ihres Betriebssystems nach.

12 Funktionen

12.1 Basic Settings

12.1.1 Zugang zum Web-Interface konfigurieren

Das Web-Interface dient zur Konfiguration des EBW-H100. Es wird durch eine Abfrage von Benutzername und Kennwort (alternativ auch über einen Radius-Server) gegen unbefugte Zugriffe geschützt. Das Web-Interface kann für eine Konfiguration von einem Rechner aus dem internen Netz oder für eine Fernkonfiguration aus dem WAN über das HTTP- und HTTPS-Protokoll konfiguriert werden. Für eine bessere Unterscheidbarkeit kann ein Standort eingetragen werden. Sie können den Port festlegen, unter dem Sie das Web-Interface erreichen.

Konfiguration mit Web-Interface (Menü „Basic Settings“, Seite „Web-Interface“)

Für eine **Authentifizierung lokal am Gerät** wählen Sie den Radiobutton „Authentifizierung mit Kennwort“ und geben Sie die Zugangsdaten in die entsprechenden Felder ein.

Für eine **Authentifizierung am Radius-Server** wählen Sie den Radiobutton „Authentifizierung am Radius-Server“.

ⓘ Dazu muss der Radius-Server konfiguriert sein (im Menü „Basic Settings“ auf der Seite „Radius-Server“).

Um eine Authentifizierung mit Kennwort zu ermöglichen, falls der **Radius-Server nicht erreichbar** ist bzw. nicht antwortet, aktivieren Sie die Checkbox „Authentifizierung mit Kennwort nach Radius-Timeout“.

Um festzulegen, über welche Zugriffsmöglichkeiten (lokal oder aus der Ferne über HTTP oder HTTPS) die **Konfiguration zulässig ist**, aktivieren bzw. deaktivieren Sie die jeweiligen Checkboxen.

Den **Port des Web-Interface** legen Sie im Eingabefeld „HTTP Port des Web-Interface“ bzw. „HTTPS Port des Web-Interface“ fest. Standardmäßig ist Port 80 (HTTP) bzw. Port 443 (HTTPS) für das Web-Interface eingestellt.

Eine **Bezeichnung des Routers oder Standorts** kann im Feld „Standort“ eingegeben werden. Diese Bezeichnung erscheint dann in der Titelzeile des Browserfensters sowie der Startseite des Web-Interface und erleichtert eine Unterscheidung wenn mehrere Web-Interface-Fenster geöffnet sind.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.1.2 IP-Adressen einstellen

Der EBW-H100 muss im LAN unter einer bestimmten IP-Adresse erreichbar sein. Dazu müssen Sie eine statische IP-Adresse eingeben. Sie können dabei eine IPv4- und eine IPv6-Adresse eingeben. Mit SLAAC (StateLess Address AutoConfiguration) kann sich der Router selbständig eine oder mehrere IPv6-Adressen konfigurieren. Wenn im LAN ein Router mit Router Advertisement IPv6-Adressprefixe verkündet, konfiguriert sich der Router zusätzlich zu seinen bereits konfigurierten IPv6-Adressen eine Weitere mit dem verkündeten Prefix.

Dem lokalen Netzwerk kann eine virtuelle Netzadresse zugewiesen werden. Geräte im lokalen Netzwerk können anschließend über das WAN mit der virtuellen Adresse angesprochen werden. Der Router tauscht den Netzwerkanteil der virtuellen IP-Adresse gegen den Netzwerkanteil des lokalen Netzwerkes aus und leitet das Paket an das Ziel weiter.

Konfiguration mit Web-Interface (Menü „Basic Settings“, Seite „IP-Adresse (LAN)“)

Um eine **statische IP-Adresse** einzustellen, geben Sie die **IPv4-Adresse** des Routers im LAN sowie die **Netzmaske** ein.

ⓘ Bei Änderung der lokalen IP-Adresse wird automatisch der Adressbereich des DHCP-Servers angepasst, wenn sich die Netzmaske nicht verändert hat. Bei einer veränderten Netzmaske wird der DHCP-Server deaktiviert und muss von Hand konfiguriert werden. Darauf wird in einer Meldung hingewiesen.

Die **MAC-Adresse** finden Sie unter den Eingabefeldern für die IP-Adresse und Netzmaske unter „MAC-Adresse“ auf dieser Seite.

Damit sich der **Router selbständig eine oder mehrere IPv6-Adressen konfiguriert**, markieren Sie die Checkbox „IPv6-Adresse automatisch beziehen (SLAAC)“.

Geben Sie im Eingabefeld „IPv6-Adresse“ die **IPv6-Adresse** des Routers im LAN ein oder wählen Sie den Link „Neue ULA generieren“, um eine ULA (Unique Local Address) zu generieren.

Um dem lokalen Netzwerk eine **virtuelle Netzadresse** zuzuweisen, markieren Sie die Checkbox „Netmapping aktivieren“ und geben Sie die Netzadresse (d.h. den gesamten IP-Bereich) in das Feld „Virtuelle Netzadresse“ ein (z.B. 192.168.2.0). Diese virtuelle Adresse ist nur von der WAN- bzw. VPN-Seite aus sichtbar.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

ⓘ Soll die Kommunikation aus Sicherheitsgründen auf nur eine IP-Version (IPv4 oder IPv6) beschränkt werden, darf hier für die zu sperrende Version keine IP-Adresse angegeben werden.
Wenn IPv6 gesperrt werden soll, müssen auch SLAAC und der Router-Advertiser deaktiviert sein.
Wenn IPv4 gesperrt werden soll, müssen DHCP-Server und –Client deaktiviert sein.
Bei der IP-Adresse der LAN (ext)-Schnittstelle ist genauso zu verfahren.
Außerdem ist die Firewall für die zu blockierende IP-Version zu aktivieren und es müssen alle Firewall-Regeln manuell so abgeändert werden, dass sie keinen Datenverkehr dieser IP-Version erlauben.

12.1.3 Statische Routen eintragen

Sie können im EBW-H100 statische Routen für die Weiterleitung von Datenpaketen definieren, die beim Systemstart geladen werden.

Konfiguration mit Web-Interface (Menü „Basic Settings“, Seite „Routing“)

Um eine **statische Route** einzutragen, **geben Sie** im Abschnitt „Neue Route hinzufügen“ die **Netzadresse**, die **Netzmaske** sowie den **Gateway** in die jeweiligen Felder für IPv4 oder IPv6 ein. Alle Felder müssen ausgefüllt werden, damit eine neue Route für die jeweilige IP-Version in die Tabelle übernommen wird. Übernehmen Sie die Route, indem Sie auf „OK“ klicken.

Um eine **bestehende Route zu löschen**, aktivieren Sie unter „Bestehende Routen“ die Checkbox der Route(n), die gelöscht werden soll(en).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

ⓘ Hier kann weder ein Default-Gateway eingetragen werden, noch kann NAT ein- oder ausgeschaltet werden. Dies wird in den Menüs „Dial-In“, „Dial-Out“ bzw. „LAN (ext)“ auf der dortigen Seite „Routing“ konfiguriert.

12.1.4 Hostnamen eintragen

Sie können den Host- und Domainnamen des EBW-H100 hier angeben.

Außerdem kann eine Hosttabelle erstellt werden, in der IP-Adressen mit Hostnamen verknüpft werden. Wenn der Router bei einem PC als DNS-Server eingetragen ist, kann dieser anstelle der IP-Adressen die Hostnamen zur Adressierung benutzen.

Konfiguration mit Web-Interface (Menü „Basic Settings“, Seite „Hostnamen“)

Um den **Hostnamen** einzutragen, geben Sie den Hostnamen ein.

Um den **Domainnamen** einzutragen, geben Sie den Domainnamen ein.

Um einen neuen Host in die Hosttabelle einzutragen, geben Sie im Abschnitt „Neuen Host hinzufügen“ die **IP-Adresse** und den zugehörigen **Hostnamen** in die jeweiligen Felder ein. Übernehmen Sie den Host in die Tabelle, indem Sie auf „OK“ klicken.

Um einen **bestehenden Host zu löschen**, aktivieren Sie unter „Bestehende Hosts“ die Checkbox des/der Hosts, der/die gelöscht werden soll(en).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.1.5 MAC-Filter konfigurieren

Im EBW-H100 kann ein MAC-Filter aktiviert werden, der dann an der lokalen Ethernet-Schnittstelle nur noch Pakete akzeptiert, die von Netzwerkgeräten kommen, die explizit im Filter zugelassen sind.

ⓘ Dies gilt nur für Verbindungen, welche vom Gerät im lokalen LAN initiiert werden, nicht für Verbindungen, die von Seiten des WAN initiiert wurden.

Hinweis

Verlust der Erreichbarkeit!

Wenn die MAC-Adresse des Rechners, mit dem die Konfiguration vorgenommen wird, nicht eingetragen ist, ist keine weitere Konfiguration mehr möglich.

Tragen Sie unbedingt die MAC-Adresse des Rechners, mit dem die Konfiguration vorgenommen wird, in die Liste erlaubter Absender-MAC-Adressen ein, bevor Sie den MAC-Filter aktivieren.

Konfiguration mit Web-Interface (Menü „Basic Settings“, Seite „MAC-Filter“)

Um den **MAC-Filter zu aktivieren**, aktivieren Sie die Checkbox „MAC-Filter aktivieren“.

Um eine neue **Absender-MAC-Adresse einzutragen**, geben Sie diese in das Feld „Neue Absender-MAC-Adresse zulassen“ ein. Die MAC-Adresse kann mit oder ohne Doppelpunkten eingetragen werden, andere Formate werden nicht unterstützt. Übernehmen Sie den Eintrag, indem Sie auf „OK“ klicken.

Um eine **bestehende Absender MAC-Adresse zu löschen**, aktivieren Sie unter „Erlaubte Absender-MAC-Adressen“ die Checkbox der Adresse(n), die gelöscht werden soll(en).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.1.6 Zugriffschutz über Radius-Server konfigurieren

Der Zugang zum Web-Interface oder der Befehlszeilen-Schnittstelle (CLI) kann optional über einen Radius-Server im Netzwerk gegen unbefugte Zugriffe geschützt werden. Dazu müssen die Zugangsdaten für den Radius-Server im EBW-H100 konfiguriert werden.

Konfiguration mit Web-Interface (Menü „Basic Settings“, Seite „Radius“)

Um einen **Zugriffschutz über einen Radius-Server zu konfigurieren,** tragen Sie dessen Adresse und Port in die entsprechenden Felder ein. Standardmäßig ist Port 1812 eingestellt.
Geben Sie noch das „Shared Secret“ (Authentifizierungsschlüssel) in das zugehörige Feld ein.

ⓘ Diese Einstellungen sind nur relevant, wenn die Authentifizierung am Radius-Server im Menü „Basic Settings“ auf der Seite „Web-Interface“ und/oder der Seite „CLI“ ausgewählt ist.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.1.7 Zugang zur Befehlszeilen-Schnittstelle CLI konfigurieren

Neben der Konfiguration über das Web-Interface oder die Konfigurationsdatei, kann ein EBW-H100 auch über ein CLI (Command Line Interface), eine Befehlszeilen-Schnittstelle, konfiguriert werden. Es wird durch eine Abfrage von Benutzername und Kennwort (alternativ auch über einen Radius-Server) gegen unbefugte Zugriffe geschützt. Der Zugang zum CLI kann entweder aus dem lokalen Netz oder aus der Ferne über Telnet oder SSH (verschlüsselt) erfolgen. Sie können für Telnet und SSH den Port festlegen, unter dem Sie das CLI erreichen. Außerdem können Sie die Eingabeaufforderung (Prompt) im CLI konfigurieren.

Eine detaillierte Beschreibung der Konfiguration über das CLI findet sich im entsprechenden Zusatzhandbuch.

Konfiguration mit Web-Interface (Menü „Basic Settings“, Seite „CLI“)

Für eine **Authentifizierung lokal am Gerät** wählen Sie den Radiobutton „Authentifizierung mit Kennwort“ und geben Sie die Zugangsdaten in die entsprechenden Felder ein.

Für eine **Authentifizierung am Radius-Server** wählen Sie den Radiobutton „Authentifizierung am Radius-Server“.

ⓘ Dazu muss der Radius-Server konfiguriert sein (im Menü „Basic Settings“ auf der Seite „Radius-Server“).

Um eine Authentifizierung mit Kennwort zu ermöglichen, falls der **Radius-Server nicht erreichbar** ist bzw. nicht antwortet, aktivieren Sie die Checkbox „Authentifizierung mit Kennwort nach Radius-Timeout“.

Um festzulegen, über welche Zugriffsmöglichkeiten (lokal oder aus der Ferne über Telnet oder SSH) die **Konfiguration zulässig ist**, aktivieren bzw. deaktivieren Sie die jeweiligen Checkboxen.

Die **zulässige Konfiguration** können Sie über die jeweilige Checkbox aktivieren bzw. deaktivieren.

ⓘ Wenn keine dieser Checkboxen aktiviert ist, ist kein Zugriff auf das CLI möglich!

Den **Telnet-Port** legen Sie im Eingabefeld „Telnet-Port“ fest. Standardmäßig ist Port 23 eingestellt.

Den **SSH-Port** legen Sie im Eingabefeld „SSH-Port“ fest. Standardmäßig ist Port 22 eingestellt.

Die **Eingabeaufforderung (Prompt)** legen Sie im Eingabefeld „CLI-Prompt“ fest. Standardmäßig ist „> “ eingestellt.

Die **SSH-MD5-Prüfsumme** dient der positiven Identifizierung des Geräts bei einer SSH-Verbindung. Der zu Grunde liegende Schlüssel kann mit der Schaltfläche „SSH-Schlüssel neu erstellen“ neu erzeugt werden.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.2 UMTS

12.2.1 PIN der SIM-Karte eingeben

Für eine Einbuchung ins Mobilfunknetz und den Aufbau von CSD- bzw. IP-Verbindungen wird die PIN der eingesetzten SIM-Karte benötigt (sofern die SIM-Karte mit einer PIN geschützt ist).

Hinweis!

Mögliche Sperrung der SIM-Karte!

Durch Eingeben einer falschen PIN kann die SIM-Karte gesperrt werden wodurch eine Einbuchung ins Mobilfunknetz nicht mehr möglich ist.

Achten Sie beim Eingeben oder Ändern der PIN darauf, die richtige PIN für die SIM-Karte einzugeben. Die SIM-Karte kann mit der zugehörigen PUK wieder entsperrt werden. Zum Entsperren mit der PUK benötigen Sie ein Mobiltelefon, in das Sie die gesperrte SIM-Karte einsetzen und die PUK eingeben können. Alternativ können Sie die SIM-Karte mit dem Befehl **`AT+CPIN=PUK,NEW_PIN`** im Terminal entsperren.

Konfiguration mit Web-Interface (Menü „UMTS“)

Geben Sie die **PIN der eingesetzten SIM-Karte** in das Eingabefeld „PIN“ ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

ⓘ Die Eingabe einer PIN wird auch dann gespeichert, wenn die Freischaltung der SIM-Karte nicht erfolgreich war. Das ist erlaubt, um eine Konfiguration auch ohne eingelegte SIM-Karte zu ermöglichen. Aus diesem Grund wird auch eine falsche PIN gespeichert!

12.2.2 Netzwahl einstellen

Sie können bestimmen, in welches Mobilfunknetz sich der EBW-H100 einbucht. Dazu muss Ihre SIM-Karte Roaming unterstützen. Das Gerät kann sich dann mit dem am Standort am stärksten empfangbaren Netz, mit einem bestimmten bevorzugten Netz (das nicht unbedingt das am besten empfangene Netz sein muss) oder ausschließlich mit dem Netz eines bestimmten Providers verbinden. Bestimmen Sie einen „bevorzugten Provider“, wird versucht, immer mit dem Netz dieses Providers zu verbinden. Schlägt der Verbindungsversuch zum Netz des bevorzugten Providers fehl, bucht sich der Router in das am besten empfangbare Netz irgendeines Providers ein. Diese Einstellungen erfolgen für jede SIM-Karte getrennt.

Konfiguration mit Web-Interface (Menü „UMTS“)

Um die **Art der Netzwahl auszuwählen**, wählen Sie über Radiobuttons, ob sich die SIM-Karte ins stärkste Netz, bei einem bevorzugten Provider und dessen Netz oder ausschließlich im Netz eines von Ihnen bestimmten Providers einbuchen soll.

Damit das **Netz eines bestimmten Providers beim Einbuchen bevorzugt wird**, wählen Sie den Radiobutton für die Option „Bevorzugt bei diesem Provider einbuchen“. Geben Sie die Nummer des Providers im Eingabefeld dahinter an. Die Nummer des Providers können Sie über den Link unter dem Fragezeichen neben „Providerliste aus Modem auslesen“ herausfinden (dies ist nur möglich, wenn eine SIM-Karte eingelegt ist und mit der richtigen PIN entsperrt wurde). Um die Daten auslesen zu können, muss eine SIM Karte eingelegt sein und der Router muss in ein Mobilfunknetz eingebucht sein.

Damit das **Netz eines bestimmten Providers beim Einbuchen ausschließlich verwendet wird**, wählen Sie den Radiobutton für die Option „Ausschließlich bei diesem Provider einbuchen“. Geben Sie die Nummer des Providers im Eingabefeld dahinter an. Die Nummer des Providers können Sie über den Link unter dem Fragezeichen neben „Providerliste aus Modem auslesen“ herausfinden (dies ist nur möglich, wenn eine SIM-Karte eingelegt ist und mit der richtigen PIN entsperrt wurde).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.2.3 Tägliches Aus- und Einbuchen einstellen

Der EBW-H100 kann sich innerhalb von 24 Stunden zu bestimmten Uhrzeiten in das Mobilfunknetz aus- und auch zeitgesteuert wieder einbuchen. So können Sie die Verbindung auf bestimmte Zeiten begrenzen. Durch das periodische Aus- und Einbuchen erhöhen Sie die Verfügbarkeit, die sonst durch verschiedene Umstände, bei denen ein Neueinbuchen ins Netz erforderlich wäre, beinträchtig sein könnte, z.B. Wartungsarbeiten in den Mobilfunknetzen, die ein erneutes Einbuchen erforderlich machen. Wir empfehlen Ihnen die Verwendung dieser Funktion.

ⓘ Es wird unbedingt empfohlen, täglich in das Mobilfunknetz neu einzubuchen, um eine hohe Verfügbarkeit zu erreichen.

Konfiguration mit Web-Interface (Menü „UMTS“)

Geben Sie die **gewünschte Uhrzeit für das tägliche Ausbuchen** in die Eingabefelder „Tägliches Ausbuchen um“ im Format „hh:mm“ ein.

Geben Sie die **gewünschte Uhrzeit für das tägliche Einbuchen** in die Eingabefelder „Tägliches Einbuchen um“ im Format „hh:mm“ ein.

Schalten Sie die Funktion ein durch Aktivieren der Checkbox „Tägliches Aus- und Einbuchen aktivieren“.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.2.4 Terminal

Diese Funktion ermöglicht die direkte Übermittlung von AT-Befehlen an das Kommunikationsgerät des EBW-H100. Die Anzeige der Antwort erfolgt direkt unterhalb des Eingabefelds.

Konfiguration mit Web-Interface (Menü „UMTS“)

Geben Sie den **gewünschten AT-Befehl** im Abschnitt „Terminal“ in das Eingabefeld „AT-Kommando“ ein.

Übermitteln Sie den Befehl, indem Sie auf „OK“ klicken.

12.3 Dial-In

12.3.1 Dial-In einrichten

Sie können den EBW-H100 als Einwahl-Server bzw. eingehenden PPP-Server verwenden. Die Dial-In-Funktion ermöglicht, dass sich Benutzer aus der Ferne per Modem über die Rufnummer der SIM-Karte im Gerät mit dem Netzwerk dahinter verbinden (die SIM-Karte muss dafür CSD (Circuit Switched Data) unterstützen). Ähnlich der Einwahl bei einem Internetprovider authentifizieren sich die Benutzer per Benutzernamen und Kennwort. Zur Authentifizierung der PPP-Nutzer stehen die Methoden PAP oder CHAP zur Verfügung. Erfolgreich authentifizierte Nutzer können eine PPP-Verbindung aufbauen, um auf das Netzwerk des EBW-H100 zuzugreifen.

Konfiguration mit Web-Interface (Menü „Dial-In“, Seite „Dial-In“)

Um den **Dial-In**-Server zu **aktivieren**, wählen Sie den Radiobutton „Ja“ für „Dial-In aktivieren“.

Um den **Dial-In vor einem LAN (ext) zu priorisieren**, markieren Sie die Checkbox „Dial-In vor LAN (ext) priorisieren“. Dann wird nach einem authorisierten Dial-In die LAN (ext)-Verbindung abgebaut und anschließend die Dial-In-Verbindung aktiviert. Ansonsten wird ein eingehender Dial-In abgebrochen, sofern LAN (ext) aktiv ist.

Sie können eine **Leerlaufzeit** bestimmen, nach der Einwahlverbindungen geschlossen werden, sobald kein Datentransfer mehr stattfindet. Geben Sie die Zeit in Sekunden in das Eingabefeld „Idle Time“ ein. Wenn die Verbindung trotz Leerlauf aufrecht erhalten werden soll, geben Sie den Wert „0“ ein.

Legen Sie die **Zahl der Klingelzeichen** fest, nach denen ein Anruf entgegengenommen wird. Geben Sie die Anzahl der Klingelzeichen bis zum Abheben in das Eingabefeld „Klingelzeichen bis zur Anrufannahme“ ein.

Um eine **Benutzernamen- und Kennwort-basierte PPP-Authentifizierung** zu verwenden, aktivieren Sie die Checkbox „Authentifizierung für Dial-In“. Wenn Sie diese Checkbox deaktivieren, kann jeder Anrufer eine PPP Verbindung aufbauen. Geben Sie bis zu 10 verschiedene **Kombinationen aus Benutzername und Kennwort** in die Felder „Benutzername“ und Kennwort“ ein und legen Sie über den jeweiligen Radiobutton fest, ob für diesen Benutzer eine **Authentifizierung per „PAP“ oder „CHAP“** erfolgen soll. Der Benutzername darf nicht dem der Dial-Out-Verbindung entsprechen.

Wenn für den jeweiligen Benutzer ein **Callback nach erfolgreicher Authentifizierung** möglich sein soll, aktivieren Sie die Checkbox „Rückruf aktiv“. Wenn bei einem Callback die Authentifizierung notwendig ist, aber hier kein Häkchen gesetzt ist, dann erfolgt auch kein Callback. In dem Fall wird dem Anrufer ein gewöhnlicher Dial-In ermöglicht.

Optional können Sie die **IP-Adressen der Endpunkte der PPP-Verbindung** festlegen, falls diese Adressen in einem der Netzwerke am Gerät oder an der Gegenstelle schon vergeben sind. Standardmäßig ist die IP-Adresse des EBW-H100 die 192.168.254.1. Die Standard-Adresse der Gegenstelle ist 192.168.254.2.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.3.2 Automatischer Rückruf (Callback)

Sie können einen automatischen Rückruf zu einer vordefinierten Zielrufnummer des EBW-H100 mit einem Datenanruf oder Telefonanruf auslösen. Dafür können Sie berechtigte Anrufer einstellen. Die Anrufer können sich über die PPP-Authentifizierungsmethoden PAP oder CHAP oder über Ihre per CLIP mitgeteilte Rufnummer identifizieren. Die Verbindung, die dann vom Router aufgebaut wird, müssen Sie zuvor im Menü „Dial-Out“ konfigurieren. Es sind ausschließlich Verbindungen zum vorkonfigurierten Dial-Out Ziel möglich.

Konfiguration mit Web-Interface (Menü „Dial-In“, Seite „Dial-In“)

Um eine **Dial-Out-Verbindung durch einen Anrufer auszulösen**, aktivieren Sie die Checkbox „Automatischen Rückruf nach erfolgreicher PPP-Authentifikation aktivieren“. Die Dial-Out-Verbindung, die durch einen Anrufer ausgelöst wird, muss dafür zuvor im Menü „Dial-Out“ konfiguriert sein.
Damit Anrufer eine Verbindung auslösen können, müssen sie sich entweder via PPP-Authentifizierung oder über ihre Rufnummer identifizieren. Wählen Sie dazu in der Radiobutton-Auswahl entweder „Nach erfolgreicher PPP-Authentifizierung“ oder „Nach Anruf von einer dieser Rufnummern“ aus. Wenn Sie letztere Option wählen, geben Sie noch bis zu 5 Rufnummern in die Felder dahinter ein, nach deren Anruf ein Rückruf erfolgen kann.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.3.3 Routing

Sie können im EBW-H100 Routen für die Weiterleitung von Datenpaketen definieren. Weiterhin können Sie NAT (Network Address Translation) getrennt für eingehende und ausgehende Pakete aktivieren. Bei eingehenden IP-Verbindungen ersetzt der Router die Absender-IP-Adresse des ankommenden IP-Pakets durch seine eigene lokale IP-Adresse.

ⓘ Auf Grund der „Stateful Firewall“ kann es zu Verzögerungen kommen bis Änderungen an diesen Funktionen wirksam werden. Dies kann der Fall sein, wenn bereits Verbindungen bzw. Verbindungsversuche stattgefunden haben.

Konfiguration mit Web-Interface (Menü „Dial-In“, Seite „Routing“)

Um die **IPv4-Default-Route zu löschen**, deaktivieren Sie die Checkbox „Default Route setzen“.

Um die **IPv6-Default-Route zu löschen**, deaktivieren Sie die Checkbox „IPv6-Default Route setzen“.

Um **NAT für eingehende Pakete zu deaktivieren**, deaktivieren Sie die Checkbox „NAT für eingehende IPv4-Pakete aktivieren“.

Um **NAT für ausgehende Pakete zu deaktivieren**, deaktivieren Sie die Checkbox „NAT für ausgehende IPv4-Pakete aktivieren“.

ⓘ Der Router gibt bei aktivierter Firewall automatisch eigene Dienste (z.B. DNS, VPN, NTP, etc.) frei. Wenn Sie die Checkbox „NAT für ausgehende IPv4-Pakete aktivieren“ deaktivieren, müssen diese Dienste manuell in der Firewall zugelassen werden.

Um eine **neue Route hinzuzufügen**, geben Sie Abschnitt „Neue Route hinzufügen“ die „Netzadresse“ und die „Netzmaske“ in die jeweiligen Felder für IPv4 oder IPv6 ein. Alle Felder müssen ausgefüllt werden, damit eine neue Route für die jeweilige IP-Version in die Tabelle übernommen wird. Übernehmen Sie die Route, indem Sie auf „OK“ klicken.

Um eine **bestehende Route zu löschen**, aktivieren Sie unter „Bestehende Routen“ die Checkbox der Route(n), die gelöscht werden soll(en).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.3.4 Firewall-Regel erstellen oder löschen

Für Dial-In-Verbindungen steht eine Firewall zur Verfügung. Sie dient dazu, unerwünschten Datenverkehr zu verhindern. Die Logik der Firewall ist, dass jeglicher Datenverkehr verboten ist, der nicht explizit durch eine Regel erlaubt wurde.

Hier definieren Sie, welche Verbindungen über den Router zugelassen sind. Wenn Sie die Firewall für die Verbindungsart „Dial-In“ einschalten, sind nur noch Verbindungen möglich, die durch Firewall-Regeln erlaubt werden. Alle anderen Verbindungen werden blockiert.

ⓘ Auf Grund der „Stateful Firewall“ kann es zu Verzögerungen kommen bis Änderungen an diesen Funktionen wirksam werden. Dies kann der Fall sein, wenn bereits Verbindungen bzw. Verbindungsversuche stattgefunden haben.

Konfiguration mit Web-Interface (Menü „Dial-In“, Seite „Firewall“)

Um die **Firewall für IPv4-Dial-In-Verbindungen zu aktivieren**, aktivieren Sie die Checkbox „Firewall für Dial-In-Verbindungen aktivieren“.

Um die **Firewall für IPv6-Dial-In-Verbindungen zu aktivieren**, aktivieren Sie die Checkbox „IPv6-Firewall für Dial-In-Verbindungen aktivieren“.

ⓘ Es wird dringend empfohlen, die Firewall für IPv6 immer aktiviert zu lassen, auch wenn IPv6 nicht genutzt wird.

Um eine **Regel für eine zugelassene IP-Verbindung zu erstellen**, gehen Sie wie folgt vor.

Wählen Sie im Abschnitt „Neue Verbindung zulassen“ in der Dropdown-Liste „Datenrichtung“ für die Regel eine **Datenrichtung** aus.

Bestimmen Sie das **Protokoll der zugelassenen Verbindung** in der Dropdown-Liste „Protokoll“.

Wählen Sie die **IP-Version**, für welche die Regel gelten soll, in der Dropdown-Liste „IP-Version“.

Sie können zusätzlich dafür sorgen, dass die Regel **ausschließlich für einen bestimmten Dial-In-Benutzer angewandt wird**; wählen Sie hierzu in der Dropdown-Liste „Dial-In Benutzername“ den entsprechenden Dial-In-Benutzernamen aus.

Geben Sie in den Eingabefeldern „**Absender-IP-Adresse**“, „**Ziel-IP-Adresse**“ und **Ziel-Port** die weiteren Spezifikationen für die durch den Router zugelassen Verbindungen an. Es können Regeln erstellt werden, die nicht nur für einzelne Maschinen (Hosts) gelten, sondern für ganze Netze. In dem Fall muss die Netzmaske nach dem „/“ eingegeben werden.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um einzelne **Firewall-Regeln temporär auszuschalten**, deaktivieren Sie im Abschnitt „Zugelassene Verbindungen …“ die Checkbox in der Spalte „aktiv“ in der Übersicht der Firewall-Regeln. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

Um **eine oder mehrere Regeln** zu **löschen**, aktivieren Sie die Checkbox in der Spalte „löschen“ in der Übersicht der Firewall-Regeln. Klicken Sie auf „OK“, um die Einstellung zu übernehmen.

12.4 Dial-Out

12.4.1 Dial-Out einrichten

Sie können den EBW-H100 für den Dial-Out einsetzen. Es wird automatisch eine PPP-Verbindung zu einer Gegenstelle hergestellt, wenn Netzwerkverkehr in Richtung des Netzes der Gegenstelle auftritt. Der Netzwerkverkehr, der einen Verbindungsaufbau auslösen darf, kann über Regeln beschränkt werden. Dieser optionale „Wählfilter“ sorgt dafür, dass nur Pakete von bzw. zu bestimmten IP-Adressen oder von bzw. zu bestimmten Ports die Dial-Out-Verbindung auslösen. Diese Dial-Out-Verbindung ist vergleichbar mit der Einwahl eines PC ins Internet. Erst nach dieser Einwahl ist es möglich, IP-Daten (z.B. Webinhalte) zu übertragen oder z.B. aus der Ferne auf Geräte im lokalen Netz des EBW-H100 zuzugreifen.

Konfiguration mit Web-Interface (Menü „Dial-Out“, Seite „Dial-Out“)

Um den **Dial-Out einzuschalten**, wählen Sie in der Auswahl „Dial-Out aktivieren“ die Option „Ja“.

Geben Sie für eine **GSM-CSD-Verbindung die Rufnummer der PPP-Gegenstelle** (z.B. den Internetprovider) in das Eingabefeld „Rufnummer“ für Ziel A ein. Sie können eine weitere Rufnummer (oder „*99***1#“ für eine paketbasierte Verbindung, siehe unten) bei Ziel B eingeben.

Geben Sie für eine **paketbasierte Verbindung (GPRS/EDGE/UMTS/HSDPA)** in das Eingabefeld bei „Rufnummer“ für Ziel A „*99***1#“ ein. Geben Sie für Ziel A den APN Ihres Mobilfunkproviders in das Feld „Access Point Name“ ein, über den die paketbasierte Verbindung aufgebaut werden soll. Sie können einen weiteren APN bei Ziel B eingeben. Alternativ können Sie für Ziel B auch eine GSM-CSD-Verbindung mit einer gewöhnlichen Rufnummer definieren.

Geben Sie **Benutzername und Kennwort** für die PPP-Einwahl-Ziele A und B an. Die Angabe des Ziels B ist optional. Der Benutzername darf nicht gleich dem eines Dial-In-Benutzers sein.

Wählen Sie für Ziel A und B die jeweils zu verwendende **PPP-Authentifizierungsmethode (PAP; CHAP, und PAP oder CHAP)** in der Auswahl „Authentifizierung“ aus.

Die **Priorität der Ziele** konfigurieren Sie unter „Priorität“. Dazu stehen Ihnen die Optionen „Zuletzt erfolgreiches Ziel“, „Ziel A“ oder „Ziel wechseln“ (anderes als das letzte verwendete Ziel) zur Verfügung. Das jeweilige Ziel wird dann zuerst verwendet. Funktioniert der Verbindungsaufbau zu diesem Ziel nicht, so versucht er das andere Ziel zu erreichen.

Über die „**Idle Time**“ können Sie bestimmen, wie lange die Verbindung aufrecht erhalten wird, wenn kein Datentransfer mehr stattfindet. Geben Sie die gewünschte Leerlaufzeit in das Eingabefeld „Idle Time“ in Sekunden ein.
Um die Verbindung unbegrenzt lange zu halten geben Sie als Zeit den Wert „0“ ein.

Über die **maximale Verbindungszeit** können Sie die Dauer einer Verbindung beschränken. Geben Sie eine maximale Verbindungszeit an, wird die Verbindung nach Ablauf dieser Zeit geschlossen. Um die Verbindung zeitlich unbegrenzt (bis zum Verbindungsabbau aus anderen Gründen) geöffnet zu lassen, geben Sie als Zeit den Wert „0“ in das Eingabefeld „maximale Verbindungszeit“ ein.

Um die **MTU** (maximale erlaubte Anzahl an Bytes in einem zu sendenden Paket) anzupassen, ändern Sie den Eintrag im entsprechenden Feld.

Um die **MRU** (maximale erlaubte Anzahl an Bytes in einem zu empfangenden Paket) anzupassen, ändern Sie den Eintrag im entsprechenden Feld.

ⓘ Die Standardeinstellung von MTU und MRU ist für die meisten Anwendungen passend und muss nur in Ausnahmefällen geändert werden.

Falls dem Router bei einem Dial-Out keine IP-Adresse für einen zu benutzenden DNS-Server mitgeteilt wird, muss die Checkbox "DNS-Server-Adresse anfordern" deaktiviert werden. Ansonsten kann eventuell keine Verbindung zustande kommen.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.4.2 Standleitungsbetrieb einrichten

Sie können den EBW-H100 so einstellen, dass eine PPP-Verbindung dauerhaft aufrecht erhalten bleibt. Diese Betriebsart ist interessant für private Netze, bei denen keine Minutengebühren anfallen, oder für Abrechnungsmodelle, in denen nur die übertragenen Datenvolumen bezahlt werden (z.B. paketbasierte Netze). In diesem Betriebsmodus wird die Verbindung sofort nach dem Einschalten aufgebaut. Die Verbindung wird periodisch auf ihre Funktion geprüft. Die Verbindungsüberprüfung kann entweder über eine DNS-Abfrage eines Hostnamens oder über Ping an einen Host durchgeführt werden.

Konfiguration mit Web-Interface (Menü „Dial-Out“, Seite „Dial-Out“)

Um die **Standleitung einzurichten**, aktivieren Sie die Checkbox „Verbindung sofort aufbauen und dauerhaft halten“.

Geben Sie, falls notwendig, eine andere Zeit in Minuten zur **Verbindungsüberprüfung** in das Eingabefeld „Zeitintervall der Verbindungsüberprüfung“ ein. Die Werkseinstellung ist 60 Minuten. Wird nach dieser Zeit eine geschlossene Verbindung festgestellt, versucht der EBW-H100 nach einer Minute die Verbindung neu aufzubauen. Schlägt der Versuch fehl, wird nach 5 Minuten erneut versucht, die Verbindung neu aufzubauen. Der nächste Versuch findet nach 30 Minuten statt, schlägt auch dieser Versuch fehl, wird alle 60 Minuten versucht, die Verbindung neu aufzubauen.

Wählen Sie die **Methode zur Verbindungsüberprüfung** in der Auswahl „Art der Verbindungsüberprüfung“ aus und geben Sie einen Hostnamen oder eine „IP-Adresse“ an. Wenn die Checkbox „Bestehende PPP-Verbindung im Fehlerfall erneut aufbauen“ markiert ist, sorgt ein fehlgeschlagener Ping oder DNS-Request dafür, dass eine eventuell bestehende WAN-Verbindung abgebaut wird. Auf jeden Fall wird anschließend versucht, wieder eine Verbindung aufzubauen.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.4.3 Periodischen Dial-Out-Verbindungsaufbau einrichten

Der EBW-H100 kann die zuvor konfigurierte Dial-Out-Verbindung zeitgesteuert auf und abbauen. Die Dial-Out-Verbindung wird täglich zu einer bestimmten Uhrzeit aufgebaut und zu einer anderen Uhrzeit wieder abgebaut.

Mit dieser Funktion werden jeweils einzelne Ereignisse ausgelöst, es wird keine Sperrzeit o.ä. definiert. Beispiel: Wenn ein Abbau um 14:00 Uhr und ein automatischer Aufbau um 16:00 Uhr definiert wird, so können andere Ereignisse auch innerhalb dieses Zeitraums einen Verbindungsaufbau (Dial-Out) auslösen, z.B. ein einfaches Paket, dass dem Wählfilter entspricht. Ebenso wird nach einem zeitgesteuerten Verbindungsaufbau die Verbindung automatisch abgebaut, falls z.B. die konfigurierte „Idle Time“ abgelaufen ist.

Konfiguration mit Web-Interface (Menü „Dial-Out“, Seite „Dial-Out“)

Um eine **Verbindung zu einer bestimmten Uhrzeit täglich aufzubauen**, aktivieren Sie die Checkbox „Verbindung täglich automatisch aufbauen um“ und geben Sie eine Uhrzeit für den Verbindungsaufbau in die Eingabefelder für Stunden und Minuten ein.

Um eine **Verbindung zu einer bestimmten Uhrzeit täglich abzubauen**, aktivieren Sie die Checkbox „Verbindung täglich automatisch abbauen um“ und geben Sie eine Uhrzeit für den Verbindungsabbau in die Eingabefelder für Stunden und Minuten ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.4.4 Routing

Sie können im EBW-H100 Routen für die Weiterleitung von Datenpaketen definieren. Weiterhin können Sie NAT getrennt für eingehende und ausgehende Pakete aktivieren.

ⓘ Auf Grund der „Stateful Firewall“ kann es zu Verzögerungen kommen bis Änderungen an diesen Funktionen wirksam werden. Dies kann der Fall sein, wenn bereits Verbindungen bzw. Verbindungsversuche stattgefunden haben.

Konfiguration mit Web-Interface (Menü „Dial-Out“, Seite „Routing“)

Um die **IPv4-Default-Route zu löschen**, deaktivieren Sie die Checkbox „Default Route setzen“.

Um die **IPv6-Default-Route zu löschen**, deaktivieren Sie die Checkbox „IPv6-Default Route setzen“.

Um **NAT für eingehende Pakete zu deaktivieren**, deaktivieren Sie die Checkbox „NAT für eingehende IPv4-Pakete aktivieren“.

Um **NAT für ausgehende Pakete zu deaktivieren**, deaktivieren Sie die Checkbox „NAT für ausgehende IPv4-Pakete aktivieren“.

ⓘ Der Router gibt bei aktivierter Firewall automatisch eigene Dienste (z.B. DNS, VPN, NTP, etc.) frei. Wenn Sie die Checkbox „NAT für ausgehende IPv4-Pakete aktivieren“ deaktivieren, müssen diese Dienste manuell in der Firewall zugelassen werden.

Um eine **neue Route hinzuzufügen**, geben Sie Abschnitt „Neue Route hinzufügen“ die „Netzadresse“ und die „Netzmaske“ in die jeweiligen Felder für IPv4 oder IPv6 ein. Alle Felder müssen ausgefüllt werden, damit eine neue Route für die jeweilige IP-Version in die Tabelle übernommen wird. Übernehmen Sie die Route, indem Sie auf „OK“ klicken.

Um eine **bestehende Route zu löschen**, aktivieren Sie unter „Bestehende Routen“ die Checkbox der Route(n), die gelöscht werden soll(en).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.4.5 Wählfilter einrichten

Um unnötige Kosten durch unerwünschte Dial-Out-Vorgänge zu verhindern kann optional ein Wählfilter aktiviert werden. Mit diesem Wählfilter kann der Netzwerkverkehr beschränkt werden, der einen Dial-Out Vorgang auslösen kann. Sobald eine Dial-Out-Verbindung aufgebaut ist, können allerdings alle Teilnehmer im Netzwerk auf die Dial-Out-Verbindung zugreifen und IP-Daten übertragen. Falls auch während der Dial-Out-Verbindung der Netzwerkverkehr beschränkt werden soll, kann dies mit der Firewall-Funktion erreicht werden.

Hier definieren Sie, welche Pakete die Dial-Out-Verbindung über den EBW-H100 initiieren dürfen. Wenn Sie den Wählfilter einschalten, sind nur noch Dial-Out-Verbindungen möglich, die durch Wählfilterregeln erlaubt werden. Alle andern Verbindungen werden blockiert.

Konfiguration mit Web-Interface (Menü „Dial-Out“, Seite „Wählfilter“)

Um den **Wählfilter einzuschalten**, aktivieren Sie die Checkbox „Wählfilter für Dial-Out-Verbindungen aktivieren“.

Um eine **Regel für einen Wählfilter zu erstellen**, gehen Sie wie folgt vor.

Wählen Sie das **Protokoll der zugelassenen Verbindung** in der Dropdown-Liste „Protokoll“.

Geben Sie in den Eingabefeldern „**Absender-IP-Adresse**“, „**Ziel-IP-Adresse**“ und „**Ziel-Port“** die weiteren Spezifikationen für die zugelassen Verbindungen durch den EBW-H100 an. Es können Regeln erstellt werden, die nicht nur für einzelne Maschinen (Hosts) gelten, sondern für ganze Netze. In dem Fall muss die Netzmaske nach dem „/“ eingegeben werden.

Um DNS-Anfragen an den Router, die einen Verbindungsaufbau initiieren würden (DNS-Relay), explizit zu erlauben, aktivieren Sie die Checkbox „DNS-Anfragen der Absender-IP-Adresse dürfen eine Verbindung initiieren“.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um einzelne **Dial-Out-Regeln temporär auszuschalten**, deaktivieren Sie die Checkbox in der Spalte „aktiv“ im Abschnitt „Diese Datenpakete dürfen einen Dial-Out initiieren“. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

Um **eine oder mehrere Regeln** zu **löschen**, aktivieren Sie die Checkbox in der Spalte „löschen“ im Abschnitt „Diese Datenpakete dürfen einen Dial-Out initiieren“. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

12.4.6 Firewall-Regel erstellen oder löschen

Für Dial-Out-Verbindungen steht eine Firewall zur Verfügung. Sie dient dazu, unerwünschten Datenverkehr zu verhindern. Die Logik der Firewall ist, dass jeglicher Datenverkehr verboten ist, der nicht explizit durch eine Regel erlaubt wurde.

Hier definieren Sie, welche Verbindungen über den Router zugelassen sind. Wenn Sie die Firewall für die Verbindungsart „Dial-Out“ einschalten, sind nur noch Verbindungen möglich, die durch Firewall-Regeln erlaubt werden. Alle anderen Verbindungen werden blockiert.

ⓘ Auf Grund der „Stateful Firewall“ kann es zu Verzögerungen kommen bis Änderungen an diesen Funktionen wirksam werden. Dies kann der Fall sein, wenn bereits Verbindungen bzw. Verbindungsversuche stattgefunden haben.

Konfiguration mit Web-Interface (Menü „Dial-Out“, Seite „Firewall)

Um die **Firewall für IPv4-Dial-Out-Verbindungen zu aktivieren**, aktivieren Sie die Checkbox „Firewall für Dial-Out-Verbindungen aktivieren“.

Um die **Firewall für IPv6-Dial-Out-Verbindungen zu aktivieren**, aktivieren Sie die Checkbox „IPv6-Firewall für Dial-Out-Verbindungen aktivieren“.

ⓘ Es wird dringend empfohlen, die Firewall für IPv6 immer aktiviert zu lassen, auch wenn IPv6 nicht genutzt wird.

Um eine **Regel für eine zugelassene IP-Verbindung zu erstellen**, gehen Sie wie folgt vor.

Wählen Sie im Abschnitt „Neue Verbindung zulassen“ in der Dropdown-Liste „Datenrichtung“ für die Regel eine **Datenrichtung** aus.

Bestimmen Sie das **Protokoll der zugelassenen Verbindung** in der Dropdown-Liste „Protokoll“.

Wählen Sie die **IP-Version**, für welche die Regel gelten soll, in der Dropdown-Liste „IP-Version“.

Geben Sie in den Eingabefeldern „**Absender-IP-Adresse**“, „**Ziel-IP-Adresse**“ und **Ziel-Port** die weiteren Spezifikationen für die durch den Router zugelassen Verbindungen an. Es können Regeln erstellt werden, die nicht nur für einzelne Maschinen (Hosts) gelten, sondern für ganze Netze. In dem Fall muss die Netzmaske nach dem „/“ eingegeben werden.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um einzelne **Firewall-Regeln temporär auszuschalten**, deaktivieren Sie im Abschnitt „Zugelassene Verbindungen …“ die Checkbox in der Spalte „aktiv“ in der Übersicht der Firewall-Regeln. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

Um **eine oder mehrere Regeln** zu **löschen**, aktivieren Sie die Checkbox in der Spalte „löschen“ in der Übersicht der Firewall-Regeln. Klicken Sie auf „OK“, um die Einstellung zu übernehmen.

12.4.7 Port-Forwarding-Regel erstellen oder löschen

Bei aktiviertem Port-Forwarding leitet der Router vom WAN eingehende Pakete an die Maschinen im LAN weiter, die in den Port-Forwarding-Regeln festgelegt wurden.

Aus dem WAN ist nur die WAN-IP-Adresse des EBW-H100 erreichbar, wenn NAT für ins WAN gehende Pakete aktiviert ist. Anhand dieser IP-Adresse können die lokalen Endgeräte im Netz des Geräts mit Hilfe von Port-Forwarding trotzdem erreicht werden. Pakete aus dem WAN, die an die WAN-IP-Adresse an einem Port x gesendet werden, können an eine Maschine mit der IP-Adresse Y an den Port y weitergeleitet werden. Wird alternativ ein ganzer Port-Bereich angegeben, werden die Pakete an dieselben Ports der Ziel-IP-Adresse weitergeleitet. Es ist möglich, die Regeln so anzulegen, dass sie nur für WAN-Verbindungen, nur für OpenVPN-Verbindungen oder generell gelten.

ⓘ Auf Grund der „Stateful Firewall“ kann es zu Verzögerungen kommen bis Änderungen an diesen Funktionen wirksam werden. Dies kann der Fall sein, wenn bereits Verbindungen bzw. Verbindungsversuche stattgefunden haben.

Konfiguration mit Web-Interface (Menü „Dial-Out“, Seite „Port-Forwarding“)

Um das **Port-Forwarding** zu **aktivieren**, aktivieren Sie die Checkbox „Port-Forwarding für Dial-Out-Verbindungen aktivieren“.

Um eine **Port-Forwarding-Regel** zu **erstellen**, wählen Sie im Abschnitt „Neue Regel erstellen“ das Protokoll aus und geben den Port bzw. Bereich der Ports für die am EBW-H100 eingehenden Pakete an. Geben Sie eine IP-Adresse für das Umleitungsziel im Eingabefeld „an IP-Adresse“ und einen Port im Eingabefeld „an Port“ ein; an diese Adresse und diesen Port werden die Pakete weitergeleitet. Bei Angabe eines Port-Bereichs ist kein Ziel-Port erforderlich, da dieser immer dem Port-Bereich im WAN entspricht. Wählen Sie in der Dropdown-Liste „anwenden“ noch aus, ob die Regel immer, nur für WAN-Verbindungen oder nur für OpenVPN-Verbindungen gelten soll.

Um eine **bereits erstellte Regel** zu **deaktivieren**, deaktivieren Sie die Checkbox „aktiv“ der entsprechenden Regel und klicken Sie anschließend auf „OK“.

Um eine **bereits erstellte Regel** zu **löschen**, aktivieren Sie die Checkbox „löschen“ der entsprechenden Regel und klicken Sie anschließend auf „OK“.

Die Regeln in der Liste werden von oben nach unten abgearbeitet. Sollten sich also zwei Regeln widersprechen (z.B. zweimal derselbe Port), so wird nur die Regel ausgeführt, die weiter oben in der Liste steht.

12.4.8 Exposed Host festlegen

Optional können alle Pakete, die keiner Port-Forwarding-Regel entsprechen, an einen vorbestimmten Rechner im LAN, den „Exposed Host“, weitergeleitet werden (z.B. zu Diagnosezwecken). Der „Exposed Host“ erhält alle Pakete, die nicht aus dem lokalen Netz des EBW-H100 angefordert wurden oder durch eine Port-Forwarding-Regel nicht bereits an einen Teilnehmer im lokalen Netz weitergeleitet wurden. Wird kein „Exposed Host“ konfiguriert, werden diese eingehenden Pakete verworfen.

Konfiguration mit Web-Interface (Menü „Dial-Out“, Seite „Port-Forwarding“)

Um einen **„Exposed Host“** zu **definieren**, geben Sie im Eingabefeld „Exposed Host“ die IP-Adresse eines Rechners im LAN ein, der von außen über alle Ports erreichbar sein soll.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.5 LAN (ext)

12.5.1 Schnittstelle zum externen Netz (LAN/WAN) einrichten

Der EBW-H100 vermittelt in seiner Funktion als Router den Datenverkehr zwischen zwei IP-Netzen, einem „internen“ und einem „externen“. Die LAN ext-Schnittstelle dient zur Anbindung des Routers an das externe Netzwerk. Dieses externe Netzwerk kann ein weiteres LAN sein, das über ein Ethernet-Kabel erreichbar ist. Dann muss für die LAN ext-Schnittstelle eine IP-Adresse eingestellt sein oder bezogen werden. Diese IP-Adresse muss im Adressraum des externen LANs liegen, in das der EBW-H100 routen soll. Mit SLAAC (StateLess Address AutoConfiguration) kann sich der Router selbständig eine oder mehrere IPv6-Adressen konfigurieren. Wenn im LAN ein Router mit Router Advertisement IPv6-Adressprefixe verkündet, konfiguriert sich der Router zusätzlich zu seinen bereits konfigurierten IPv6-Adressen eine Weitere mit dem verkündeten Prefix. Das externe Netzwerk kann aber auch ein WAN sein, das über einen DSL-Anschluss angebunden wird. In diesem Fall müssen Sie die Schnittstelle für den PPPoE-Betrieb einrichten, damit über ein DSL-Modem mit dem WAN kommuniziert werden kann.

Konfiguration mit Web-Interface (Menü „LAN (ext)“, Seite „LAN (ext)“)

Für eine Verbindung **mit einem LAN**, wählen Sie den Radiobutton „statische IP-Adresse“. Geben Sie dann in die Eingabefelder „statische IP-Adresse“ und „Netzmaske“ eine IPv4-Adresse sowie eine Netzmaske ein. Die IP-Adresse muss eine Adresse aus dem externen LAN sein, mit dem Sie das Gerät verbinden.

Damit sich der **Router selbständig eine oder mehrere IPv6-Adressen konfiguriert**, markieren Sie die Checkbox „IPv6-Adresse automatisch beziehen (SLAAC)“.

Geben Sie im Eingabefeld „IPv6-Adresse“ die **IPv6-Adresse** des Routers im LAN ein oder wählen Sie den Link „Neue ULA generieren“, um eine ULA (Unique Local Address) zu generieren.

Um das Gerät **per DSL mit einem WAN** zu verbinden, konfigurieren Sie zuerst im Menü „LAN (ext)“ auf der Seite „DSL“ die DSL-Verbindung. Wählen Sie dann den Radiobutton „PPPoE-Verbindung“.

Um den **DHCP-Client zu aktivieren**, wählen Sie den Radiobutton „DHCP-Client“. Dann bezieht der Router über die LAN ext-Schnittstelle eine IP-Adresse von einem DHCP-Server. Um **für jeden Eintrag in der Hosttabelle eine weitere IP-Adresse zu beziehen**, aktivieren Sie die Checkbox „Für jeden Eintrag in der Hosttabelle eine weitere IP-Adresse anfordern“. Dann wird für jeden Eintrag der Hosttabelle eine weitere IP-Adresse beantragt und der LAN ext-Schnittstelle zugeordnet. Für den Hostnamen wird der eigene Hostname mit dem Hostnamen des Tabelleintrags verknüpft. Alle Pakete, die an diese zusätzlichen IP-Adressen gesendet werden, werden zu der IP-Adresse des Hosttabelleneintrages weitergeleitet.

Um das Gerät **als Bridge zu betreiben**, wählen Sie den Radiobutton „Bridge“. Die LAN ext-Schnittstelle verhält sich dann wie ein weiterer Switch-Port.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.5.2 Redundantes WAN einrichten

Der EBW-H100 ermöglicht die Verwendung des integrierten Kommunikationsgeräts als redundante WAN-Schnittstelle. Dabei ist die LAN ext-Schnittstelle immer der primäre Kommunikationsweg. Sobald die regelmäßige Überprüfung der Verbindung über die LAN ext-Schnittstelle dreimal hintereinander fehlschlägt (oder optional der Ethernet-Link verloren geht), wird eine Verbindung über das integrierte Kommunikationsgerät aufgebaut. Für die redundante Verbindung gelten dann die Einstellungen, die für eine Dial-Out-Verbindung festgelegt wurden. Nach dem Ablauf einer konfigurierten Zeit oder nachdem der Ethernet-Link wieder hergestellt wurde erfolgt ein automatisches Zurückschalten auf die LAN ext-Schnittstelle. Schlägt die Verbindungsüberprüfung wieder dreimal fehl, wird wieder auf das redundante WAN umgeschaltet.

Konfiguration mit Web-Interface (Menü „LAN (ext)“, Seite „Redundantes WAN“)

Um das **redundante WAN zu aktivieren**, markieren Sie die Checkbox „Redundantes WAN aktivieren“.

Geben Sie das **Zeitintervall für die Verbindungsüberprüfung** in Minuten in das Feld „Zeitintervall der Verbindungsüberprüfung“ ein.

Um eine **Verbindungsüberprüfung über eine DNS-Abfrage** durchzuführen, wählen Sie im Abschnitt „Art der Verbindungsüberprüfung“ den Radiobutton „DNS-Abfrage“ und geben das Ziel in das dahinterliegende Feld ein. Bei der DNS-Abfrage wird vorausgesetzt, dass dem EBW-H100 ein DNS-Server bekannt ist.

Um eine **Verbindungsüberprüfung über einen Ping** durchzuführen, wählen Sie im Abschnitt „Art der Verbindungsüberprüfung“ den Radiobutton „Ping an“ und geben das Ziel in das dahinterliegende Feld ein. Die Verbindungsüberprüfung gilt dann als erfolgreich, wenn die Gegenstelle mit einem "Pong" antwortet.

Um eine **Verbindungsüberprüfung über den Verlust des Ethernet-Links** durchzuführen, wählen Sie im Abschnitt „Art der Verbindungsüberprüfung“ den Radiobutton „Ethernet-Link verloren“.

Um **nach Ablauf eines Zeitintervalls auf die LAN ext-Schnittstelle zurückschalten**, wählen Sie im Abschnitt „Zurückschalten auf LAN (ext)“ den Radiobutton „nach Intervall“ und geben Sie das Intervall in Minuten in das Feld dahinter ein.

Um **bei wieder hergestelltem Ethernet-Link auf die LAN ext-Schnittstelle zurückschalten**, wählen Sie im Abschnitt „Zurückschalten auf LAN (ext)“ den Radiobutton „bei wieder hergestelltem Ethernet-Link“.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.5.3 DSL einrichten

Der EBW-H100 kann sich über ein DSL-Modem mit einem WAN verbinden. Das DSL-Modem wird über die LAN ext-Schnittstelle angeschlossen. Das Gerät kann dann über eine PPPoE-Verbindung mit dem DSL-Modem kommunizieren. Die LAN ext-Schnittstelle müssen Sie dafür auf PPPoE-Betrieb einstellen. Damit dann über das DSL-Modem eine Verbindung zum Provider aufgebaut werden kann, müssen Sie noch die DSL-Verbindung mit Ihren Zugangsdaten konfigurieren sowie die Option „Defaultroute setzen“ aktivieren.

Konfiguration mit Web-Interface (Menü „LAN (ext)“, Seite „DSL“)

Um den **DSL-Zugang zu konfigurieren**, schließen Sie das DSL-Modem an die LAN ext-Schnittstelle an.
Geben Sie dann in die Eingabefelder „Benutzername“ und „Kennwort“ Ihren Benutzernamen und Ihr Kennwort für den DSL-Zugang ein.

Geben Sie **optional eine Leerlaufzeit** im Feld „Idle Time“ in Sekunden ein, nach der die Verbindung abgebaut wird, sobald kein Datentransfer mehr stattfindet. Geben Sie „0“ ein, so bleibt die Verbindung beliebig lange aufgebaut.

Geben Sie **optional eine maximale Verbindungszeit** im Feld „Maximale Verbindungszeit“ in Sekunden ein, nach deren Ablauf die Verbindung unterbrochen wird. Geben Sie „0“ ein, um den zeitgesteuerten Verbindungsabbau auszuschalten.

Um die **MTU (maximale erlaubte Anzahl an Bytes in einem zu sendenden Paket) anzupassen**, ändern Sie den Eintrag im entsprechenden Feld.

Um die **MRU (maximale erlaubte Anzahl an Bytes in einem zu empfangenden Paket) anzupassen**, ändern Sie den Eintrag im entsprechenden Feld.

ⓘ Die Standardeinstellung von MTU und MRU ist für die meisten Anwendungen passend und muss nur in Ausnahmefällen geändert werden.

Wenn Ihr DSL-Zugang es erfordert, **Ethernet-Pakete über die PPPoE-Verbindung mit VLAN-Tags zu versehen**, kann dies im entsprechenden Feld eingetragen werden.

ⓘ Wenn das DSL-Modem einen Sync erreicht, aber keine PPPoE-Verbindung herstellen kann, kann dies an einem fehlenden oder falschen VLAN-Tag liegen. Weitere Informationen dazu erhalten Sie von Ihrem Provider.

Um nach dem Beziehen einer IPv6-Adresse einen **IPv6 Prefix vom DSL-Provider zu beziehen**, aktivieren Sie die Checkbox „IPv6-Adresse und -Prefix beziehen“. Der Router weist sich dann eine lokale IPv6-Adresse aus diesem Netzwerk zu.

Damit die **IP-Adressen der Nameserver vom DSL-Provider bezogen werden**, aktivieren Sie die Checkbox „DNS-Server-Adresse anfordern“.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um eine **Default-Route zu setzen**, aktivieren Sie im Menü „LAN (ext)“auf der Seite „Routing“ die Checkbox „Default Route setzen zu Gateway“. Ohne die Defaultroute zum DSL-Modem kann das Gerät den Datenverkehr zwischen dem internen Netz am Switch und der DSL-Verbindung nicht vermitteln.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.5.4 Standleitungsbetrieb einrichten

Sie können den EBW-H100 so einstellen, dass die zuvor konfigurierte DSL-Verbindung dauerhaft aufrecht erhalten bleibt. In diesem Betriebsmodus wird die Verbindung sofort nach dem Einschalten aufgebaut. Das Gerät prüft die Verbindung periodisch auf ihre Funktion. Die Verbindungsüberprüfung kann entweder über eine DNS-Abfrage eines Hostnamens oder über Ping an einen Host durchgeführt werden.

Konfiguration mit Web-Interface (Menü „LAN (ext)“, Seite „DSL“)

Um die **Standleitung einzurichten**, aktivieren die Checkbox „Verbindung sofort aufbauen und dauerhaft halten“.

Geben Sie, falls notwendig, eine andere Zeit in Minuten zur **Verbindungsüberprüfung** in das Eingabefeld „Zeitintervall der Verbindungsüberprüfung“ ein. Die Werkseinstellung ist 5 Minuten. Wird nach dieser Zeit eine geschlossene Verbindung festgestellt, versucht der EBW-H100 nach einer Minute die Verbindung neu aufzubauen. Schlägt der Versuch fehl, wird nach 5 Minuten erneut versucht, die Verbindung neu aufzubauen. Der nächste Versuch findet nach 30 Minuten statt, schlägt auch dieser Versuch fehl, versucht das Gerät alle 60 Minuten die Verbindung neu aufzubauen.

Wählen Sie die **Methode zur Verbindungsüberprüfung** in der Auswahl „Art der Verbindungsüberprüfung“ aus und geben Sie einen Hostnamen oder eine IP-Adresse an. Wenn die Checkbox „Bestehende PPP-Verbindung im Fehlerfall erneut aufbauen“ markiert ist, sorgt ein fehlgeschlagener Ping oder DNS-Request dafür, dass eine eventuell bestehende Verbindung abgebaut wird. Auf jeden Fall wird anschließend versucht, wieder eine Verbindung aufzubauen.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.5.5 Periodischen DSL-Verbindungsaufbau einrichten

Der EBW-H100 kann die zuvor konfigurierte DSL-Verbindung zeitgesteuert auf und abbauen. Die DSL-Verbindung wird täglich zu einer bestimmten Uhrzeit aufgebaut und zu einer anderen Uhrzeit wieder abgebaut.

Mit dieser Funktion werden jeweils einzelne Ereignisse ausgelöst, unabhängig davon ob bereits andere Zeiten für den Verbindungsabbau definiert wurden. Beispiel: Wenn Sie bereits einen täglichen Verbindungsabbau um 14:00 Uhr und ein täglichen Verbindungsaufbau um 16:00 Uhr einstellen, so können andere Einstellungen und Ereignisse auch innerhalb dieses Zeitraums einen Verbindungsaufbau auslösen, z.B. ein Paket, dass dem Wählfilter entspricht. Ebenso wird die Verbindung abgebaut, falls z.B. die konfigurierte „Idle Time“ abgelaufen ist.

Konfiguration mit Web-Interface (Menü „LAN (ext)“, Seite „DSL“)

Um eine **Verbindung zu einer bestimmten Uhrzeit täglich aufzubauen**, aktivieren Sie die Checkbox „Verbindung täglich automatisch aufbauen um“ und geben Sie eine Uhrzeit für den Verbindungsaufbau in die Eingabefelder für Stunden und Minuten ein.

Um eine **Verbindung zu einer bestimmten Uhrzeit täglich abzubauen**, aktivieren Sie die Checkbox „Verbindung täglich automatisch abbauen um“ und geben Sie eine Uhrzeit für den Verbindungsabbau in die Eingabefelder für Stunden und Minuten ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.5.6 Routing

Das Routing ist die Kernfunktion des EBW-H100. Routing bedeutet, dass ankommende Datenpakete nach bestimmten, von Ihnen definierten Regeln an bestimmte Netzwerkgeräte weiter vermittelt werden.

Die Routen bestimmen, wohin Pakete weitergeleitet werden. Über eine Netzadresse und die Netzmaske wird unterschieden, ob eine Route auf ein IP-Paket angewendet wird oder nicht. Trifft ein Paket ein, für dessen Ziel eine Route existiert, so leitet das Gerät das Paket an die in der Route definierte Gateway-Adresse weiter.

Sie können eine Default-Route angeben. Alle eingehenden Pakete, die keiner Route zugeordnet werden können, werden an dieses Gateway gesendet. Wenn Sie ein DSL-Modem an die LAN ext-Schnittstelle angeschlossen haben, können Sie die Default-Route auf das DSL-Modem setzen.

Weiterhin wird das Verfahren der Network Address Translation unterstützt. Wenn NAT aktiv ist, ersetzt das Gerät die Absenderadresse der Pakete einer ausgehenden Verbindung durch seine Eigene. Die eigentliche Absenderadresse speichert das Gerät in seiner NAT-Tabelle. Empfängt es ein Antwortpaket der Gegenstelle dieser Verbindung, so ersetzt es die Zieladresse des Pakets durch die des ursprünglichen Absenders.

ⓘ Auf Grund der „Stateful Firewall“ kann es zu Verzögerungen kommen bis Änderungen an diesen Funktionen wirksam werden. Dies kann der Fall sein, wenn bereits Verbindungen bzw. Verbindungsversuche stattgefunden haben.

Konfiguration mit Web-Interface (Menü „LAN (ext)“, Seite „Routing“)

Um eine **IPv4-Default-Route zu setzen**, aktivieren Sie die Checkbox „Default Route setzen zu Gateway“ und geben Sie dahinter das Default-Gateway an. Im DSL-Betrieb ist das Eingabefeld nicht sichtbar.

Um eine **IPv6-Default-Route zu setzen**, aktivieren Sie die Checkbox „IPv6-Default Route setzen zu Gateway“ und geben Sie dahinter das Default-Gateway an. Im DSL-Betrieb ist das Eingabefeld nicht sichtbar.

Um **NAT für eingehende Pakete zu deaktivieren**, deaktivieren Sie die Checkbox „NAT für eingehende IPv4-Pakete aktivieren“. Das kann im LAN-Betrieb sinnvoll sein, wenn die gerouteten Pakete nicht verändert werden sollen.

Um **NAT für ausgehende Pakete zu deaktivieren**, deaktivieren Sie die Checkbox „NAT für ausgehende IPv4-Pakete aktivieren“. Das kann im LAN-Betrieb sinnvoll sein, wenn die gerouteten Pakete nicht verändert werden sollen.

ⓘ Der Router gibt bei aktivierter Firewall automatisch eigene Dienste (z.B. DNS, VPN, NTP, etc.) frei. Wenn Sie die Checkbox „NAT für ausgehende IPv4-Pakete aktivieren“ deaktivieren, müssen diese Dienste manuell in der Firewall zugelassen werden.

Um eine **neue Route hinzuzufügen**, geben Sie Abschnitt „Neue Route hinzufügen“ die Netzadresse, die dazugehörige Netzmaske und ein Gateway in die jeweiligen Felder für IPv4 oder IPv6 ein. Alle Felder müssen ausgefüllt werden, damit eine neue Route für die jeweilige IP-Version in die Tabelle übernommen wird. Übernehmen Sie die Route, indem Sie auf „OK“ klicken.

Um eine **bestehende Route zu löschen**, aktivieren Sie unter „Bestehende Routen“ die Checkbox der Route(n), die gelöscht werden soll(en).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.5.7 Wählfilter einrichten

Mit dem Wählfilter kann der Netzwerkverkehr beschränkt werden, der einen Verbindungsaufbau auslösen kann. Ohne Wählfilter lösen alle Pakete mit externem Ziel einen Verbindungsaufbau aus. Ist der Wählfilter aktiv, können nur durch die Regeln erlaubte Pakete einen Verbindungsaufbau auslösen.

Konfiguration mit Web-Interface (Menü „LAN (ext)“, Seite „Wählfilter“)

Um den Wählfilter einzuschalten, aktivieren Sie die Checkbox „Wählfilter für LAN (ext)-Schnittstelle aktivieren“.

Um **Verbindungen über ein bestimmtes Protokoll zuzulassen**, wählen Sie im Abschnitt „Neue Regel erstellen“ in der Dropdown-Liste „Protokoll“ das zugelassene Protokoll aus.

Um **Verbindungen von bestimmten Absender-IP-Adressen zuzulassen**, tragen Sie im Feld „Absender-IP-Adresse“ die zugelassene Absender-IP-Adresse ein.

Um **Verbindungen zu bestimmten Ports zuzulassen**, tragen Sie im Feld „Ziel-Port“ den zugelassenen Ziel-Port ein.

Um **Verbindungen zu bestimmten IP-Adressen zuzulassen**, tragen Sie im Feld „Ziel-IP-Adresse“ die zugelassene Ziel-IP-Adresse ein.

Optional können Sie mit der Checkbox „DNS-Anfragen der Absender-IP-Adresse dürfen eine Verbindung initiieren“ **erlauben, dass DNS-Anfragen** der festgelegten Absender-IP-Adressen **einen Verbindungsaufbau auslösen** dürfen.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um einzelne **Wählfilterregeln temporär auszuschalten**, deaktivieren Sie im Abschnitt „Diese Datenpakete dürfen einen Dial-Out initiieren“ die Checkbox in der Spalte „aktiv“. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

Um **eine oder mehrere Regeln** zu **löschen**, aktivieren Sie im Abschnitt „Diese Datenpakete dürfen einen Dial-Out initiieren“ die Checkbox in der Spalte „löschen“. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

12.5.8 Firewall-Regel erstellen oder löschen

Für alle Verbindungen über die LAN ext-Schnittstelle steht eine Firewall zur Verfügung. Sie dient dazu, unerwünschten Datenverkehr zu verhindern. Die Logik der Firewall ist, dass jeglicher Datenverkehr verboten ist, der nicht explizit durch eine Regel erlaubt wurde. Wenn Sie die Firewall für die Verbindungsart „Dial-Out“ einschalten, sind nur noch Verbindungen möglich, die durch Firewall-Regeln erlaubt werden. Alle anderen Verbindungen werden blockiert.

ⓘ Auf Grund der „Stateful Firewall“ kann es zu Verzögerungen kommen bis Änderungen an diesen Funktionen wirksam werden. Dies kann der Fall sein, wenn bereits Verbindungen bzw. Verbindungsversuche stattgefunden haben.

Konfiguration mit Web-Interface (Menü „LAN (ext)“, Seite „Firewall“)

Um die **Firewall für IPv4-Verbindungen über die LAN ext-Schnittstelle zu aktivieren**, aktivieren Sie die Checkbox „Firewall für LAN (ext)-Schnittstelle aktivieren“.

Um die **Firewall für IPv6- Verbindungen über die LAN ext-Schnittstelle zu aktivieren**, aktivieren Sie die Checkbox „IPv6-Firewall für LAN (ext)-Schnittstelle aktivieren“.

ⓘ Es wird dringend empfohlen, die Firewall für IPv6 immer aktiviert zu lassen, auch wenn IPv6 nicht genutzt wird.

Um eine **Regel für eine zugelassene IP-Verbindung zu erstellen**, gehen Sie wie folgt vor.

Wählen Sie im Abschnitt „Neue Verbindung zulassen“ in der Dropdown-Liste „Datenrichtung“ für die Regel eine **Datenrichtung** aus.

Bestimmen Sie das **Protokoll der zugelassenen Verbindung** in der Dropdown-Liste „Protokoll“.

Wählen Sie die **IP-Version**, für welche die Regel gelten soll, in der Dropdown-Liste „IP-Version“.

Geben Sie in den Eingabefeldern „**Absender-IP-Adresse**“, „**Ziel-IP-Adresse**“ und **Ziel-Port** die weiteren Spezifikationen für die durch den Router zugelassen Verbindungen an. Es können Regeln erstellt werden, die nicht nur für einzelne Maschinen (Hosts) gelten, sondern für ganze Netze. In dem Fall muss die Netzmaske nach dem „/“ eingegeben werden.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um einzelne **Firewall-Regeln temporär auszuschalten**, deaktivieren Sie im Abschnitt „Zugelassene Verbindungen …“ die Checkbox in der Spalte „aktiv“ in der Übersicht der Firewall-Regeln. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

Um **eine oder mehrere Regeln** zu **löschen**, aktivieren Sie die Checkbox in der Spalte „löschen“ in der Übersicht der Firewall-Regeln. Klicken Sie auf „OK“, um die Einstellung zu übernehmen.

12.5.9 IP-Forwarding-Regel erstellen oder löschen

IP-Forwarding-Regeln legen zusätzliche IP-Adressen an der LAN (ext)-Schnittstelle an, wenn auf der Seite „LAN (ext)“ die Option „statische IP-Adresse“ gewählt wurde. Pakete an eine dieser IP-Adressen werden an die mit ihr verknüpfte IP-Adresse im lokalen LAN weitergeleitet.

ⓘ Die Firewall gilt auch für diese zusätzlichen IP-Adressen! Daher müssen diese zusätzlichen IP-Adressen im Menü „LAN (ext)“auf der Seite „Firewall“ zugelassen werden, wenn die Firewall aktiviert ist. Ansonsten würden alle Pakete verworfen, die an diese IP-Adressen gerichtet sind.

Konfiguration mit Web-Interface (Menü „LAN (ext)“, Seite „IP-Forwarding“)

Um **IP-Forwarding** zu **aktivieren**, aktivieren Sie die Checkbox „IP-Forwarding aktivieren“.

Um eine **IP-Forwarding-Regel** zu **erstellen**, geben Sie im Abschnitt „Neue Regel erstellen“ die zusätzliche IP-Adresse mit Netzmaske in das Feld „LAN (ext) IP-Adresse“ und die Zieladresse in das Feld „Ziel-IP-Adresse“ ein. An diese Adresse werden dann die Pakete an die zusätzliche Adresse weitergeleitet. Übernehmen Sie den Eintrag, indem Sie auf „OK“ klicken.

Um eine **bereits erstellte Regel** zu **löschen**, aktivieren Sie unter „Bestehende Regeln“ die Checkbox der Regel(n), die gelöscht werden soll(en).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.5.10 Port-Forwarding-Regel erstellen oder löschen

Bei aktiviertem Port-Forwarding leitet der Router vom WAN eingehende Pakete an die Maschinen im LAN weiter, die in den Port-Forwarding-Regeln festgelegt wurden.

Aus dem WAN ist nur die WAN-IP-Adresse des EBW-H100 erreichbar, wenn NAT für ins WAN gehende Pakete aktiviert ist. Anhand dieser IP-Adresse können die lokalen Endgeräte im Netz des Geräts mit Hilfe von Port-Forwarding trotzdem erreicht werden. Pakete aus dem WAN, die an die WAN-IP-Adresse an einem Port x gesendet werden, können an eine Maschine mit der IP-Adresse Y an den Port y weitergeleitet werden. Wird alternativ ein ganzer Port-Bereich angegeben, werden die Pakete an dieselben Ports der Ziel-IP-Adresse weitergeleitet. Es ist möglich, die Regeln so anzulegen, dass sie nur für WAN-Verbindungen, nur für OpenVPN-Verbindungen oder generell gelten.

ⓘ Auf Grund der „Stateful Firewall“ kann es zu Verzögerungen kommen bis Änderungen an diesen Funktionen wirksam werden. Dies kann der Fall sein, wenn bereits Verbindungen bzw. Verbindungsversuche stattgefunden haben.

Konfiguration mit Web-Interface (Menü „LAN (ext)“, Seite „Port-Forwarding“)

Um das **Port-Forwarding** zu **aktivieren**, aktivieren Sie die Checkbox „Port-Forwarding für LAN (ext)-Schnittstelle aktivieren“.

Um eine **Port-Forwarding-Regel** zu **erstellen**, wählen Sie im Abschnitt „Neue Regel erstellen“ das Protokoll aus und geben den Port bzw. Bereich der Ports für die am EBW-H100 eingehenden Pakete an. Geben Sie eine IP-Adresse für das Umleitungsziel im Eingabefeld „an IP-Adresse“ und einen Port im Eingabefeld „an Port“ ein; an diese Adresse und diesen Port werden die Pakete weitergeleitet. Bei Angabe eines Port-Bereichs ist kein Ziel-Port erforderlich, da dieser immer dem Port-Bereich im WAN entspricht. Wählen Sie in der Dropdown-Liste „anwenden“ noch aus, ob die Regel immer, nur für WAN-Verbindungen oder nur für OpenVPN-Verbindungen gelten soll.

Um eine **bereits erstellte Regel** zu **deaktivieren**, deaktivieren Sie die Checkbox „aktiv“ der entsprechenden Regel und klicken Sie anschließend auf „OK“.

Um eine **bereits erstellte Regel** zu **löschen**, aktivieren Sie die Checkbox „löschen“ der entsprechenden Regel und klicken Sie anschließend auf „OK“.

Die Regeln in der Liste werden von oben nach unten abgearbeitet. Sollten sich also zwei Regeln widersprechen (z.B. zweimal derselbe Port), so wird nur die Regel ausgeführt, die weiter oben in der Liste steht.

12.5.11 Exposed Host festlegen

Optional können alle Pakete, die keiner Port-Forwarding-Regel entsprechen, an einen vorbestimmten Rechner im LAN, den „Exposed Host“, weitergeleitet werden (z.B. zu Diagnosezwecken). Der „Exposed Host“ erhält alle Pakete, die nicht aus dem lokalen Netz des EBW-H100 angefordert wurden oder durch eine Port-Forwarding-Regel nicht bereits an einen Teilnehmer im lokalen Netz weitergeleitet wurden. Wird kein „Exposed Host“ konfiguriert, werden diese eingehenden Pakete verworfen.

Konfiguration mit Web-Interface (Menü „LAN (ext)“, Seite „Port-Forwarding“)

Um einen **„Exposed Host“** zu **definieren**, geben Sie im Eingabefeld „Exposed Host“ die IP-Adresse eines Rechners im LAN ein, der von außen über alle Ports erreichbar sein soll.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.6 VPN

12.6.1 VPN Allgemein

Ein VPN (virtuelles privates Netzwerk) wird eingesetzt, um IP-Endgeräte oder ganze Netzwerke gesichert miteinander zu verbinden. Daten werden damit fälschungssicher an ein Ziel übertragen und sind für Dritte nicht lesbar.

Sie können den EBW-H100 für eine OpenVPN-, PPTP-, IPsec- oder GRE-Verbindung konfigurieren.

Die genaue Vorgehensweise zum Erstellen einer Zertifikatsstruktur und Konfigurieren eines VPN-Teilnehmers ist in einer Reihe von Konfigurations-handbüchern beschrieben. Diese sind über unsere Webseite (http://www.insys-icom.de/cg/) oder unseren Support (support@insys-icom.de) erhältlich.

12.6.2 OpenVPN Allgemein

Sie können den EBW-H100 als OpenVPN-Server oder als OpenVPN-Client nutzen.

Abbildung 4 zeigt eine Beispielkonfiguration für eine OpenVPN-Verbindung. Hier ist ein EBW-H100 als OpenVPN-Server und ein zweiter als OpenVPN-Client konfiguriert. Sowohl Client als auch Server können durch beliebige OpenVPN-fähige Geräte ersetzt werden. Im Beispiel besteht eine WWAN-Verbindung zwischen den beiden Geräten. Über diese WWAN-Verbindung ist eine OpenVPN-Verbindung aufgebaut.

Sobald eine WAN-Verbindung aufgebaut wurde, können IP-Verbindungen zwischen den beiden Netzwerken aufgebaut werden. OpenVPN nutzt eine vorhandene WAN-Verbindung, um einen VPN-Tunnel aufzubauen. Ein Tunnel besteht aus einer IP-Verbindung, in deren Payload alle zu tunnelnden Pakete transportiert werden. OpenVPN stellt für den Datenverkehr eine virtuelle Netzwerkkarte zur Verfügung, über die dann der verschlüsselte Datenverkehr gesendet wird.

Abbildung 4: OpenVPN-Verbindung und IP-Adressen in der Beispielkonfiguration

In der Beispielkonfiguration haben die Endpunkte der OpenVPN-Verbindung die IP-Adressen 10.1.0.1 und 10.1.0.2. Der VPN-Tunnel wird innerhalb einer schon bestehenden WAN-Verbindung aufgebaut. Den OpenVPN-Clients und -Servern muss auch bekannt sein welches Netzwerk sich hinter den jeweiligen Tunnelenden befindet. In der Beispielkonfiguration ist das auf der einen Seite das Netzwerk 192.168.200.0/24. Auf der anderen Seite ist dies das Netzwerk 192.168.1.0/24. Sobald der Tunnel aufgebaut ist, werden Daten für diese Zielnetze durch den OpenVPN-Tunnel übertragen. Sollen nur Daten über die WAN-Schnittstelle übertragen werden, deren Ziel im Netzwerk hinter dem Tunnelende liegt, empfiehlt es sich, nach erfolgreicher Konfiguration die Firewall zu aktivieren. Damit kann die Kommunikation auf den Port beschränkt werden, über den der OpenVPN-Tunnel aufgebaut wird (Standardeinstellung UDP-Port 1194).

Der EBW-H100 unterstützt verschiedene Authentifizierungsmethoden beim Aufbau des VPN-Tunnels:

Authentifizierungsart	Verwendung	Besonderheit
Keine	Zu Testzwecken und zum Verbinden von Netzwerken ohne Verschlüsselung.	Keine verschlüsselte Verbindung. Am Server können sich nicht mehrere Clients gleichzeitig anmelden.
Statischer Schlüssel	Zum verschlüsselten Verbinden von je einem Client und Server in kleineren Anwendungen	Verschlüsselte Verbindung. Am Server können sich nicht mehrere Clients gleichzeitig anmelden.
Benutzername/Kennwort und gemeinsames CA-Zertifikat (nur beim OpenVPN-Client einstellbar)	Zum verschlüsselten Verbinden von einem oder mehreren Clients zu einem OpenVPN-Server.	Flexible Anwendung für mehrere Clients. Nicht mit dem EBW-H100 als OpenVPN-Server nutzbar.
Zertifikatsbasiert, jeder Teilnehmer hat ein individuelles Zertifikat und Schlüssel.	Zum verschlüsselten Verbinden von einem oder mehreren Clients zu einem OpenVPN-Server.	Lösung für maximale Sicherheit, allerdings etwas aufwändiger zu konfigurieren. Dies ist der empfohlene Betriebsmodus.

Tabelle 9: Authentifizierungsmethoden bei OpenVPN

Für detaillierte Informationen und Troubleshooting empfehlen wir auch die Webseite von OpenVPN: http://openvpn.net/howto.html

12.6.3 OpenVPN-Server einrichten

Sie können den EBW-H100 als OpenVPN-Server nutzen, wenn Sie z.B. vertrauliche Daten über ein unsicheres Netzwerk übertragen wollen. Dieser Abschnitt beschreibt die Einrichtung eines OpenVPN-Servers. Die Grundeinstellungen sind ab Werk auf sinnvolle Standardwerte gesetzt, die Sie aber unter besonderen Umständen abändern können. Hier legen Sie fest, über welchen Port der EBW-H100 den OpenVPN-Tunnel erzeugt und ob die OpenVPN-Übertragung mit dem UDP oder TCP-Protokoll umgesetzt wird. Weiterhin legen Sie hier fest, ob den Clients das Server-Netz mitgeteilt wird, die Gegenstelle ihre IP-Adresse ändern darf, LZO-Komprimierung verwendet wird, Pakete vor dem Tunneln maskiert werden, welcher Verschlüsselungsalgorithmus während der Übertragung verwendet wird, wie groß die Tunnelpakete sein sollen und in welchen Zeitintervallen der OpenVPN-Server VPN-Pings verschickt. Zusätzlich haben Sie hier die Möglichkeit, den OpenVPN-Status anzuzeigen, die momentane Konfigurationsdatei anzuzeigen, eine Konfiguration für eine OpenVPN-Gegenstelle zu erzeugen sowie ein Log der letzten Verbindung anzuzeigen. Die erzeugte Konfiguration können Sie z.B. zum Erstellen einer OpenVPN-Konfigurationsdatei verwenden, die als Grundlage für den Betrieb einer OpenVPN-Instanz auf einem Client-PC dienen kann. Das OpenVPN-Paket für Windows-Clients können Sie auf der Webseite von INSYS icom herunterladen (www.insys-icom.de/treiber).

Dieses Programm dient als Gegenstelle, wenn Sie die OpenVPN-Verbindung von einem Windows-PC aus aufbauen wollen.

Konfiguration mit Web-Interface (Menü „Dial-In“/„Dial-Out“/„LAN (ext)“, Seite „OpenVPN-Server“)

Um bei **einer Verbindung den OpenVPN-Server** zu verwenden, aktivieren Sie die Checkbox „OpenVPN-Server aktivieren“.

Um den **Status des OpenVPN-Servers anzuzeigen**, wählen Sie den Link „OpenVPN-Server Status“.

Um die **Meldungen des letzten Verbindungsvorgangs anzuzeigen**, wählen Sie den Link „Verbindungs-Log der letzten Verbindung“.

Um die **Konfigurationsdatei des Routers als OpenVPN-Server anzuzeigen**, wählen Sie den Link „Konfigurationsdatei anzeigen“.

Um eine **Beispielkonfiguration für einen OpenVPN-Client anzuzeigen**, wählen Sie den Link „Beispielkonfigurationsdatei für die Gegenstelle erstellen“.

Um den **lokalen Port am EBW-H100 sowie den Port an der Gegenstelle festzulegen**, geben Sie in den Eingabefeldern „Tunneln über Port (lokal / Gegenstelle)“ einen Wert für die gewünschten Ports an (Voreinstellung 1194).

Das **Protokoll der OpenVPN-Übertragung** wählen Sie mit den Radiobuttons „UDP“ oder „TCP“ aus. Es empfiehlt sich, UDP zu verwenden, um die Latenz gering zu halten.

Damit den **Clients die Route zum Netzwerk hinter dem Server mitgeteilt** wird, aktivieren Sie die Checkbox „Server-Netz den Clients mitteilen“. Wird diese Einstellung deaktiviert, kann eine Kommunikation nur aus dem Netzwerk des Servers initiiert werden.

Damit **entfernte OpenVPN-Gegenstellen während einer Verbindung Ihre IP-Adresse verändern können** („**Floating**“), aktivieren Sie die Checkbox „Gegenstelle darf Ihre IP-Adresse dynamisch ändern (float)“. Diese Einstellung ist standardmäßig aktiv.

Um die **LZO-Komprimierung an- oder abzuschalten**, aktivieren oder deaktivieren Sie die Checkbox „LZO-Komprimierung aktivieren“. Werden bereits stark komprimierte Daten (z.B. jpg) übertragen, hat die Komprimierung kaum Effekt, werden hingegen gut komprimierbare Daten (z.B. Text) übertragen, kann die Komprimierung eine deutliche Reduzierung des übertragenen Datenvolumens erreichen. Schalten Sie die Kompression ab, falls Ihre Gegenstelle keine LZO-Kompression unterstützt.

Um die **Pakete mit der virtuellen Tunnel-IP-Adresse zu maskieren**, aktivieren Sie die Checkbox „Pakete vor dem Tunnel maskieren“. Der Empfänger des Paketes sieht dann als Absender die IP-Adresse des Tunnelendes und nicht die des eigentlichen Absenders.

Um eine **andere Verschlüsselungsmethode** als die voreingestellte für die OpenVPN-Verbindung zu verwenden, wählen Sie in der Dropdown-Liste „Verschlüsselungs-Algorithmus“ eine der Verschlüsselungsmethoden. Zur Verfügung stehen Blowfish 128 Bit, DES 64 Bit, DES EDE 128 Bit, DES EDE3 192 Bit, DESX 192 Bit, CAST5 128 Bit, IDEA 128 Bit, RC2 128 Bit, RC2 40 Bit, RC2 64 Bit, AES 128 Bit, AES 192 Bit, AES 256 Bit und keine Verschlüsselung.

Um einen **anderen Hash-Algorithmus** als den voreingestellten für die OpenVPN-Verbindung zu verwenden, wählen Sie in der Dropdown-Liste „Hash-Algorithmus“ einen der Hash-Algorithmen. Zur Verfügung stehen SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 und kein Hash-Algorithmus.

Um die **Ausführlichkeit der Meldungen im Verbindungslog** einzustellen, geben Sie im Feld „Log-Level“ den Grad der Ausführlichkeit ein, wobei „0“ das Führen des Logs komplett deaktiviert und „9“ die meisten Details aufzeichnet.

Um eine bestimmte **Fragmentierungsgröße für die OpenVPN-Tunnelpakte** in Bytes vorzugeben, verwenden Sie das Eingabefeld „Fragmentierung der Tunnelpakete“. Geben Sie hier die gewünschte maximale Paketgröße in Bytes an. Geben Sie hier keinen Wert an, haben die OpenVPN-Pakete eine maximale Größe von 1500 Bytes. Die tatsächlich pro Paket übertragene Nutzdatenmenge ist geringer, da durch OpenVPN ein „Protokoll-Overhead“ entsteht, d.h. die zu übertragenden Protokoll-Informationen verbrauchen einen Teil der Paketgröße.

Um das **Intervall bis zur Schlüsselerneuerung anzupassen**, verwenden Sie das Eingabefeld „Intervall bis zur Schlüsselerneuerung“. Geben Sie hier das Zeitintervall in Sekunden ein, nach dessen Ablauf neue Schlüssel erzeugt werden.

Um das **VPN-Ping-Intervall anzupassen**, verwenden Sie das Eingabefeld „Ping-Intervall“. Geben Sie hier das Zeitintervall in Sekunden ein, in dem der OpenVPN-Server des EBW-H100 Ping-Pakete an die OpenVPN-Gegenstelle versendet. Der regelmäßige Ping dient zum Offenhalten der Verbindung über diverse Router und Gateways, die evtl. an der Verbindung beteiligt sind und bei fehlender Kommunikation den Kanal schließen würden.

Um das **Ping-Restart-Intervall anzupassen**, verwenden Sie das Eingabefeld „Ping-Restart-Intervall“. Geben Sie hier ein, nach wie vielen Sekunden der Tunnel neu aufgebaut werden soll, wenn während der gesamten Zeit kein Ping von der Gegenstelle angekommen ist. Mit dem Wert „0“ wird der Tunnel nie abgebaut, auch wenn kein Ping mehr empfangen wird.

ⓘ Das Ping-Intervall und das Ping-Restart-Intervall müssen zusammenpassen. Typische Werte sind 30 und 60 (default). Das Ping-Intervall sollte max. die Hälfte des Ping-Restart-Intervalls betragen. Bei schlechten WAN-Verbindungen empfehlen wir das Ping-Intervall zu reduzieren und ggf. das Ping-Restart-Intervall zu erhöhen.

Um die **Authentifizierung mit Zertifikaten zu konfigurieren**, wählen Sie den Radiobutton „Authentifizierung mit Zertifikaten“. Dabei wird unter der Option angezeigt, ob die einzelnen Zertifikate und Schlüssel vorhanden sind (grüner Haken) oder nicht (rotes Kreuz). Vorhandene Zertifikate können auch heruntergeladen (blauer Pfeil) oder wieder gelöscht (rotes Kreuz auf weißem Kästchen) werden. Der private Schlüssel kann nur gelöscht werden. Markieren Sie die Checkbox „tls-auth aktivieren“, um zusätzlich zu den Zertifikaten auch einen statischen Schlüssel zu verwenden. In diesem Fall wird der im Abschnitt „Authentifizierung mit statischem Schlüssel“ gespeicherte statische Schlüssel verwendet. Optional kann in der Dropdown-Liste „Benutzungsrichtung des Schlüssels“ eine Richtung vorgegeben werden (siehe dazu den im Anschluss folgenden Hinweis). Markieren Sie die Checkbox „Kommunikation zwischen Clients erlauben“, um auch den Clients eine Kommunikation untereinander zu ermöglichen. Definieren Sie den IP-Adress-Pool für die Clients in den Feldern „IPv4-Adress-Pool / Netzmaske“ bzw. „IPv6-Adress-Pool / Netzmaske“. Um eine neue Route zu einem Client-Netzwerk anzulegen, geben Sie im Abschnitt „Neue Route zu Client-Netzwerk anlegen“ den Common Name des Clients in das Feld „Name im Zertifikat“ sowie seine Netzadresse und Netzmaske in die Felder „IPv4-Netzadresse / Netzmaske“ bzw. „IPv6-Netzadresse / Netzmaske“ ein. Geben Sie optional die VPN-IPv4-Adresse für das Tunnelende eines Clients in das Feld „VPN-IPv4-Adresse“ ein. Es wird jedem Tunnelende immer jeweils eine IPv4- und eine IPv6-Adresse zugeteilt, auch wenn der Tunnel einer IP-Version gar nicht benutzt wird. Klicken Sie auf „OK“, um die neue Route zu übernehmen. Bestehende Routen können Sie löschen, indem Sie die Checkbox in der Spalte „löschen“ der entsprechenden Route markieren und auf „OK“ klicken.

ⓘ Wird tls-auth benutzt, kann optional angegeben werden, dass der statische Schlüssel nur für eine bestimmte Richtung benutzt werden soll. Wichtig dabei ist, dass diese Einstellung mit der VPN-Gegenstelle abgestimmt ist, d.h. bei beiden ist keine Richtung eingestellt oder die Einstellungen sind komplementär (0/1 bzw. 1/0).

ⓘ Eine Verknüpfung einer Netzadresse mit „DEFAULT“ als „Common Name“ kann als „Standard-Route“ angelegt werden. Sie wird immer als Route benutzt, wenn sich ein Client mit einem Zertifikat anmeldet, für dessen „Common Name“ noch keine Verknüpfung eingetragen ist.

Um die **Authentifizierung mit statischem Schlüssel zu konfigurieren**, wählen Sie den Radiobutton „Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel“. Dabei wird unter der Option angezeigt, ob der statische Schlüssel vorhanden ist (grüner Haken) oder nicht (rotes Kreuz). Ein vorhandener Schlüssel kann auch heruntergeladen (blauer Pfeil) oder wieder gelöscht (rotes Kreuz auf weißem Kästchen) werden. Ist kein Schlüssel vorhanden, wird die Gegenstelle weder authentifiziert noch wird der Datenverkehr durch den OpenVPN-Tunnel verschlüsselt. Klicken Sie auf den Link „Statischen Schlüssel neu erstellen“, um einen neuen statischen Schlüssel zu erstellen. Dieser statische Schlüssel muss dann heruntergeladen und auch auf die Gegenstelle hochgeladen werden. Für einen funktionierenden Tunnel müssen bei dieser Authentifizierungsart beide OpenVPN-Gegenstellen über den gleichen statischen Schlüssel verfügen. Geben Sie die IP-Adresse oder den Domain-Namen der Gegenstelle in das Feld „IP-Adresse oder Domainname der Gegenstelle“ ein. Optional können Sie die IP-Adresse oder den Domain-Namen einer alternativen Gegenstelle in das Feld „Alternative Gegenstelle“ eingeben. Geben Sie die IP-Adresse des lokalen Tunnelendes in das Feld „IPv4-Tunneladresse lokal“ bzw. „IPv6-Tunneladresse lokal“ und die des entfernten Tunnelendes in das Feld „IPv4-Tunneladresse der Gegenstelle“ bzw. „IPv6-Tunneladresse der Gegenstelle“ ein. Geben Sie die Adresse sowie die zugehörige Netzmaske des Netzwerks hinter dem OpenVPN-Tunnel in die Felder „IPv4-Netzadresse hinter dem Tunnel“ bzw. „IPv6-Netzadresse hinter dem Tunnel“ und „IPv4-Netzmaske hinter dem Tunnel“ bzw. „IPv6-Netzmaske hinter dem Tunnel“ ein.

Um alle oben getroffenen **Einstellungen zu übernehmen**, klicken Sie auf die Schaltfläche „OK“.

Um ein **Zertifikat oder einen Schlüssel hochzuladen**, klicken Sie im Abschnitt „Schlüssel oder Zertifikate laden“ auf die Schaltfläche „Durchsuchen…“ (Schaltfläche abhängig vom verwendeten Browser). Wählen Sie dann im Fenster „Datei hochladen“ die gewünschte Datei auf dem entsprechenden Datenträger aus und klicken Sie auf die Schaltfläche „Öffnen“. Falls die Datei verschlüsselt ist, müssen Sie noch das Kennwort in das Feld „Kennwort (nur bei verschlüsselter Datei)“ eintragen. Klicken Sie dann auf die Schaltfläche „OK“ um die Datei hochzuladen.

12.6.4 OpenVPN-Client einrichten

Sie können den EBW-H100 als OpenVPN-Client nutzen, um sich mit einem OpenVPN-Server über ein unsicheres Netz zu verbinden. Dieser Abschnitt beschreibt die Einrichtung eines OpenVPN-Clients. Die Grundeinstellungen sind ab Werk auf sinnvolle Standardwerte gesetzt, die Sie aber an das VPN anpassen müssen, mit dem sich der EBW-H100 verbinden soll. Hier legen Sie fest, mit welcher IP-Adresse oder Domain und über welche Ports der OpenVPN-Tunnel aufgebaut wird, und ob die OpenVPN-Übertragung mit dem UDP- oder TCP-Protokoll umgesetzt wird. Wenn die Gegenstelle nur über einen Proxy-Server erreicht werden kann, kann dieser entsprechend konfiguriert werden. Weiterhin legen Sie hier fest, ob eine Default-Route gesetzt wird, die lokale Adresse und der Port fixiert werden, die Gegenstelle ihre IP-Adresse ändern darf, LZO-Komprimierung verwendet wird, Pakete vor dem Tunneln maskiert werden, welcher Verschlüsselungsalgorithmus während der Übertragung verwendet wird, wie groß die Tunnelpakete sein sollen und in welchen Zeitintervallen der OpenVPN-Client VPN-Pings an den Server verschickt. Zusätzlich haben Sie hier die Möglichkeit, den OpenVPN-Status, die momentane Konfigurationsdatei, eine Konfiguration für eine OpenVPN-Gegenstelle (den OpenVPN-Server) und ein Log der letzten Verbindung anzuzeigen.

Konfiguration mit Web-Interface (Menü „Dial-In“/„Dial-Out“/„LAN (ext)“, Seite „OpenVPN-Client“)

Um bei **einer Verbindung den OpenVPN-Client** zu verwenden, aktivieren Sie die Checkbox „OpenVPN-Client aktivieren“.

Um den **Status des OpenVPN-Clients anzuzeigen**, wählen Sie den Link „OpenVPN-Client Status“.

Um die **Meldungen des letzten Verbindungsvorgangs anzuzeigen**, wählen Sie den Link „Verbindungs-Log der letzten Verbindung“.

Um die **Konfigurationsdatei des Routers als OpenVPN-Client anzuzeigen**, wählen Sie den Link „Konfigurationsdatei anzeigen“.

Um eine **Beispielkonfiguration für einen OpenVPN-Server anzuzeigen**, wählen Sie den Link „Beispielkonfigurationsdatei für die Gegenstelle erstellen“.

Um die **IP-Adresse oder den Domainnamen der Gegenstelle zu bestimmen**, mit dem Sie den Router die OpenVPN-Verbindung aufbauen lassen, geben Sie im Feld „IP-Adresse oder Domainname der Gegenstelle“ eine IP-Adresse oder einen Domainnamen an.

Optional kann eine **alternative Gegenstelle bestimmt werden**, mit der die OpenVPN-Verbindung aufgebaut werden soll, falls die oben konfigurierte Gegenstelle nicht erreichbar ist. Geben Sie dazu im Feld „Alternative Gegenstelle“ eine IP-Adresse oder einen Domainnamen an.

Um den **lokalen Port am EBW-H100 sowie den Port an der Gegenstelle festzulegen**, geben Sie in den Eingabefeldern „Tunneln über Port (lokal / Gegenstelle)“ einen Wert für die gewünschten Ports an.

Das **Protokoll der OpenVPN-Übertragung** wählen Sie mit den Radiobuttons „UDP“ oder „TCP“ aus. Wir empfehlen, UDP zu verwenden, um die Latenz gering zu halten.

Wenn die Gegenstelle nur über einen **Proxy-Server** erreicht werden kann, geben Sie dessen IP-Adresse oder Domainnamen in das Feld „IP-Adresse oder Domainname des Proxy-Servers“ ein, wählen Sie dessen Art mit Hilfe der Radiobuttons „HTTP“ oder „SOCKS5“ und tragen Sie seinen Port in das Feld „Port“ ein. Falls der Proxy-Server eine Authentifizierung erfordert, tragen Sie die Zugangsdaten in die Felder „Benutzername“ und „Kennwort“ ein.

Um eine **Default-Route zu setzen**, aktivieren Sie die Checkbox „Default Route setzen (redirect-gateway)“. Dann wird jeglicher Datenverkehr durch den Tunnel geroutet.

Es ist nicht zwingend nötig, den **lokalen Port und die IP-Adresse der OpenVPN Verbindung** fest vorzuschreiben. Wenn Sie die Verwendung des Ports und der IP-Adresse offen lassen wollen, deaktivieren Sie die Checkbox „Lokale Adresse und Port fixieren (nobind)“.

Damit **entfernte OpenVPN-Gegenstellen während einer Verbindung Ihre IP-Adresse verändern können** („**Floating**“), aktivieren Sie die Checkbox „Gegenstelle darf Ihre IP-Adresse dynamisch ändern (float)“. Diese Einstellung ist standardmäßig aktiv.

Um die **LZO-Komprimierung an- oder abzuschalten**, aktivieren oder deaktivieren Sie die Checkbox „LZO-Komprimierung aktivieren“. Werden bereits stark komprimierte Daten (z.B. jpg) übertragen, hat die Komprimierung kaum Effekt, werden hingegen gut komprimierbare Daten (z.B. Text) übertragen, kann die Komprimierung eine deutliche Reduzierung des übertragenen Datenvolumens erreichen. Schalten Sie die Kompression ab, falls Ihre Gegenstelle keine LZO-Kompression unterstützt.

Um die **Pakete mit der virtuellen Tunnel-IP-Adresse zu maskieren**, aktivieren Sie die Checkbox „Pakete vor dem Tunnel maskieren“. Der Empfänger des Paketes sieht dann als Absender die IP-Adresse des Tunnelendes und nicht die des eigentlichen Absenders.

Um eine **andere Verschlüsselungsmethode** als die voreingestellte für die OpenVPN-Verbindung zu verwenden, wählen Sie in der Dropdown-Liste „Verschlüsselungs-Algorithmus“ eine der Verschlüsselungsmethoden. Zur Verfügung stehen Blowfish 128 Bit, DES 64 Bit, DES EDE 128 Bit, DES EDE3 192 Bit, DESX 192 Bit, CAST5 128 Bit, IDEA 128 Bit, RC2 128 Bit, RC2 40 Bit, RC2 64 Bit, AES 128 Bit, AES 192 Bit, AES 256 Bit und keine Verschlüsselung.

Um einen **anderen Hash-Algorithmus** als den voreingestellten für die OpenVPN-Verbindung zu verwenden, wählen Sie in der Dropdown-Liste „Hash-Algorithmus“ einen der Hash-Algorithmen. Zur Verfügung stehen SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 und kein Hash-Algorithmus.

Um die **Ausführlichkeit der Meldungen im Verbindungslog** einzustellen, geben Sie im Feld „Log-Level“ den Grad der Ausführlichkeit ein, wobei „0“ das Führen des Logs komplett deaktiviert und „9“ die meisten Details aufzeichnet.

Um eine bestimmte **Fragmentierungsgröße für die OpenVPN-Tunnelpakte** in Bytes vorzugeben, verwenden Sie das Eingabefeld „Fragmentierung der Tunnelpakete“. Geben Sie hier die gewünschte maximale Paketgröße in Bytes an. Geben Sie hier keinen Wert an, haben die OpenVPN-Pakete eine maximale Größe von 1500 Bytes. Die tatsächlich pro Paket übertragene Nutzdatenmenge ist geringer, da durch OpenVPN ein „Protokoll-Overhead“ entsteht, d.h. die zu übertragenden Protokoll-Informationen verbrauchen einen Teil der Paketgröße.

Um das **Intervall bis zur Schlüsselerneuerung anzupassen**, verwenden Sie das Eingabefeld „Intervall bis zur Schlüsselerneuerung“. Geben Sie hier das Zeitintervall in Sekunden ein, nach dessen Ablauf neue Schlüssel erzeugt werden.

Um das **VPN-Ping-Intervall anzupassen**, verwenden Sie das Eingabefeld „Ping-Intervall“. Geben Sie hier das Zeitintervall in Sekunden ein, in dem der OpenVPN-Client des EBW-H100 Ping-Pakete an die OpenVPN-Gegenstelle versendet. Der regelmäßige Ping dient zum Offenhalten der Verbindung über diverse Router und Gateways, die evtl. an der Verbindung beteiligt sind und bei fehlender Kommunikation den Kanal schließen würden.

Um das **Ping-Restart-Intervall anzupassen**, verwenden Sie das Eingabefeld „Ping-Restart-Intervall“. Geben Sie hier ein, nach wie vielen Sekunden der Tunnel neu aufgebaut werden soll, wenn während der gesamten Zeit kein Ping von der Gegenstelle angekommen ist. Mit dem Wert „0“ wird der Tunnel nie abgebaut, auch wenn kein Ping mehr empfangen wird.

Um zusätzlich einen **Ping per ICMP-Protokoll** an eine Domain oder eine IP-Adresse zu senden, geben Sie diese in das Eingabefeld „Zusätzlicher ICMP-Ping an“ ein. Es empfiehlt sich, hier einen Domainnamen oder eine IP-Adresse einzutragen, die nur durch den Tunnel erreichbar ist. Ist der Ping nicht erfolgreich, wird ein eventuell bestehender Tunnel abgebaut und ein neuer Tunnel aufgebaut. Das Intervall der Pings beträgt 15 Minuten.

Um die **Authentifizierung mit Zertifikaten zu konfigurieren**, wählen Sie den Radiobutton „Authentifizierung mit Zertifikaten“. Dabei wird unter der Option angezeigt, ob die einzelnen Zertifikate und Schlüssel vorhanden sind (grüner Haken) oder nicht (rotes Kreuz). Vorhandene Zertifikate können auch heruntergeladen (blauer Pfeil) oder wieder gelöscht (rotes Kreuz auf weißem Kästchen) werden. Der private Schlüssel kann nur gelöscht werden. Alternativ oder zusätzlich zu der Benutzung eines Client-Zertifikates und eines privaten Schlüssels kann eine Benutzername/Kennwort-Kombination für die Authentifizierung beim OpenVPN-Server benutzt werden (es wird jedoch auf alle Fälle das CA-Zertifikat benötigt, über das jeder Teilnehmer dieses VPNs verfügen muss). Geben Sie dazu einen Benutzernamen in das Feld „Benutzername“ sowie das zugehörige Kennwort in das Feld „Kennwort“ ein. Um den Zertifikatstyp der Gegenstelle zu prüfen, markieren Sie die Checkbox „Zertifikatstyp der Gegenstelle überprüfen“. Markieren Sie die Checkbox „tls-auth aktivieren“, um zusätzlich zu den Zertifikaten auch einen statischen Schlüssel zu verwenden. In diesem Fall wird der im Abschnitt „Authentifizierung mit statischem Schlüssel“ gespeicherte statische Schlüssel verwendet. Optional kann in der Dropdown-Liste „Benutzungsrichtung des Schlüssels“ eine Richtung vorgegeben werden (siehe dazu den im Anschluss folgenden Hinweis).

ⓘ Wird tls-auth benutzt, kann optional angegeben werden, dass der statische Schlüssel nur für eine bestimmte Richtung benutzt werden soll. Wichtig dabei ist, dass diese Einstellung mit der VPN-Gegenstelle abgestimmt ist, d.h. bei beiden ist keine Richtung eingestellt oder die Einstellungen sind komplementär (0/1 bzw. 1/0).

Um die **Authentifizierung mit statischem Schlüssel zu konfigurieren**, wählen Sie den Radiobutton „Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel“. Dabei wird unter der Option angezeigt, ob der statische Schlüssel vorhanden ist (grüner Haken) oder nicht (rotes Kreuz). Ein vorhandener Schlüssel kann auch heruntergeladen (blauer Pfeil) oder wieder gelöscht (rotes Kreuz auf weißem Kästchen) werden. Ist kein Schlüssel vorhanden, wird die Gegenstelle weder authentifiziert noch wird der Datenverkehr durch den OpenVPN-Tunnel verschlüsselt. Klicken Sie auf den Link „Statischen Schlüssel neu erstellen“, um einen neuen statischen Schlüssel zu erstellen. Dieser statische Schlüssel muss dann heruntergeladen und auch auf die Gegenstelle hochgeladen werden. Geben Sie die IP-Adresse des lokalen Tunnelendes in das Feld „IPv4-Tunneladresse lokal“ bzw. „IPv6-Tunneladresse lokal“ und die des entfernten Tunnelendes in das Feld „IPv4-Tunneladresse der Gegenstelle“ bzw. „IPv6-Tunneladresse der Gegenstelle“ ein. Geben Sie die Adresse sowie die zugehörige Netzmaske des Netzwerks hinter dem OpenVPN-Tunnel in die Felder „IPv4-Netzadresse hinter dem Tunnel“ bzw. „IPv6-Netzadresse hinter dem Tunnel“ und „IPv4-Netzmaske hinter dem Tunnel“ bzw. „IPv6-Netzmaske hinter dem Tunnel“ ein.

Um alle oben getroffenen **Einstellungen zu übernehmen**, klicken Sie auf die Schaltfläche „OK“.

Um ein **Zertifikat oder einen Schlüssel hochzuladen**, klicken Sie im Abschnitt „Schlüssel oder Zertifikate laden“ auf die Schaltfläche „Durchsuchen…“ (Schaltfläche abhängig vom verwendeten Browser). Wählen Sie dann im Fenster „Datei hochladen“ die gewünschte Datei auf dem entsprechenden Datenträger aus und klicken Sie auf die Schaltfläche „Öffnen“. Falls die Datei verschlüsselt ist, müssen Sie noch das Kennwort in das Feld „Kennwort (nur bei verschlüsselter Datei)“ eintragen. Klicken Sie dann auf die Schaltfläche „OK“ um die Datei hochzuladen.

12.6.5 PPTP Allgemein

PPTP (Point-to-Point Tunneling Protocol) ist ein VPN (virtuelles privates Netzwerk), das für neue Installationen nicht mehr empfohlen wird. Eine moderne Alternative ist OpenVPN.

PPTP baut über einen mit dem GRE-Protokoll (Generic Routing Encapsulation) erstellten Tunnel eine WWAN-Verbindung auf. Für den Tunnelaufbau ist unerlässlich, dass das GRE-Protokoll uneingeschränkt zwischen den beiden PPTP-Teilnehmern geroutet wird und dass eine TCP-Verbindung mit Port 1723 möglich ist. Der TCP-Port 1723 ist fix und kann nicht verändert werden. Das GRE-Protokoll wird im Internet nicht immer direkt geroutet. In dem Fall kann das erfolgende NAT verhindern, dass ein Tunnel aufgebaut werden kann.

Für sichere Tunnel wird dringend empfohlen, möglichst lange Kennwörter mit Sonderzeichen und die Verschlüsselungsart MPPE-128 Bit zu verwenden.

12.6.6 PPTP-Server einrichten

Hier werden die Einstellungen für den EBW-H100 als PPTP-Server konfiguriert. Maximal 5 PPTP-Clients können sich gleichzeitig an diesem Server anmelden. Es können zwar mehrere Benutzer angelegt werden, aber gleichzeitig können nur 5 Tunnel aktiv sein.

Konfiguration mit Web-Interface (Menü „Dial-In“/„Dial-Out“/„LAN (ext)“, Seite „PPTP-Server“)

Für einen Betrieb als **PPTP-Server**, aktivieren Sie die Checkbox „PPTP-Server aktivieren“.

Um die **Meldungen des letzten Verbindungsvorgangs anzuzeigen**, wählen Sie den Link „Verbindungslog der letzten Verbindung“.

Um das **Authentifizierungsverfahren auszuwählen, mit dem sich der PPTP-Client am Server authentifizieren** muss, wählen Sie dieses aus der Dropdown-Liste „Authentifizierung“ aus. Wenn der Datenverkehr über die PPTP-Verbindung mit MPPE verschlüsselt werden soll, ist zwingend die Authentifizierungsart MS-CHAP-v2 erforderlich. Weiter zur Verfügung stehen PAP, CHAP, MS-CHAP oder keine Authentifizierung.

Um die **Verschlüsselung auszuwählen, die für die PPTP-Verbindung** verwendet wird, wählen Sie diese aus der Dropdown-Liste „Verschlüsselung“ aus. Dieselbe Verschlüsselung muss auch für den Client konfiguriert werden. Zur Verfügung stehen MPE 40, MPE 128 oder keine Verschlüsselung.

Um die **MTU** (maximale erlaubte Anzahl an Bytes in einem zu sendenden Paket) anzupassen, ändern Sie den Eintrag im entsprechenden Feld.

Um die **MRU** (maximale erlaubte Anzahl an Bytes in einem zu empfangenden Paket) anzupassen, ändern Sie den Eintrag im entsprechenden Feld.

ⓘ Die Standardeinstellung von MTU und MRU ist für die meisten Anwendungen passend und muss nur in Ausnahmefällen geändert werden.

Geben Sie die **IP-Adresse des lokalen Tunnelendes** in das Feld „IPv4-Tunneladresse lokal“ ein. Wenn keine Adresse explizit angegeben wird, benutzt der PPTP-Server die IP-Adresse 192.168.0.1. Falls diese Adresse bereits belegt ist, kann hier eine andere Adresse angegeben werden.

Definieren Sie den **verfügbaren IP-Adressen-Pool für die Tunnelenden der PPTP-Clients** in den Feldern „IP-Adressen-Pool“. Dieser Pool muss im Netzwerk des LANs liegen. Die PPTP-Clients adressieren ihr Ziel direkt mit IP-Adressen im LAN des EBW-H100.

Um einen **neuen Benutzer hinzuzufügen**, der für die Verbindungen von PPTP-Clients zugelassen ist, geben Sie für diesen einen Benutzernamen und ein Kennwort in die entsprechenden Felder ein. Klicken Sie auf „OK“, um den Benutzer zu übernehmen. Bestehende Benutzer können Sie löschen, indem Sie die Checkbox in der Spalte „löschen“ des entsprechenden Benutzers markieren und auf „OK“ klicken.

Um alle oben getroffenen **Einstellungen für den geladenen Tunnel zu übernehmen**, klicken Sie auf die Schaltfläche „OK“.

12.6.7 PPTP-Client einrichten

Hier werden die Einstellungen für den PPTP-Client konfiguriert. Alle Pakete durch den PPTP-Tunnel werden vom EBW-H100 mit seiner Tunnel-Adresse maskiert.

Konfiguration mit Web-Interface (Menü „Dial-In“/„Dial-Out“/„LAN (ext)“, Seite „PPTP-Client“)

Um den EBW-H100 als **PPTP-Client** zu verwenden, aktivieren Sie die Checkbox „PPTP-Client aktivieren“.

Um die **Meldungen des letzten Verbindungsvorgangs anzuzeigen**, wählen Sie den Link „Verbindungslog der letzten Verbindung“.

Um die **IP-Adresse oder den Domainnamen der Gegenstelle zu bestimmen**, zu der die VPN-Verbindung aufgebaut werden soll, geben Sie im Feld „IP-Adresse oder Domainname der Gegenstelle“ eine IP-Adresse oder einen Domainnamen an.

Geben Sie den **Benutzernamen und das Kennwort** mit denen sich der PPTP-Client am Server anmeldet in die entsprechenden Felder ein.

Um die **Verschlüsselung auszuwählen, die für die PPTP-Verbindung** verwendet wird, wählen Sie diese aus der Dropdown-Liste „Verschlüsselung“ aus. Es muss die Verschlüsselung gewählt werden, die auch der PPTP-Server verwendet. Zur Verfügung stehen MPE 40, MPE 128 oder keine Verschlüsselung.

Um die **Default-Route zu diesem PPTP-Tunnel zu setzen**, aktivieren Sie die Checkbox „Default Route setzen“. Dann wird jeglicher Datenverkehr durch den Tunnel geroutet. Dies ist jedoch nur dann möglich, wenn vorher noch keine vorrangige Default-Route gesetzt war.

Wird keine Default-Route zum Tunnel gesetzt, muss das **lokale Subnetz hinter dem Tunnel definiert** werden. Geben Sie dieses Netzwerk mit passender Netzmaske in das Feld „Lokales Subnetz der Gegenstelle“ ein. Nur so werden Pakete in das Netzwerk hinter dem PPTP-Tunnel durch den Tunnel geroutet.

Um die **MTU** (maximale erlaubte Anzahl an Bytes in einem zu sendenden Paket) anzupassen, ändern Sie den Eintrag im entsprechenden Feld.

Um die **MRU** (maximale erlaubte Anzahl an Bytes in einem zu empfangenden Paket) anzupassen, ändern Sie den Eintrag im entsprechenden Feld.

ⓘ Die Standardeinstellung von MTU und MRU ist für die meisten Anwendungen passend und muss nur in Ausnahmefällen geändert werden.

Um eine **Verbindungsüberprüfung durch einen Ping per ICMP-Protokoll** an eine Domain oder eine IP-Adresse einzustellen, geben Sie diese in das Eingabefeld „Zusätzlicher ICMP-Ping an“ ein. Es empfiehlt sich, hier einen Domainnamen oder eine IP-Adresse einzutragen, die nur durch den Tunnel erreichbar ist. Ist die Verbindungsprüfung nicht erfolgreich, wird ein eventuell bestehender Tunnel abgebaut und ein neuer Tunnel aufgebaut. Das Intervall der Pings beträgt 15 Minuten.

ⓘ Wenn ein Tunnel abbricht, wird dieser nicht automatisch wieder aufgebaut, sondern der Aufbau erfolgt erst nach einem neuen WAN-Verbindungsaufbau. Deshalb sollte der Zustand des Tunnels unbedingt mit einem ICMP-Ping geprüft werden.

Um alle oben getroffenen **Einstellungen für den geladenen Tunnel zu übernehmen**, klicken Sie auf die Schaltfläche „OK“.

12.6.8 IPsec einrichten

IPsec (Internet Protocol Security) ist ein Sicherheitsprotokoll für die sichere Kommunikation über IP-Netze und kann zum Aufbau virtueller privater Netzwerke (VPN) verwendet werden. Dabei können zwei Subnetze über zwei geeignete Router (z.B. INSYS MoRoS 2.1) über einen sicheren Tunnel miteinander verbunden werden. Es ist möglich, bis zu 10 verschiedene Tunnel zu konfigurieren.

Ein Tunnel kann auch als Fallback-Tunnel für einen anderen aktiven Tunnel verwendet werden. Beim Aufbau der WAN-Verbindung wird immer der aktive Tunnel gestartet. Wenn der zusätzliche ICMP-Ping erfolglos ist, wird der aktive Tunnel beendet und der Fallback-Tunnel gestartet. Schlägt bei einem Fallback-Tunnel die Verbindungsüberprüfung per ICMP-Ping fehl, wird der Fallback-Tunnel beendet und der aktive Tunnel gestartet.

Konfiguration mit Web-Interface (Menü „Dial-In“/„Dial-Out“/„LAN (ext)“, Seite „IPsec“)

Um bei **einer Verbindung IPsec** zu verwenden, aktivieren Sie die Checkbox „IPsec aktivieren“.

Um den **aktuellen Zustand der IPsec-Tunnel anzuzeigen**, wählen Sie den Link „IPsec Status“.

Um die **Meldungen des letzten Verbindungsvorgangs anzuzeigen**, wählen Sie den Link „Verbindungslog der letzten Verbindung“.

Um **NAT-Traversal zu konfigurieren**, verwenden Sie die Dropdown-Liste „NAT-Traversal“ zur Auswahl der entsprechenden Option. Wenn Sie „aktivieren“ (Standardeinstellung) wählen, werden, falls ein NAT-Router erkannt wird, alle ESP (Encapsulating Security Payload)-Pakete zusätzlich in ein UDP-Paket verpackt und über den UDP-Port 4500 versendet. Wenn Sie „erzwingen“ wählen, wird dieses Verhalten ohne Kontrolle auf einen NAT-Router erzwungen (dabei muss auch die Gegenstelle NAT-Traversal aktiviert haben). Wenn Sie „deaktivieren“ wählen, wird eine UDP-Datenkapselung verhindert, was im Betrieb mit einem NAT-Router zu Problemen führen kann. Diese Einstellung gilt global für alle Tunnel.

Um das **Intervall der Keep-Alive-Pakete zu konfigurieren**, die gesendet werden, wenn NAT-Traversal verwendet wird, geben Sie die Zeit in Sekunden in das Feld „Keep-Alive Intervall“ ein. Dadurch kann verhindert werden, dass z.B. eine Stateful Firewall die Verbindung nach zu langer Inaktivität blockiert.

Um den **Tunnel auszuwählen, dessen Einstellungen bearbeitet werden sollen**, wählen Sie den gewünschten Tunnel aus der Dropdown-Liste „Tunnelname“ und klicken Sie dann auf die Schaltfläche „zum Bearbeiten laden“. Wenn Einstellungen am aktuell geladenen Tunnel erfolgt sind, müssen diese zuvor mit der Schaltfläche „OK“ übernommen werden, bevor ein neuer Tunnel geladen wird, um diese nicht zu verlieren. Das Laden eines Tunnels speichert keine bereits vorgenommenen Einstellungen!

Um den geladenen **Tunnel zu aktivieren**, wählen Sie in der Dropdown-Liste „Tunnel aktivieren“ die Option „aktiv“.

Um den geladenen **Tunnel als Fallback-Tunnel für einen aktiven Tunnel festzulegen**, wählen Sie in der Dropdown-Liste „Tunnel aktivieren“ die Option „Fallback für …“.

Um dem geladenen **Tunnel einen beschreibenden Namen zuzuweisen**, geben Sie diesen in das Feld „Tunnelname“ ein. Dies erleichtert die Zuordnung von Meldungen im Log oder der Status-Ansicht.

Um die **Gegenstelle festzulegen, zu der der Tunnel aufgebaut werden soll**, geben Sie in das Feld „IP-Adresse oder Domainname der Gegenstelle“ entweder die IP-Adresse oder den Domainname der Gegenstelle ein. Wird keine Gegenstelle angegeben, werden eingehende Verbindungsanfragen von allen Gegenstellen akzeptiert, aber es kann keine Verbindung initiiert werden. In diesem Fall muss die „Aktion bei Verbindungsabbruch“ der Dead-Peer-Detection auf „hold“ gestellt werden, da bei einem Abbruch der bestehenden Verbindung sonst keine neu eingehende Verbindungsanfrage mehr angenommen werden kann.

Um ein **zu tunnelndes Netzwerk hinter dem Switch des EBW-H100 zu definieren**, kann dieses Netzwerk mit passender Netzmaske in das Feld „Eigenes lokales Subnetz“ eingegeben werden. Dieses muss nicht das wirkliche lokale Subnetz sein, sondern kann auch hinter weiteren Gateways liegen. In solch einem Fall muss darauf geachtet werden, dass die benötigten Routing-Regeln korrekt angelegt werden. Wird dieses Feld nicht ausgefüllt, wird automatisch das lokale Subnetz verwendet.

Um das **lokale Subnetz hinter der Gegenstelle zu definieren**, geben Sie dieses Netzwerk mit passender Netzmaske in das Feld „Lokales Subnetz der Gegenstelle“ ein. Es werden nur die Daten in ESP-Pakete gepackt, welche an dieses Netz adressiert sind.

Um die **ID der Gegenstelle festzulegen**, geben Sie diese in das Feld „ID der Gegenstelle“ ein. Standardmäßig wird die jeweilige IP-Adresse als ID verwendet. Weicht die eigentliche IP-Adresse von der empfangenen ID ab (z.B. durch dazwischen liegende NAT-Router) oder ist sie nicht bekannt, kann die ID der Gegenstelle explizit angegeben werden (ein selbstdefinierter String, der ein „@“ beinhalten muss). Bei Verwendung von Zertifikaten wird standardmäßig der DN (Distinguished Name) als ID verwendet. Der Domainname der Gegenstelle kann ebenso als ID verwendet werden, da er durch einen DNS-Lookup aufgelöst wird.

Um die **eigene ID anzupassen**, geben Sie diese in das Feld „Eigene ID“ ein. Dies ist nur nötig, wenn die standardmäßige ID nicht verwendet werden kann oder soll.

Um nur ein **bestimmtes Protokoll und einen bestimmten Port für das lokale Tunnelende zuzulassen**, geben Sie die IANA-Protokollnummer und den Port (sofern das Protokoll Ports unterstützt) in die Felder „Lokales Protokoll und Port“ ein. Fehlt hier eine Angabe des Protokolls und/oder Ports sind alle Protokolle bzw. Ports zugelassen.

Um nur ein **bestimmtes Protokoll und einen bestimmten Port für das Tunnelende der Gegenstelle zuzulassen**, geben Sie die IANA-Protokollnummer und den Port (sofern das Protokoll Ports unterstützt) in die Felder „Protokoll und Port der Gegenstelle“ ein. Fehlt hier eine Angabe des Protokolls und/oder Ports sind alle Protokolle bzw. Ports zugelassen.

Um den **Authentifizierungs-Modus festzulegen**, wählen Sie diesen in der Dropdown-Liste „Authentifizierungs-Modus“ aus. Der Main-Modus ist sicherer, da alle Authentifizierungsdaten verschlüsselt übertragen werden. Der Aggressive-Modus ist schneller, da er auf diese Verschlüsselung verzichtet und die Authentifizierung über eine Passphrase erfolgt.

Um die **Verschlüsselungs- und Hash-Algorithmen sowie die Diffie-Hellman-Gruppe für den IKE-Schlüsselaustausch zu definieren**, wählen Sie diese aus den Dropdown-Listen „Schlüsselparameter IKE“ aus. Zur Verfügung stehen DES EDE3, AES 128/192/256 sowie SHA1 oder MD5 und DH 768/1024/1536.

Um die **Verschlüsselungs- und Hash-Algorithmen für die IPsec-Verbindung zu definieren**, wählen Sie diese aus den Dropdown-Listen „Schlüsselparameter IPsec“ aus. Zur Verfügung stehen DES EDE3, AES 128/192/256 sowie SHA1 oder MD5.

Um die **maximale Anzahl an Verbindungsversuchen einzugeben**, ab deren Überschreiten die Gegenstelle als nicht erreichbar gilt, geben Sie diese in das Feld „Maximale Verbindungsversuche“ ein. Eine Eingabe von „0“ bedeutet hier eine unendliche Anzahl an Versuchen.

Um die **empfangenen Pakete mit der lokalen IP-Adresse des EBW-H100 zu maskieren**, aktivieren Sie die Checkbox „Pakete durch den Tunnel maskieren“. Der Empfänger des Paketes sieht dann als Absender die lokale IP-Adresse des EBW-H100 und nicht die des eigentlichen Absenders aus dem lokalen Netz der Gegenstelle.

Um die **Dead-Peer-Detection zu konfigurieren**, geben Sie das Intervall, in dem Anfragen an die Gegenstelle gesendet werden, in Sekunden in das Feld „Intervall Dead-Peer-Detection“ und die maximale Zeit, in der diese Anfragen beantwortet werden müssen, in Sekunden in das Feld „Timeout Dead-Peer-Detection“ ein. Das Verhalten bei einer als abgebrochen erkannten Verbindung, wählen Sie in der Dropdown-Liste „Aktion bei Verbindungsabbruch“. Wählen Sie hier „restart“ (Standardeinstellung) wird die Verbindung neu gestartet, bei „clear“ abgebaut und bei „hold“ gehalten.

Um die **Perfect-Forward-Secrecy zu aktivieren**, aktivieren Sie die Checkbox „Perfect-Forward-Secrecy aktivieren“. Damit kann verhindert werden, dass aus einer gehackten Verschlüsselung der nächste Schlüssel schneller herausgefunden werden kann. Beide Gegenstellen müssen in dieser Einstellung übereinstimmen, damit die Verbindung aufgebaut werden kann.

Um das **Intervall für die Schlüsselerneuerung der IKE SA zu konfigurieren**, geben Sie den Wert in Sekunden in das Feld „Intervall bis zur Schlüsselerneuerung der IKE SA“ ein. Der Mindestwert ist 3600 Sekunden (1 Stunde). Durch die regelmäßige Erneuerung der verwendeten Schlüssel kann die Sicherheit der IPsec-Verbindung über einen längeren Zeitraum gewährleistet werden.

Um das **Intervall für die Schlüsselerneuerung der IPsec SA zu konfigurieren**, geben Sie den Wert in Sekunden in das Feld „Intervall bis zur Schlüsselerneuerung der IPsec SA“ ein. Der Mindestwert ist 3600 Sekunden (1 Stunde). Durch die regelmäßige Erneuerung der verwendeten Schlüssel kann die Sicherheit der IPsec-Verbindung über einen längeren Zeitraum gewährleistet werden.

Um **zusätzlich einen Ping per ICMP-Protokoll an eine IP-Adresse zu senden**, geben Sie diese Adresse, die sich im lokalen Subnetz der Gegenstelle befinden muss, in das Feld „Zusätzlicher ICMP-Ping an“ ein. Ist der Ping nicht erfolgreich, wird ein eventuell bestehender Tunnel abgebaut und ein neuer Tunnel aufgebaut. Das Ping-Intervall beträgt 15 Minuten. Eine zusätzliche zweite IP-Adresse als Ping-Ziel kann durch ein „#“ getrennt hinter der ersten angegeben werden.

Um die **Authentifizierung bei einer IPsec-Verbindung zu konfigurieren**, wählen Sie entweder den Radiobutton „Authentifizierung mit Zertifikaten“ oder den Radiobutton „Authentifizierung mit Passphrase (PSK)“. Die Authentifizierung mit Zertifikaten kann für den Main-Modus verwendet werden. Dabei wird unter der Option angezeigt, ob die einzelnen Zertifikate und Schlüssel vorhanden sind (grüner Haken) oder nicht (rotes Kreuz). Vorhandene Zertifikate können auch heruntergeladen (blauer Pfeil) oder wieder gelöscht (rotes Kreuz auf weißem Kästchen) werden. Der private Schlüssel kann nur gelöscht werden. Die Authentifizierung mit Passphrase kann für den Main- und Aggressive-Modus verwendet werden. Dafür muss im Feld unter der Option die Passphrase, die alle IPsec-Teilnehmer verwenden, eingetragen werden.

Um alle oben getroffenen **Einstellungen für den geladenen Tunnel zu übernehmen**, klicken Sie auf die Schaltfläche „OK“.

Um ein **Zertifikat oder einen Schlüssel hochzuladen**, klicken Sie im Abschnitt „Schlüssel oder Zertifikate laden“ auf die Schaltfläche „Durchsuchen…“. Wählen Sie dann im Fenster „Datei hochladen“ die gewünschte Datei auf dem entsprechenden Datenträger aus und klicken Sie auf die Schaltfläche „Öffnen“. Falls die Datei verschlüsselt ist, müssen Sie noch das Kennwort in das Feld „Kennwort (nur bei verschlüsselter Datei)“ eintragen. Klicken Sie dann auf die Schaltfläche „OK“ um die Datei hochzuladen.

12.6.9 GRE-Tunnel einrichten

Mit dem Generic Routing Encapsulation Protokoll können Daten durch eine bestehende Verbindung transparent übertragen werden, ohne dass die Originalpakete verändert werden.

Konfiguration mit Web-Interface (Menü „Dial-In“/„Dial-Out“/„LAN (ext)“, Seite „GRE“)

Um einen **GRE-Tunnel zu aktivieren**, aktivieren Sie die Checkbox „GRE-Tunnel aktivieren“.

Geben Sie die **Tunnel-Gegenstelle** als IP-Adresse oder Domainname in das Feld „IP-Adresse oder Domainname der Gegenstelle“ ein.

Geben Sie die **eigene IP-Adresse**, die als Tunnelendpunkt verwendet werden soll, in das Feld „Eigene IP-Adresse“ ein. Dies kann beispielsweise die WAN-, VPN- oder die lokale LAN-Adresse sein.

Geben Sie die **IP-Adresse des lokalen Tunnelendes** in das Feld „Tunnelende lokal“ ein. Optional kann hier eine Netzmaske eingegeben werden. Dann wird automatisch eine entsprechende Route zu diesem Netzwerk angelegt, wodurch z.B. die Tunneladresse der Gegenstelle erreichbar ist.

Um die **MTU** (maximale erlaubte Anzahl an Bytes in einem zu sendenden Paket) anzupassen, ändern Sie den Eintrag im entsprechenden Feld.

ⓘ Die Standardeinstellung von MTU ist für die meisten Anwendungen passend und muss nur in Ausnahmefällen geändert werden.

Wenn Sie eine **TTL (Time to Live) festlegen** möchten, geben Sie diese in das Feld „TTL (Time to Live)“ ein. Wird keine TTL angegeben, wird für das GRE-Paket der TTL-Wert aus dem getunnelten Paket verwendet.

Um eine **neue Route hinzuzufügen**, geben Sie im Abschnitt „Neue Route hinzufügen“ die „IPv4-Netzadresse“ und die „Netzmaske“ sowie den „Gateway“ in die jeweiligen Felder ein. Alle Felder müssen ausgefüllt werden, damit eine neue Route in die Tabelle übernommen wird. Übernehmen Sie die Route, indem Sie auf „OK“ klicken.

Um eine **bestehende Route zu löschen**, aktivieren Sie unter „Bestehende Routen“ die Checkbox der Route(n), die gelöscht werden soll(en).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.7 Meldungen

12.7.1 Versand von Meldungen konfigurieren

Der EBW-H100 kann bei verschiedenen Ereignissen eine E-Mail, eine SMS oder einen SNMP-Trap an beliebige Empfänger versenden. Dazu stehen eine Reihe vordefinierter Ereignisse zur Verfügung, wie zum Beispiel Aufbau von Verbindungen oder VPN-Tunnel.

Konfiguration mit Web-Interface (Menü „Meldungen“, Seite „Konfiguration“)

Um den **Versand einer E-Mail** zu ermöglichen, müssen Sie im Abschnitt „E-Mail“ die notwendigen Daten für das E-Mail-Konto eingeben. Geben Sie dazu die E-Mail-Adresse in das Feld „E-Mail-Adresse“ ein. Geben Sie den Vor- und Nachnamen der Person, die das E-Mail-Konto besitzt, (oder einen beliebigen Text) in das Feld „Realer Name“ ein. Tragen Sie den Domain-Namen oder die IP-Adresse des SMTP-Servers in das Feld „SMTP-Server“ sowie den Port, an dem der SMTP-Server E-Mails entgegennimmt, in das Feld „SMTP-Port“ ein (normalerweise Port 25). Tragen Sie den Benutzernamen für das E-Mail-Konto in das Feld „Benutzername“ sowie das zugehörige Kennwort in das Feld „Kennwort“ ein. Markieren Sie die Checkbox „SSL/TLS verwenden“, um die E-Mails verschlüsselt zu versenden.

Um den **SMS-Versand** zu ermöglichen, müssen Sie im Abschnitt „SMS“ die Nummer des SMS Service Centers Ihres Mobilfunkanbieters im Eingabefeld „SCN (Service Center Number) SIM-Karte 1“ angeben. Wenn die SIM-Karte bereits freigeschaltet ist und der Provider der SIM-Karte erkannt wird, wird dessen SCN vorgeschlagen. Die Einstellung wird jedoch erst nach einem Klick auf „OK“ dauerhaft gespeichert und verwendet.
Mit dem **SMS-Protokoll** wird festgelegt, welche Zeichen im SMS-Text erlaubt sind. Beim GSM-Zeichensatz werden für ein zu übertragendes Zeichen 8 Bit benötigt, daher sind maximal 140 Zeichen möglich. Beim UCS2-Zeichensatz benötigt jedes Zeichen 16 Bit, daher können maximal 70 Zeichen versendet werden. Der GSM-Zeichensatz ist auf 127 verschiedene Zeichen beschränkt, der UCS2-Zeichensatz enthält deutlich mehr Zeichen und Symbole für verschiedene Sprachen.

Um den **Versand von SNMP-Traps** zu ermöglichen, müssen Sie im Abschnitt „SNMP-Traps“ die SNMP-Version angeben. Um SNMP v2c zu verwenden, wählen Sie den Radiobutton „SNMP v2c“. Weiterhin muss der Community-String in das Feld „Community“ eingegeben werden. Um SNMP v3 zu verwenden, wählen Sie den Radiobutton „SNMP v3“. Weiterhin muss der SNMP-Benutzername in das Feld „Benutzername“ eingegeben werden. Um eine SNMP v3-Authentifizierung optional zu verwenden, wählen Sie die Authentifizierungsmethode in der Dropdown-Liste „Authentifizierung“ aus und geben Sie das Kennwort für die Authentifizierung (mindestens 8 Zeichen) in das entsprechende Feld ein. Um eine SNMP v3-Verschlüsselung optional zu verwenden, wählen Sie die Verschlüsselungsmethode in der Dropdown-Liste „Verschlüsselung“ aus und geben Sie das Kennwort für die Verschlüsselung (mindestens 8 Zeichen) in das entsprechende Feld ein. Voraussetzung für eine Verschlüsselung ist eine Authentifizierung.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.7.2 SMS-Empfang aktivieren

Der EBW-H100 kann Befehle per SMS empfangen. Die Ausführung des Befehls kann durch ein Kennwort geschützt werden.

ⓘ Es wird dringend empfohlen, einen Kennwortschutz zu verwenden.

Ist ein Kennwort konfiguriert, muss die SMS das Kennwort enthalten; ist kein Kennwort konfiguriert, darf die SMS kein Kennwort enthalten. Bei Regelverstoß wird die SMS in beiden Fällen nicht verarbeitet. Beim Kennwort wird Groß- und Kleinschreibung beachtet. Das Kennwort muss, gefolgt von einem Komma, vor dem Befehl stehen und darf Leerzeichen enthalten, Leerzeichen außerhalb des Kennworts werden ignoriert.

Pro SMS kann ein Befehl als SMS-Text versandt werden. Mehrere Befehle in einer SMS werden nicht unterstützt, es wird nur der erste Befehl ausgeführt. Bei den Befehlen ist Groß- und Kleinschreibung unerheblich. Die Syntax lautet:

[<Kennwort>,]<Befehl>

Der EBW-H100 kann eingegangene SMS quittieren. Ist dies konfiguriert, wird eine SMS mit dem empfangenen Text an den Absender zurück gesandt. Falls ein Standort eingetragen ist, wird dieser vorangestellt. Die Syntax lautet

[Standort;]SMS received:"[<Kennwort>,]<Befehl>"

ⓘ Durch das Quittieren eingegangener SMS können unter Umständen erhebliche Kosten entstehen. Ursachen sind u. a. Roaming-Gebühren oder Pingpongeffekte, bei denen durch die Quittierungs-SMS an den Absender der initialen (Spam-) SMS eine weitere SMS von diesem Absender ausgelöst wird, die wiederum quittiert wird, usw.

Folgende Befehle werden verarbeitet:

Befehl	Wirkung
dial	Es wird eine Dial-Out-Verbindung gestartet bzw. eine bestehende Dial-Out-Verbindung beendet.
dial start	Eine Dial-Out-Verbindung wird aufgebaut, wenn aktuell keine Verbindung besteht.
dial stop	Eine bestehende Dial-Out-Verbindung wird abgebaut. Es wird keine neue Verbindung initiiert.
ipsec	Die IPsec-Verbindung wird neu gestartet. Alle bestehenden Tunnel werden dabei abgebaut.
openvpn	Die OpenVPN-Verbindung wird neu gestartet. Ein bestehender Tunnel wird dabei abgebaut.
pptp	Die PPTP-Verbindung wird neu gestartet. Alle bestehenden Tunnel werden dabei abgebaut.
reset	Ein Neustart des Geräts wird durchgeführt.
sandbox	Die Sandbox wird neu gestartet.

Befehl	Wirkung
update	Ein automatisches Update wird ausgeführt.

Tabelle 10: Liste der SMS-Befehle

Beispielsweise löst eine SMS mit dem Text **`TOPsecret,reset`** einen Neustart aus, wenn das Kennwort „TOPsecret“ lautet. Eine SMS mit dem Text **`openvpn`** startet die OpenVPN-Verbindung neu, falls kein Kennwort konfiguriert ist.

SMS-Nachrichten, die nicht dieser Syntax entsprechen, können optional in die Sandbox verschoben werden. Dazu muss im Sandbox-Image das Unterverzeichnis „/var/spool/sms_in“ existieren. Darin wird die SMS als Datei mit einem zufälligen Dateinamen angelegt. Die erste Zeile der Datei enthält die Rufnummer des Absenders, die weiteren Zeilen enthalten den SMS-Text. Wenn ein Kennwort konfiguriert wurde, gilt für in die Sandbox weitergeleitete SMS: Wurde ein SMS-Text mit gültigem Kennwort empfangen wird, wird das Kennwort und das trennende Komma vom Text entfernt. Bei einem Text mit ungültigem oder fehlendem Kennwort wird der originale Text in die Sandbox weitergeleitet.

Konfiguration mit Web-Interface (Menü „Meldungen“, Seite „Konfiguration“)

Um den **SMS-Empfang zu aktivieren**, markieren Sie die Checkbox „SMS-Empfang aktivieren“.

Damit der EBW-H100 den **Eingang einer SMS quittiert**, markieren Sie die Checkbox „Eingegangene SMS quittieren“. Dann wird JEDE eingegangene SMS mit einer Antwort-SMS quittiert, nicht nur SMS zur Ausführung von Befehlen.

ⓘ Es wird nur der Eingang der SMS quittiert und nicht die damit ausgelöste Aktion. Soll die Aktion quittiert werden, muss diese als Meldung konfiguriert werden.

Um ein **Kennwort für den SMS-Empfang** zu setzen, geben Sie dieses in das Feld „Kennwort“ ein. Das Kennwort darf aus Buchstaben (groß und klein, ohne Umlaute), Ziffern, Interpunktionszeichen (ohne Komma), Klammern, Unterstrich, Leerzeichen und den Zeichen %, & und * bestehen und 20 Zeichen lang sein.

Um **nicht auswertbare SMS an die Sandbox weiterzuleiten**, markieren Sie die Checkbox „Nicht auswertbare SMS an Sandbox weiterleiten“. Dann werden alle SMS, die nicht ausgewertet werden können, an die Sandbox weitergeleitet, um sie dort zu verarbeiten.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.7.3 E-Mail-Versand konfigurieren

Der EBW-H100 kann bei verschiedenen, vordefinierten Ereignissen eine E-Mail an beliebige Empfänger versenden. An jede E-Mail kann ein Anhang angehängt werden, der aus den verschiedenen Log-Dateien ausgewählt werden kann. Weiterhin ist es möglich, die Status-Seite des Web-Interface an den Meldungstext anzuhängen. Es ist möglich, eine Reihe verschiedener Kombinationen aus Empfänger, Ereignis, Anhang und Text anzulegen und zu verwalten.

Der Versand einer E-Mail ist nur möglich, wenn die Zugangsdaten für das E-Mail-Konto im Menü „Meldungen“ auf der Seite „Konfiguration“ korrekt eingetragen sind.

Konfiguration mit Web-Interface (Menü „Meldungen“, Seite „E-Mail“)

Um den **Versand von E-Mail-Meldungen** zu aktivieren, markieren Sie die Checkbox „E-Mail-Meldungen aktivieren“.

Um eine **E-Mail-Meldung zu erstellen**, müssen Sie diese im Abschnitt „Neue E-Mail-Meldung erstellen“ definieren. Geben Sie dazu die E-Mail-Adresse des Empfängers in das Feld „Empfänger“ ein. Wählen Sie aus der Dropdown-Liste „Ereignis“ das jeweilige Ereignis aus, bei dem die E-Mail versandt werden soll. Wählen Sie aus der Dropdown-Liste „Anhang“ die jeweilige Log-Datei aus, die an die E-Mail angehängt werden soll. Existiert diese Datei auf dem EBW-H100 nicht, wird die E-Mail ohne Anhang versendet. Markieren Sie die Checkbox „Status an Meldungstext anhängen“, wenn die Status-Seite des Web-Interface an den Meldungstext angehängt werden soll. Geben Sie den Text für die Meldung in das Eingabefeld „Text“ ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um einzelne **E-Mail-Meldungen temporär auszuschalten**, deaktivieren Sie im Abschnitt „Bestehende E-Mail-Meldungen“ die Checkbox in der Spalte „aktiv“ in der Übersicht der E-Mail-Meldungen. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

Um **eine oder mehrere E-Mail-Meldungen zu löschen**, markieren Sie im Abschnitt „Bestehende E-Mail-Meldungen“ die Checkbox in der Spalte „löschen“ in der Übersicht der E-Mail-Meldungen. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

12.7.4 SMS-Versand konfigurieren

Der EBW-H100 kann bei verschiedenen, vordefinierten Ereignissen eine SMS an beliebige Empfänger versenden. Der Text einer SMS-Meldung kann aus bis zu 140 Zeichen bestehen, wobei nicht alle Zeichen zulässig sind und beim Versenden selbständig aus dem eingegebenen Text entfernt werden. Es ist möglich, eine Reihe verschiedener Kombinationen aus Empfänger, Ereignis und Text anzulegen und zu verwalten.

Der Versand einer SMS ist nur möglich, wenn die SCN im Menü „Meldungen“ auf der Seite „Konfiguration“ korrekt eingetragen ist.

Konfiguration mit Web-Interface (Menü „Meldungen“, Seite „SMS“)

Um den **Versand von SMS-Meldungen** zu aktivieren, markieren Sie die Checkbox „SMS-Meldungen aktivieren“.

Um eine **SMS-Meldung zu erstellen**, müssen Sie diese im Abschnitt „Neue SMS-Meldung erstellen“ definieren. Geben Sie dazu die Rufnummer des Empfängers in das Feld „Rufnummer“ ein. Wählen Sie aus der Dropdown-Liste „Ereignis“ das jeweilige Ereignis aus, bei dessen Eintreten die SMS versandt werden soll. Geben Sie den Text für die Meldung in das Eingabefeld „Text“ ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um einzelne **SMS-Meldungen temporär auszuschalten**, deaktivieren Sie im Abschnitt „Bestehende SMS-Meldungen“ die Checkbox in der Spalte „aktiv“ in der Übersicht der SMS-Meldungen. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

Um **eine oder mehrere SMS-Meldungen zu löschen**, markieren Sie im Abschnitt „Bestehende SMS-Meldungen“ die Checkbox in der Spalte „löschen“ in der Übersicht der SMS-Meldungen. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

12.7.5 SNMP-Trap-Versand konfigurieren

Der EBW-H100 kann bei verschiedenen, vordefinierten Ereignissen einen SNMP-Trap an beliebige Empfänger versenden. Es ist möglich, eine Reihe verschiedener Kombinationen aus Empfänger und Ereignis anzulegen und zu verwalten. Die SNMP-Traps sind in der MIB (Management Information Base) beschrieben.

Der Versand eines SNMP-Trap ist nur möglich, wenn die Einstellungen für die SNMP-Traps im Menü „Meldungen“ auf der Seite „Konfiguration“ korrekt konfiguriert sind.

Konfiguration mit Web-Interface (Menü „Meldungen“, Seite „SNMP-Traps“)

Um den **Versand von SNMP-Traps** zu aktivieren, markieren Sie die Checkbox „SNMP-Traps aktivieren“.

Um die **private MIB herunterzuladen**, klicken Sie auf den Link „Private MIB herunterladen“.

Um einen **SNMP-Trap zu erstellen**, müssen Sie diesen im Abschnitt „Neuen SNMP-Trap erstellen“ definieren. Geben Sie dazu die IP-Adresse oder den Domain-Namen und den zugehörigen Port des Empfängers in die Felder „IP-Adresse oder Domainname“ und „Port“ ein. Wählen Sie aus der Dropdown-Liste „Ereignis“ das jeweilige Ereignis aus, bei dessen Eintreten der SNMP-Trap ausgelöst werden soll.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um einzelne **SNMP-Traps temporär auszuschalten**, deaktivieren Sie im Abschnitt „Bestehende SNMP-Traps“ die Checkbox in der Spalte „aktiv“ in der Übersicht der SNMP-Traps. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

Um **einen oder mehrere SNMP-Traps zu löschen**, markieren Sie im Abschnitt „Bestehende SNMP-Traps“ die Checkbox in der Spalte „löschen“ in der Übersicht der SNMP-Traps. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

12.8 Server-Dienste

12.8.1 DNS-Forwarding einrichten

Sie können den EBW-H100 als DNS-Relay-Server nutzen. Wenn er bei den lokal angeschlossenen Netzwerkgeräten als DNS-Server konfiguriert wird, leitet er die DNS-Anfragen entweder an die vorher konfigurierten DNS-Server im Internet weiter oder benutzt die beim Verbindungsaufbau übergebenen DNS Server. Wenn in der lokalen Hosttabelle (Menü „Basic Settings“, Seite „Hostnamen“) IP-Adressen mit Hostnamen verknüpft sind, werden zuerst diese verarbeitet.

Konfiguration mit Web-Interface (Menü „Server-Dienste“, Seite „DNS“)

Um das **DNS-Relay zu deaktivieren**, deaktivieren Sie die Checkbox „DNS-Relay aktivieren“.

Geben Sie zur **Angabe weiterer optionaler DNS-Server** die IP-Adressen der jeweiligen Nameserver in die Eingabefelder „Erste DNS-Server Adresse“ bzw. „Erste IPv6-DNS-Server-Adresse“ und „Zweite DNS-Server Adresse“ bzw. „Zweite IPv6-DNS-Server-Adresse“ ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.8.2 Dynamisches DNS-Update einrichten

Der EBW-H100 kann die IP-Adresse, die Ihm dynamisch bei der Interneteinwahl zugewiesen wurde, einem DynDNS-Provider mitteilen, um so aus dem Internet unter einem Domainnamen erreichbar zu sein. Damit ist das Netzwerk hinter dem Router aus dem Internet auch bei dynamisch zugeteilten IP-Adressen immer unter demselben Domainnamen erreichbar (falls eingehende Verbindungen nicht durch den Provider gesperrt sind). Dafür wird bei jeder Einwahl die beim DynDNS-Provider mit dem Domainnamen verknüpfte IP-Adresse aktualisiert. Damit Sie diese Funktion nutzen können, benötigen Sie einen Account bei einem DynDNS-Provider.

Alternativ oder zusätzlich zum DynDNS-Protokoll können bis zu fünf weitere DNS-Einträge beim Anbieter FreeDNS mit der IP-Adresse des Routers aktualisiert werden.

ⓘ Bei paketbasierten Wireless-Verbindungen (GPRS/EDGE/UMTS/HSDPA) muss auch eine öffentliche IP-Adresse vom Provider zugewiesen worden sein. Ansonsten ist das Gerät trotz dieses Dienstes nicht erreichbar.

Konfiguration mit Web-Interface (Menü „Server-Dienste“, Seite „Dyn. DNS-Update“)

Um das **dynamische DNS-Update einzurichten**, aktivieren Sie die Checkbox „Dynamisches DNS-Update aktivieren“.

Wählen Sie einen **DynDNS-Provider** aus der Dropdown-Liste „DynDNS-Provider“.

Um **einen eigenen DynDNS-Server zu definieren**, wählen Sie in der Dropdown-Liste „DynDNS-Provider“ den Eintrag „Userdefined DynDNS“ und geben Sie einen DynDNS-Server im Eingabefeld „Benutzerdefinierter DynDNS-Server“ an.

Geben Sie den zu **aktualisierenden Domainnamen** im Eingabefeld „Domainname“ ein.

Geben Sie den **Benutzernamen und das Kennwort** Ihres DynDNS-Accounts in die Eingabefelder „Benutzername“ und „Kennwort“ ein.

Um **einen DNS-Eintrag bei FreeDNS zu verwenden**, tragen Sie den von FreeDNS generierten Hash-Wert in eines der Felder „Hash“ ein.

ⓘ Dieser Hash-Wert wird beim Anlegen einer zu aktualisierenden Domain automatisch erstellt. Er kann aus dem "quick cron example" entnommen werden oder aus den zum Download angebotenen curl- oder wget-Skripten ausgelesen werden. Er wird aus Benutzernamen, Kennwort und der zu aktualisierenden Domain gebildet und sieht beispielsweise so aus:
azVRU6MzSaVRcWc0WWs193c4MImQ6vTA37fDIz1Dc=

Um statt der IPv4-Adresse die **IPv6-Adresse bei FreeDNS einzutragen**, aktivieren Sie die Checkbox „IPv6“ hinter dem jeweiligen Hash-Eintrag.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.8.3 DHCP-Server einrichten

Der DHCP-Server des EBW-H100 kann auf Anfrage anderen Geräten im LAN automatisch eine Adresse zuweisen. Diese automatisch vergebenen, dynamischen IP-Adressen sind nur für eine gewisse Zeit gültig. Die Gültigkeitsdauer der vom DHCP-Server vergebenen IP-Adressen steuern Sie über die „Lease Time“. Sollte sich im Netzwerk, in dem der EBW-H100 eingesetzt wird, bereits ein DHCP-Server befinden, so muss diese Funktion im Gerät unbedingt abgeschaltet werden, da sich ansonsten Clients ihre IP-Adresse vom falschen DHCP-Server zuteilen lassen.

IP-Adressen, die im IP-Pool liegen und für die eine Verknüpfung mit einer MAC-Adresse existiert, sind ausschließlich für diesen DHCP-Client reserviert. Die IP-Adresse liegt somit nicht mehr im IP-Pool. Es sollten für diese MAC-IP-Adress-Verknüpfungen keine IP-Adressen aus dem IP-Pool gewählt werden. Der Pool sollte nur für die DHCP-Clients zur Verfügung stehen, von denen keine MAC-Adresse bekannt ist oder berücksichtigt werden soll.

Konfiguration mit Web-Interface (Menü „Server-Dienste“, Seite „DHCP“)

Um den **DHCP-Server** einzurichten, aktivieren Sie die Checkbox „DHCP-Server aktivieren“.

Geben Sie in den Eingabefeldern „Erste und letzte IP-Adresse“ die **erste IP-Adresse** und die **letzte IP-Adresse** des Adressraumes ein, aus dem der DHCP-Server des Geräts Adressen im LAN vergibt. Der IP-Adressraum des DHCP-Servers muss in demselben Netzwerk liegen wie die IP-Adresse des EBW-H100.

Geben Sie im Eingabefeld „Lease Time“ eine **Gültigkeitsdauer** in Sekunden für die vom DHCP-Server zu vergebenden **IP-Adressen** ein. Der Standardwert ist 3600 Sekunden.

Um den **DHCP-Clients einen speziellen DNS-Server mitzuteilen**, geben Sie Eingabefeld „Alternative DNS-Server-Adresse“ dessen IP-Adresse ein. Ist das Feld leer, bekommen die Clients die lokale IP-Adresse des Routers und die IP-Adressen der fest eingestellten DNS-Server mitgeteilt.

Um einen **alternativen Gateway anzugeben**, geben Sie in das Eingabefeld „Alternative Default-Gateway-Adresse“ dessen IP-Adresse ein. Ist das Feld leer, wird den Clients die IP-Adresse des Routers als Gateway vorgeschlagen.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um die vom DHCP-Server vergeben IP-Adressen sowie deren „Lease Time“ (Gültigkeitsdauer) zu sehen, verwenden Sie den Link „DHCP-Lease Times anzeigen“.

Um bestimmten **DHCP-Clients immer die gleiche IP-Adresse zu geben**, können Sie im Abschnitt „Neue Zuordnung von MAC-Adresse und IP-Adresse“ feste Zuordnungen definieren. Geben Sie dazu in das Eingabefeld „MAC-Adresse“ die MAC-Adresse des jeweiligen DHCP-Clients und in das Feld „IP-Adresse“ die IP-Adresse, mit dem der DHCP-Client verknüpft werden soll, ein. Die MAC-Adresse kann mit oder ohne Doppelpunkten eingetragen werden, andere Formate werden nicht unterstützt. Speichern Sie die Zuordnung, indem Sie auf „OK“ klicken.

Um **eine oder mehrere Zuordnungen** zu **löschen**, aktivieren Sie im Abschnitt „Feste Zuordnung von IP-Adressen zu MAC-Adressen“ die Checkbox in der Spalte „löschen“ und klicken Sie auf „OK“, um die Einstellung zu übernehmen.

12.8.4 Router Advertiser konfigurieren

Mit dem Router Advertiser können IPv6-Prefixe im lokalen LAN bekannt geben werden. Im LAN angeschlossene Maschinen können sich anhand dieser empfangenen Prefixe selbständig eine oder mehrere IPv6-Adressen konfigurieren (SLAAC).

Als Hilfestellung zum Konfigurieren der zu verteilenden Prefixe wird angezeigt, welcher Prefix im EBW-H100 eingestellt ist und welche Prefixe an der LAN (ext)-Schnittstelle angezeigt werden.

Konfiguration mit Web-Interface (Menü „Server-Dienste“, Seite „Router Advertiser“)

Um den **Router Advertiser** zu verwenden, aktivieren Sie die Checkbox „Router Advertiser aktivieren“.

Wählen Sie die **Präferenz** im Dropdown-Listenfeld „Präferenz“ aus. Sie gibt an, mit welcher Wichtigkeit die Maschinen im LAN die empfangenen Routen behandeln sollen. Sind mehrere Router-Advertiser im LAN, die Default-Routen verteilen, entscheidet die Präferenz darüber, welche Default-Route die Maschine letztendlich benutzt.

Um einen **neuen Prefix hinzuzufügen**, geben Sie Abschnitt „Neuen Prefix hinzufügen“ die IPv6-Netzadresse und die dazugehörige Netzmaske in die jeweiligen Felder ein. Übernehmen Sie den Prefix, indem Sie auf „OK“ klicken.

Um einen **bestehenden Prefix zu löschen**, aktivieren Sie unter „Bestehende Prefixe“ die Checkbox des/der Prefix(e), der/die gelöscht werden soll(en).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.8.5 Proxy-Server konfigurieren

Der EBW-H100 bietet einen Proxy-Server. Dieser dient **nicht** als Cache für häufig aufgerufene Internetseiten. Er dient zum Verzögern der Verbindungs-Timeouts bei langsam aufbauenden Verbindungen und zum Ausfiltern von unerwünschten URLs (z.B. www.xyz.xx).

Der Proxy unterstützt die Protokolle HTTP und HTTPS.

Konfiguration mit Web-Interface (Menü „Server-Dienste“, Seite „Proxy“)

Um den **Proxy-Server einzuschalten**, aktivieren Sie die Checkbox „Proxy-Server aktivieren“.

Stellen Sie im Eingabefeld „**Port des Proxy-Servers**“ den Port ein, unter dem Sie den Proxy-Server aus dem internen Netz unter der IP-Adresse des EBW-H100 erreichen wollen.

Um **Verbindungen nach einer bestimmten Zeit zu beenden, die nicht mehr aktiv scheinen,** können Sie im Eingabefeld „Timeout für inaktive Verbindungen“ die Zeitdauer anpassen.

Um eine **Überlastung zu vermeiden**, können Sie die Anzahl der Clients beschränken, die sich gleichzeitig verbinden können. Geben Sie die maximale Anzahl gleichzeitig erlaubter Clients in das Eingabefeld „Maximale Anzahl an erlaubten Clients“ ein.

Um die **Verfügbarkeit des Proxys zu erhöhen**, können Sie eine minimale Anzahl von Proxy-Server-Prozessen festlegen. Geben Sie die gewünschte Anzahl von ständig laufenden Proxy-Server-Prozessen im Eingabefeld „Minimale Anzahl an freien Proxy-Servern“ ein.

Um eine **Überlastung mit Proxy-Anfragen zu verhindern**, können Sie eine maximale Anzahl von Proxy-Server-Prozessen festlegen. Für jede Anfrage eines Clients wird ein einzelner Proxy-Server-Prozess auf dem EBW-H100 gestartet. Geben Sie dazu eine gewünschte maximale Anzahl von gleichzeitigen Proxy-Server-Prozessen in das Eingabefeld „Maximale Anzahl an freien Proxy-Servern“ ein. Werden mehr Anfragen empfangen als Proxy-Server verfügbar sind, werden die überzähligen Anfragen abgewiesen.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.8.6 URL-Filter einrichten

Der Proxy-Server kann mit Hilfe des URL-Filters die möglichen URLs beschränken, die aus dem internen Netz des EBW-H100 von Rechnern aufgerufen werden können. Damit werden nur noch Zugriffe auf URLs erlaubt, die in der Filterliste eingetragen sind, alle anderen URLs sind gesperrt. Um den Zugriff auf das Internet nur noch über den Proxy zuzulassen, ist außerdem die Aktivierung der Firewall erforderlich. Ohne die Firewall wäre der Zugriff auf beliebige URLs durch einfache Umgehung des Proxy möglich.

Auf den Clients (.z.B. einem Web-Browser auf einem PC), die über den Proxy Verbindungen aufbauen sollen, müssen die IP-Adresse und der Port des Proxy eingestellt sein.

Konfiguration mit Web-Interface (Menü „Server-Dienste“, Seite „Proxy“)

Um den **URL Filter einzuschalten**, aktivieren Sie die Checkbox „Filter aktivieren“.

Um eine **zulässige URL einzutragen**, die aus dem internen Netz erreichbar sein soll, tragen Sie die gewünschte URL in die Eingabefelder „Erlaubte URLs“ ein.

Um eine **URL aus der Liste zu löschen**, löschen Sie den Text der URL aus der Liste.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.8.7 IPT konfigurieren

Der EBW-H100 ermöglicht auch eine Datenübertragung über einen IPT-Kanal. Dabei kann er als IPT-Slave fungieren.

Konfiguration mit Web-Interface (Menü „Server-Dienste“, Seite „IPT“)

Um **IPT zu aktivieren**, markieren Sie die Checkbox „IPT-Slave aktivieren“.

Um den **aktuellen Zustand des IPT-Slave** anzuzeigen, wählen Sie den Link „IPT-Status“.

Um die **Meldungen des IPT-Slave** anzuzeigen, wählen Sie den Link „IPT-Log“. Damit können Sie bei einem erfolglosen Verbindungsversuch Rückschlüsse auf die Fehlerursache erhalten.

Um die **Verbindung zum IPT-Master** zu konfigurieren, geben Sie dessen IP-Adresse oder den Domain-Namen in das Eingabefeld „IP-Adresse oder Domainname“ ein. Geben Sie den Port, auf dem der IPT-Master die Verbindung entgegennimmt in das Eingabefeld „Port“ ein. Geben Sie die Zugangsdaten für die Anmeldung am IPT-Master in die Eingabefelder „Benutzername“ und „Kennwort“ ein. Diese Daten sind für den primären IPT-Master einzugeben. Optional kann ein sekundärer IPT-Master angegeben werden, der nach einem erfolglosen Verbindungsversuch zum primären IPT-Master verwendet wird.

Um den **IPT Device Identifier** festzulegen, geben Sie diesen in das Eingabefeld „IPT Device Identifier“ ein. Standardmäßig ist eine Kombination des Kürzels „INS“ und der MAC-Adresse des EBW-H100 eingetragen.

Um die **Wartezeit zwischen den Verbindungsversuchen** zu erhöhen, markieren Sie die Checkbox „Wartezeit zwischen Verbindungsversuchen erhöhen“. In diesem Fall steigt die Wartezeit zwischen den Verbindungsaufbauversuchen an (1, 5, 15, 30, 60 Minuten). Ansonsten versucht der EBW-H100 jede Minute, eine Verbindung aufzubauen.

Um die **maximale Zeit zwischen IPT-Request und IPT-Response** festzulegen, ab deren Überschreitung eine Verbindung zum IPT-Master getrennt und wieder neu aufgebaut wird, geben Sie diese Zeit in Sekunden in das Feld „Timeout zwischen Anfrage und Antwort“ ein.

Um die **maximale Zeit zwischen zwei Zeichen eines IPT-Kommandos** festzulegen, ab deren Überschreitung eine Verbindung zum IPT-Master getrennt und wieder neu aufgebaut wird, geben Sie diese Zeit in Sekunden in das Feld „Timeout zwischen Zeichen“ ein.

Um eine **Verschleierung der IPT-Verbindung** zu aktivieren, markieren Sie die Checkbox „Verschleierung verwenden“. Wird die Verschleierung verwendet, so muss ein Challenge und ein Fix Scramble Key angegeben werden. Mit dem Fix Scramble Key wird die Anmeldung am IPT-Master verschlüsselt, während der Challenge Scramble Key für die Verschlüsselung nach der erfolgreichen Anmeldung verwendet wird. Während der Challenge Scramble Key vom Slave an den Master übergeben wird, muss der Fix Scramble Key sowohl am Master als auch am Slave identisch eingestellt sein. Beide Schlüssel müssen die feste Länge von 32 Byte besitzen, welche in der Konfiguration hexadezimal mit 64 Stellen anzugeben sind.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken. Dabei wird der IPT-Slave neu gestartet. Bestehende IPT-Verbindungen zum Master oder bestehende IPT-Datentunnel werden vorher abgebaut.

12.8.8 SNMP-Agent konfigurieren

Der EBW-H100 verfügt über einen SNMP-Agent, der die eingehenden SNMP-Get-Requests beantwortet. Alle Parameter, die in der ASCII-Konfigurationsdatei vorkommen, können mittels SNMP-Get-Requests ausgelesen werden (davon ausgenommen sind Benutzername und Kennwort der Authentifizierung für das Web-Interface). Diese Parameter sind in der MIB (Management Information Base) beschrieben.

Konfiguration mit Web-Interface (Menü „Server-Dienste“, Seite „SNMP-Agent“)

Um den **SNMP-Agent** zu aktivieren, markieren Sie die Checkbox „SNMP-Agent aktivieren“.

Um die **private MIB herunterzuladen**, klicken Sie auf den Link „Private MIB herunterladen“.

Um SNMP-Get-Requests **nur aus dem lokalen Netz** zuzulassen und Antworten nur ins lokale Netz zu senden, markieren Sie die Checkbox „SNMP nur lokal zulassen“.

Um den **Port** festzulegen, auf dem der SNMP-Agent UDP-Nachrichten empfängt, geben Sie den Port in das Feld „Port“ ein.

Um eine **Kontakt-Information** für den SNMP-Agent anzugeben, können Sie diese in das Feld „Kontakt-Information“ eintragen.

Um eine **Beschreibung** für den SNMP-Agent anzugeben, können Sie diese in das Feld „Beschreibung“ eintragen.

Um den **SNMP-Agent** zu verwenden, müssen Sie die SNMP-Versionen angeben und konfigurieren, die verwendet werden sollen. Um SNMP v1 oder SNMP v2c zu verwenden, markieren Sie die Checkbox „SNMP v1/v2c verwenden“ und geben Sie den Community-String in das Feld „Community“ ein. Um SNMP v3 zu verwenden, markieren Sie die Checkbox „SNMP v3 verwenden“ und geben Sie den SNMP-Benutzernamen in das Feld „Benutzername“ ein. Um eine SNMP v3-Authentifizierung zu verwenden, wählen Sie die Authentifizierungsmethode in der Dropdown-Liste „Authentifizierung“ aus und geben Sie das Kennwort für die Authentifizierung (mindestens 8 Zeichen) in das entsprechende Feld ein. Um eine SNMP v3-Verschlüsselung zu verwenden, wählen Sie die Verschlüsselungsmethode in der Dropdown-Liste „Verschlüsselung“ aus und geben Sie das Kennwort für die Verschlüsselung (mindestens 8 Zeichen) in das entsprechende Feld ein. Voraussetzung für eine Verschlüsselung ist eine Authentifizierung.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.8.9 MCIP konfigurieren

MCIP (Management Control and Information Protocol) ist ein minimalistisches Protokoll zum Austausch kurzer Telegramme zwischen einem MCIP-Server und MCIP-Gerätetreibern basierend auf TCP. Gerätetreiber melden sich beim MCIP-Server an und teilen ihm mit, welche Objekt-IDs (OIDs) durch ihn angesprochen werden können. Den im Router enthaltenen Objekten kann eine OID zugewiesen werden, so dass sie in MCIP-Telegrammen adressiert werden können. Der Zustand der Objekte kann über die Gerätetreiber gesetzt und/oder abgefragt werden.

Konfiguration mit Web-Interface (Menü „Server-Dienste“, Seite „MCIP“)

Damit sich **Gerätetreiber beim MCIP-Server über TCP anmelden** dürfen, aktivieren Sie die Checkbox „Eingehende TCP-Verbindungen annehmen an Port“ und geben Sie den TCP-Port im Feld dahinter an.

Um **MCIP-Verbindungen auf das lokale Netzwerk zu beschränken**, aktivieren Sie die Checkbox „MCIP nur lokal zulassen“. Dann werden keine MCIP-Verbindungen über die WAN-Schnittstelle angenommen.

Ordnen Sie den im EBW-H100 enthaltenen **Objekten eine Objekt-ID** zu, indem Sie diese in das Feld hinter dem jeweiligen Objekt eintragen. Eine OID ist eine Nummer zwischen 1001 und 65534.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.9 Systemkonfiguration

Der EBW-H100 zeigt Systemdaten wie Firmware-Version, Seriennummer, Hardware-Stand oder die Firmware-Prüfsumme zusammen mit kurzen Systemmeldungen über Ereignisse und Fehler im Menü „System“ auf der Seite „Systemdaten“ an. Diese Informationen sind hilfreich und sollten zusammen mit der eingestellten IP-Adresse bekannt sein, wenn Sie mit dem Support Kontakt aufnehmen. Weiterhin ermöglichen verschiedene Links die Anzeige von Systemzuständen oder Verbindungs-Logs.

12.9.1 System-Log anzeigen

Der EBW-H100 ermöglicht die Anzeige des ausführlichen System-Logs im Menü „System“ auf der Seite „Systemdaten“ an. Die Anzahl der angezeigten Zeilen und das Aktualisierungsintervall können dabei eingestellt werden.

Konfiguration mit Web-Interface (Menü „System“, Seite „Systemdaten“)

Um die **ausführlichen Systemmeldungen über das Web-Interface anzusehen**, klicken Sie auf den Link „Anzeigen des ausführlichen System Logs“.

Um die **Anzeige des System-Logs zu konfigurieren**, geben Sie auf der Seite „Systemlog“ in das Feld „Aktualisierung alle“ das Intervall für die Aktualisierung des Logs in Sekunden sowie in das Feld „Anzeige von … Zeilen“ die Anzahl der anzuzeigenden Zeilen ein und wählen Sie „OK“.

12.9.2 Anzeigen der letzten Systemmeldungen

Der EBW-H100 zeigt kurze Systemmeldungen über Ereignisse und Fehler im Menü „System“ auf der Seite „Systemdaten“ an. Für Analysezwecke können Sie sich die letzten Meldungen anzeigen lassen.

Konfiguration mit Web-Interface (Menü „System“, Seite „Systemdaten“)

Um die letzten **Systemmeldungen anzuzeigen**, klicken Sie auf den Link „Anzeigen der letzten Systemmeldungen“.

12.9.3 Uhrzeit und Zeitzone einstellen

Der EBW-H100 besitzt eine interne Uhr, um zeitabhängige Vorgänge steuern zu können. Diese Uhr müssen Sie einstellen, damit zeitabhängige Vorgänge auch zum gewünschten Zeitpunkt pünktlich ausgeführt werden und Systemmeldungen richtig datiert sind. Die Uhr kann automatisch über einen NTP-Server aus dem Internet aktualisiert werden. Bei jedem Verbindungsaufbau wird versucht, die Uhrzeit vom festgelegten NTP-Server zu synchronisieren. Die Zeitzone muss im Gegensatz zur Uhrzeit selbst manuell dem Standort angepasst werden. Auf dem Router selbst kann auch ein NTP-Server für das lokale Netz gestartet werden. Dann ist es sehr empfehlenswert, dass der Router seine Uhr über eine WAN-Verbindung auch regelmäßig synchronisiert, damit die Gangungenauigkeit der internen Uhr durch eine regelmäßige Synchronisierung kompensiert wird, um im Laufe der Zeit keine ungenaue Uhrzeit im Netzwerk zu verbreiten.

ⓘ Die Uhrzeit wird bei einer Trennung von der Spannungsversorgung nicht gepuffert!

Konfiguration mit Web-Interface (Menü „System“, Seite „Zeit“)

Um die **Uhrzeit sowie das Datum einzustellen** geben Sie die Werte für Tag, Monat, Jahr sowie Stunden und Minuten in die Eingabefelder „TT MM JJJJ hh mm“ ein.

Stellen Sie **die Zeitzone des Einsatzorts** ein, in dem Sie diese aus der Dropdown-Liste „Zeitzone“ auswählen.

Um die **Uhrzeit sowie das Datum per NTP-Server zu synchronisieren**, aktivieren Sie die Checkbox „Uhrzeitsynchronisierung über“ und geben Sie den Namen eines NTP-Servers oder dessen IP-Adresse in das Eingabefeld ein.

Um die **Uhrzeit sowie das Datum per NTP-Server täglich zu einem bestimmten Zeitpunkt zu synchronisieren**, aktivieren Sie die Checkbox „Zusätzlich jeden Tag um“ und geben Sie die Uhrzeit für die tägliche Synchronisierung in das Eingabefeld ein.

Um die **Uhrzeit sowie das Datum per NTP-Server sofort zu synchronisieren**, aktivieren Sie die Checkbox „Uhrzeit sofort synchronisieren“. Dann wird einmalig mit dem Speichern der Einstellungen versucht, eine Verbindung mit dem NTP-Server aufzubauen, um die Uhrzeit zu synchronisieren. Dies ermöglicht einen sofortigen Test der NTP-Server-Einstellungen.

Um **selbst als NTP-Server zu fungieren**, aktivieren Sie die Checkbox „Lokalen Zeit-Server aktivieren“. Dann werden an UDP-Port 123 lokale NTP-Anfragen beantwortet.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.9.4 Zurücksetzen (Reset)

Sie können den EBW-H100 über das Web-Interface oder mit dem Reset-Taster auf der Gerätevorderseite zurücksetzen. Mit dem Reset-Taster können Sie durch einmaliges, kurzes Drücken einen Software-Reset auslösen. Ein mindestens drei Sekunden dauerndes Drücken löst einen Hardware-Reset aus. Beide Male wird ein Neustart durchgeführt. Durch dreimaliges, kurzes Drücken innerhalb von zwei Sekunden laden Sie die Werkseinstellungen (siehe Abschnitt Anzeige- und Bedienelemente – Funktion der Bedienelemente).

Konfiguration mit Web-Interface (Menü „System“, Seite „Reset“)

Um **neu zu starten**, wählen Sie den Radiobutton „Neustart“ aus. Klicken Sie auf „OK“, um den Neustart durchzuführen.

Um **neu zu starten und gleichzeitig die Werkseinstellungen zu laden**, wählen Sie über den Radiobutton „Grundeinstellungen laden und neu starten“ aus. Klicken Sie anschließend auf „OK“, um den Neustart durchzuführen und das Gerät auf die Werkseinstellungen zurückzusetzen.

Um einen **täglichen Neustart zu einem bestimmten Zeitpunkt zu konfigurieren**, aktivieren Sie die Checkbox „Täglicher Neustart um“ und geben Sie die Uhrzeit für den täglichen Neustart in das Eingabefeld ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.9.5 Update

Sie können den EBW-H100 über das Web-Interface mit einer neuen Firmware oder einer neuen Konfiguration versorgen. Eine detaillierte Beschreibung dieser Vorgänge finden Sie in den folgenden Abschnitten „Aktualisieren der Firmware“ und „Hochladen der Konfigurationsdatei“ dieses Handbuchs.

Weiterhin ist eine tägliche automatische Aktualisierung von Firmware-Dateien, Konfigurationsdateien (binär und ASCII) oder Sandbox-Image-Dateien möglich. Dazu müssen diese auf einem Server entsprechend bereitgestellt werden.

Hinweis

Verlust der Erreichbarkeit!

Durch eine Änderung der Konfiguration kann Ihr EBW-H100 eventuell nicht mehr für eine weitere Konfiguration erreichbar sein (z.B. durch Verändern der IP-Adresse).

Prüfen Sie kritische Einstellungen, wie IP-Adresse oder Zugangsdaten (Benutzernamen, Kennwörter), besonders sorgfältig.

Konfiguration mit Web-Interface (Menü „System“, Seite „Update“)

Um das **automatische tägliche Update zu aktivieren**, markieren Sie die Checkbox „Automatisches tägliches Update aktivieren“.

Um das **Dateiübertragungsprotokoll auszuwählen**, wählen Sie den Radiobutton „HTTP“ bzw. „FTP“.

Um den **Speicherort der Aktualisierungsdateien anzugeben**, geben Sie in das Feld „Server“ die IP-Adresse oder den Domain-Namen des Servers und in das Feld “Port“ den entsprechenden Port ein. Beim Server können auch Unterverzeichnisse angegeben werden, in denen nach den Dateien gesucht werden soll.

Um die **tägliche Aktualisierung auf einen festen, von der MAC abhängigen Zeitpunkt festzulegen**, wählen Sie unter „Update-Zeitpunkt“ den Radiobutton „von MAC abhängig“.

Um die **tägliche Aktualisierung auf einen benutzerdefinierten Zeitpunkt festzulegen**, wählen Sie unter „Update-Zeitpunkt“ den Radiobutton „fest“ und geben Sie dahinter die Uhrzeit für die Aktualisierung an.

Um die **tägliche Aktualisierung direkt nach dem WAN-Verbindungsaufbau durchzuführen**, wählen Sie unter „Update-Zeitpunkt“ den Radiobutton „nach jedem WAN-Verbindungsaufbau“.

Wenn der **Zugriff auf die Dateien nur nach einer Authentifizierung** erfolgen kann, geben Sie in den Feldern „Benutzername“ und „Kennwort“ die entsprechenden Zugangsdaten an.

Um zu Testzwecken die **automatische Aktualisierung sofort auszulösen**, markieren Sie die Checkbox „Sofort nach Updates suchen“.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um eine **Firmware- oder Konfigurationsdatei (binär oder ASCII) hochzuladen**, klicken Sie im Abschnitt „Manuelles Update“ die Schaltfläche „Durchsuchen…“. Wählen Sie dann im Fenster „Datei hochladen“ die gewünschte Image-Datei auf dem entsprechenden Datenträger aus und klicken Sie auf die Schaltfläche „Öffnen“. Klicken Sie dann auf die Schaltfläche „OK“ um die Datei hochzuladen.

12.9.6 Aktualisieren der Firmware

Sie können die Firmware des EBW-H100 manuell aktualisieren. Die Firmware ist eine Zusammenstellung von Betriebsystem und Programmen, in der die Gerätefunktionen implementiert sind. Die aktuellste Firmware finden Sie unter www.insys-icom.de/firmware.

Hinweis

Funktionsverlust durch fehlerhaftes Update!

Durch einen Verbindungsabbruch während des Updates und einen darauffolgenden Neustart kann der EBW-H100 seine Funktion verlieren.

Solange die rote Status-LED leuchtet, dürfen Sie keinerlei Aktionen am Web-Interface durchführen, die Spannungsversorgung nicht trennen und keinen Reset ausführen.

Starten Sie bei nach einem fehlgeschlagenen Update das Gerät nicht neu und setzen Sie sich mit dem Support von INSYS icom in Verbindung.

Vollständiges Update der Firmware

Im Folgenden erfahren Sie, welche die Schritte Sie prinzipiell zum Update der Firmware durchführen müssen.

- Sie haben Zugriff auf das Web-Interface.
- Falls Sie über eine Wählverbindung auf das Web-Interface zugreifen, muss die Verbindung lange genug bestehen, um die Uploads durchzuführen. Die Option „maximale Verbindungszeit“ sollte für das Update auf „0“ gesetzt werden, ebenso wie die „Idle Time“.
- Sie haben sichergestellt, dass die Stromversorgung während dem Updatevorgang nicht ausgeschaltet werden kann.
- Sie besitzen die Firmware-Dateien mit den Namen „system_<rev>“ und „data_<rev>“. Die Dateien sind auf dem PC auffindbar, von dem Sie das Update durchführen wollen.

1. ***Wechseln Sie im Menü „System“ auf die Seite „Update“.***

2. ***Klicken Sie im Abschnitt „Manuelles Update“ auf Durchsuchen... und wählen Sie die Datei „system_<rev>“ aus.***

3. ***Klicken Sie auf OK, um mit dem Update zu beginnen.***

   ✓ Eine Seite mit einer Sicherheitsabfrage erscheint. Vergleichen Sie die angezeigte MD5-Prüfsumme mit der MD5-Prüfsumme der Datei (z.B. mit dem Programm md5sum.exe). Wenn sie übereinstimmen, wurde die Datei korrekt übertragen und Sie können mit der Aktualisierung fortfahren. Der Vorgang dauert je nach Firmwaregröße unterschiedlich lange, bis die Datei vollständig übertragen ist.

4. ***Bestätigen Sie die Abfrage mit Ja.***

   ✓ Der Updatevorgang startet. Der Browser wartet. Während des Updates leuchtet die Status/VPN-LED rot auf.

   ✓ Nach dem vollständigen Update wird eine Seite angezeigt, die Ihnen den erfolgreichen Updatevorgang bestätigt. Bis zum Erscheinen dieser Anzeige darf keinesfalls eine Aktion am Web-Interface durchgeführt werden.

   ⓘ Eine Aktualisierung der Datei „data_<rev>“ ist nicht immer erforderlich. Weitere Informationen dazu finden Sie in dem PDF-Dokument, dass im Firmware-Paket enthalten ist.

5. ***Um auch die Datei „data_<rev>“ hochzuladen, gehen Sie mit der zweiten Datei „data_<rev>“ vor wie mit der ersten Datei, ohne vorher einen Neustart auszuführen. Wiederholen Sie die Schritte ab Schritt 1. Nach dem Hochladen erfolgt ein automatischer Neustart.***

6. ***Wenn Sie nur die Datei „system_<rev>“ hochgeladen haben, wechseln Sie im Menü „System“ auf die Seite „Reset“, wählen Sie „Neustart“ und klicken Sie auf OK.***

   ✓ Die neue Firmware ist nun aktiv.

Hinweis

Deaktivierung der Sandbox!

Wenn ein Firmwareupdate durchgeführt wird, wird eine eventuell laufende Sandbox vorher deaktiviert.

Beachten Sie bei Ihrer Anwendung, dass eine laufende Sandbox deaktiviert wird, wenn ein Firmware-Update erfolgt.

12.9.7 Hochladen der Konfigurationsdatei

Sie können eine zuvor herunter geladene bzw. bearbeitete Konfigurationsdatei auf den EBW-H100 hochladen, um die momentane Konfiguration durch die in der Datei enthaltenen Einstellungen zu ersetzen.

Hochladen der Konfigurationsdatei

→ Sie besitzen eine Konfigurationsdatei für Ihre Version des EBW-H100.

1. ***Wechseln Sie im Web-Interface unter „System" auf die Seite „Update".***

2. ***Klicken Sie im Abschnitt „Manuelles Update" auf Durchsuchen... und wählen Sie die Konfigurationsdatei (z.B. configuration.bin) aus.***

3. ***Klicken Sie auf OK, um mit dem Hochladen zu beginnen.***

   ✓ Eine Seite mit einer Sicherheitsabfrage erscheint.

4. ***Bestätigen Sie die Abfrage mit Ja.***

   ✓ Der Updatevorgang der Konfiguration startet.

   ✓ Nach dem vollständigen Hochladen der Konfiguration wird eine Seite angezeigt, die Ihnen den erfolgreichen Updatevorgang bestätigt.

5. ***Wechseln Sie im Menü „System" auf die Seite „Reset", wählen Sie „Neustart" und klicken Sie auf OK.***

   ✓ Die neue Konfiguration ist nun aktiv.

12.9.8 Download

Sie können die vollständige Konfiguration des EBW-H100 in binärer, verschlüsselter Form über das Web-Interface herunterladen. Mit dieser Datei können Sie weitere, gleiche Geräte konfigurieren oder eine funktionierende Konfiguration sicher aufbewahren.

Weiterhin ist es möglich, eine ASCII-Textdatei der Konfiguration oder eine „leere“ Konfigurationsdatei (ASCII-Vorlage) herunterzuladen. Eine Beschreibung der ASCII-Konfigurationsdatei finden Sie im entsprechenden Zusatzhandbuch.

Das Herunterladen der verschiedenen Log-Dateien ist ebenso möglich. Je nach Ausführung werden verschiedene Log-Dateien zur Verfügung gestellt. Dabei steht immer die aktuelle Log-Datei zur Verfügung. Wenn diese Log-Datei eine Größe von 1 MByte überschreitet, wird sie mit einem Zeitstempel versehen und als bzip2-komprimierte Archiv-Datei abgespeichert. Es werden bis zu vier der letzten Archiv-Dateien für den Download vorgehalten.

Für Support-Fälle gibt es die Möglichkeit, ein Support-Paket herunterzuladen. Dieses enthält den Status des laufenden Geräts und die gesamte Konfiguration und somit alle Daten, um bei Inanspruchnahme des Hersteller-Supports eine gute Grundlage zur Problemerkennung zu liefern. Das Support-Paket wird verschlüsselt, so dass die darin enthaltenen geheimen Kennwörter oder Schlüssel beim unsicheren Versand des Support-Pakets nicht unautorisiert ausgelesen werden können.

Konfiguration mit Web-Interface (Menü „System“, Seite „Download“)

Um die **binäre Konfigurationsdatei herunterzuladen**, klicken Sie auf den Link „Binär“. Im Link wird auch der Name der zuletzt hochgeladenen Konfiguration angezeigt. Sie werden dann vom Browser aufgefordert, die Datei abzuspeichern.

Um die **ASCII-Konfigurationsdatei herunterzuladen**, klicken Sie mit der rechten Maustaste auf den Link „ASCII“ und wählen Sie im Kontextmenü „Ziel speichern unter…“. Speichern Sie dann die Datei ab.

Um eine **leere ASCII-Konfigurationsdatei herunterzuladen**, klicken Sie mit der rechten Maustaste auf den Link „ASCII-Vorlage“ und wählen Sie im Kontextmenü „Ziel speichern unter…“. Speichern Sie dann die Datei ab.

Um die **Log-Dateien herunterzuladen**, klicken Sie mit der rechten Maustaste auf den jeweiligen Link und wählen Sie im Kontextmenü „Ziel speichern unter…“. Speichern Sie dann die Datei ab.

Um das **Support-Paket herunterzuladen**, klicken Sie auf den Link „Neues Support-Paket erstellen“. Klicken Sie auf den daraufhin erscheinenden Download-Link, um das Support-Paket zu speichern.

12.9.9 Sandbox

Der EBW-H100 verfügt über eine frei programmierbare Sandbox. Die Sandbox ist eine Art virtueller Maschine, die auf dem Gerät läuft. In der Sandbox kann man Programme starten, Daten sammeln und Dienste anbieten, die im System des eigentlichen Geräts nicht vorhanden sind. Außerdem kann der EBW-H100 aus der Sandbox heraus über eine ASCII-Konfigurationsdatei konfiguriert werden. Weiterhin kann eine aktuelle Konfiguration in die Sandbox importiert werden. Weitere Einzelheiten dazu finden Sie im Zusatzhandbuch für die ASCII-Konfigurationsdatei.

Weitere Informationen zur Sandbox und deren Verwendung finden Sie unter http://www.insys-icom.de/Sandbox.

Konfiguration mit Web-Interface (Menü „System“, Seite „Sandbox“)

Um die **Sandbox zu aktivieren**, markieren Sie die Checkbox „Sandbox aktivieren“.

Um das **Kennwort für den Benutzer „user“** zu konfigurieren, geben Sie das gewünschte Kennwort in das Feld „Neues Kennwort“ ein (das Default-Kennwort ist „user“). Der Benutzername selbst kann nicht verändert werden. Erlaubt sind hier nur die Zeichen 0 bis 9, a bis z, A bis Z und die Sonderzeichen ! " # $ % : ' ( ) * + , - . / ; < = > ? @ [ ] \ ^ _ { } | ~. Das kaufmännische Und „&“ ist nicht erlaubt.

Der Dateiname des aktuell **gespeicherten Sandbox-Images** wird hinter „Gespeichertes Sandbox-Image:“ zusammen mit seiner MD5-Prüfsumme angezeigt.

Der Dateiname des aktuell **installierten Sandbox-Image** wird hinter „Installiertes Sandbox-Image:“ zusammen mit seiner MD5-Prüfsumme angezeigt.

Um ein **gespeichertes Sandbox-Image zu installieren**, muss die Checkbox „Gespeichertes Sandbox-Image installieren“ markiert werden. Das Image wird dann beim Speichern der Einstellungen mit „OK“ installiert.

ⓘ Wenn sich ein installiertes Sandbox-Image nicht mehr starten lässt (weil z.B. wichtige Dateien aus Versehen gelöscht wurden), kann durch das erneute Installieren des Standard-Images wieder der Ursprungszustand der Sandbox hergestellt werden.

Um die **RS232-Schnittstelle für die Sandbox zu reservieren**, muss die Checkbox „RS232-Schnittstelle für Sandbox reservieren“ markiert werden.

Um eine **Konfiguration ohne Authentifizierung aus der Sandbox zuzulassen**, muss die Checkbox „ASCII-Konfiguration ohne Authentifizierung aus der Sandbox zulassen“ markiert werden. In dem Fall wird einmal in der Minute in der Sandbox nach der Datei /var/spool/ascii_config.txt gesucht. Existiert diese, wird der EBW-H100 mit dieser ASCII-Datei konfiguriert. Anschließend wird die Datei in der Sandbox gelöscht.

Um ein **neues Sandbox-Image beim automatischen Update zu installieren**, muss die Checkbox „Neues Sandbox-Image beim Automatischen Update installieren“ markiert werden. Ansonsten wird es nur gespeichert und muss manuell installiert werden.

Hinweis

Unbefugter Zugriff auf das Gerät!

Wenn die Konfiguration ohne Authentifizierung aus der Sandbox zugelassen ist, kann die Konfiguration für unberechtigte Zugriffe manipuliert werden.

Stellen Sie sicher, dass nur autorisierte Benutzer Zugriff auf die Sandbox haben! Durch unbefugten Zugriff auf die Sandbox kann die Konfiguration über diese Funktion geändert werden, so dass der Angreifer Zugriff auf die Konfiguration und somit auch zu weiteren vertraulichen Informationen, wie z.B. VPN-Schlüssel oder Kennwörter, erlangt.

Um ein **neues Sandbox-Image hochzuladen**, klicken Sie im Abschnitt „Neues Sandbox-Image laden“ auf die Schaltfläche „Durchsuchen…“. Wählen Sie dann im Fenster „Datei hochladen“ die gewünschte Image-Datei auf dem entsprechenden Datenträger aus und klicken Sie auf die Schaltfläche „Öffnen“. Klicken Sie dann auf die Schaltfläche „OK“ um die Datei hochzuladen.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.9.10 Debugging

Verschiedene Werkzeuge des EBW-H100 ermöglichen es, Probleme mit Netzwerkverbindungen zu analysieren.

Mit dem Werkzeug "PING" können ICMP-Pings (Ping-Pakete) versendet werden. Damit lässt sich oft auf einfache Art und Weise testen, ob eine bestimmte Maschine im Netzwerk erreichbar ist. Das Werkzeug „TRACEROUTE“ zeigt die Route, die ein IP-Paket zu seinem Ziel benutzt. Mit dem Werkzeug "DNS LOOKUP" können DNS-Informationen über eine IP-Adresse oder einen Domain-Namen erfragt werden. Mit Hilfe des Werkzeugs "TCPDUMP" können Netzwerkpakete aufgezeichnet werden.

Konfiguration mit Web-Interface (Menü „System“, Seite „Debugging“)

Um ein **Ping-Paket zu versenden**, wählen Sie das Werkzeug „PING“ für IPv4-Pings bzw. „PING6“ für IPv6-Pings in der Dropdown-Liste aus, geben Sie die IP-Adresse, an die Sie das Ping-Paket senden wollen, oder den Domain-Namen in das Feld „Parameter“ ein und klicken Sie auf „OK“. Optional können davor noch zusätzliche Parameter angegeben werden, wie z.B. „-s 300“ (versendet 300 Bytes Nutzdaten im ICMP-Ping) oder „-c 3“ (versendet 3 Pings hintereinander). Die Antwort wird unten auf der Seite angezeigt.

Um die **Route eines IP-Pakets zu verfolgen**, wählen das Werkzeug „TRACEROUTE“ für IPv4-Pakete bzw. „TRACEROUTE6“ für IPv6-Pakete in der Dropdown-Liste aus, geben Sie die IP-Adresse, an die Sie das IP-Paket senden wollen, oder den Domain-Namen in das Feld „Parameter“ ein und klicken Sie auf „OK“. Optional kann die standardmäßige Zahl von 3 Hops noch erhöht werden, indem davor noch mit dem Parameter „-m 5“ die Anzahl der Hops auf beispielweise 5 erhöht wird. Die Antwort wird unten auf der Seite angezeigt.

Um **DNS-Informationen abzufragen**, wählen das Werkzeug „DNS LOOKUP“ in der Dropdown-Liste aus, geben Sie die IP-Adresse oder den Domain-Namen, die abgefragt werden sollen, in das Feld „Parameter“ ein und klicken Sie auf „OK“. Wenn kein DNS-Server konfiguriert wurde oder von einem externen Provider oder Router zugewiesen wurde, kann diese Anfrage bis zu 40 Sekunden dauern.

Um die **Aufzeichnung von Netzwerkpaketen zu starten**, wählen Sie das Werkzeug „TCPDUMP“ in der Dropdown-Liste aus, geben Sie mit dem Parameter „-i“ mindestens das Netzwerkgerät in das Feld „Parameter“ ein (z.B. "-i br0" für die LAN-Schnittstelle) und klicken Sie auf „OK“. Die zur Verfügung stehenden Netzwerkgeräte können ermittelt werden, indem Sie im Menü „System“ auf der Seite „Systemdaten“ den Link „Anzeigen des System-Status“ wählen. Nach dem Starten läuft die Aufzeichnung so lange, bis sie entweder manuell gestoppt wird, die geloggte Netzwerkschnittstelle geschlossen wird (z.B. die Mobilfunkschnittstelle) oder bis die Aufzeichnung eine Größe von 1 MB erreicht hat. Die Aufzeichnung wird nach dem Stoppen sofort im Text-Format angezeigt und kann über den dann erscheinenden Link „TCPDUMP Aufzeichnung“ als Datei heruntergeladen werden. Sie kann mit „tcpdump“ oder „wireshark“ auf einer externen Maschine betrachtet werden. Die Aufzeichnung wird bei einem Neustart des Geräts nicht gespeichert.

12.10 Überwachung

Die Monitoring App (Überwachungsapplikation) des EBW-H100 wird nach dem Aufruf des Menüpunkts „Monitoring“ in einem separatem Fenster Ihres Browsers angezeigt. Dabei handelt es sich um eine Software-Applikation, die auf dem Gerät läuft und unabhängig vom Gerät konfiguriert wird.

Hier ist zu beachten, dass die Funktionalität der Überwachungsapplikation von Einstellungen am Gerät beeinflusst (z.B. Schnittstellenreservierungen für die Sandbox) werden kann.

Die Funktion und Konfiguration ist im Zusatzhandbuch für die Monitoring App beschrieben. Das Zusatzhandbuch kann auf der Dokumentationsseite (www.insys-icom.de/doku) unter dem jeweiligen Router heruntergeladen werden.

13 Wartung, Reparatur und Störungsbeseitigung

13.1 Wartung

Das Produkt ist wartungsfrei und erfordert keine besondere regelmäßige Wartung.

13.2 Störungsbeseitigung

Sollten während des Betriebs des Produkts eine Störung auftreten, finden Sie Hinweise zur Störungsbeseitigung in der „Knowledge Base“ auf unserer Webseite (http://www.insys-icom.de/knowledge/). Falls Sie weitere Unterstützung benötigen, setzen Sie sich mit Ihrem Vertriebspartner oder dem Support von INSYS icom in Verbindung. Sie erreichen unsere Support-Abteilung per E-Mail unter support@insys-tec.de.

13.3 Reparatur

Senden Sie defekte Produkte mit detaillierter Fehlerbeschreibung an die Bezugsquelle Ihres Geräts. Falls Sie das Gerät direkt von INSYS icom bezogen haben senden Sie das Gerät bitte an: INSYS MICROELECTRONICS GmbH, Hermann-Köhl-Str. 22, 93049 Regensburg.

Vor dem Versand des Geräts:

- Entfernen Sie möglicherweise eingelegte SIM-Karten.
- Sichern Sie die auf dem Gerät befindlichen Konfigurationen und ggf. weitere darauf gespeicherte Daten.
- Sichern Sie möglicherweise auf dem Gerät laufende Sandbox-Applikationen.

Vorsicht!

Kurzschlüsse und Beschädigung durch unsachgemäße Reparaturen und Modifikationen sowie Öffnen von Produkten!

Brandgefahr und Beschädigung des Produkts.

Das Öffnen des Produkts für Reparaturarbeiten oder Modifikationen ist nicht erlaubt.

14 Entsorgung

14.1 Rücknahme der Altgeräte

Gemäß den Vorschriften der WEEE ist die Rücknahme und Verwertung von INSYS-Altgeräten für unsere Kunden wie folgt geregelt:

Bitte senden Sie Ihre Altgeräte frachtfrei an folgende Adresse:

Frankenberg-Metalle
Gärtnersleite 8
96450 Coburg
Deutschland

Diese Vorschrift gilt für Geräte aus Lieferungen ab dem 13.08.2005.

ⓘ Bitte denken Sie vor der der Entsorgung des Geräts auch an evtl. gespeicherte Passwörter oder Sicherheitszertifikate. Es ist empfehlenswert, evtl. vorhandene Zugänge für das Gerät (z.B. auf Ihrem VPN-Server) zu sperren und das Gerät (falls möglich) auf Werkseinstellungen zurückzusetzen, bevor Sie es weitergeben oder entsorgen.

15 Konformitätserklärung

Hiermit erklärt INSYS Microelectronics GmbH, dass hierin beschriebene Funkanlagentypen den Richtlinien 2014/53/EU und 2011/65/EU entsprechen. Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar:
www.insys-icom.de/doku

Zur Einhaltung der CE-Konformität ist u.a. die Einhaltung der DIN EN62311 notwendig. Diese reguliert die Exposition von Personen in elektromagnetischen Feldern.

Dazu ist die Beachtung folgender Rahmenbedingungen notwendig:

- Bei bestimmungsgemäßem Gebrauch des Produkts kommen Personen der Antenne nicht für längere Zeit näher als 20 cm.
- Verwenden Sie nur Antennen, die wir in unserem Bewertungsverfahren für dieses Produkt freigegeben haben.

16 FCC Statement

Note: This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment under FCC rules.

17 Exportbeschränkung

Die von der INSYS Microelectronics GmbH verwendeten Chipsätze für analoge Modems und Mobilfunk-Adapter unterliegen Exportrestriktionen nach der US-amerikanischen ECCN-Klassifizierung (5A991).

Es ist daher zum Zeitpunkt der Veröffentlichung dieses Dokuments nicht erlaubt, diese Kommunikationsgeräte in folgende Länder zu exportieren: Kuba, Iran, Nordkorea, Sudan, Syrien.

Die aktuell gültige Länderliste finden Sie im Abschnitt „Country Group E“ im Dokument „Supplement No. 1 to Part 740“ der Export Administration Regulations (EAR) (http://www.bis.doc.gov). Für eine Ausnahmegenehmigung setzen Sie sich bitte direkt mit den US-amerikanischen Behörden in Verbindung.

Wir möchten Sie darauf hinweisen, dass die US-amerikanische Exportgesetzgebung in Deutschland Wirkung entfalten kann. Unter anderem können nach amerikanischem Recht amerikanische Firmen daran gehindert werden, ausländische Verletzer der EAR zu beliefern.

Hinweis

Exportbeschränkung!

Mögliches Vergehen gegen Ausfuhrverordnungen.

Dieses Gerät verwendet Verschlüsselungstechnologien und unterliegt daher der Ausfuhrkontrolle nach deutschem (AL Klassifizierung 5A002) und europäischen Recht (EG-DUAL-USE VO 428/2009). Die Ausfuhr aus Deutschland erfordert eine Genehmigung des Bundesamtes für Wirtschaft und Ausfuhrkontrolle.

Dieses Gerät kann Komponenten mit US-amerikanischem Ursprung enthalten. Allfällige Exportauflagen nach US-Recht (ECCN-Klassifizierung) werden, sofern möglich, auf Belegen genannt bzw. können jederzeit angefragt werden.

18 Lizenzen

Die im EBW-H100 verwendeten Software -Technologien und Programme der Firmware sind zum Teil an die im Folgenden aufgeführten Lizenzen gebunden. Der Quellcode der an diese Lizenzen gebunden Teile der Firmware des EBW-H100 kann auf Anfrage von INSYS MICROLECTRONICS bezogen werden.

18.1 GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is

covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE

PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

18.2 GNU LIBRARY GENERAL PUBLIC LICENSE

Version 2, June 1991

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to

certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

- b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

- c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

- d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to

these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

18.3 Sonstige Lizenzen

OpenVPN license:

Copyright (C) 2002-2005 OpenVPN Solutions LLC <info@openvpn.net>

OpenVPN is distributed under the GPL license version 2 (see below).

Special exception for linking OpenVPN with OpenSSL:

In addition, as a special exception, OpenVPN Solutions LLC gives permission to link the code of this program with the OpenSSL library (or with modified versions of OpenSSL that use the same license as OpenSSL), and distribute linked combinations including the two. You must obey the GNU General Public License in all respects for all of the code used other than OpenSSL. If you modify this file, you may extend this exception to your version of the file, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version.

LZO license:

LZO is Copyright (C) Markus F.X.J. Oberhumer, and is licensed under the GPL.

Special exception for linking OpenVPN with both OpenSSL and LZO:

Hereby I grant a special exception to the OpenVPN project (http://openvpn.net/) to link the LZO library with the OpenSSL library (http://www.openssl.org).

Markus F.X.J. Oberhumer

OpenSSL License:

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in

the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT

LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

19 Glossar

Hier werden die wichtigsten Begriffe und Abkürzungen aus dem Handbuch kurz beschrieben.

APN: Access Point Name, Rechnername der Mobilfunkteilnehmern des GPRS-Netzes Zugang zum Internet bietet.

AT-Befehl: Kommando an Geräte wie z.B. Modems, mit dem dieses Gerät eingestellt wird.

Broadcast: Datenpaket, das an alle Teilnehmer eines Netzwerks gesendet wird.

Caller ID: Die Rufnummer, die der Anrufer übermittelt und von dem angerufenen Gerät interpretiert werden kann.

Client: Gerät welches Dienste von einem anderen Gerät (Server) anfordert.

CLIP: Calling Line Identification Presentation ist ein Leistungsmerkmal für ankommende Rufe im analogen und ISDN Telefonnetz sowie bei Mobilfunk. Dem Empfänger wird die Caller-ID des Anrufers übermittelt.

CHAP: Challange Handshake Authentication Protocol, Ein Authentifizierungsprotokoll, das oft bei PPP-Verbindungen benutzt wird.

DHCP: Dynamic Host Configuration Protocol, DHCP-Server können DHCP-Clients auf deren Anfrage dynamisch eine IP-Adresse und andere Parameter übergeben.

Dial-In: Das Gerät kann über eine Wählverbindung angerufen werden und eine Verbindung zum LAN herstellen.

Dial-Out: Das Gerät kann über eine Wählverbindung anrufen, und z.B. eine Verbindung ins Internet herstellen.

DFÜ: Datenfernübertragung, Daten können zwischen Computern über weite Distanzen übertragen. Die Übertragung wird oft mit Modems und dem PPP-Protokoll realisiert.

DNS: Domain Name System, Dienst der für die Umsetzung von Domainnamen in IP-Adressen benutzt wird.

Domainname: Die Domain ist der Name einer Internetseite (z.B. insys-icom). Sie besteht aus dem Namen und einer Erweiterung (Top Level Domain, z.B. .de), (z.B. insys-icom.de).

EDGE: Enhanced Data Rates for GSM Evolution bezeichnet eine Technik zur Erhöhung der Datenrate in GSM-Mobilfunknetzen durch Einführung eines zusätzlichen Modulationsverfahrens. Mit EDGE werden GPRS zu E-GPRS (Enhanced GPRS) und HSCSD zu ECSD erweitert.

Firewall: Netzwerkregeln, die vor allem Datenpakete zu bestimmten Absendern oder Zielen blocken.

Gateway: Dies ist eine Maschine, die wie ein Router arbeitet. Im Gegensatz zum Router kann ein Gateway auch Datenpakete von unterschiedlichen Hardware-Netzwerken routen.

GPRS: General Packet Radio Service, Weiterentwicklung des ->GSM-Mobilfunknetzes um höhere Datenübertragungsraten erreichen zu können.

GSM: Global System for Mobile communications, Mobilfunknetz für Sprach- und Datenübertragung.

ICMP: Internet Control Message Protocol, Protokoll, das oftmals für die Steuerung eines Netzwerks benutzt wird. Das Programm „ping" benutzt z.B. ICMP.

IP-Adresse: Internet Protokoll Adresse, die IP-Adresse eines Gerätes in einem Netzwerk unter der es erreicht werden kann. Sie besteht aus vier Byte und wird dezimal angegeben, (z.B. 192.168.1.1)

ISP: Internet Service Provider, dieser kann über eine Wählverbindung (z.B. mit analogen Modem oder ISDN-TA) angerufen werden. Der ISP sorgt dann dafür, dass man über diese Wählverbindung einen Zugang zum Internet erhält.

LAN: Lokal Area Network, ein Netzwerk aus Rechnern, die örtlich relativ nah beisammen sind.

MAC-Adresse: Media Access Control Address. Eine MAC ist ein Teil einer Ethernet-Schnittstelle. Jede Ethernet-Schnittstelle hat eine weltweit einzigartige Nummer, die MAC-Adresse.

MSN: Multiple Subscribers Number. Geräte die an einem S0-Bus aktiv sind, benötigen eine Teilnehmerkennung in Form einer Endgerätenummer.

Netzmaske: Definiert eine logische Gruppierung von IP-Adressen in Netzadresse und Geräteadressen.

Netzadresse: Besteht aus der Überlappung von IP-Adresse und Netzmaske. Sie endet immer mit „.0". Die Netzmaske (z.B. 255.255.255.0) wird binär über eine IP-Adresse (z.B. 192.168.1.1) gelegt, der noch „sichtbare" Teil dieser Überlappung (Maskierung) ist die Netzadresse (hier: 192.168.1.0).

Netzwerkregeln: Sie entscheiden, wie die unterschiedlichen Datenpakete in einem Netzwerkgerät gehandhabt werden, sie können z.B. Datenpakete an oder von bestimmten Netzwerkteilnehmern gesperrt oder umgeleitet werden.

PAP: Password Authentication Protocol, ein Authentikationsprotokoll, das oft bei PPP-Verbindungen benutzt wird.

Port: (1) Buchse am Switch, an der Ethernet-Geräte angeschlossen werden.
(2) Bestandteil eines Sockets bei Datenverbindungen

Port-Forwarding: Netzwerkregeln, die Datenpakete von bestimmten Absendern zu besonderen Empfängern eines Netzwerkes umleiten.

PPP: Point to Point Protocol, ein Protokoll, das zwei Maschinen über eine serielle Leitung so miteinander verbindet, dass sie TCP/IP-Pakete austauschen können.

PPPoE: Point to Point Protocol over Ethernet, ein Protokoll, das zwei Geräte über eine Ethernetleitung so miteinander verbindet, dass sie TCP/IP-Pakete austauschen können.

Router: Dies ist eine Maschine, die in einem Netzwerk dafür sorgt, dass die bei ihm eintreffenden Daten eines Protokolls zum vorgesehenen Zielnetz bzw. Subnetz weitergeleitet werden.

SCN: Service Center Number, Rufnummer des Rechners, der Kurzmitteilungen (->SMS) über das GSM-Netz entgegennimmt und zu den Empfängern weiterleitet.

Server: Gerät, das anderen Geräten (Client) Dienste zur Verfügung stellt, z.B. Webserver.

SMS: Short Message Service, Kurzmitteilungen können über das Mobilfunknetz GSM versendet werden

Socket: Datenverbindungen, die per ->TCP oder ->UDP zustande kommen, arbeiten zur Addressierung mit Sockets. Ein Socket besteht aus einer IP-Adresse und einem Port (vgl. Anschrift: Straßenname und Hausnummer)

Switch: Ein Gerät, das mehrere Maschinen mit Ethernet verbinden kann. Im Gegensatz zu einem Hub „denkt“ ein Switch mit, d.h. er kann sich die MAC-Adressen merken, die an einem Port angeschlossen sind und lenkt den Verkehr effizienter zu den einzelnen Ports.

TCP: Transmission Control Protocol, ein Transportprotokoll, um den Datenaustausch zwischen Netzwerkgeräten zu ermöglichen. Es arbeitet „verbindungsorientiert“, d.h. die Datenübertragung ist gesichert.

UDP: User Datagram Protocol, Transportprotokoll, um Datenaustausch zwischen Netzwerkgeräten zu ermöglichen. Es arbeitet „verbindungslos“, d.h. die Datenübertragung ist ungesichert.

UMTS: Universal Mobile Telecommunications System steht für den Mobilfunkstandard der dritten Generation (3G), mit dem deutlich höhere Datenübertragungsraten (384 kbit/s bis 7,2 Mbit/s) als mit dem Mobilfunkstandard der zweiten Generation (2G), dem GSM-Standard (9,6 kbit/s bis 220 kbit/s) möglich sind.

URL: “Uniform Resource Locator”, sie bezeichnet die Adresse, unter der ein Service im Webbrowser gefunden werden kann. In diesem Handbuch wird als URL meist die IP-Adresse des Geräts eingegeben.

VPN: Virtual Private Network, über bestehende unsichere Netzwerke werden logische Verbindungen (sog. Tunnel) aufgebaut. Die Endpunkte dieser Verbindungen („Tunnelenden“) und die Geräte dahinter können als eigenes, logisches Netzwerk betrachtet werden. Mit Verschlüsselung der Datenübertragung über die Tunnel und die vorherige gegenseitige Authentifizierung der Teilnehmer an diesem logischen Netzwerk kann ein sehr hoher Grad an Abhör- und Manipulationssicherheit erreicht werden.

WAN: Wide Area Network, ein Netzwerk aus Rechnern, die örtlich weit auseinander liegen.

20 Tabellen & Abbildungen

20.1 Tabellenverzeichnis

20.2 Abbildungsverzeichnis

21 Stichwortverzeichnis