SIEMENS

SIMATIC NET

UMTS-Router mit HSDPA SCALANCE M873-0

Systemhandbuch

C79000-G8900-C251-01

Ausgabe 02/2011

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

Gefahr

bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Warnung

bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Vorsicht

mit Warndreieck bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Vorsicht

ohne Warndreieck bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Achtung

bedeutet, dass ein unerwünschtes Ergebnis oder Zustand eintreten kann, wenn der entsprechende Hinweis nicht beachtet wird.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch

Beachten Sie Folgendes:

Warnung

Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Automation and Drives
Postfach 48 48
90437 NÜRNBERG
DEUTSCHLAND

Dokumentbestell-Nr. C79000-G8900-C251-01
Ausgabe 02/2011

Externe Stromversorgung

Verwenden Sie nur eine externe Stromversorgung die ebenfalls der EN60950 entspricht. Die Ausgangsspannung der externen Stromversorgung darf 30V DC nicht überschreiten. Der Ausgang der externen Stromversorgung muss kurzschlussfest sein.

Warnung

Das SCALANCE M873-0 darf nur aus Stromversorgungen nach IEC/EN60950-1 Abschnitt 2.5 "Stromquelle mit begrenzter Leistung" versorgt werden.

Die externe Stromversorgung für das SCALANCE M873-0 muss den Bestimmungen für NEC Klasse 2 Stromkreisen entsprechen, wie im National Electrical Code ® (ANSI/NFPA 70) festgelegt.

Beachten Sie die Abschnitte "Schraubklemmen für die Spannungsversorgung" und "Installationsvorschriften" dieser Dokumentation (Kapitel 2.7) sowie die Einbau- und Nutzungsvorschriften des jeweiligen Herstellers der Stromversorgung, der Batterie oder des Akkumulators.

SIM-Karte

Zur Installation der SIM-Karte muss das Gerät geöffnet werden. Trennen Sie das Gerät vor dem Öffnen von der Versorgungsspannung. Statische Aufladungen können das Gerät im geöffneten Zustand beschädigen. Entladen Sie die elektrische Aufladung Ihres Körpers vor dem Öffnen des Geräts. Berühren Sie dazu eine geerdete Oberfläche, z.B. das Metallgehäuse des Schaltschranks. Beachten Sie das Kapitel 2.7.

Schalteingänge und Schaltausgänge

Der Schalteingang und der Schaltausgang sind jeweils gegenüber den anderen Anschlüssen des SCALANCE M873-0 galvanisch getrennt. Wenn die am SCALANCE M873-0 angeschlossene Installation ein Signal des Schalteingangs oder des Schaltausgangs galvanisch mit der Versorgungsspannung verbindet, dann darf zwischen jedem Signal des Schalteingangs oder -ausgangs und jedem Anschluss der Versorgungsspannung des SCALANCE M873-0 die Spannung jeweils 60 V nicht überschreiten.

Umgang mit Kabeln

Ziehen Sie niemals einen Kabelstecker am Kabel aus seiner Buchse, sondern ziehen Sie am Stecker. Kabelstecker mit Schraubbefestigungen (Sub-D) müssen immer fest angeschraubt werden. Führen Sie die Kabel nicht ohne Kantenschutz über scharfe Ecken und Kanten. Sorgen Sie gegebenenfalls für eine ausreichende Zugentlastung der Kabel.

Achten Sie darauf, dass aus Sicherheitsgründen der Biegeradius der Kabel eingehalten wird.

Die Nichteinhaltung der Biegeradien des Antennenkabels führt zu Verschlechterung der Sende- und Empfangseigenschaften des Gerätes. Der minimale Biegeradius darf statisch den 5-fachen Kabeldurchmesser und dynamisch den 15-fachen Kabeldurchmesser nicht unterschreiten.

Funkgerät

Warnung

Verwenden Sie das Gerät niemals in Bereichen, in denen der Betrieb von Funkeinrichtungen untersagt ist. Das Gerät enthält einen Funksender, der gegebenenfalls medizinische elektronische Geräte wie Hörgeräte oder Herzschrittmacher in ihrer Funktion beeinträchtigen kann. Ihr Arzt oder der Hersteller solcher Geräte können Sie beraten.

Damit keine Datenträger entmagnetisiert werden, lagern Sie keine Disketten, Kreditkarten oder andere magnetische Datenträger in der Nähe des Gerätes.

Antennen-Montage

Warnung

Das Einhalten der empfohlenen Strahlungsgrenzwerte der deutschen Strahlenschutzkommission (www.ssk.de) vom 13./14. September 2001 muss gewährleistet sein.

Montage einer Außenantenne

Vorsicht

Bei der Installation einer Antenne im Freien ist es zwingend erforderlich, dass die Antenne durch Fachpersonal fachgerecht montiert wird.

Die Außenantenne muss zum Blitzschutz geerdet werden. Der Schirm der Außenantenne muss zuverlässig mit der Schutzerde verbunden werden.

Bei der Installation sind den jeweiligen nationalen Installationsrichtlinien Folge zu leisten.

In den USA ist dies der National Electric Code NFPA 70, Artikel 810.

In Deutschland ist dies die Normenreihe VDE 0185 (DIN EN 62305) Teil 1 bis 4 bei Gebäuden mit Blitzschutzeinrichtung und die Normenreihe VDE 0855 (DIN EN 60728-11) bei Fehlen einer Blitzschutzeinrichtung.

Hinweise und Warnungen zur Einhaltung von Sicherheits-, Telekom-, EMV und anderer Standards

Vorsicht

Beachten Sie die in die in Kapitel 11 aufgeführten Hinweise und Warnungen, bevor Sie das SCALANCE M873-0 in Betrieb nehmen.

Verbindungskosten bei (E-) GPRS

Achtung

Beachten Sie, dass auch beim (Wieder-) Aufbau einer Verbindung, bei Verbindungsversuchen zur Gegenstelle (z.B. Server ausgeschaltet, falsche Zieladresse, etc.) sowie zum Erhalt einer Verbindung kostenpflichtige Datenpakete ausgetauscht werden.

Firmware mit Open Source GPL/LGPL

Die Firmware von SCALANCE M873-0 enthält Open-Source-Software unter GPL-/ LGPL-Bedingungen. Gemäß des Abschnitts 3b von GPL und des Abschnitts 6b von LGPL bieten wir Ihnen den Sourcecode an. Schreiben Sie an

s_opsource@gmx.net
s_opsource@gmx.de

Geben Sie als Betriffttext Ihrer E-Mail 'Open Source M873-0' an, um Ihre Nachricht leicht herausfiltern zu können.

Firmware mit OpenBSD

Die Firmware von SCALANCE M873-0 enthält Teile aus der OpenBSD-Software. Die Verwendung von OpenBSD-Software verpflichtet zum Abdruck des folgenden Copyright-Vermerkes:

```
* Copyright (c) 1982, 1986, 1990, 1991, 1993
* The Regents of the University of California. 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 acknowledgement:
*    This product includes software developed by the University of California,
*    Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*    without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``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 REGENTS 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.
```

Vorwort

Zweck dieser Dokumentation

Diese Dokumentation begleitet Sie auf Ihrem Weg zum erfolgreichen Einsatz des UMTS-Routers mit HSDPA SCALANCE M873-0. Sie führt in das Thema ein und gibt Ihnen eine Übersicht über das Einsatzgebiet der Hardware. Sie erläutert Ihnen, wie das Modem unter Berücksichtigung der Betriebsbedingungen in Betrieb genommen und konfiguriert wird. Die vorliegende Dokumentation zeigt die technischen Daten und die erfüllten Normen und Zulassungen für den UMTS-Router mit HSDPA M873-0.

Gültigkeitsbereich der Dokumentation

Das vorliegende Handbuch ist gültig für folgende Produktversionen:

- UMTS-Router mit HSDPA SCALANCE M873-0

  Bestellnummer: 6GK5 873-0AA10-1AA2

  Hardware-Erzeugnisstand 2.x

Verwendungszweck: UMTS-Router mit HSDPA für industrielle Anwendungen

Service & Support

Zusätzlich zu unserer Produkt-Dokumentation unterstützt Sie die umfassende Online-Info-Plattform rund um unseren Service & Support zu jeder Zeit von jedem Ort der Welt aus. Sie finden sie im Internet unter folgender Adresse:
www.siemens.com/automation/service&support

Dort finden Sie folgende Informationen:

- Neuigkeiten aus dem Support, Newsletter
- Produktinformationen, Produkt-Support, Applikationen & Tools
- Technisches Forum
- Zugang zu unserem weiteren Service & Support-Angebot:
  - Technical Consulting
  - Engineering Support
  - Field Service
    Telefon: +49 (0)911 895 7444
  - Ersatzteile und Reparaturen
    Telefon: +49 (0)911 895 7448
  - Optimierung und Modernisierung
  - Technical Support
    Die kompetente Beratung bei technischen Fragen mit einem breiten Spektrum an bedarfsgerechten Leistungen rund um unsere Produkte und Systeme.

    Telefon: +49 (0)911 895 7222

    www.siemens.de/automation/support-request

Kontaktdaten finden Sie im Internet unter folgender Adresse:
www.automation.siemens.com/partner

SITRAIN - das Siemens-Training für Automation und Industrial Solutions

Mit mehr als 300 verschiedenen Kursen deckt SITRAIN das gesamte Siemens-Produkt- und Systemspektrum im Bereich der Automatisierungs- und Antriebstechnik ab. Des Weiteren werden maßgeschneiderte Weiterbildungsmaßnahmen durchgeführt, die auf Ihre Anforderungen zugeschnitten sind. Ergänzend zu unserem klassischen Kursangebot bieten wir eine Kombination von verschiedenen Lernmedien und Sequenzen an. So können z. B. Selbstlernprogramme auf CD-ROM oder im Internet zur Vor- und Nachbereitung genutzt werden.

Ausführliche Informationen zu unserem Schulungsangebot und Kontaktdaten unserer Kundenberater finden Sie unter folgender Internet-Adresse:

www.siemens.de/sitrain

Siemens-Literatur

- Die Bestellnummern für die hier relevanten Siemens-Produkte finden Sie in den folgenden Katalogen:
  - SIMATIC NET Industrielle Kommunikation / Industrielle Identifikation, Katalog IK PI
  - SIMATIC Produkte für Totally Integrated Automation und Micro Automation, Katalog ST 70

  Die Kataloge sowie zusätzliche Informationen können Sie bei Ihrer Siemens-Vertretung anfordern.
- Die SIMATIC NET-Handbücher finden Sie auf den Internet-Seiten des Siemens Customer Support für Automatisierung:

  http://support.automation.siemens.com/WW/view/de

  Geben Sie dort die Beitrags-ID des jeweiligen Handbuchs als Suchbegriff ein. Die ID ist unter einigen Literaturstellen in Klammern angegeben.

  → Die aktuelle Version dieser Dokumentation finden Sie unter der Beitrags-ID 47889630.
- Alternativ finden Sie die SIMATIC NET-Dokumentation unter den Seiten des Produkt-Support:

  http://support.automation.siemens.com/WW/view/de/10805878

  Navigieren Sie zur gewünschten Produktgruppe und nehmen Sie folgende Einstellungen vor:

  → Beitragsliste → Beitragstyp "Handbücher / Betriebsanleitungen"

Inhaltsverzeichnis

Einsatz und Funktionen 1

1.1 Einleitung

Das SCALANCE M873-0 bietet einen drahtlosen Anschluss zum Internet oder zu einem privaten Netzwerk. Das SCALANCE M873-0 bietet diesen Anschluss an jedem Ort, an dem ein UMTS-Netz (Universal Mobile Telecommunication System = Mobilfunknetz 3. Generation) oder GSM-Netz (Global System for Mobile Communication = Mobilfunknetz) verfügbar ist, das IP-basierte Datendienste bereitstellt. Bei UMTS sind das der HSDPA data service (High Speed Download Data Access) oder der UMTS data service. Bei GSM sind das EGPRS (Enhanced General Packet Radio Service = EDGE) oder GPRS (General Packet Radio Service).
Voraussetzung dafür ist eine SIM-Karte eines UMTS/GSM-Mobilfunkbetreibers mit entsprechend freigeschalteten Diensten.

Das SCALANCE M873-0 verbindet so eine lokal angeschlossene Applikation oder ganze Netzwerke über drahtlose IP-Verbindungen mit dem Internet. Möglich ist auch die direkte Verbindung mit einem Intranet, an dem wiederum die externen Gegenstellen angeschlossen sind.

Dazu vereinigt das Gerät folgende Funktionen:

- Funkmodem für die flexible Datenkommunikation per HSDPA, UMTS, EGPRS oder GPRS

- Firewall für den Schutz vor unberechtigtem Zugriff
  Der dynamische Paketfilter untersucht Datenpakete anhand der Ursprungs- und Zieladresse (stateful inspection firewall) und blockiert unerwünschten Datenverkehr (Anti-Spoofing).

Typische SINAUT-Anwendungsbeispiele

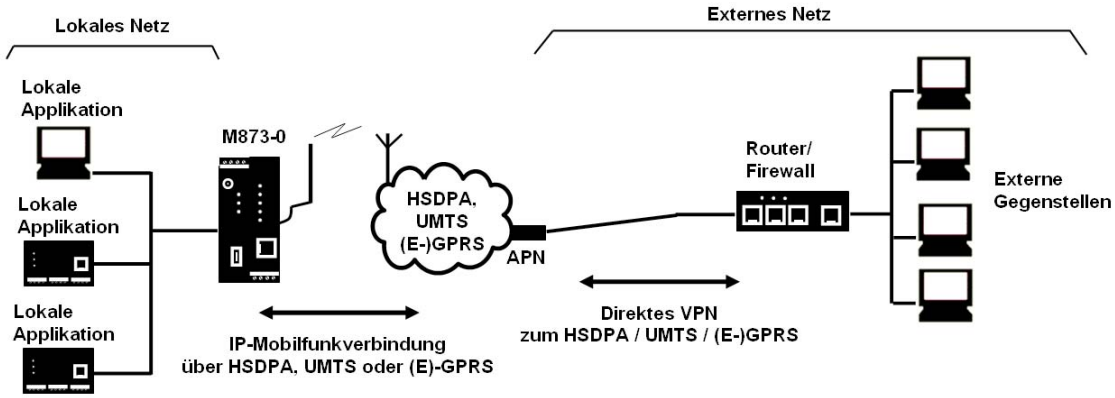


Abbildung 1-1 Verbindung über HSDPA, UMTS, EGPRS oder GPRS und ein direktes VPN zum externen Netz

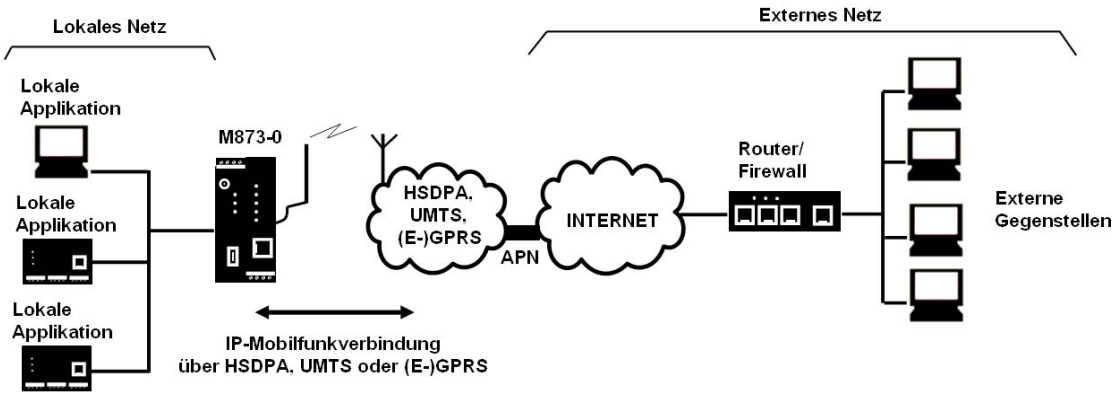


Abbildung 1-2 Verbindung über HSDPA, UMTS, EGPRS oder GPRS und das Internet zum externen Netz

Konfiguration

Die Konfiguration des Geräts erfolgt über eine Web-Oberfläche, die sich einfach mit einem Web-Browser anzeigen lässt. Der Zugriff kann über folgende Wege stattfinden:

- Die lokale Schnittstelle
- HSDPA, UMTS, EGPRS/GPRS oder
- CSD (Circuit Switched Data = Datenwählverbindungen) des GSM

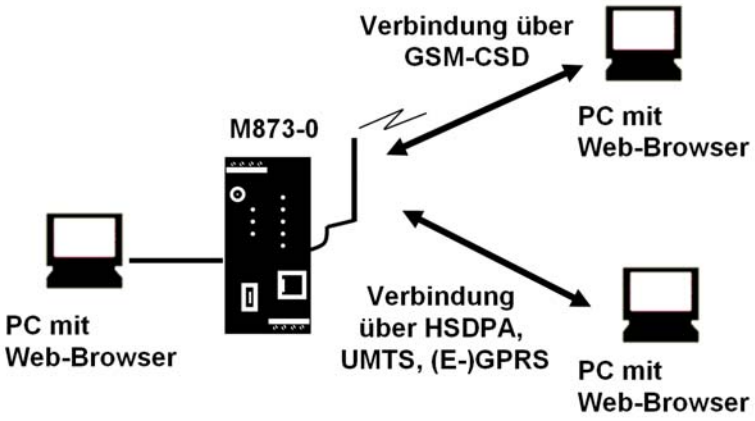


Abbildung 1-3 Konfigurationsverbindungen

Firewall-Funktionen

Das SCALANCE M873-0 bietet folgende Firewall-Funktionen, um das lokale Netz und sich selbst gegen Angriffe von Außen zu schützen:

- Stateful Inspection Firewall
- Anti-Spoofing
- Port Forwarding
- NAT

Weitere Funktionen

Das SCALANCE M873-0 bietet folgende weitere Funktionen:

- DNS Cache
- DHCP Server
- NTP
- Remote Logging
- Schalteingang
- Web-Oberfläche zur Konfiguration
- Versand von Alarm-SMS
- SMS-Versand aus dem lokalen Netz
- SSH-Konsole zur Konfiguration
- DynDNS-Client
- Datenwählverbindung zur Wartung und Fernkonfiguration

Inbetriebnahme 2

2.1 Sicherheitshinweise

Sicherheitshinweise für den Geräteeinsatz

Die folgenden Sicherheitshinweise sind für Aufstellung und Betrieb des Gerätes und alle damit zusammenhängenden Arbeiten wie Montage, Anschließen, Geräteaustausch oder Öffnen des Gerätes zu beachten.

Allgemeine Hinweise für den Einsatz im Ex-Bereich

Warnung

Explosionsgefahr beim Anschließen oder Abklemmen des Geräts

EXPLOSIONSGEFAHR

IN EINER LEICHT ENTZÜNDLICHEN ODER BRENNBAREN UMGEBUNG DÜRFEN KEINE LEITUNGEN AN DAS GERÄT ANGESCHLOSSEN ODER VOM GERÄT GETRENNT WERDEN.

Warnung

Austausch von Komponenten

EXPLOSIONSGEFAHR

DER AUSTAUSCH VON KOMPONENTEN KANN DIE EIGNUNG FÜR CLASS I, DIVISION 2 ODER ZONE 2 BEEINTRÄCHTIGEN.

Hinweise für den Einsatz im Ex-Bereich gemäß ATEX

Warnung

Anforderungen an den Schaltschrank

Bei Einsatz in explosionsgefährdeter Umgebung entsprechend Class I, Division 2 oder Class I, Zone 2 muss das Gerät in einen Schaltschrank oder in ein Gehäuse eingebaut werden.

Um die EU-Richtlinie 94/9 (ATEX 95) zu erfüllen, muss das Gehäuse mindestens die Anforderungen von IP54 nach EN 60529 erfüllt.

Warnung

Geeignete Kabel für Temperaturen über 70°C

Wenn am Kabel oder an der Gehäusebuchse Temperaturen über 70°C auftreten oder die Temperatur an den Adernverzweigungsstellen der Leitungen über 80°C liegt, müssen besondere Vorkehrungen getroffen werden. Wenn das Gerät bei Umgebungstemperaturen von 50°C bis 70°C betrieben wird, dann müssen Sie Kabel mit einer zulässigen Betriebstemperatur von mindesten 80°C verwenden.

Warnung

Schutz vor transienter Überspannung

Treffen Sie Maßnahmen, um transiente Überspannungen von mehr als 40% der Nennspannung zu verhindern. Das ist gewährleistet, wenn Sie die Geräte ausschließlich mit SELV (Sicherheitskleinspannung) betreiben.

2.2 Schritt für Schritt

Gehen Sie bei der Inbetriebnahme des SCALANCE M873-0 in folgenden Schritten vor:

Schritt		Kapitel
1.	Machen Sie sich mit den Voraussetzungen für den Betrieb des SCALANCE M873-0 vertraut.	2.3
2.	Lesen Sie sehr sorgfältig die Sicherheitshinweise und weitere Hinweise am Beginn dieses Dokuments und befolgen Sie diese unbedingt.	
3.	Machen Sie sich vertraut mit den Bedienelementen, Anschlüssen und Betriebsanzeigen des SCALANCE M873-0.	2.4 - 2.7
4.	Schließen Sie einen PC mit Web-Browser (Admin-PC) an die lokale Schnittstelle (10/100 BASE-T) des SCALANCE M873-0 an.	3.1, 3.3

5.	Tragen Sie über die Web-Oberfläche des SCALANCE M873-0 die PIN (Persönliche Identifikations-Nummer) der SIM-Karte ein.	5.1
6.	Trennen Sie das SCALANCE M873-0 von der Versorgungsspannung.	2.7
7.	Legen Sie die SIM-Karte in das Gerät ein.	2.8
8.	Schließen Sie die Antenne an.	2.7
9.	Verbinden Sie das SCALANCE M873-0 mit der Versorgungsspannung.	2.7
10.	Richten Sie das SCALANCE M873-0 nach Ihren Anforderungen ein.	3 bis 9
11.	Schließen Sie Ihre lokale Applikation an.	2.7

2.3 Voraussetzungen für den Betrieb

Um das SCALANCE M873-0 betreiben zu können, müssen die folgenden Informationen vorliegen und die folgenden Voraussetzungen erfüllt sein:

Antenne

Eine Antenne, angepasst auf die Frequenzbänder des von Ihnen gewählten Mobilfunkbetreibers: 850 MHz, 900 MHz, 1800 MHz, 1900 MHz oder 2100 MHz. Verwenden Sie nur Antennen aus dem Zubehör zum SCALANCE M873-0.

Siehe Kapitel 2.7.

Spannungsversorgung

Eine Spannungsversorgung mit einer Spannung zwischen 12 V_{DC} und 60 V_{DC}, die einen ausreichenden Strom liefern kann.

Siehe Kapitel 2.7.

SIM-Karte

Eine SIM-Karte des ausgewählten Mobilfunkbetreibers.

PIN

Die PIN (= Personel Identification Number) der SIM-Karte

HSDPA / UMTS, EGPRS / GPRS Freischaltung

Die SIM-Karte muss von Ihrem Mobilfunkbetreiber für die Dienste HSDPA, UMTS data, EGPRS oder GPRS freigeschaltet sein.

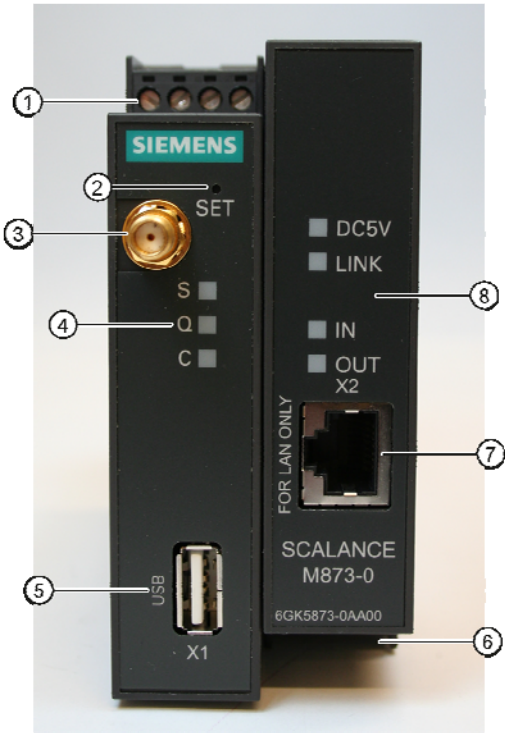
Die Zugangsdaten müssen bekannt sein:

- Access Point Name (APN)
- Benutzername
- Passwort

CSD 9600 bit/s Freischaltung

Die SIM-Karte muss von Ihrem Mobilfunkbetreiber für den CSD-Dienst freigeschaltet sein, wenn Sie die Fernkonfiguration über Datenwählverbindungen nutzen möchten, siehe Kapitel 7.3.

2.4 Gerätefront



1) Anschlussklemmen der Stromversorgung
2) Service-Taster (SET)
3) Antennenbuchse Typ SMA
4) Betriebsanzeigen S, Q, C
5) X1 (Service; USB) – ohne Funktion
6) Anschlussklemmen der Schalt-Ein- und Ausgänge (Nicht angeschlossen)
7) X2 (10/100-Base-T - RJ45-Buchse) zum Anschluss des lokalen Netz
8) Betriebsanzeigen DC5V, LINK, IN, OUT

Abbildung 2-1 Gerätefront

2.5 Service-Taster (SET)

Auf der Frontseite des SCALANCE M873-0 befindet sich ein kleines Loch (siehe B), das mit SET beschriftet ist und hinter dem sich ein Taster befindet. Benutzen Sie einen spitzen Gegenstand, z. B. eine aufgebogene Büroklammer, um den Taster zu drücken.

Wenn Sie den Taster länger als 5 Sekunden drücken, führt das SCALANCE M873-0 einen Neustart durch und lädt dabei die Werkseinstellungen.

2.6 Betriebsanzeigen

Das SCALANCE M873-0 hat 7 Signalleuchten (LEDs) zur Anzeige des Betriebszustands.

Die 3 Signalleuchten auf der linken Gerätehälfte zeigen den Zustand des Funkmodems an:

LED	Zustand	Bedeutung
***S** (Status)*	Langsam blinkend	PIN-Übergabe
	Schnell blinkend	PIN-Fehler / SIM-Fehler
	EIN	PIN-Übergabe erfolgreich
***Q** (Quality)*	AUS	Nicht im GSM-Netz eingebucht
	Kurz aufblinkend	Signalstärke schlecht (CSQ < 6)
	Langsam blinkend	Signalstärke mittel (CSQ= 6..10)
	EIN, mit kurzen Unterbrechungen	Signalstärke gut (CSQ=11-18)
	EIN	Signalstärke sehr gut (CSQ > 18)
***C** (Connect)*	AUS	Keine Verbindung
	Schnell blinkend	Service Ruf über CSD aktiv
	Langsam blinkend	EGPRS/GPRS-Verbindung aktiv
	EIN	HSDPA/UMTS-Verbindung aktiv
S, Q, C gemeinsam	Schnelles Lauflicht	Booten
	Langsames Lauflicht	Update
	Synchrones schnelles Blinken	Fehler

Die 4 Signalleuchten auf der rechten Gerätehälfte zeigen den Zustand weiterer Gerätefunktionen an:

LED	Zustand	Bedeutung
DC 5V	EIN	Gerät eingeschaltet, Betriebsspannung liegt an
	AUS	Gerät ausgeschaltet, Betriebsspannung fehlt
LINK	EIN	Ethernet-Verbindung zur lokalen Applikation bzw. zum lokalen Netz hergestellt
	AUS	Keine Ethernet-Verbindung zur lokalen Applikation bzw. zum lokalen Netz
	EIN mit kurzen Unterbrechungen	Datentransfer über die Ethernet-Verbindung
IN	EIN	Schalteingang aktiv
	AUS	Schalteingang nicht aktiv
OUT	EIN	Reserviert für zukünftige Anwendungen
	AUS	Reserviert für zukünftige Anwendungen

2.7 Anschlüsse

Die Anschlüsse des M873-0 befinden sich an der Gerätefront.

X2 (10/100-Base-T)

Am Anschluss 10/100-Base-T wird das lokale Netz, mit den lokalen Applikationen angeschlossen, z. B. eine programmierbare Steuerung, eine Maschine mit Ethernet-Schnittstelle zur Fernüberwachung, ein Notebook bzw. PC.

Zum Einrichten des SCALANCE M873-0 schließen Sie hier den Admin-PC mit Web-Browser an.

Die Schnittstelle unterstützt Autonegation. Somit wird automatisch erkannt, ob 10 Mbit/s oder 100 Mbit/s Übertragungsgeschwindigkeit auf dem Ethernet genutzt wird.

Das verwendete Anschlusskabel muss einen RJ45-Stecker haben. Es kann ein Cross-over- oder ein Patch-Kabel sein.

X1 (Service; USB)

Diese Schnittstelle ist beim SCALANCE M873-0 ohne Funktion und reserviert für spätere Anwendungen. Schließen Sie hier keine Geräte an. Der Betrieb des SCALANCE M873-0 könnte gestört werden.

SMA-Antennenbuchse

Das SCALANCE M873-0 hat eine Antennenbuchse vom Typ SMA zum Anschluss der Antenne.

Die verwendete Antenne muss eine Impedanz von ca. 50 Ohm haben. Sie muss abgestimmt sein für GSM 900 MHz und DCS 1800 MHz oder GSM 850 MHz und PCS 1900 MHz, sowie für UMTS 2100 MHz, je nachdem, welche Frequenzbänder ihr GSM-Netzbetreiber verwendet. In Europa und China werden GSM 900 MHz, DCS 1800MHz und UMTS 2100 MHz verwendet. In den USA verwendet man GSM 850 MHz und PCS 1900 MHz (auch für UMTS). Erkundigen Sie sich bei Ihrem Netzbetreiber.

Die Anpassung (VSWR) der Antenne muss 1:2,5 oder besser sein.

Achtung:

Verwenden Sie nur Antennen aus dem Zubehörprogramm für das SCALANCE M873-0. Andere Antennen können die Produkteigenschaften stören oder sogar zu Defekten führen.

Bei der Installation der Antenne ist auf eine ausreichend gute Signalqualität zu achten (CSQ > 11). Nutzen Sie die Signalleuchten des SCALANCE M873-0, die Ihnen die Signalqualität anzeigen. Achten Sie darauf, dass sich keine großen metallischen Gegenstände (z. B. Stahlbeton) in der Nähe der Antenne befinden.

Beachten Sie die Montage- und Gebrauchsanleitung der verwendeten Antenne.

Warnung:

Bei Außenmontage der Antenne muss die Antenne zwecks Blitzschutzes geerdet werden. Diese Arbeiten müssen von qualifiziertem Personal durchgeführt werden.

Beachten Sie den Warnhinweis zur Montage einer Außenmontage von Antennen am Beginn dieses Dokuments.

Schraubklemmen für die Spannungsversorgung

Abbildung 2-2 Schraubklemmen Versorgung (24V 0V)

Das SCALANCE M873-0 arbeitet mit einer Gleichspannung von DC 12-60 V, nominell DC 24 V. Diese Versorgungsspannung wird an die Schraubklemmen der linken Gerätehälfte angeschlossen.

Die Stromaufnahme beträgt etwa 450 mA bei 12 V und 100 mA bei 60 V.

Warnung:

Das Netzteil des SCALANCE M873-0 ist nicht potentialgetrennt. Beachten Sie die Sicherheitshinweise am Anfang dieses Handbuchs.

Installationsvorschriften

Verwenden Sie nur Kupferleitungen.

Draht:	0,5...3 mm^2 (AWG 20...18)
Litze:	0,5...2,5 mm^2
Anzugsmoment für Schraubklemmen:	0,6...0,8 Nm

Schalteingang / Schaltausgang

Abbildung 2-3 Schalteingänge / Schaltausgänge

Schalteingang I1+/I1-

Das SCALANCE M873-0 hat einen Schalteingang. Der Schalteingang hat seine Anschlüsse an den Schraubklemmen der rechten Gerätehälfte. Die Klemmen sind mit I1+/I1- bezeichnet.

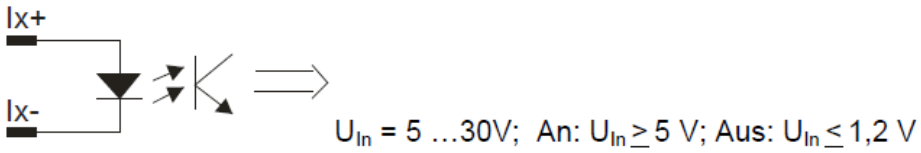


Abbildung 2-4 Schalteingang I1+/I1-

Zur Funktion des Schalteingangs siehe Kapitel 9.

Warnung:

Der Schalteingang ist gegenüber den anderen Anschlüssen des SCALANCE M873-0 galvanisch getrennt. Verbindet die am SCALANCE M873-0 angeschlossene Installation ein Signal des Schalteingangs galvanisch mit der Versorgungsspannung, darf zwischen jedem Signal des Schalteingangs und jedem Anschluss der Versorgungsspannung des SCALANCE M873-0 die Spannung jeweils 60 V nicht überschreiten.

Schaltausgang O1a/O1b

Das SCALANCE M873-0 hat einen Schaltausgang. Der Schaltausgang hat seine Anschlüsse an den Schraubklemmen der rechten Gerätehälfte. Die Klemmen sind mit O1a/O1b bezeichnet.

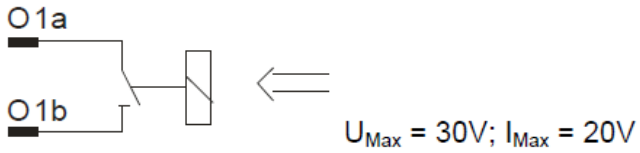


Abbildung 2-5 Schaltausgang O1a/O1b

Der Schaltausgang ist reserviert für spätere Anwendungen.

Warnung:

Der Schaltausgang ist gegenüber den anderen Anschlüssen des SCALANCE M873-0 galvanisch getrennt. Verbindet die am SCALANCE M873-0 angeschlossene Installation ein Signal des Schaltausgangs galvanisch mit der Versorgungsspannung, darf zwischen jedem Signal des Schaltausgangs und jedem Anschluss der Versorgungsspannung des SCALANCE M873-0 die Spannung jeweils 60 V nicht überschreiten.

2.8 Die SIM-Karte einlegen

Achtung:

Bevor Sie die SIM-Karte einlegen, tragen Sie im SCALANCE M873-0 über die Web-Oberfläche die PIN der SIM-Karte ein. Siehe Kapitel 5.1.

Abbildung 2-6 SIM-Karten-Schublade

1. Nachdem Sie die PIN der SIM-Karte eingetragen haben, trennen Sie das SCALANCE M873-0 vollständig von der Versorgungsspannung.

2. Die Schublade für die SIM-Karte befindet sich auf der Geräterückseite. In der Gehäuseöffnung befindet sich direkt neben der Schublade für die SIM-Karte ein kleiner gelber Taster. Drücken Sie auf diesen Taster mit einem spitzen Gegenstand, z. B. einem Bleistift.
   Bei Druck auf den Taster kommt die SIM-Karten-Schublade aus dem Gehäuse.

3. Legen Sie die SIM-Karte so in die Schublade, dass ihre vergoldeten Kontakte sichtbar bleiben.

4. Schieben Sie die Schublade mit der SIM-Karte vollständig in das Gehäuse.

Achtung:
Legen Sie die SIM-Karte auf keinen Fall im Betrieb ein oder entfernen Sie sie. Die SIM-Karte und das SCALANCE M873-0 könnten beschädigt werden.

2.9 Hutschienenmontage

Das SCALANCE M873-0 ist zur Montage auf Hutschienen nach DIN EN 50022 vorgesehen. Eine entsprechende Halterung befindet sich an der Geräterückseite.

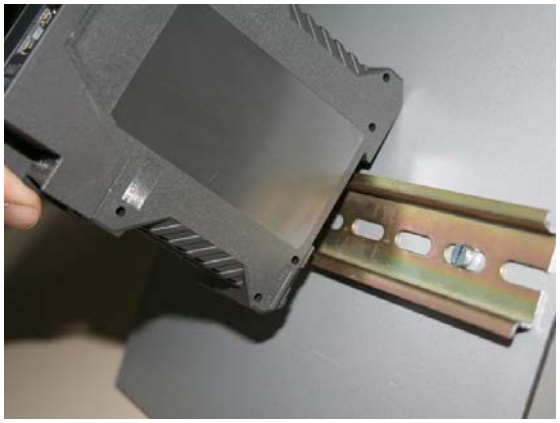


Abbildung 2-7 Hutschienenmontage

Konfiguration 3

Die Konfiguration der Router- und Firewall-Funktionen erfolgt lokal oder aus der Ferne über die web-basierte Administrations-Oberfläche des SCALANCE M873-0.

Fernkonfiguration

Eine Fernkonfiguration über HTTPS oder CSD Zugang ist nur möglich, wenn das SCALANCE M873-0 für Fernzugriffe konfiguriert ist. Gehen Sie zur Fernkonfiguration des Geräts vor, wie in Kapitel 7 beschrieben ist.

Konfiguration über die lokale Schnittstelle

Die Voraussetzungen für die Konfiguration über die lokale Schnittstelle sind:

- Der Rechner (Admin-PC), mit dem Sie die Konfiguration vornehmen, muss entweder ...
  - ... direkt an der Ethernet-Buchse des SCALANCE M873-0 per Netzwerkkabel angeschlossen sein

    oder
  - ... über das lokale Netz direkten Zugriff auf das SCALANCE M873-0 haben.
- Der Netzwerkadapter des Rechners (Admin-PC), mit dem Sie die Konfiguration vornehmen, muss folgende TCP/IP Konfiguration haben:

  IP-Adresse: 192.168.1.2

  Subnetzmaske: 255.255.255.0

  Statt der IP-Adresse 192.168.1.2 können Sie auch andere IP-Adressen aus dem Bereich 192.169.1.x verwenden.
- Wenn Sie über das SCALANCE M873-0 mit dem Admin-PC über das SCALANCE M873-0 auch auf das externe Netz zugreifen möchten, sind zusätzlich folgende Einstellungen erforderlich:

  Standardgateway: 192.168.1.1
- Bevorzugter DNS-Server: Adresse des Domain Name Servers

3.1 TCP/IP Konfiguration des Netzwerkadapters unter Windows XP

Einrichten der LAN-Verbindung

1. Klicken Sie "Start", "Verbinden mit ...", "Alle Verbindungen anzeigen…".
2. Klicken Sie auf "LAN-Verbindung".
3. Wählen Sie im Dialogfeld "Eigenschaften von LAN-Verbindung" die Registerkarte "Allgemein" und markieren Sie dort den Eintrag "Internetprotokoll (TCP/IP)".
4. Öffnen Sie Eigenschaften durch Klicken auf diese Schaltfläche.

Das Fenster "Eigenschaften von Internetprotokoll TCP/IP" erscheint (siehe Abbildung 3-1).

Hinweis:
Der Weg, der zum Dialogfeld "Eigenschaften von LAN-Verbindung" führt, hängt von Ihren Windows-Einstellungen ab. Können Sie das Dialogfeld nicht finden, suchen Sie in der Windows-Hilfe nach "LAN-Verbindung" oder "Eigenschaften von Internetprotokoll TCP/IP".

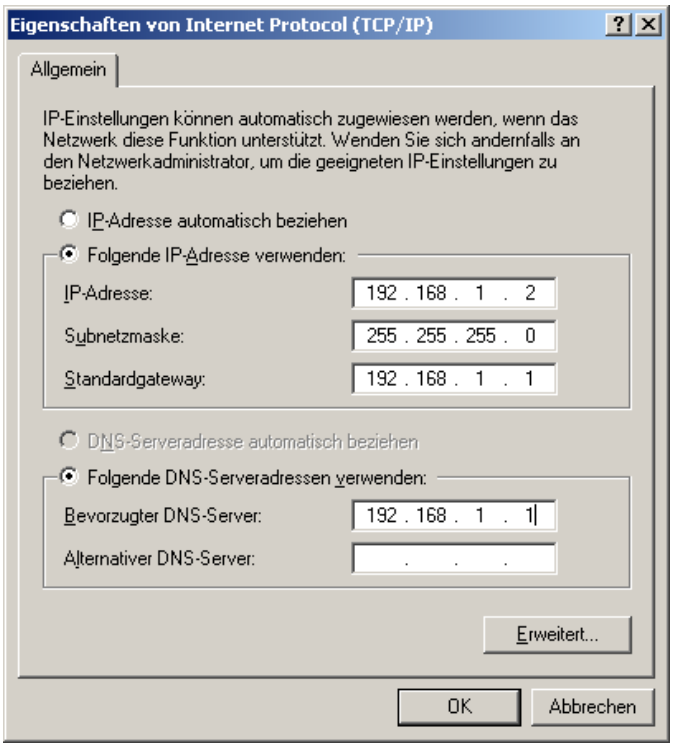


Abbildung 3-1 Dialog "Eigenschaften von Internet Protocol (TCP/IP)"

Geben Sie folgende Werte ein, um die Web-Oberfläche des SCALANCE M873-0 zu erreichen:

- IP-Adresse: 192.168.1.2
- Subnetzmaske: 255.255.255.0

Geben Sie zusätzlich folgende Werte ein, wenn Sie mit dem Admin-PC über das SCALANCE M873-0 auf das externe Netz zugreifen wollen:

- Standardgateway: 192.168.1.1
- Bevorzugter DNS-Server: 192.168.1.1

Bevorzugter DNS-Server

Wenn Sie Adressen über einen Domain-Namen aufrufen (z. B. www.siemens.com), dann muss auf einem Domain Name Server (DNS) nachgeschlagen werden, welche IP-Adresse sich hinter dem Namen verbirgt. Als Domain Name Server können Sie festlegen:

- DNS-Adresse des Netzbetreibers, oder
- Lokale IP-Adresse des SCALANCE M873-0, sofern dieses zum Auflösen von Hostnamen in IP-Adressen konfiguriert ist (siehe Kapitel 4.3). Das ist die Werkseinstellung.

Um den Domain Name Server in der TCP/IP-Konfiguration Ihres Netzwerkadapters festzulegen, gehen Sie wie zuvor beschrieben vor.

3.2 Erlaubte Zeichen bei Benutzernamen, Passwörtern und weiteren Eingaben

Bei Eingaben von Benutzernamen, Passwörtern, Hostnamen, APN und PIN sind folgende darstellbare ASCII-Zeichen erlaubt:

Benutzernamen, Passwörter, PIN

a b c d e f g h I j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9 ! $ % & ' ( ) * + , . / : ; < = > ? @ [\ ] ^ _ ` { | }

Host-Namen, APN

a b c d e f g h I j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9 . -

3.3 Konfigurations-Verbindung herstellen

Web-Browser einrichten

Gehen Sie wie folgt vor:

1. Starten Sie einen Web-Browser.
   (z. B. MS Internet Explorer ab Version 7 oder Mozilla Firefox ab Version 2; der Web-Browser muss SSL (d. h. HTTPS) unterstützen.)

2. Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt.

   Nehmen Sie im MS Internet Explorer diese Einstellung wie folgt vor: Menü "Extras", "Internetoptionen...", Registerkarte "Verbindungen": Unter "DFÜ- und VPN-Einstellungen" muss "Keine Verbindung wählen" aktiviert sein.

Startseite des SCALANCE M873-0 aufrufen

3. Geben Sie in der Adresszeile des Browsers die IP-Adresse des SCALANCE M873-0 vollständig ein. Gemäß Werkseinstellung lautet diese:

   https://192.168.1.1

   Folge: Ein Sicherheitshinweis erscheint.

Abbildung 3-2 Sicherheitshinweis bestätigen

4. Quittieren Sie den entsprechenden Sicherheitshinweis mit „Laden dieser Webseite fortsetzen".

Hinweis

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbst unterzeichneten Zertifikat ausgeliefert. Bei Zertifikaten mit Unterschriften, die dem Betriebssystem nicht bekannt sind, erfolgt ein Sicherheitshinweis. Sie können sich das Zertifikat anzeigen lassen.
Aus dem Zertifikat muss erkenntlich sein, dass es für die Siemens AG ausgestellt wurde. Die Web-Oberfläche wird über eine IP-Adresse adressiert und nicht über einen Namen, daher stimmt der im Sicherheitszertifikat angegebene Name nicht mit dem im Zertifikat überein.

Benutzername und Passwort eingeben

5. Sie werden aufgefordert, den Benutzernamen und das Passwort (Kennwort) anzugeben:

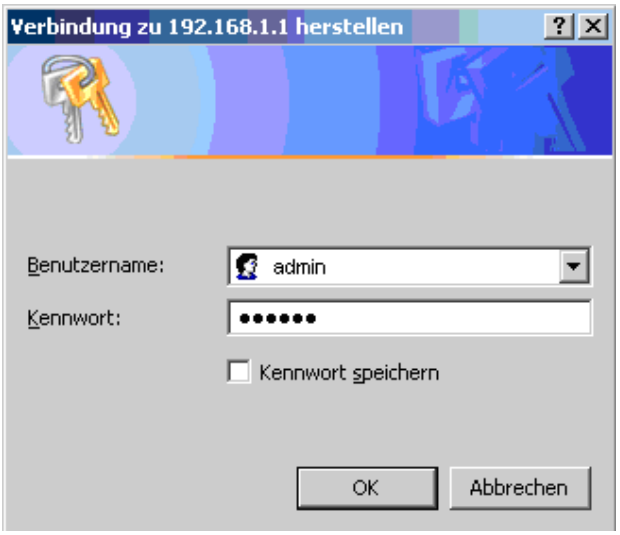


Abbildung 3-3 Benutzernamen und Passwort eingeben

Die werkseitige Voreinstellung lautet:

Benutzername: admin

Kennwort: sinaut

Hinweis

Sie sollten auf jeden Fall das Passwort (Kennwort) ändern. Die werkseitige Voreinstellung ist allgemein bekannt und ist kein ausreichender Schutz. Im Kapitel 3.8 ist beschrieben, wie das Passwort geändert werden kann.

Die Startseite wird angezeigt

Nach Eingabe von Benutzername und Passwort erscheint im Web-Browser die Startseite des SCALANCE M873-0 mit einem Überblick über den Betriebszustand, siehe Kapitel 3.4.

Die Startseite wird nicht angezeigt

Sollte auch nach wiederholtem Versuch der Browser melden, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Überprüfen Sie die Hardware-Verbindung. Dazu bei einem Windows-Rechner über die DOS-Eingabeaufforderung (Menü "Start", "Programme", "Zubehör", "Eingabeaufforderung") folgenden Befehl eingeben:

  ping 192.168.1.1

  Wenn innerhalb der vorgegebenen Zeitspanne die Meldung über den Rück-Empfang der 4 ausgesendeten Pakete nicht erscheint, überprüfen Sie das Kabel, die Anschlüsse und die Netzwerkkarte.

- Achten Sie darauf, dass der Browser keinen Proxy Server verwendet. Im MS Internet Explorer (Version 7.0) nehmen Sie diese Einstellung wie folgt vor: Menü "Extras", "Internetoptionen...", Registerkarte "Verbindungen": Unter "LAN-Einstellungen" auf die Schaltfläche "Einstellungen..." klicken, im Dialogfeld "Einstellungen für lokales Netzwerk (LAN)" dafür sorgen, dass unter "Proxyserver" der Eintrag "Proxyserver für LAN verwenden" nicht aktiviert ist.

- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Unter Windows Menü "Start", "Verbinden mit ...", "Systemsteuerung", "Alle Verbindungen anzeigen" unter LAN oder Höchstgeschwindigkeits-Internet die betreffende Verbindung mit der rechten Maustaste klicken und im Kontextmenü "Deaktivieren" wählen.

- Geben Sie die Adresse des SCALANCE M873-0 mit Schrägstrich ein:

  https://192.168.1.1/

3.4 Startseite der Web-Oberfläche

Nach Aufrufen der Web-Oberfläche des SCALANCE M873-0 und der Eingabe von Benutzernamen und Passwort erscheint ein Überblick über den aktuellen Betriebszustand des SCALANCE M873-0.

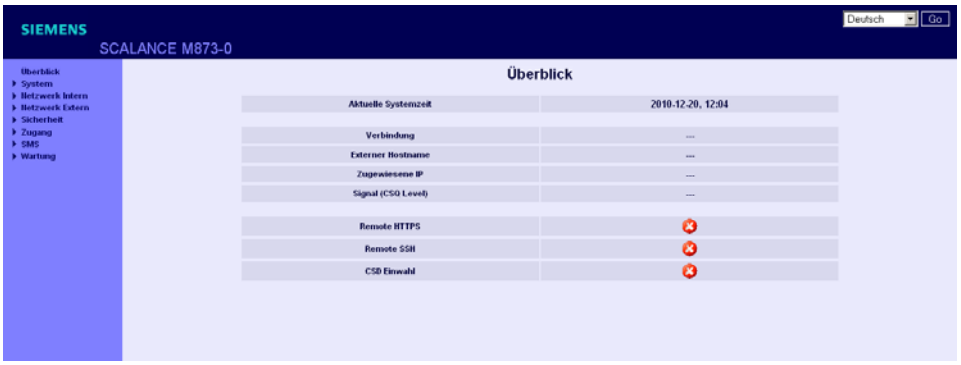


Abbildung 3-4 Startseite / Überblick

Hinweis

Benutzen Sie die Funktion "Aktualisieren" des Web-Browsers, um die angezeigten Werte auf den aktuellen Stand zu bringen.

Aktuelle Systemzeit

Zeigt die aktuelle Systemzeit des SCALANCE M873-0 an, im Format:

Jahr – Monat – Tag, Stunden – Minuten

Verbindung

Zeigt an, ob und welche Funkverbindung besteht:

- UMTS-Verbindung (IP-Verbindung über HSDPA, UMTS)
- GPRS/EDGE-Vebindung (IP-Verbindung über EGPRS oder GPRS)
- CSD-Verbindung (Service-Verbindung über CSD)

Externer Hostname

Zeigt den Hostnamen (z. B. m873.mydns.org) des SCALANCE M873-0 an, wenn ein DynDNS-Dienst verwendet wird.

Signal (CSQ Level)

Gibt die Stärke des GSM-Signals als CSQ-Wert an.

- CSQ < 6: Signalstärke schlecht
- CSQ= 6..10: Signalstärke mittel
- CSQ=11-18: Feldstärke gut
- CSQ > 18: Feldstärke sehr gut
- CSQ = 99: Keine Verbindung zum GSM-Netz

Zugewiesene IP-Adresse

Zeigt die IP-Adresse an, unter der das SCALANCE M873-0 im Funknetz zu erreichen ist. Diese IP-Adresse wird dem SCALANCE M873-0 vom Funknetz zugewiesen.

Hinweis

Es kann vorkommen, dass eine IP-Datenverbindung und auch eine zugewiesene IP-Adresse angezeigt werden, die Verbindungsqualität aber dennoch nicht ausreicht um Daten zu übertragen. Aus diesem Grund empfehlen wir, die aktive Verbindungsüberwachung zu nutzen (siehe Kapitel 5.2).

Remote HTTPS

Zeigt an, ob Zugriffe auf die Web-Oberfläche des SCALANCE M873-0 aus der Ferne über das Funknetz erlaubt sind (siehe Kapitel 7.1).

- Weißer Haken auf grünem Punkt: Der Zugriff ist erlaubt.
- Weißes Kreuz auf rotem Punkt: Der Zugriff ist nicht erlaubt.

Remote SSH

Zeigt an, ob Zugriffe auf die SSH-Konsole des SCALANCE M873-0 aus der Ferne über das Funknetz erlaubt sind (siehe Kapitel 7.2).

- Weißer Haken auf grünem Punkt: Der Zugriff ist erlaubt.
- Weißes Kreuz auf rotem Punkt: Der Zugriff ist nicht erlaubt.

CSD Einwahl

Zeigt an, ob CSD-Serviceanrufe aus der Ferne erlaubt sind (siehe Kapitel 7.3).

- Weißer Haken auf grünem Punkt: Der Zugriff ist erlaubt.
- Weißes Kreuz auf rotem Punkt: Der Zugriff ist nicht erlaubt.

3.5 Spracheinstellung

Das SCALANCE M873-0 unterstützt die web-basierte Administrations-Oberfläche in englischer und deutscher Sprache.

Abbildung 3-5 Sprachauswahl

Automatisch

Das SCALANCE M873-0 wählt entsprechend den Einstellungen des benutzten Web-Browsers die Sprache der Administrations-Oberfläche:

- Deutsch, wenn der Web-Browser auf deutsche Sprache eingestellt ist
- Englisch, in allen anderen Fällen.

Deutsch

Das SCALANCE M873-0 verwendet die deutsche Sprache, unabhängig vom verwendeten Web-Browser.

Englisch

Das SCALANCE M873-0 verwendet die englische Sprache, unabhängig vom verwendeten Web-Browser.

Zum Umschalten der Sprache betätigen Sie die Schaltfläche "GO" und laden Sie mit dem Web-Browser die Web-Seite neu.

3.6 Konfiguration vornehmen

Zur Konfiguration des SCALANCE M873-0 gehen Sie wie folgt vor:

Konfiguration durchführen

1. Per Menü den gewünschten Einstellbereich aufrufen.
2. Auf der betreffenden Seite die gewünschten Einträge machen oder mit Zurücksetzen die aktuelle, nicht gespeicherte Eingabe wieder löschen.
3. Mit Speichern bestätigen, so dass die Einstellungen vom Gerät übernommen werden.

Abbildung 3-6 Menüleiste

Hinweise

Je nachdem, wie Sie das SCALANCE M873-0 konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

Tragen Sie bei der Eingabe von IP-Adressen, die IP-Adress-Teilnummern immer ohne führende Nullen ein, z. B.: 192.168.0.8.

Fehleingaben

Das SCALANCE M873-0 prüft Ihre Eingaben. Fehler werden beim Speichern erkannt und das betroffene Eingabefeld wird markiert.

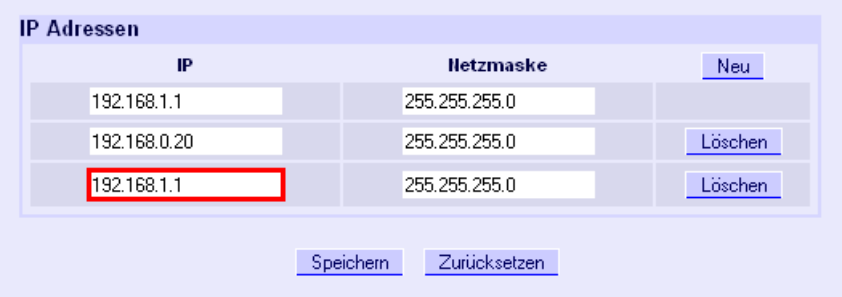


Abbildung 3-7 Markierte Fehleingabe

3.7 Konfigurationsprofile

Die Einstellungen des SCALANCE M873-0 können in Konfigurationsprofilen (Dateien) gespeichert werden und jederzeit neu geladen werden.

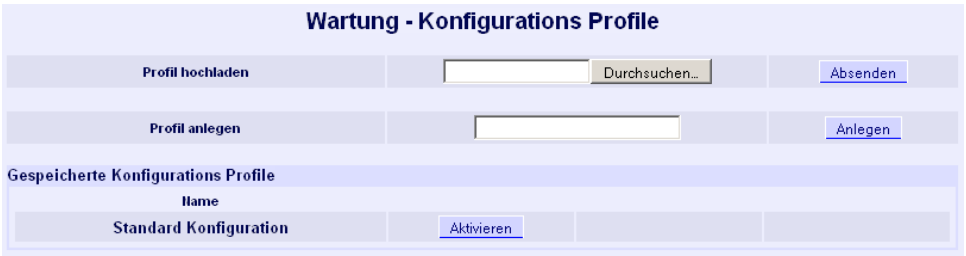


Abbildung 3-8 Menübefehl "Wartung" > "Konfigurations-Profile"

Profil hochladen

Lädt ein zuvor erstelltes und auf den Admin-PC gespeichertes Konfigurationsprofil in das SCALANCE M873-0. Dateien mit Konfigurationsprofilen haben die Dateiendung *.tgz.

Mit "Durchsuchen" können Sie auf dem Admin-PC nach Konfigurationsprofilen suchen. Mit "Absenden" laden Sie das Konfigurationsprofil in das SCALANCE M873-0.

Das Profil wird dann in der Tabelle der gespeicherten Konfigurations-Profile angezeigt.

Profil anlegen

Speichert die aktuellen Einstellungen des SCALANCE M873-0 in einem Konfigurationsprofil.

Geben Sie zunächst einen Namen für das Profil in dem Eingabefeld ein. Mit "Anlegen" werden die Einstellungen in einem Profil mit diesem Namen gespeichert und dann in der Tabelle der gespeicherten Konfigurations-Profile angezeigt.

Gespeicherte Konfigurations-Profile

Download

Lädt das Profil auf den Admin-PC.

Aktivieren

Das SCALANCE M873-0 übernimmt die Einstellungen des ausgewählten Konfigurationsprofils und arbeitet mit diesen weiter.

Löschen

Das Konfigurationsprofil wird gelöscht.

Das Profil "Standard Konfiguration" enthält die Werkseinstellungen und kann nicht gelöscht werden.

3.8 Passwort ändern

Der Zugang zum SCALANCE M873-0 ist durch ein Zugangspasswort geschützt. Dieses Zugangspasswort schützt sowohl den Zugang über die

- lokale Schnittstelle auf die Web-Oberfläche und
- lokale Schnittstelle auf die SSH-Konsole

wie auch den Zugang über

- UMTS/GPRS per https auf die Web-Oberfläche und
- UMTS/GPRS auf die SSH-Konsole

Zugangspasswort (Werkseinstellung)

Die Werkseinstellung für das SCALANCE M873-0 lautet:

- Passwort: admin
- Benutzername: sinaut (kann nicht verändert werden)

Hinweis

Ändern Sie das Passwort sofort nach Inbetriebnahme. Die werkseitige Voreinstellung ist allgemein bekannt und bietet keinen ausreichenden Schutz.

Hinweis

Der Benutzername für den SSH-Zugang weicht von dem Benutzernamen der web-basierten Administrations-Oberfläche ab.

Benutzername: root (kann nicht verändert werden)

Das Passwort entspricht dem Zugangspasswort für das SCALANCE M873-0 wie oben festgelegt.

Neues Zugangspasswort (mit Wiederholung)

Um das Passwort zu ändern, geben Sie bei "Neues Zugangspasswort" das neu ausgewählte Passwort ein und wiederholen Sie die Eingabe im Feld "Neues Zugangspasswort (Wiederholung)".

Mit "Zurücksetzen" werden Ihre noch nicht gespeicherten Eingaben verworfen. Mit "Speichern" wird das neue Passwort übernommen.

3.9 Neustart

Obwohl das SCALANCE M873-0 für den Dauerbetrieb ausgelegt ist, kann es bei solch einem komplexen System zu Störungen kommen, oftmals ausgelöst durch äußere Einwirkung. Ein Neustart kann diese Störungen beheben.

Der Neustart setzt die Funktionen des SCALANCE M873-0 zurück. Aktuelle Einstellungen entsprechend des Konfigurationsprofils ändern sich nicht. Nach dem Neustart arbeitet das SCALANCE M873-0 mit diesen Einstellungen weiter.

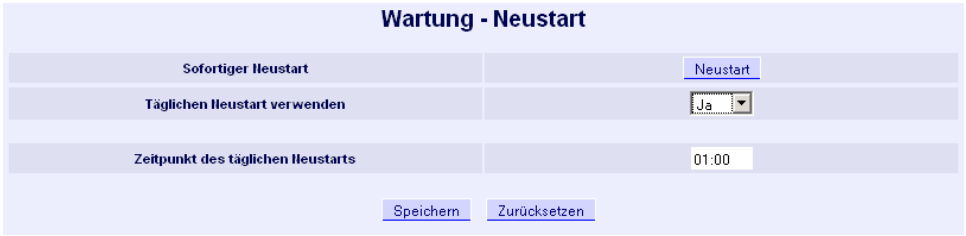


Abbildung 3-9 Menübefehl "Wartung" > "Neustart"

Sofortiger Neustart

Der Neustart wird sofort ausgeführt, wenn Sie auf "Neustart" klicken.

Täglichen Neustart verwenden

Der Neustart wird automatisch einmal am Tag ausgeführt, wenn Sie die Funktion mit "Ja" einschalten.

Geben Sie den Zeitpunkt "des täglichen Neustarts" fest. Der Neustart erfolgt bei der angegebenen Systemzeit. Bestehende Verbindungen werden unterbrochen.

Werkseinstellung

Täglichen Neustart verwenden:	**Nein**
Zeitpunkt des täglichen Neustarts:	**01:00**

3.10 Werkseinstellung laden

Die Werkseinstellungen des SCALANCE M873-0 lassen sich auf verschiedene Weisen wiederherstellen.

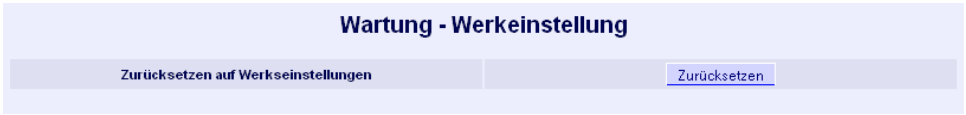


Abbildung 3-10 Menübefehl "Wartung" > "Werkseinstellung"

Zurücksetzen auf Werkseinstellung

Das Betätigen der Schaltfläche "Zurücksetzen" lädt die werkseitigen Einstellungen, setzt die Passwörter zurück und löscht die gespeicherten Konfigurationsprofile und die archivierten Logbücher.

Service-Taster (SET)

Das Zurücksetzen auf Werkseinstellungen kann auch über den Service-Taster (SET) ausgelöst werden (siehe Kapitel 2.5).

Standardkonfiguration

Wenn nur die werkseitigen Einstellungen geladen werden sollen, ohne dass die Konfigurationsprofile und die archivierten Logbücher gelöscht werden, aktivieren Sie nur die Standardkonfiguration wie in Kapitel 3.7 beschrieben.

Lokale Schnittstelle

4

Die lokale Schnittstelle ist die Schnittstelle des SCALANCE M873-0 zum Anschluss des lokalen Netzes. Die Schnittstelle ist am Gerät mit X2 gekennzeichnet. Es handelt sich um eine Ethernet-Schnittstelle mit 10 Mbit/s oder 100 Mbit/s Datenrate.

Das lokale Netz ist das Netzwerk, das an der lokalen Schnittstelle des SCALANCE M873-0 angeschlossen ist. Das lokale Netz enthält mindestens eine lokale Applikation.

Lokale Applikationen sind Netzwerkkomponenten im lokalen Netz, zum Beispiel eine programmierbare Steuerung, eine Maschine mit Ethernet-Schnittstelle zur Fernüberwachung, ein Notebook bzw. PC oder der Admin-PC.

Konfigurieren Sie entsprechend Ihren Anforderungen die lokale Schnittstelle und die damit verbundenen Funktionen wie in diesem Kapitel beschrieben.

4.1 IP-Adressen der lokalen Schnittstelle

An dieser Stelle werden die IP-Adressen und die Netzmasken eingestellt, unter der das SCALANCE M873-0 von lokalen Applikationen erreichbar ist.

Abbildung 4-1 Menübefehl "Netzwerk Intern" > "Grundeinstellungen" > "Lokale IPs"

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

- IP 192.168.1.1
- Netzmaske 255.255.255.0

Diese werkseitig eingestellte IP-Adressen und Netzmaske kann frei verändert werden, sollten jedoch den geltenden Empfehlungen (RFC 1918) folgen.

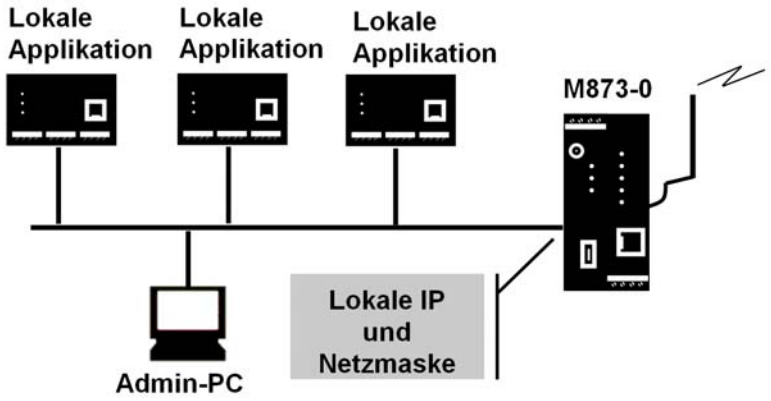


Abbildung 4-2 Darstellung lokales Netz

Sie können weitere Adressen festlegen, unter denen das SCALANCE M873-0 von lokalen Applikationen erreicht werden kann. Dies ist dann hilfreich, wenn z. B. das lokale Netz in Subnetze unterteilt wird. Dann können mehrere lokale Applikationen aus verschiedenen Subnetzen das SCALANCE M873-0 unter unterschiedlichen Adressen erreichen.

Neu

Fügt weitere IP-Adressen und Netzmasken hinzu, die Sie wiederum ändern können.

Löschen

Entfernt die jeweilige IP-Adresse und Netzmaske. Der erste Eintrag kann nicht gelöscht werden.

4.2 DHCP Server zum lokalen Netz

Das SCALANCE M873-0 beinhaltet einen DHCP Server (DHCP = Dynamic Host Configuration Protokoll). Ist der DHCP Server eingeschaltet, weist er den Applikationen, die an der lokalen Schnittstelle des SCALANCE M873-0 angeschlossen sind, automatisch die IP-Adressen, Netzmasken, das Gateway und den DNS-Server zu. Dazu muss bei den lokalen Applikationen das automatische Beziehen der IP-Adresse und der Konfigurationsparameter per DHCP aktiviert sein.

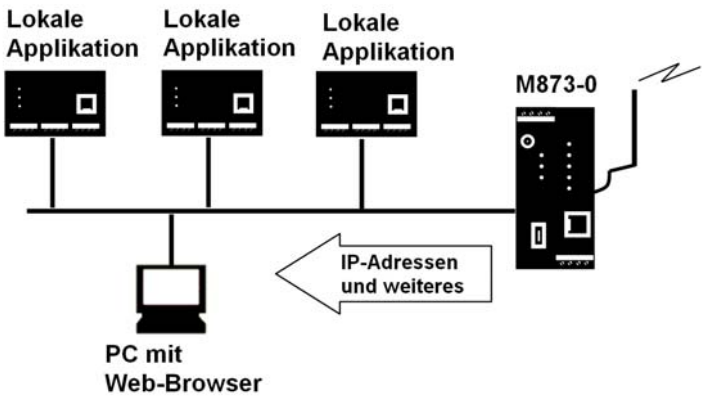


Abbildung 4-3 DHCP-Server-Funktion

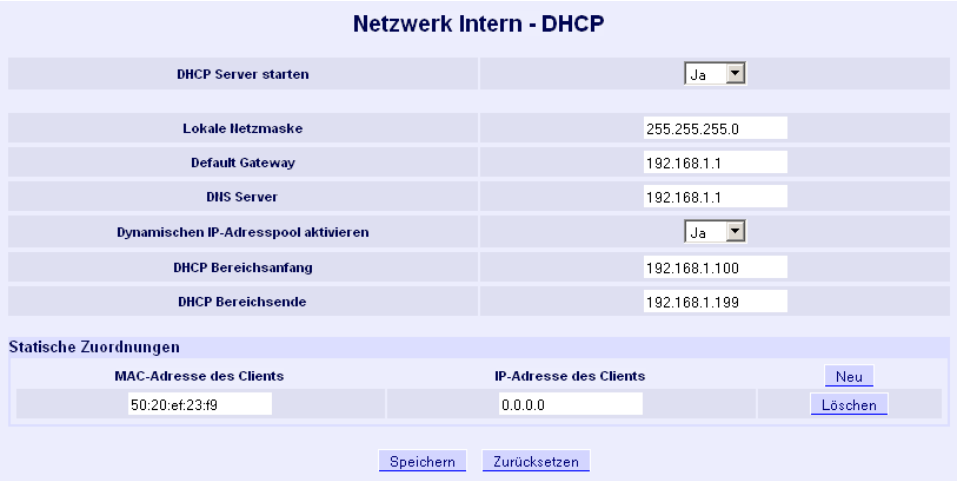


Abbildung 4-4 Menübefehl "Netzwerk Intern" > "Grundeinstellungen" > "DHCP"

DHCP Server starten

Mit "DHCP Server" starten – "Ja" schalten Sie den DHCP Server des SCALANCE M873-0 ein, mit "Nein" wird er ausgeschaltet.

Lokale Netzwerkmaske

Tragen Sie hier die lokale Netzmaske ein, die den lokalen Applikationen zugewiesen werden soll.

Default Gateway

Tragen Sie hier das Default Gateway ein, das den lokalen Applikationen zugewiesen werden soll.

DNS Server

Tragen Sie hier den DNS Server ein, der den lokalen Applikationen zugewiesen werden soll.

Dynamischen IP-Adresspool aktivieren

Bei "Ja" werden die IP-Adressen, die der DHCP Server des SCALANCE M873-0 vergibt aus einem dynamischen Adresspool entnommen.

Bei "Nein" müssen die IP-Adressen unter "Statische Zuordnung" den MAC-Adressen der lokalen Applikationen zugeordnet werden.

DHCP Bereichsanfang

Gibt die erste Adresse des dynamischen Adresspools an.

DHCP Bereichsende

Gibt die letzte Adresse des dynamischen Adresspools an.

Statische Zuordnung

Bei Statischer Zuordnung der IP-Adressen, können Sie den MAC-Adressen lokaler Applikationen korrespondierende IP-Adressen festlegen.

Fordert eine lokale Applikation per DHCP die Zuweisung einer IP-Adresse, übermittelt die Applikation bei der DHCP-Anfrage seine MAC-Adresse. Ist dieser MAC-Adresse eine IP-Adresse statisch zugeordnet, weist das SCALANCE M873-0 der Applikation die korrespondierende IP-Adresse zu.

MAC-Adresse des Clients – MAC-Adresse der anfragenden lokalen Applikation

IP-Adresse des Clients – zugeordnete IP-Adresse

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

DHCP Server starten	**Nein**
Lokale Netzwerkmaske	**255.255.255.0**
Default Gateway	**192.168.1.1**
DNS Server	**192.168.1.1**
Dynamischen IP-Adresspool aktivieren	**Nein**
DHCP Bereichsanfang	**192.168.1.100**
DHCP Bereichsende	**192.168.1.199**

4.3 DNS zum lokalen Netz

Das SCALANCE M873-0 stellt dem lokalen Netz einen Domain Name Server (DNS) bereit.

Tragen Sie in Ihrer lokalen Applikation die IP-Adresse des SCALANCE M873-0 als Domain Name Server (DNS) ein, dann beantwortet das SCALANCE M873-0 die DNS-Abfragen aus seinem Cache. Kennt es zu einer Domain-Adresse nicht die dazugehörige IP-Adresse, leitet das SCALANCE M873-0 die Abfrage weiter an einen externen Domain Name Server (DNS).

Die Zeitspanne, in der das SCALANCE M873-0 eine Domain-Adresse im Cache behält, ist abhängig vom adressierten Host. Die DNS-Abfrage an einen externen Domain Name Server, liefert außer der IP-Adresse auch die Lebensdauer dieser Information zurück.

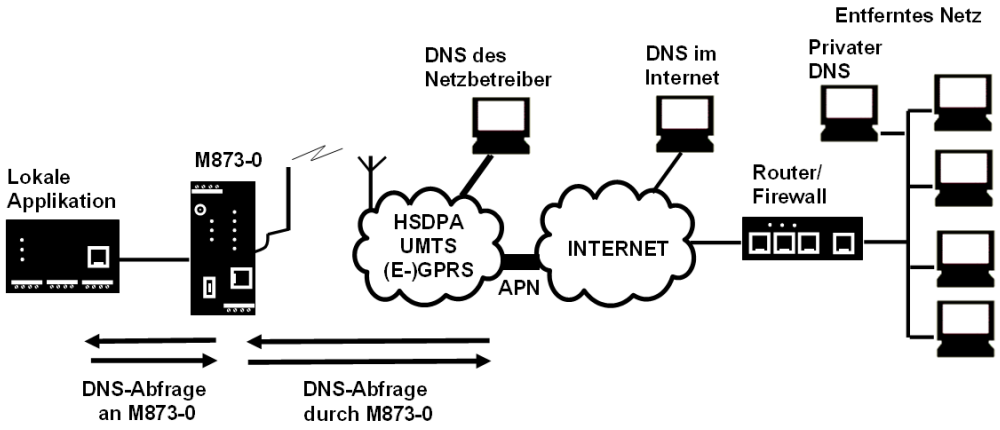


Abbildung 4-5 DNS-Funktion

Als externe Domain Name Server (DNS) können Server des Netzbetreibers, Server im Internet oder Server im privaten externen Netz verwendet werden.

Abbildung 4-6 Menübefehl "Netzwerk Intern" > "Grundeinstellungen" > "DNS"

Benutzter Nameserver

Wählen Sie aus, bei welchem Domain Name Server (DNS) das SCALANCE M873-0 nachfragen soll:

Provider definiert

Beim Verbindungsaufbau der UMTS/GPRS-Verbindung übermittelt der Netzbetreiber automatisch eine oder mehrere DNS-Adressen. Diese werden dann verwendet.

Benutzer definiert

Sie wählen als Anwender Ihre bevorzugten DNS aus. Die DNS können mit dem Internet verbunden sein oder es kann ein privater DNS in Ihrem Netz sein.

Nutzer definierter Nameserver

Wenn Sie die Option "Benutzer definiert" gewählt haben, dann geben Sie die IP-Adresse des ausgewählten DNS als "Server IP-Adresse" ein.

Mit "Neu" können Sie weitere DNS hinzufügen.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Benutzter Nameserver	**Provider definiert**
Nutzer definierter Nameserver	**-**
Bei neuem Eintrag	**0.0.0.0**

4.4 Lokaler Hostname

Das SCALANCE M873-0 kann aus dem lokalen Netz, auch über einen Hostnamen adressiert werden. Legen Sie dazu einen Hostnamen fest, z. B. M873.

Das SCALANCE M873-0 kann dann zum Beispiel von einem Web-Browser als M873 aufgerufen werden.

Abbildung 4-7 Menübefehl "Netzwerk Intern" > "Grundeinstellungen" > "DNS"

Hinweis

Das Sicherheitskonzept des SCALANCE M873-0 macht es erforderlich, dass für jede lokale Applikation, die diese Hostname-Funktion nutzen soll, eine ausgehende Firewall-Regel erstellt wird. Siehe Kapitel 6.1.

Wenn Sie kein DHCP verwenden (siehe Kapitel 4.2), müssen im SCALANCE M873-0 und in den lokalen Applikationen manuell identische Suchpfade eingetragen werden. Wenn Sie DHCP verwenden, erhalten die lokale Applikationen den im SCALANCE M873-0 eingetragenen Suchpfad per DHCP.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Suchpfad	**example.local**
Host-Name	**SINAUT**

4.5 Systemzeit / NTP

Die Systemzeit des SCALANCE M873-0 kann manuell gesetzt werden oder mit einem Zeitserver automatisch synchronisiert werden.

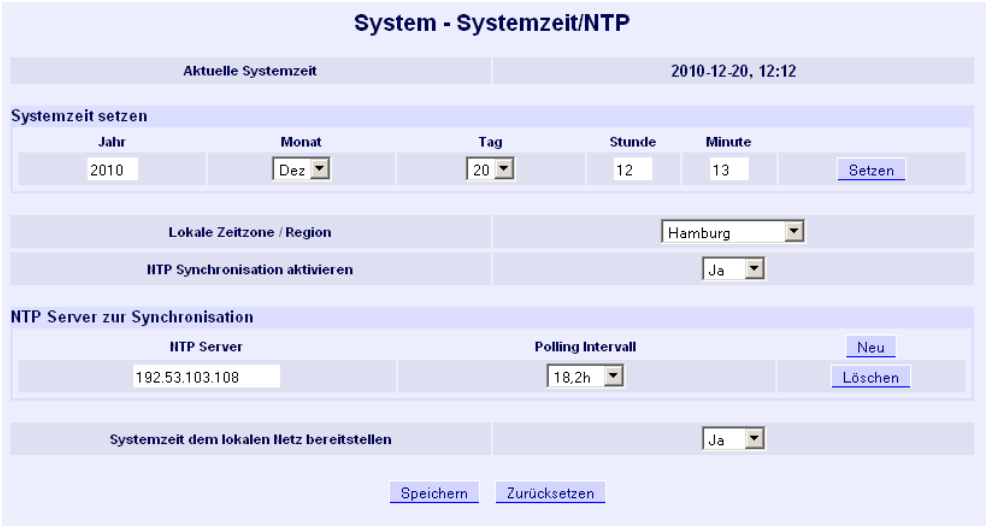


Abbildung 4-8 Menübefehl "System" > "Systemzeit"

Systemzeit manuell setzen

An dieser Stelle setzen Sie die Systemzeit für das SCALANCE M873-0. Diese Systemzeit wird:

- als Zeitstempel für alle Logbuch-Einträge benutzt und
- dient als Zeitbasis für alle zeitgesteuerten Funktionen.

Wählen Sie Jahr, Monat und Tag sowie Stunde und Minute.

NTP Synchronisation aktivieren

Das SCALANCE M873-0 kann die Systemzeit auch über NTP (= Network Time Protocol) von einem Zeitserver beziehen. Im Internet gibt es eine Reihe von Zeitservern von denen die aktuelle Uhrzeit sehr präzise mittels NTP bezogen werden kann.

Lokale Zeitzone / Region

Die NTP-Zeitserver übermitteln die UTC (= Universal Time Coordinated), d.h. die koordinierte Weltzeit. Wählen Sie eine Stadt in der Nähe des Standortes aus, an dem das SCALANCE M873-0 arbeiten soll und legen Sie so die Zeitzone fest. Dann wird die Uhrzeit dieser Zeitzone als Systemzeit verwendet.

NTP-Server

Klicken Sie auf "Neu", um einen NTP Server hinzuzufügen und geben Sie die IP-Adresse eines solchen NTP-Servers ein oder verwenden Sie den ab Werk voreingestellten NTP-Server. Sie können parallel mehrere NTP-Server angeben.

Die Eingabe der NTP-Adresse als Hostname (z. B. timeserver.org) ist nicht möglich.

Polling Intervall

Die Zeitsynchronisation erfolgt zyklisch. Das Intervall in dem die Synchronisation stattfindet bestimmt das SCALANCE M873-0 automatisch. Spätestens nach 36 Stunden findet erneut eine Synchronisation statt. Das Polling-Intervall legt fest, wie lange das SCALANCE M873-0 mindestens bis zur nächsten Synchronisation wartet.

Achtung

Die Synchronisation der Systemzeit über NTP verursacht ein zusätzliches Datenaufkommen auf der UMTS/GPRS-Verbindung. Je nach Teilnehmervertrag mit dem Mobilfunkbetreiber sind damit erhöhte Kosten verbunden.

Systemzeit dem lokalen Netz bereitstellen

Das SCALANCE M873-0 kann selber als NTP-Zeitserver für die Applikationen dienen, die an seiner lokalen Netzwerkschnittstelle angeschlossen sind. Zur Aktivierung dieser Funktion wählen Sie "Ja".

Der NTP-Zeitserver im SCALANCE M873-0 ist über die eingestellte lokale IP-Adresse des SCALANCE M873-0 erreichbar, siehe Kapitel 4.1.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Lokale Zeitzone	**UTC**
NTP Synchronisation aktivieren	**Nein**
NTP-Server	**192.53.103.108**
Polling Intervall	**1.1 Stunden**
Systemzeit dem lokalen Netz bereitstellen	**Nein**

4.6 Zusätzliche interne Routen

Teilt sich das lokale Netz in Subnetze auf, können Sie zusätzliche Routen definieren. Siehe auch Glossar.

Abbildung 4-9 Menübefehl "Netzwerk Intern" > "Zusätzliche interne Routen"

Mit "Neu" legen Sie eine weitere Route zu einem Subnetz fest.

Geben Sie folgendes an:

- die IP-Adresse des Subnetzes (Netzwerkes), ferner
- die IP-Adresse des Gateways, über das das Subnetz angeschlossen ist.

Sie können beliebig viele interne Routen festlegen. Mit "Löschen" entfernen Sie eine interne Route.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Zusätzliche interne Routen	**-**
Vorgabe für neue Routen:	**Nein**
Netzwerk:	**192.168.2.0/24**
Gateway:	**192.168.0.254**

Externe Schnittstelle

5

Die externe Schnittstelle des SCALANCE M873-0 verbindet das SCALANCE M873-0 mit dem externen Netz. Zur Kommunikation wird HSDPA, UMTS, EGPRS oder GPRS auf dieser Schnittstelle verwendet.

Externe Netze sind das Internet oder ein privates Intranet.

Externe Gegenstellen sind Netzwerkkomponenten im externen Netz, z. B. Web-Server im Internet, Router im Intranet, ein zentraler Firmenserver oder ein Admin-PC.

Konfigurieren Sie entsprechend Ihren Anforderungen die externe Schnittstelle und die damit verbundenen Funktionen wie in diesem Kapitel beschrieben.

5.1 Zugangsparameter zum UMTS/GPRS

Für den Zugang zu den Diensten HSDPA, UMTS, EGPRS oder GPRS und zum grundlegenden GSM-Funknetz sind Zugangsparameter erforderlich, die Sie von Ihrem Mobilfunkbetreiber (Provider) erhalten.

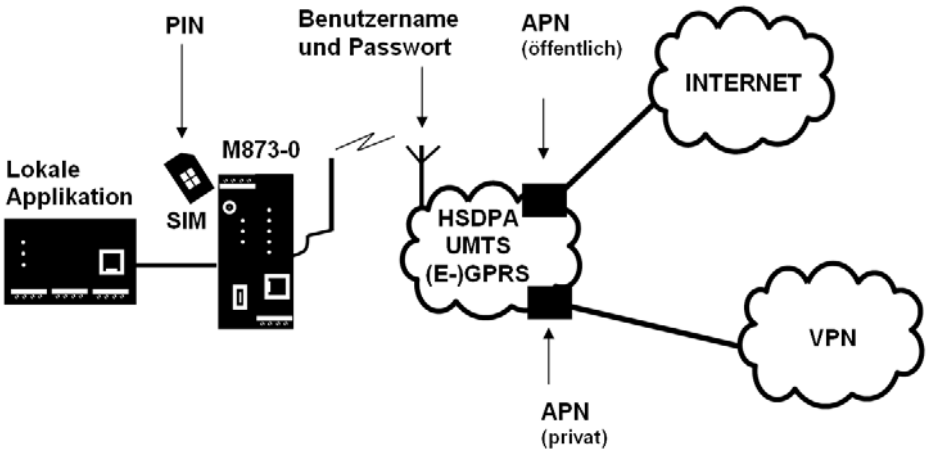


Abbildung 5-1 Zugangsparameter

Die PIN schützt die SIM-Karte vor unbefugter Benutzung des Modems.

Benutzername und Passwort schützen den Zugang zum UMTS/GPRS-Netz.

Der APN (Access Point Name) definiert den Übergang vom UMTS/GPRS-Netz zu weiteren verbundenen IP-Netzen, z. B. den Übergang von einem öffentlichen APN zum Internet oder von einem privaten APN zu einem Virtual Private Network (VPN).

Modus der Provider-Auswahl - Manuell

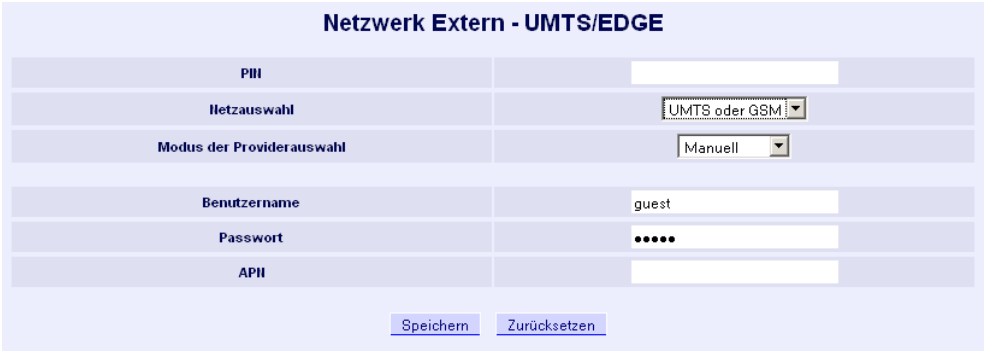


Abbildung 5-2 Menübefehl "Netzwerk Extern" > "EDGE/GPRS" - Provider-Auswahl manuell

Wenn Sie als Modus der Provider-Auswahl "Manuell" auswählen, dann geben Sie Benutzername, Passwort und APN für den UMTS- oder GPRS-Dienst händisch ein.

Modus der Provider-Auswahl - Automatisch

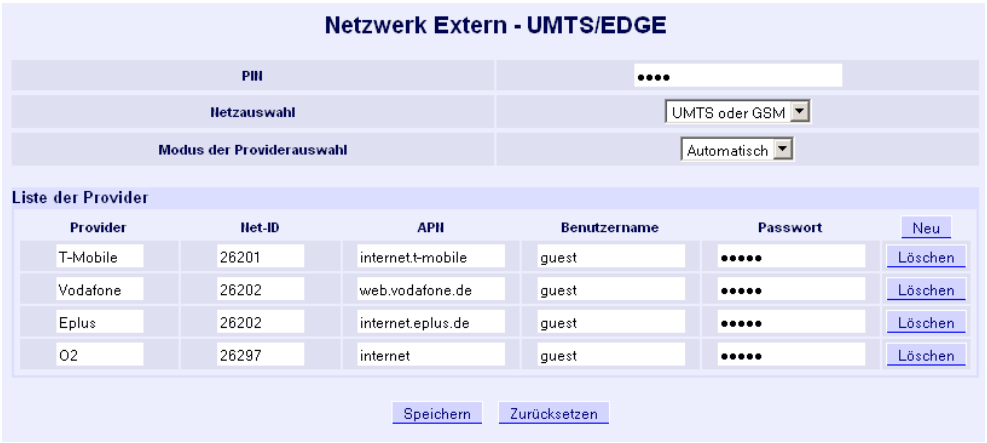


Abbildung 5-3 Menübefehl "Netzwerk Extern" > "EDGE/GPRS" - Provider-Auswahl automatisch

Wenn Sie als Modus der Provider-Auswahl "Automatisch" auswählen, dann werden die Zugangsdaten für den UMTS- oder GPRS-Dienst automatisch anhand der Net-ID der SIM-Karte aus der Liste der Provider ausgewählt. In der Liste können Sie mehrere Einträge angelegen.

Mit "Neu" fügen Sie einen neuen Eintrag hinzu. Mit "Löschen" entfernen Sie Einträge.

PIN

Geben Sie hier die PIN zu Ihrer SIM-Karte ein. Sie erhalten die PIN von Ihrem Netzbetreiber.

Das SCALANCE M873-0 arbeitet auch mit PIN-losen SIM-Karten, in diesem Fall geben Sie NONE ein. Das Eingabefeld bleibt in diesem Fall leer.

Hinweis

Wenn keine Eingabe erfolgt, wird das Eingabefeld der PIN nach dem Speichern rot umrandet.

Netzauswahl

Wählen Sie den Typ des Mobilfunknetzes aus, das verwendet werden soll:

- UMTS (mit den Diensten UMTS data und HSDPA)
- GSM (mit dem Diensten EGPRS, GPRS und CSD)

Provider (nur bei Provider-Auswahl "Automatisch")

Geben Sie hier als Freitext eine Bezeichnung für den UMTS- oder GPRS-Dienst an, z. B. den Namen des Providers (z. B. Vodafone, Eplus, mein GPRS-Zugang).

Net-ID (nur bei Provider-Auswahl "Automatisch")

Geben Sie hier die Identifikationsnummer (Net-ID) des Netzbetreibers ein, auf die sich die UMTS oder GPRS Zugangsdaten in der gleichen Zeile der Liste der Provider beziehen.

Jeder UMTS oder UMTS- oder GSM/GPRS-Netzbetreiber hat eine weltweit einmalig vergebene Identifikations-Nummer, die als Public Land Mobile Network (PLMN) bezeichnet wird. PLMN setzt sich zusammen aus (MCC) und (MNC). Sie finden die Net-ID in den Unterlagen Ihres UMTS- oder GSM/GPRS-Netzbetreibers oder auf dessen Internetseiten.

Die Net-ID ist auf der SIM-Karte gespeichert. Das SCALANCE M873-0 liest die Net-ID von der SIM-Karte und wählt die entsprechenden UMTS oder GPRS Zugangsdaten aus der Liste der Provider.

Benutzername

Geben Sie hier den Benutzername für UMTS/GPRS ein. Einige Mobilfunkbetreiber verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall tragen Sie in das jeweilige Feld "gast" ein.

Passwort

Geben Sie hier das Passwort für UMTS/GPRS ein. Einige Mobilfunkbetreiber verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall tragen Sie in das jeweilige Feld "gast" ein.

APN

Geben Sie hier den Namen des Übergangs von UMTS/GPRS zu weiteren Netzen ein.

Sie finden den APN in den Unterlagen Ihres Mobilfunkbetreibers, auf dessen Internetseite oder erfragen den APN bei der Hotline Ihres GSM/GPRS-Netzbetreibers.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Modus der Provider-Auswahl	**Manuell**

Modus der Provider-Auswahl - Manuell

PIN	**NONE**
Benutzername	**guest**
Passwort	**guest**
APN	**NONE**

Modus der Provider-Auswahl - Automatisch

1. Provider	**T-Mobile**
Net-ID	**26201**
Benutzername	**guest**
Passwort	**guest**
APN	**internet.t-mobile**
2. Provider	**Vodafone**
Net-ID	**26202**
Benutzername	**guest**

Passwort	**guest**
APN	**web.vodafone.de**
3. Provider	**Eplus**
Net-ID	**26203**
Benutzername	**guest**
Passwort	**guest**
APN	**internet.eplus.de**
4. Provider	**O2**
Net-ID	**26207**
Benutzername	**guest**
Passwort	**guest**
APN	**internet**
n. Provider	**NONE**
Net-ID	**NONE**
Benutzername	**NONE**
Passwort	**NONE**
APN	**NONE**

5.2 Verbindungsüberwachung UMTS/GPRS

Mit der Funktion "Prüfen der Verbindung" überprüft das SCALANCE M873-0 seine Verbindung zum UMTS/GPRS und zu den angeschlossenen externen Netzen, wie z. B. dem Internet oder einem Intranet. Dazu sendet das SCALANCE M873-0 in regelmäßigen Zeitabständen, Ping-Pakete (ICMP) an bis zu vier Gegenstellen (Ziel Hosts). Dies geschieht unabhängig von den Nutzdaten-Verbindungen. Erhält das SCALANCE M873-0 auf einen solchen Ping mindestens von einem der adressierten Gegenstellen eine Antwort, ist das SCALANCE M873-0 noch mit dem IP-Mobilfunkdienst verbunden und betriebsbereit.

Einige "Netzbetreiber" unterbrechen Verbindungen bei Inaktivität. Dem wird durch die Funktion "Prüfen der Verbindung" ebenfalls vorgebeugt.

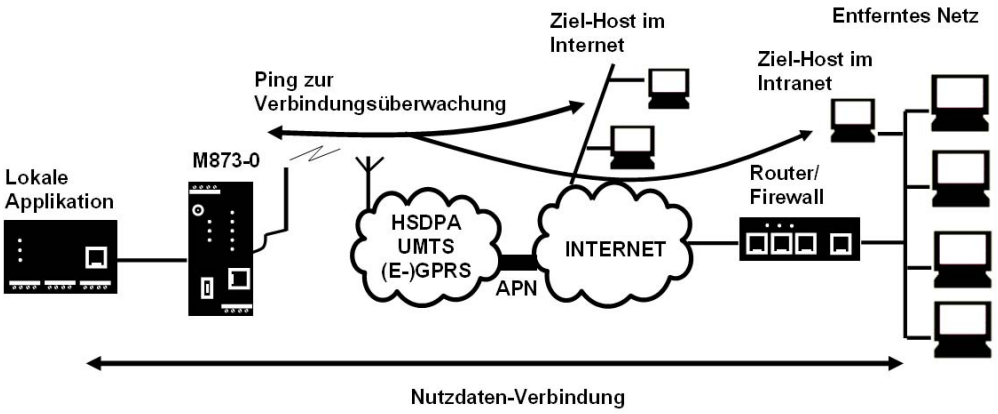


Abbildung 5-4 Verbindungsüberwachung

Achtung

Durch das Versenden der Ping-Pakete (ICMP) steigt die Anzahl der über UMTS/GPRS gesendeten und empfangenen Daten. Dies kann zu erhöhten Kosten führen.

Abbildung 5-5 Menübefehl "Netzwerk Extern" > "Erweiterte Einstellungen" > "Prüfen der Verbindung"

Prüfen der Verbindung

Bei "Ja" ist die Funktion eingeschaltet. Bei "Nein" ist die Funktion ausgeschaltet.

Zielhosts - Hostname

Wählen Sie bis zu vier Gegenstellen aus, die das SCALANCE M873-0 anpingen kann. Die Gegenstellen müssen ständig erreichbar sein und den Ping beantworten.

Hinweis

Vergewissern Sie sich, dass die ausgewählten Gegenstellen nicht gestört werden.

Intervall für Verbindungsprüfung (Minuten)

Legt das Intervall fest mit dem die Ping-Pakete der Verbindungsüberwachung vom SCALANCE M873-0 versendet werden. Die Angabe erfolgt in Minuten.

Anzahl der erlaubten Fehlversuche

Das SCALANCE M873-0 sendet gleichzeitig an alle festgelegten Gegenstellen (Zielhosts) Ping-Pakete. Antwortet mindestens eine Gegenstelle ist der Verbindungstest bestanden. Antwortet keine der Gegenstellen, handelt es sich um einen Fehlversuch. Nach Ablauf des eingestellten Intervalls wird der Vorgang wiederholt. Antwortet jetzt eine der Gegenstellen wird der Fehlversuchzähler zurückgesetzt. Ist die Anzahl der erlaubten Fehlversuche erreicht, wird die Aktion bei fehlerhafter Verbindung ausgelöst.

Aktion bei fehlerhafter Verbindung

Verbindung erneuern

Das SCALANCE M873-0 stellt erneut die Verbindung zum UMTS/GPRS her, falls die gesendeten Ping-Pakete nicht beantwortet wurden.

Neustart des M873-0

Das SCALANCE M873-0 führt einen Neustart durch, falls die gesendeten Ping-Pakete nicht beantwortet wurden.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Prüfen der Verbindung	**Nein (Ausgeschaltet)**
Hostname	**-**
Intervall für Verbindungsprüfung	**5 (Minuten)**
Anzahl der erlaubten Fehlversuche	**3 (Fehlversuche)**
Aktion bei fehlerhafter Verbindung	**Verbindung erneuern**

5.3 Hostname durch DynDNS

Dynamische Domain Name Server (DynDNS) ermöglichen es Applikationen im Internet unter einem Hostnamen (z. B. myHost.org) erreichbar zu sein, auch wenn diese Applikationen keine feste IP-Adresse haben und der Hostname nicht registriert ist. Wenn Sie das SCALANCE M873-0 bei einem DynDNS-Dienst anmelden, können Sie das SCALANCE M873-0 aus dem externen Netz auch unter einem Hostnamen erreichen, z. B. mySINAUT.dyndns.org.

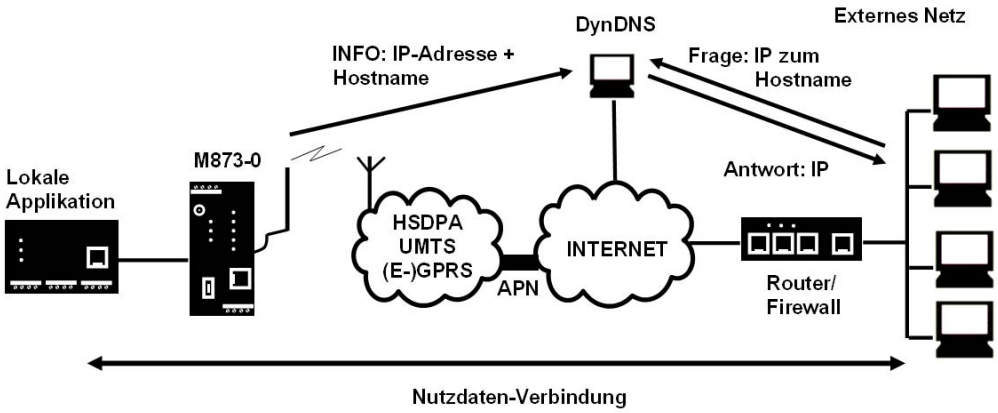


Abbildung 5-6 Dyn-DNS-Anbindung

Mehr Informationen zu DynDNS finden Sie im Glossar.

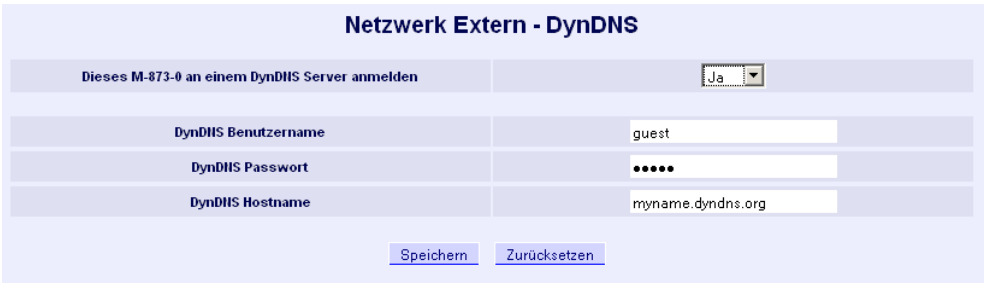


Abbildung 5-7 Menübefehl "Netzwerk Extern" > "Erweiterte Einstellungen" > "DynDNS"

Dieses M873-0 an einem DynDNS Server anmelden

Wählen Sie "Ja", wenn Sie einen DynDNS-Dienst verwenden wollen.

DynDNS-Anbieter

Das SCALANCE M873-0 ist kompatibel zu dyndns.org.

DynDNS Benutzername / Passwort

Geben Sie hier den Benutzernamen und das Passwort ein, dass Sie zur Nutzung des DynDNS-Service berechtigt. Ihr DynDNS-Anbieter teilt Ihnen diese Angaben mit.

DynDNS Hostname

Geben Sie hier den Hostnamen ein, den Sie für das SCALANCE M873-0 mit Ihrem DynDNS-Anbieter vereinbart haben, z. B. mySINAUT.dyndns.org.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Das M873-0 an einem DynDNS Server anmelden	**Nein** (ausgeschaltet)
DynDNS Benutzername	**guest**
DynDNS Passwort	**guest**
DynDNS Hostname	**myname.dyndns.org**

5.4 SRS – Siemens Remote Service

Bei aktiviertem Siemens Remote Service übermittelt das SCALANCE M873-0 seine vom EDGE/GPRS-Dienst zugewiesene externe IP-Adresse an einen einstellbaren Ziel-Server. Die Übertragung erfolgt über das gesicherte HTTPS-Protokoll.

Das Verfahren ist vergleichbar mit dem DynDNS-Dienst und erfordert einen entsprechenden Zugang auf der Server-Seite.

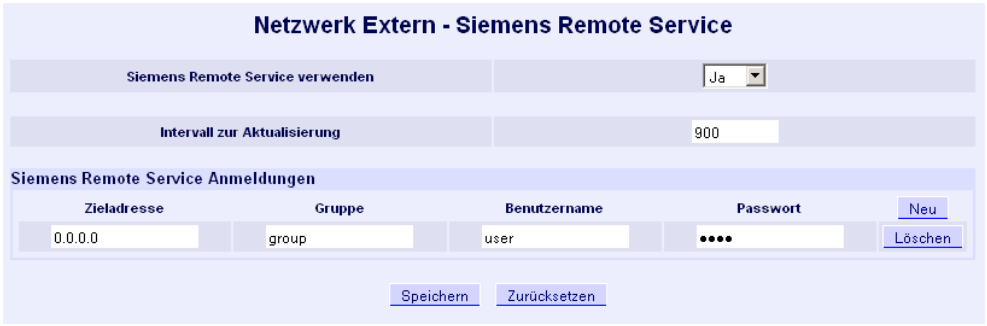


Abbildung 5-8 Menübefehl "Netzwerk Extern" > "Erweiterte Einstellungen" > "SRS"

Mit "Neu" fügen Sie weitere Ziel-Server hinzu. Mit "Löschen" entfernen Sie bestehende Einträge.

Siemens Remote Service verwenden

Wählen Sie "Ja", wenn Sie den Siemens Remote Service verwenden wollen.

Wenn Sie den Siemens Remote Service nicht verwenden wollen, dann wählen Sie "Nein".

Intervall zur Aktualisierung

Geben Sie das Intervall in Sekunden an, mit dem die zugewiesene IP-Adresse des SCALANCE M873-0 an den eingestellten Ziel-Server übertragen werden soll.

Siemens Remote Service Anmeldungen

Geben Sie hier die Zieladresse und die Zugangsdaten eines oder mehrer Ziel-Server an:

Zieladresse

Geben Sie die IP-Adresse des Ziel-Servers an.

Gruppe

Geben Sie den Gruppennamen ein.

Benutzername

Geben Sie den Benutzernamen für den Zugang am Ziel-Server ein.

Passwort

Geben Sie das Passwort für den Zugang am Ziel-Server ein.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Siemens Remote Service verwenden	**Nein** (ausgeschaltet)
Intervall zur Aktualisierung	**900 Sekunden**
Zieladresse	**0.0.0.0**
Gruppe	**group**
Benutzername	**user**
Passwort	**pass**

5.5 NAT - Network Address Translation

Listet die festgelegten Regeln für NAT (Network Address Translation) auf und ermöglicht, Regeln zu setzen oder zu löschen.

Das Gerät kann bei ausgehenden Datenpaketen die angegebenen Absender-IP-Adressen aus seinem internen Netzwerk auf seine eigene externe Adresse umschreiben, eine Technik, die als NAT (Network Address Translation) bezeichnet wird.

Diese Methode wird benutzt, wenn die internen Adressen extern nicht geroutet werden könne oder sollen, z. B. weil ein privater Adressbereich wie 192.168.x.x benutzt wird oder weil die interne Netzstruktur verborgen werden soll.

Dieses Verfahren wird auch IP-Masquerading genannt.

NAT im externen Netz verwenden

Wählen Sie "Ja", um die NAT Funktion zum externen Netz zu aktivieren.

NAT für folgende Netze verwenden

Geben Sie die Netzwerke an, für die NAT genutzt werden soll. Die Angabe erfolgt als Adressbereich. Verwenden Sie die CIDR-Syntax.

Mit "Neu" fügen Sie ein Netzwerk hinzu und mit "Löschen" entfernen Sie ein Netzwerk.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

NAT im externen Netz verwenden	**Nein** (ausgeschaltet)
Netzwerk	**0.0.0.0/0**

Sicherheitsfunktionen 6

6.1 Paketfilter

Das SCALANCE M873-0 beinhaltet eine Stateful Inspection Firewall.

Stateful Inspection Firewall ist eine Methode zur Paketfilterung. Paketfilter lassen IP-Pakete nur dann passieren, wenn dies zuvor durch Firewall-Regeln definiert wurde. In der Firewall-Regel wird folgendes festgelegt,

- welches Protokoll (TCP, UDP, ICMP) passieren darf,
- die erlaubte Quelle der IP-Pakete (Von IP / Von Port)
- das erlaubte Ziel der IP-Pakete (Nach IP / Nach Port)

Gleichfalls wird hier festgelegt, wie mit IP-Paketen verfahren wird, die nicht passieren dürfen, z. B. werden sie verworfen oder zurückgewiesen.

Bei einem einfachen Paketfilter müssen immer zwei Firewall-Regeln für eine Verbindung angelegt werden:

- Eine Regel für die Anfragerichtung von der Quelle zum Ziel und
- eine zweite Regel für die Antwortrichtung vom Ziel zur Quelle.

Anders ist das beim SCALANCE M873-0 mit Stateful Inspection Firewall. Hier wird nur für die Anfragerichtung von der Quelle zum Ziel eine Firewall-Regel angelegt. Die Firewall-Regel für die Antwortrichtung vom Ziel zur Quelle ergibt sich aus der Analyse der zuvor gesendeten Daten. Die Firewall-Regel für die Antworten wird nach Erhalt der Antworten bzw. nach Ablauf einer kurzen Zeitspanne wieder geschlossen. Antworten dürfen also nur passieren, wenn es zuvor eine Anfrage gab. So kann die Antwortregel nicht für unbefugte Zugriffe benutzt werden. Besondere Verfahren ermöglichen zudem, dass auch UDP- und ICMP-Daten passieren können, obwohl diese Daten zuvor nicht angefordert wurden.

Abbildung 6-1 Menübefehl "Sicherheit" > "Paketfilter"

Firewall Regeln Eingehend

Mit den "Firewall-Regeln Eingehend" wird festgelegt, wie mit IP-Paketen zu verfahren ist, die über UMTS/GPRS aus externen Netzen (z. B. Internet) empfangen werden. Quelle ist der Absender dieser IP-Pakete. Ziel sind die lokalen Applikationen am SCALANCE M873-0.

Entsprechend der Werkseinstellung ist zunächst keine eingehende Firewall-Regel gesetzt, d.h. es dürfen keine IP-Pakete passieren.

Neu

Fügt eine weitere Firewall-Regel hinzu, die Sie dann ausfüllen können.

Löschen

Entfernt angelegte Firewall-Regeln wieder.

Protokoll

Wählen Sie das Protokoll aus, für das diese Regel gelten soll. Zur Auswahl stehen "TCP", "UDP", "ICMP". Wenn Sie "Alle" wählen, gilt die Regel für alle drei Protokolle.

Von IP

Tragen Sie die IP-Adresse der externen Gegenstelle ein, die IP-Pakete zum lokalen Netz senden darf. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Gegenstelle an. 0.0.0.0/0 bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Glossar

Von Port

Tragen Sie den Port ein, von dem die externe Gegenstelle IP-Pakete senden darf (wird nur ausgewertet bei den Protokollen TCP und UDP).

Nach IP

Tragen Sie ein, an welche IP-Adresse im lokalen Netz IP-Pakete gesendet werden dürfen. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Applikation im lokalen Netz an. 0.0.0.0/0 bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Glossar.

Nach Port

Tragen Sie den Port ein, an den die externe Gegenstelle IP-Pakete senden darf.

Aktion

Wählen Sie aus, wie mit eintreffenden IP-Paketen zu verfahren ist:

"Erlauben" – Die Datenpakete dürfen passieren,

"Zurückweisen" – Die Datenpakete werden abgewiesen, der Absender erhält eine entsprechende Meldung,

"Verwerfen" – Die Datenpakete werden ohne Rückmeldung an den Absender verworfen.

Firewall Regeln Ausgehend

Mit den "Firewall-Regeln Ausgehend" wird festgelegt, wie mit IP-Paketen zu verfahren ist, die vom lokalen Netz empfangen werden. Quelle ist eine Applikation im lokalen Netz. Ziel ist eine externe Gegenstelle z. B. im Internet oder in einem privaten Netz.

Entsprechend der Werkseinstellung ist zunächst keine ausgehende Firewall-Regel gesetzt, d.h. es dürfen keine IP-Pakete passieren.

Neu

Fügt eine weitere Firewall-Regel hinzu, die Sie dann ausfüllen können.

Protokoll

Wählen Sie das Protokoll aus, für das diese Regel gelten soll. Zur Auswahl stehen "TCP", "UDP", "ICMP". Wenn Sie "Alle" wählen, gilt die Regel für alle drei Protokolle.

Hinweis: Wird für Protokoll "Alle" gewählt, ist eine Portzuordnung nicht wirksam.

Von IP

Tragen Sie die IP-Adresse der lokalen Applikation ein, die IP-Pakete zum externen Netz senden darf. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der lokalen Applikation an. 0.0.0.0/0 bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Glossar.

Von Port

Tragen Sie den Port ein, von dem die lokale Applikation IP-Pakete senden darf. Geben Sie dazu die Portnummer an.

(wird nur ausgewertet bei den Protokollen TCP und UDP)

Nach IP

Tragen Sie ein, an welche IP-Adresse im externen Netz IP-Pakete gesendet werden darf. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Applikation im Netz an. 0.0.0.0/0 bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Glossar.

Nach Port

Tragen Sie ein, an welchen Port die externe Gegenstelle IP-Pakete senden darf. Geben Sie dazu die Portnummer an.

(wird nur ausgewertet bei den Protokollen TCP und UDP)

Aktion

Wählen Sie aus, wie mit abgehenden IP-Paketen zu verfahren ist:

"Erlauben" – Die Datenpakete dürfen passieren,

"Zurückweisen" – Die Datenpakete werden abgewiesen, der Absender erhält eine entsprechende Meldung,

"Verwerfen" – Die Datenpakete werden ohne Rückmeldung an den Absender verworfen.

Firewall Regeln Ein-/ Ausgehend

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel das Ereignis protokolliert werden soll ("Log" ="Ja") oder nicht ("Log" ="Nein"; werkseitige Voreinstellung).

Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.4 geschrieben.

Log-Einträge für unbekannte Verbindungsversuche

Damit werden alle Verbindungsversuche protokolliert, die nicht von den festgelegten Regeln erfasst werden.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Firewall eingehend

Firewall Regeln Eingehend	**- (Alles gesperrt)**
Protokoll	**Alle**
Von IP	**0.0.0.0/0**
Von Port	**Any**
Nach IP	**0.0.0.0/0**
Nach Port	**Any**
Aktion	**Erlauben**
Log	**Nein (Ausgeschaltet)**
Log-Einträge für unbekannte Verbindungsversuche	**Nein (Ausgeschaltet)**

Firewall ausgehend

Firewall Regeln Ausgehend	**- (Alles gesperrt)**
Protokoll	**Alle**
Von IP	**0.0.0.0/0**
Von Port	**Any**
Nach IP	**0.0.0.0/0**
Nach Port	**Any**
Aktion	**Erlauben**
Log	**Nein (Ausgeschaltet)**
Log-Einträge für unbekannte Verbindungsversuche	**Nein (Ausgeschaltet)**

6.2 Port-Weiterleitung

Ist eine Regel zur Port-Weiterleitung erstellt, dann werden Datenpakete, die aus dem externen Netz auf einem festgelegten IP-Port des SCALANCE M873-0 eintreffen, weitergeleitet. Die eingehenden Datenpakete werden dann an eine festgelegte IP-Adresse und Port-Nummer im lokalen Netz weitergeleitet. Die Port-Weiterleitung kann für TCP oder UDP konfiguriert werden.

Bei Port-Weiterleitung geschieht folgendes: Der Header eingehender Datenpakete aus dem externen Netz, die an die externe IP-Adresse des SCALANCE M873-0 sowie an einen bestimmten Port gerichtet sind, werden so umgeschrieben, dass sie ins interne Netz an einen bestimmten Rechner und zu einem bestimmten Port dieses Rechners weitergeleitet werden.
D. h. die IP-Adresse und Port-Nummer im Header eingehender Datenpakete werden geändert.

Dieses Verfahren wird auch Destination-NAT oder Port Forwarding genannt.

Hinweis

Damit ankommende Datenpakete an die festgelegte IP-Adresse im lokalen Netz weitergeleitet werden können, muss für diese IP-Adresse eine entsprechende eingehende Firewall-Regel im Paketfilter eingerichtet werden. Siehe Kapitel 6.1.

Abbildung 6-2 Menübefehl "Sicherheit" > "Port-Weiterleitung"

Neu

Fügt eine neue Weiterleitungs-Regel hinzu, die Sie dann ausfüllen können.

Löschen

Entfernt angelegte Weiterleitungs-Regeln wieder.

Protokoll

Geben Sie hier das Protokoll (TCP oder UDP) an, auf das sich die Regel beziehen soll.

Eintreffend auf Port

Geben Sie hier die Portnummer (z. B. 80) an, auf dem die Datenpakete aus dem externen Netz eintreffen, die weitergeleitet werden sollen.

Weiterleiten an IP

Geben Sie hier die IP-Adresse im lokalen Netz an, an den die eintreffenden Datenpakete weitergeleitet werden sollen.

Weiterleiten an Port

Geben Sie hier die Portnummer (z. B. 80) zur IP-Adresse im lokalen Netz an, an den die eintreffenden Datenpakete weitergeleitet werden sollen.

Log

Für jede einzelne Port-Weiterleitungs-Regel können Sie festlegen, ob bei Greifen der Regel das Ereignis protokolliert werden soll (Log = Ja) oder nicht (Log = Nein; Werkseinstellung).

Das Protokoll wird in das Firewall-Logbuch geschrieben, siehe Kapitel 6.4.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Regeln zur Weiterleitung	**-**
Protokoll	**Alle**
Eintreffend auf Port	**80**
Weiterleiten an IP	**127.0.0.1**
Weiterleiten an Port	**80**
Log	**Nein (Ausgeschaltet)**

6.3 Erweiterte Sicherheitsfunktionen

Die erweiterten Sicherheitsfunktionen dienen dazu das SCALANCE M873-0 und die lokalen Applikationen gegen Angriffe zu schützen. Zum Schutz wird angenommen, dass nur eine bestimmte Anzahl von Verbindungen oder empfangener Ping-Pakete im normalen Betrieb zulässig und erwünscht sind, und das bei einer plötzlichen Häufung ein Angriff stattfindet.

Abbildung 6-3 Menübefehl "Sicherheit" > "Erweitert"

Maximale Zahl …

Die Einträge ...

- Maximale Zahl gleichzeitiger Verbindungen
- Maximale Zahl neuer eingehender TCP-Verbindungen pro Sekunde
- Maximale Zahl neuer ausgehender TCP-Verbindungen pro Sekunde
- Maximale Zahl neuer eingehender Ping-Pakete pro Sekunde
- Maximale Zahl neuer ausgehender Ping-Pakete pro Sekunde

... legen Obergrenzen fest. Die Voreinstellungen (siehe Abbildung) sind so gewählt, dass sie bei normalem praktischem Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte entsprechend ändern.

ICMP von extern zum M873-0

Mit dieser Option können Sie das Verhalten beim Empfang von ICMP-Paketen beeinflussen, die aus dem externen Netz in Richtung des SCALANCE M873-0 gesendet werden. Sie haben folgende Möglichkeiten:

- "Verwerfen": Alle ICMP-Pakete zum SCALANCE M873-0 werden verworfen.
- "Ping Erlauben": Nur Ping-Pakete (ICMP Typ 8) zum SCALANCE M873-0 werden akzeptiert.
- "Erlauben": Alle Typen von ICMP-Pakete zum SCALANCE M873-0 werden akzeptiert.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Maximale Zahl gleichzeitiger Verbindungen	**4096**
Maximale Zahl neuer eingehender TCP-Verbindungen pro Sekunde	**25**
Maximale Zahl neuer ausgehender TCP-Verbindungen pro Sekunde	**75**
Maximale Zahl neuer eingehender Ping Pakete pro Sekunde	**3**
Maximale Zahl neuer ausgehender Ping Pakete pro Sekunde	**5**
ICMP von extern zum M873-0	**Verwerfen**

6.4 Firewall-Logbuch

Im Firewall-Logbuch wird eingetragen, wann einzelne Firewall-Regeln angewendet wurden. Dazu muss zu den verschiedenen Firewall-Funktionen die LOG-Funktion aktiviert werden.

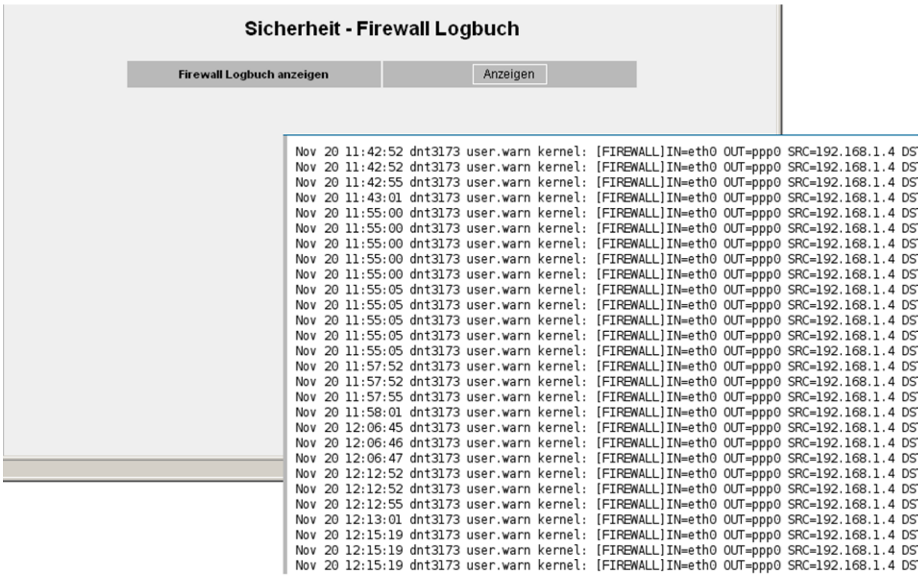


Abbildung 6-4 Sicherheit > Firewall Logbuch

Hinweis

Das Firewall-Logbuch geht bei einem Neustart verloren.

Fernzugänge 7

7.1 Fernzugang HTTPS

Der HTTPS-Fernzugang (= HyperText Transfer Protocol Secure) ermöglicht über HSDPA, UMTS, EGPRS, GPRS oder CSD einen gesicherten Zugriff aus einem externen Netz auf die Web-Oberfläche des SCALANCE M873-0.

Die Konfiguration des SCALANCE M873-0 über den HTTPS-Fernzugang erfolgt dann genauso wie die Konfiguration per Web-Browser über die lokale Schnittstelle (siehe Kapitel 3).

Abbildung 7-1 Menübefehl "Zugang" > "HTTPS"

HTTPS Fernzugang aktivieren

Ja

Der Zugriff auf die Web-Oberfläche des SCALANCE M873-0 per HTTPS aus dem externen Netz ist gestattet.

Nein

Der Zugriff per HTTPS ist nicht gestattet.

Port für HTTPS Fernzugang

Standard: 443 (Werkseinstellung)

Ein anderer Port kann festgelegt werden. Wenn jedoch ein anderer Port festgelegt wird, dann muss die externe Gegenstelle, die den Fernzugriff ausübt, bei der Adressenangabe hinter der IP-Adresse die Port-Nummer angeben.

Beispiel:
Ist dieses SCALANCE M873-0 über die Adresse 192.144.112.5 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 442 festgelegt, dann muss bei der externen Gegenstelle im Web-Browser angegeben werden:
https://192.144.112.5:442

Hinweis: Der Standard-Port für den HTTPS-Zugang bleibt neben dem neu gewählten Port offen.

Firewall-Regeln für den HTTPS-Fernzugang

Neu

Fügt eine neue Firewall-Regel für den HTTPS-Fernzugang hinzu, die dann auszufüllen ist.

Löschen

Entfernt eine angelegte Firewall-Regel für den HTTPS-Fernzugang wieder.

Von IP (extern)

Eingabefeld für die Adresse(n) des/der Rechner(s), dem/denen Fernzugang erlaubt ist. Bei den Angaben gibt es folgende Möglichkeiten:

IP-Adresse oder -Adressenbereich: 0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, wird die CIDR-Schreibweise verwendet.

Aktion

Auswahlfeld, mit dem festgelegt wird, wie bei Zugriffen auf den angegebenen HTTPS Port verfahren wird:

"Annehmen" bedeutet, die Datenpakete dürfen passieren.

"Zurückweisen" bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.

"Verwerfen" bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verworfen, so dass der Absender keine Information erhält über deren Verbleib.

Log

Für jede einzelne Firewall-Regel kann festgelegt werden, ob bei Greifen der Regel das Ereignis protokolliert werden soll ("Log" = "Ja") oder nicht ("Log" = "Nein"; werkseitige Voreinstellung).

Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.4 geschrieben.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

HTTPS Fernzugang aktivieren	**Nein (Ausgeschaltet)**
Port für HTTPS Fernzugang	**443**
Vorgabe für neue Regel:	
Von IP (extern)	**0.0.0.0/0**
Aktion	**Annehmen**
Log	**Nein (Ausgeschaltet)**

7.2 Fernzugang SSH

Der SSH-Fernzugang (= Secured SHell) ermöglicht über HSDPA, UMTS, EGPRS, GPRS oder CSD einen gesicherten Zugriff aus einem externen Netz auf das Dateisystem des SCALANCE M873-0.

Dazu muss mit einem SSH-fähigen Programm eine Verbindung von der externen Gegenstelle zum SCALANCE M873-0 aufgebaut werden.

Der SSH-Fernzugang sollte von Anwendern verwendet werden, die mit dem LINUX Dateisystem vertraut sind.

Werkseitig ist diese Option ausgeschaltet.

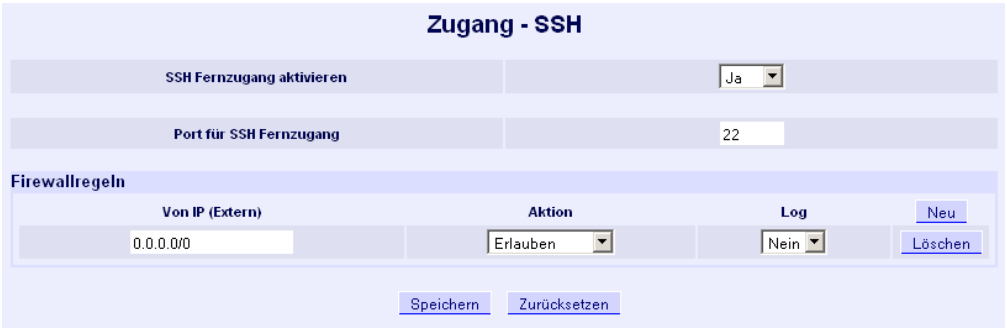


Abbildung 7-2 Menübefehl "Zugang" > "SSH"

Vorsicht

Über den SSH-Fernzugang ist es möglich, das Gerät so falsch zu konfigurieren, dass es zum Service eingeschickt werden muss.

SSH-Fernzugang aktivieren

Ja

Der Zugriff auf das Dateisystem des SCALANCE M873-0 per SSH aus dem externen Netz ist gestattet.

Nein

Der Zugriff per SSH ist nicht gestattet.

Port für SSH-Fernzugang

Standard: 22 (Werkseinstellung)

Ein anderer Port kann festlegt werden. Wenn jedoch ein anderer Port festgelegt wird, dann muss die externe Gegenstelle, die den Fernzugriff ausübt, bei der Adressenangabe vor der IP-Adresse die Port-Nummer angeben, die hier festgelegt ist. Der Standard-Port 22 für den SSH Zugang bleibt neben dem neu gewählten Port offen.

Beispiel:
Ist dieses SCALANCE M873-0 über die Adresse 192.144.112.5 aus dem externen Netz zu erreichen, und ist für den Fernzugang der Port 22222 festgelegt, dann muss bei der externen Gegenstelle im SSH-Client (z. B. PUTTY) diese Port-Nummer angegeben werden:

ssh -p 22222 192.144.112.5

Firewall-Regeln für den SSH-Fernzugang

Neu

Fügt eine neue Firewall-Regel für den SSH-Fernzugang hinzu, die dann auszufüllen ist.

Löschen

Entfernt eine angelegte Firewall-Regel für den SSH-Fernzugang wieder.

Von IP (extern)

Eingabefeld für die Adresse(n) des/der Rechner(s) , dem/denen Fernzugang erlaubt ist. Bei den Angaben haben Sie folgende Möglichkeiten:

IP-Adresse oder -Adressenbereich: 0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, wird die CIDR-Schreibweise benutzt.

Aktion

Auswahlfeld, wie bei Zugriffen auf den angegebenen SSH-Port verfahren wird:

"Annehmen" bedeutet, die Datenpakete dürfen passieren.

"Zurückweisen" bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.

"Verwerfen" bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verworfen, so dass der Absender keine Information erhält über deren Verbleib.

Log

Für jede einzelne Firewall-Regel kann festlegt werden, ob bei Greifen der Regel das Ereignis protokolliert werden soll ("Log" = "Ja") oder nicht ("Log" = "Nein"; werkseitige Voreinstellung).

Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.4 geschrieben.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

SSH Fernzugang aktivieren	**Nein (Ausgeschaltet)**
Port für SSH Fernzugang	**22**
Vorgabe für neue Regel:	
Von IP (extern)	**0.0.0.0/0**
Aktion	**Annehmen**
Log	**Nein (Ausgeschaltet)**

7.3 Fernzugang über Wählverbindung

Der Zugang CSD Einwahl ermöglicht den Zugriff auf die Web-Oberfläche des SCALANCE M873-0 über eine Daten-Wählverbindung (CSD = Circuit Switched Data). Dazu ist das SCALANCE M873-0 mit einem analogen Modem auf der Datenrufnummer oder mit einem GSM-Modem auf der Sprach- oder Datenrufnummer seiner SIM-Karte anzurufen.

Abbildung 7-3 Menübefehl "Zugang" > "CSD Einwahl"

Das SCALANCE M873-0 nimmt den Ruf an, wenn

- die Rufnummer des Telefonanschlusses von dem aus der Anruf getätigt wird, in der Liste der zugelassenen Nummern im SCALANCE M873-0 gespeichert ist und
- die Rufnummer vom Telefonnetz übertragen wird (CLIP Funktion)

Die Einwahl muss mit einem PPP-Client erfolgen, zum Beispiel über eine Windows DFÜ-Verbindung. Folgen Sie unter Windows dem "Assistenten für neue Verbindungen" und richten Sie als "Verbindung mit dem Netzwerk am Arbeitsplatz" eine "DFÜ-Verbindung" ein.

Hinweis: Diese Funktion ist nur verfügbar, wenn ein GSM-Netz verwendet wird. In UMTS-Netzen, kann diese Funktion nicht verwendet werden.

CSD Einwahl aktivieren

Ja

Der Zugriff auf die Web-Oberfläche des SCALANCE M873-0 per Daten-Wählverbindung ist gestattet.

Nein

Der Zugriff per Daten-Wählverbindung ist nicht gestattet.

PPP Benutzername / Passwort

Eingabefelder für Benutzernamen und Passwort, mit dem sich ein PPP-Client (z. B. Windows DFÜ-Verbindung) am SCALANCE M873-0 anmelden muss. Der gleiche Benutzername und das gleiche Passwort müssen vom PPP-Client verwendet werden.

Zugelassene Rufnummern

Eingabefeld für die Rufnummer des Telefonanschlusses, von dem aus die Daten-Wählverbindung aufgebaut wird. Der Telefonanschluss muss die Rufnummernübermittlung (CLIP – Calling Line Identification Presentation) unterstützen und die Funktion muss eingeschaltet sein.

Die im SCALANCE M873-0 eingetragene Rufnummer muss exakt mit der gemeldeten Rufnummer übereinstimmen und gegebenenfalls auch die Länderkennung und Vorwahl umfassen, z. B. +494012345678.

Wenn mehrere Rufnummern einer Nebenstellenanlage zugangsberechtigt sein sollen, kann das Zeichen „*“ als Joker verwenden werden, z.B. +49401234*. Alle Rufnummern die mit +49401234 beginnen werden dann akzeptiert.

Hinweis

Firewall-Regeln, die für den HTTPS- bzw. SSH-Zugang eingetragen sind, gelten auch für den CSD-Zugang. Als Quell-IP-Adresse („von IP“) für den CSD-Zugang ist 10.99.99.2 festgelegt.

Neu

Fügt eine neue zugelassene Rufnummer für den CSD-Fernzugang hinzu, die dann auszufüllen ist.

Löschen

Entfernt eine Rufnummer für den CSD-Fernzugang wieder.

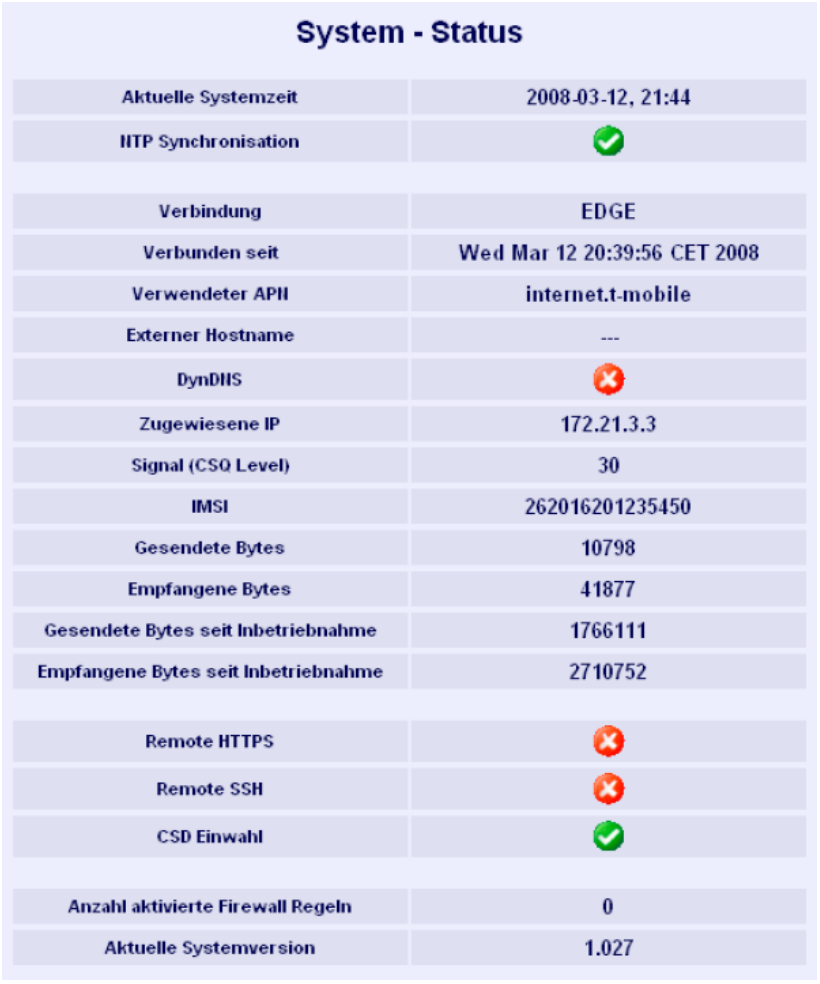
Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

CSD Einwahl aktivieren	**Nein (Ausgeschaltet)**
PPP Benutzername	**service**
PPP Passwort	**service**
Zugelassene Rufnummern	*****

Zustand, Logbuch und Diagnose 8

8.1 Anzeige Betriebszustand



System - Status

Aktuelle Systemzeit	2008-03-12, 21:44
NTP Synchronisation	✓
Verbindung	EDGE
Verbunden seit	Wed Mar 12 20:39:56 CET 2008
Verwendeter APN	internet.t-mobile
Externer Hostname	---
DynDNS	✗
Zugewiesene IP	172.21.3.3
Signal (CSQ Level)	30
IMSI	262016201235450
Gesendete Bytes	10798
Empfangene Bytes	41877
Gesendete Bytes seit Inbetriebnahme	1766111
Empfangene Bytes seit Inbetriebnahme	2710752
Remote HTTPS	✗
Remote SSH	✗
CSD Einwahl	✓
Anzahl aktivierte Firewall Regeln	0
Aktuelle Systemversion	1.027

Abbildung 8-1 Menübefehl "System" > "Status"

Hinweis
Mit der Funktion "Aktualisieren" des Web-Browsers können die angezeigten Werte auf den aktuellen Stand gebracht werden.

Aktuelle Systemzeit

Zeigt die aktuelle Systemzeit des SCALANCE M873-0 an, im Format:

Jahr – Monat – Tag, Stunden – Minuten

Verbindung

Zeigt an, welche Funkverbindung besteht:

- UMTS-Verbindung (IP-Verbindung über HSDPA, UMTS)
- GPRS/EDGE-Vebindung (IP-Verbindung über EGPRS oder GPRS)
- CSD-Verbindung (Service-Verbindung über CSD)

Hinweis

Es kann vorkommen, dass eine UMTS/GPRS-Verbindung und auch eine zugewiesene IP-Adresse angezeigt werden, die Verbindungsqualität aber dennoch nicht ausreicht, um Daten zu übertragen. Aus diesem Grund empfehlen wir, die aktive Verbindungsüberwachung (siehe Kapitel 5.2) zu nutzen.

Verbunden seit

Zeigt an, wie lange die aktuelle Verbindung zum UMTS/GPRS besteht.

Verwendeter APN

Zeigt den verwendeten APN (= Access Point Name) des UMTS/GPRS an.

Externer Hostname

Zeigt den Hostnamen (z. B. M873.mydns.org) des SCALANCE M873-0 an, wenn ein DynDNS-Dienst verwendet wird.

DynDNS

Zeigt an, ob ein DynDNS-Dienst aktiviert ist.

- Weißer Haken auf grünem Punkt: DynDNS-Dienst aktiviert.
- Weißes Kreuz auf rotem Punkt: DynDNS-Dienst nicht aktiviert

Zugewiesene IP-Adresse

Zeigt die IP-Adresse an, unter der das SCALANCE M873-0 im UMTS/GPRS zu erreichen ist. Diese IP-Adresse wird dem SCALANCE M873-0 vom UMTS/GPRS-Dienst zugewiesen.

Signal (CSQ Level)

Gibt die Stärke des GSM-Signals als CSQ-Wert an.

- CSQ < 6: Signalstärke schlecht
- CSQ= 6..10: Signalstärke mittel
- CSQ=11-18: Feldstärke gut
- CSQ > 18: Feldstärke sehr gut
- CSQ = 99: Keine Verbindung zum GSM-Netz

IMSI

Zeigt die Teilnehmerkennung an, die auf der verwendeten SIM-Karte gespeichert ist.

Anhand der IMSI (= International Mobile Subscriber Identity) erkennt der Mobilfunkbetreiber die Berechtigungen und vereinbarten Dienste der SIM-Karte.

IMEI

Zeigt die Seriennummer des SCALANCE M873-0 als GSM-Funkeinrichtung an. Die IMEI (= International Mobile Equipment Identity) wird weltweit eindeutig vergeben.

Gesendete Bytes / Empfangene Bytes

Zeigt die Anzahl der Bytes an, die während der bestehenden Verbindung zum UMTS/GPRS gesendet bzw. empfangen worden sind. Die Zähler werden bei Aufbau einer neuen Verbindung zurückgesetzt.

Hinweis

Diese Zahlen dienen nur als Anhaltspunkt für das Datenvolumen und können von der Abrechnung des Mobilfunkbetreibers deutlich abweichen.

Gesendete Bytes / Empfangene Bytes seit Inbetriebnahme

Zeigt die Anzahl der Bytes an, die seit dem letzten Laden der Werkseinstellung über UMTS/GPRS gesendet bzw. empfangen worden sind.

Die Zähler werden bei Laden der Werkseinstellung zurückgesetzt.

Remote HTTPS

Zeigt an, ob Zugriffe auf die Web-Oberfläche des SCALANCE M873-0 aus der Ferne über UMTS/GPRS erlaubt sind.

- Weißer Haken auf grünem Punkt: Der Zugriff ist erlaubt.
- Weißes Kreuz auf rotem Punkt: Der Zugriff ist nicht erlaubt.

Remote SSH

Zeigt an, ob Zugriffe auf die SSH-Konsole des SCALANCE M873-0 aus der Ferne über UMTS/GPRS erlaubt sind.

- Weißer Haken auf grünem Punkt: Der Zugriff ist erlaubt.
- Weißes Kreuz auf rotem Punkt: Der Zugriff ist nicht erlaubt.

CSD Einwahl

Zeigt an, ob CSD-Serviceanrufe aus der Ferne erlaubt sind.

- Weißer Haken auf grünem Punkt: CSD-Serviceanrufe sind möglich.
- Weißes Kreuz auf rotem Punkt: CSD-Serviceanrufe sind nicht möglich.

Anzahl aktivierter Firewall-Regeln

Zeigt an, wie viele Firewall-Regeln aktiviert sind.

Aktuelle Systemversion

Zeigt die Versionsnummer der Software des SCALANCE M873-0 an.

8.2 Logbuch

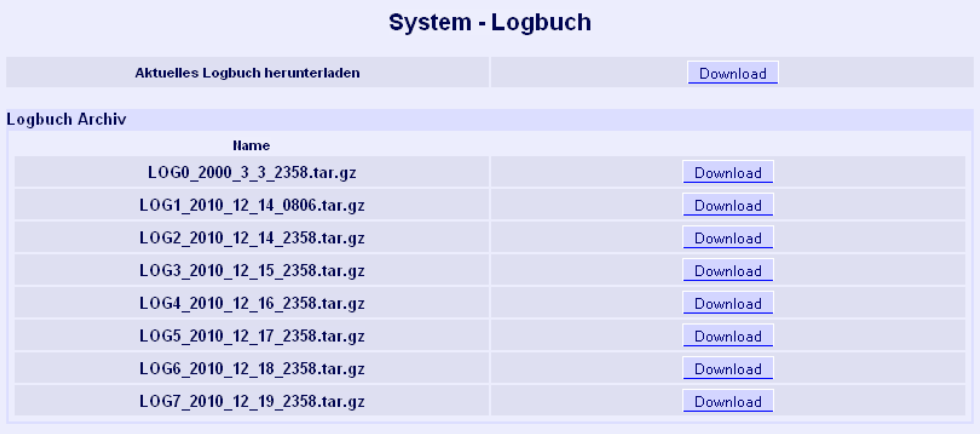


Abbildung 8-2 Menübefehl "System" > "Logbuch"

Logbuch

Im Logbuch werden wichtige Ereignisse im Betriebsablauf des SCALANCE M873-0 abgespeichert:

- Neustart
- Änderungen der Konfiguration
- Verbindungsaufbau
- Verbindungsunterbrechungen
- Signalstärke
- und Betriebsmeldungen

Das Logbuch wird bei Erreichen einer Dateigröße von 1 MByte, spätestens aber nach 24 Stunden, im Logbuch Archiv des SCALANCE M873-0 gespeichert.

Aktuelles Logbuch herunterladen

"Download" - das aktuelle Logbuch wird auf den Admin-PC geladen. Der Anwender kann das Verzeichnis auswählen, in dem die Datei gespeichert wird, und die Datei dort betrachten.

Logbuch Archiv

"Download" - Archivierte Logbuch-Dateien werden auf den Admin-PC geladen. Der Anwender kann das Verzeichnis auswählen, in dem die Dateien gespeichert werden, und die Dateien dort betrachten.

Beispiel:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
13.12.2007 11:04	3173XX	(null)	(null)	(null)	SERVICE_MASK=0	4	UH	41	CURRENT SYSTEM VERSION	1.014					
13.12.2007 19:46	3173XX	(null)	(null)	(null)	SERVICE_MASK=0	4	UH	41	CURRENT SYSTEM VERSION	1.014					
13.12.2007 19:46	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	APL	0	SYSTEM STARTING	Success					
13.12.2007 19:47	3173XX	CSQ=---	STAT=---	COPS=---	(null)	0	APL	5	CONNECTION ERROR	Missing or incorrect GSM parameter					
13.12.2007 20:03	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 20:19	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 20:36	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 20:52	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 21:09	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 21:25	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
14.12.2007 12:15	3173XX	(null)	(null)	(null)	SERVICE_MASK=0	4	UH	41	CURRENT SYSTEM VERSION	1.014					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	APL	0	SYSTEM STARTING	Success					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	0	APL	5	CONNECTION ERROR	Missing or incorrect GSM parameter					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	InternalIPs.InternalIP_0.IP:192.168.1.1					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	InternalIPs.InternalIP_0.NetMask:255.255.255.0					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	(null)	4	CH	9	CONFIGURATION FILE ACCESS	InternalIPs.InternalIP_1.IP:192.168.0.20					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	(null)	4	CH	9	CONFIGURATION FILE ACCESS	InternalIPs.InternalIP_1.NetMask:255.255.255.0					
14.12.2007 23:05	3173XX	(null)	(null)	(null)	SERVICE_MASK=0	4	UH	41	CURRENT SYSTEM VERSION	1.014					
14.12.2007 23:05	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	APL	0	SYSTEM STARTING	Success					
14.12.2007 23:05	3173XX	CSQ=---	STAT=---	COPS=---	(null)	0	APL	5	CONNECTION ERROR	Missing or incorrect GSM parameter					
14.12.2007 23:08	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:09	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:09	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	3	GPRS CONNECTION ESTABLISHED	GPRS connect					
14.12.2007 23:10	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	8	IP ASSIGNED	172.25.105.9					
14.12.2007 23:11	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:11	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	ICMPCheck.Enabled:true					
14.12.2007 23:11	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:11	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	ICMPCheck.Enabled:true					
14.12.2007 23:12	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:12	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	ICMPCheck.Enabled:true					
14.12.2007 23:13	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:13	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	NTP.Enabled:true					
14.12.2007 22:24	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:449	RXS:358	TX:1078	RX:358;
14.12.2007 22:40	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:449	RXS:358	TX:1078	RX:358;
14.12.2007 22:57	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:449	RXS:358	TX:1078	RX:358;
14.12.2007 23:13	3173XX	CSQ=10	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:449	RXS:358	TX:1078	RX:358;
14.12.2007 23:30	3173XX	CSQ=10	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:2737	RXS:3931	TX:3966	RX:3931;
14.12.2007 23:46	3173XX	CSQ=10	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:3089	RXS:4469	TX:3718	RX:4469;

Abbildung 8-3 Beispiel - Logbuch

Einträge im Logbuch

Spalte A:

Zeitstempel

Spalte B:

Produktnummer 3173xx

Spalte C:

Signalqualität (CSQ-Wert)

Spalte D:

GSM Einbuchstatus

STAT = --- = Funktion noch nicht gestartet

STAT = 1 = Im Heimatnetz eingebucht

STAT = 2 = Nicht eingebucht; Netzsuche

STAT = 3 = Einbuchen abgelehnt

STAT = 5 = Eingebucht in Fremdnetz (Roaming)

Spalte E:

Angabe der Identifikation des Netzbetreibers mit dem 3-stelligen Ländercode (MCC) und dem 2-3-stelligen Netzbetreibercode (MNC).

Beispiel: 26201 (262 = Ländercode / 01 = Netzbetreibercode)

Spalte F:

Kodierter Betriebsstatus (für Kundendienst)

Spalte G:

Kategorie der Logbuch-Meldung (für Kundendienst)

Spalte H:

Interne Quelle der Logbuch-Meldung (für Kundendienst)

Spalte I:

Interne Meldungsnummer (für Kundendienst)

Spalte J:

Logbuch-Meldung im Klartext

Spalten K-P:

Zusatzinformationen zur Klartextmeldung, wie zum Beispiel:

- Cell-ID (Identifikationsnummer der aktiven GSM-Zelle)
- Softwareversion
- TXS, RXS (Übertragene IP-Pakete der aktuellen Verbindung)
- TX, RX (Übertragene IP-Pakete seit letztem Werksneustart)

8.3 Remote Logging

Das SCALANCE M873-0 kann das System Logbuch einmal am Tag per FTP (= File Transfer Protocol) an einen FTP Server übertragen.

Übertragen wird das aktuelle System Logbuch sowie die System Log-Dateien im Archiv. Nach erfolgreicher Übertragung werden die übertragenen System Logbücher im SCALANCE M873-0 gelöscht.

Schlägt die Übertragung fehl, versucht das SCALANCE M873-0 nach 24 Stunden erneut die Daten zu übertragen.

Abbildung 8-4 Menübefehl "Wartung" > "Remote Logging"

Remote Logging (FTP Upload) verwenden

Mit "Ja" wird die Funktion eingeschaltet.

Uhrzeit

Legt die Uhrzeit fest, zu der die Logbücher übertragen werden sollen.

FTP Server

Legt die Adresse des FTP Servers fest, zu dem die Log-Dateien übertragen werden sollen. Die Adresse kann als Hostname (z. B. ftp.server.de) oder als IP-Adresse angegeben werden.

Benutzername

Legt den Benutzernamen für die Anmeldung am FTP Server fest.

Passwort

Legt das Passwort für die Anmeldung am FTP Server fest.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Remote Logging (FTP Upload) verwenden	**Nein (Ausgeschaltet)**
Uhrzeit	**00:00**
FTP Server	**NONE**
Benutzername	**guest**
Passwort	**guest**

8.4 Snapshot

Diese Funktion dient für Support-Zwecke.

Der Service-Snapshot speichert wichtige Logdateien und aktuelle Geräte-Einstellungen, die zur Fehlerdiagnose relevant sein könnten in einer Datei.

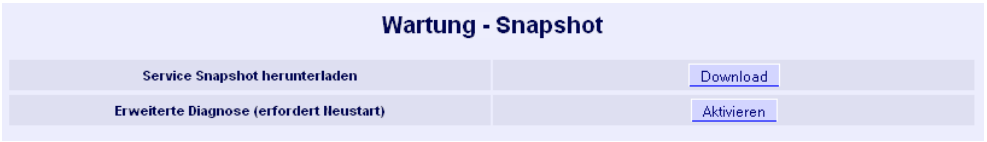


Abbildung 8-5 Menübefehl "Wartung" > "Snapshot"

Wenn Sie sich bei einem Problem mit dem SCALANCE M873-0 an unsere Hotline wenden, wird diese möglicherweise um die Snapshot-Datei bitten.

Hinweis

Diese Datei enthält die Zugangsparameter zum UMTS/GPRS sowie die Adressen der Gegenstelle. Nicht enthalten sind Benutzername und Passwort für den Zugang zum SCALANCE M873-0.

Service Snapshot herunterladen

Klicken Sie auf Download. Sie können auswählen, an welche Stelle auf dem Admin-PC die Snapshot-Datei gespeichert werden soll.

Der Dateiname der Snapshot-Datei setzt sich folgendermaßen zusammen:

<hostname>_Snapshot_<Date&TimeCode>.tgz

z. B.: m873_Snapshot_200711252237.tgz

Erweiterte Diagnose

Aktivieren Sie die "erweiterte Diagnose" nur nach Aufforderung durch die Hotline. Im Betrieb werden bei erweiterter Diagnose häufiger Informationen in die Diagnose-Logbücher geschrieben. Zusätzliche Informationen werden auch gespeichert. Dies hilft bei einer gezielten Problemanalyse.

Hinweis

Durch die häufigen Schreibzugriffe bei aktivierter erweiterter Diagnose auf den nicht-flüchtigen Speicher des SCALANCE M873-0 kann sich dessen Lebensdauer verringern.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Erweiterte Diagnose	**Aus (Aktivieren)**

8.5 Hardware Informationen

Anzeige wichtiger Informationen zur Hardware Identifikation.

Wartung - Hardware Info

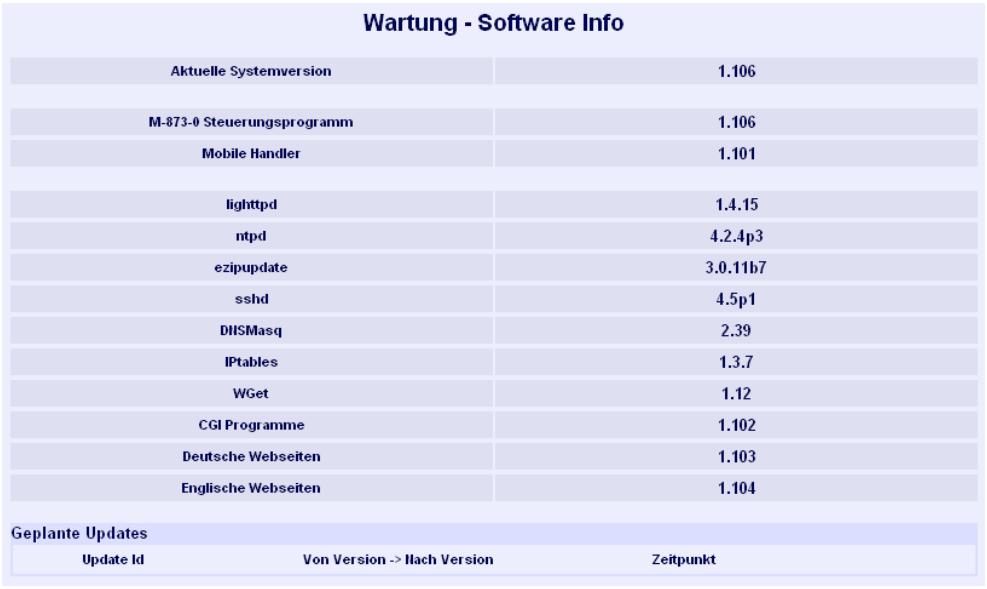
CPU	ARM9
CPU Taktfrequenz	200MHz
Anwendungsspeicher	64MB
Systemlaufzeit	Mon Dec 20 11:43:13 UTC 2010
MAC Adresse	00:25:69:61:F7:CC
IMEI	---
Produktname	SCALANCE M-873-0
Seriennummer	10038875
Hardware Version	02-20

Abbildung 8-6 Menübefehl "Wartung" > "HW Info"

8.6 Software Informationen

Anzeige wichtiger Informationen zur Software Identifikation.

Zusätzlich werden geplante Updates angezeigt. Siehe auch Kapitel 9.3.



Wartung - Software Info

Aktuelle Systemversion	1.106
M-873-0 Steuerungsprogramm	1.106
Mobile Handler	1.101
lighttpd	1.4.15
ntpd	4.2.4p3
ezipupdate	3.0.11b7
sshd	4.5p1
DNSMasq	2.39
IPtables	1.3.7
WGet	1.12
CGI Programme	1.102
Deutsche Webseiten	1.103
Englische Webseiten	1.104

Geplante Updates

Update Id	Von Version -> Nach Version	Zeitpunkt

Abbildung 8-7 Menübefehl "Wartung" > "SW Info"

Weitere Funktionen 9

9.1 Service Center

Das SCALANCE M873-0 nutzt auch den Short Message Service (SMS) von GSM. Sie können ein spezielles SMS Center festlegen.

Abbildung 9-1 Menübefehl "SMS" > "Service Center"

SMS Service Center Rufnummer

Damit die SMS-Funktion sicher funktioniert, tragen Sie hier die Rufnummer des Service Center (SMSC) ein. Ohne Eintrag an dieser Stelle wird das Standard-SMSC Ihres Netzbetreibers verwendet.

9.2 Alarm-SMS

Das SCALANCE M873-0 kann kurze Alarm-Meldungen über SMS (= Short Message Service) des GSM-Netzes versenden. Der Versand einer Alarm-SMS kann durch zwei Ereignisse ausgelöst werden:

- Ereignis 1: Schalteingang wird aktiv
- Ereignis 2: Keine UMTS/GPRS-Verbindung

Zu jedem Ereignis können Sie eine eigene Rufnummer angeben, an welche die Alarm-Meldung geschickt wird. Den Text der Alarm-Meldung können Sie frei festlegen. Folgende Zeichen stehen zur Verfügung:

a b c d e f g h I j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9 , ! ?

Abbildung 9-2 Menübefehl "SMS" > "Alarm SMS"

Alarm SMS Ereignis 1: Schalteingang

Ereignis 1: der Schalteingang wechselt von inaktiv auf aktiv, d.h. am Schalteingang wird eine ausreichende Schaltspannung angelegt. Diese Funktion kann zum Beispiel genutzt werden, um außerhalb der IP-Datenverbindungen Alarm-Meldungen der lokalen Applikationen zu versenden.

Alarm SMS Ereignis 2: Keine UMTS/ GPRS-Verbindung

Ereignis 2: Die UMTS/GPRS-Verbindung kommt trotz mehrfacher Versuche nicht zustande. Das SCALANCE M873-0 versendet daraufhin eine Alarm-Meldung.

Einstellungen

Aktivieren

Bei "Ja" wird beim Ereignis die Alarm-Meldung abgesendet, bei "Nein" nicht.

Rufnummer

Tragen Sie hier die Rufnummer des Endgeräts ein, an das die Alarm-Meldung über SMS gesendet werden soll. Das Endgerät muss SMS-Empfang über GSM oder Festnetz unterstützen.

Text

Tragen Sie hier den Text ein, der als Alarm-Meldung verschickt wird.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

SMS Service Center Rufnummer	-
Alarm SMS Ereignis 1: Keine GPRS-Verbindung	**Nein** (ausgeschaltet)
Rufnummer	-
Text	-

9.3 SMS-Versand aus dem lokalen Netzwerk

Mit der Funktion SMS-Versand können Anwendungen, die an der lokalen Schnittstelle des SCALANCE M873-0 angeschlossen sind, SMS über das GSM-Netz verschicken.

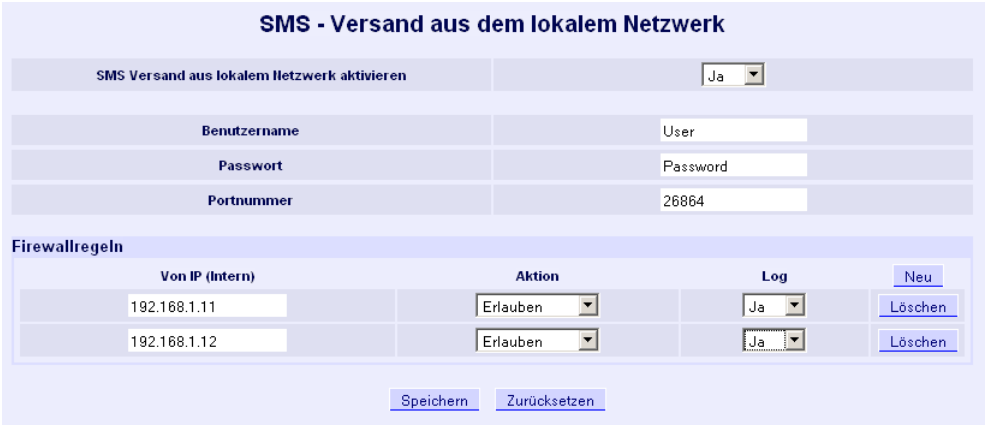


Abbildung 9-3 Menübefehl "SMS" > "SMS over IP"

Zum Versand einer SMS muss die Anwendung an der lokalen Schnittstelle eine TCP/IP-Verbindung zum SCALANCE M873-0 aufbauen.

Über diese TCP/IP-Verbindung sendet die Anwendung den Text der SMS an das SCALANCE M873-0, das den Text in eine SMS verpackt und verschickt.

Telegrammformat für die SMS-Nachricht

Der Text muss in einem Telegramm über die TCP/IP-Verbindung an das SCALANCE M873-0 übermittelt werden, das folgendem Format entspricht:

Benutzername#Passwort#CommandCode#Seq-Num;Rufnummer;Nachricht:

Beispiel:
```
benutzer#passwort#105#01;0049043465789;mein SMS Text:
```

Benutzername

Geben Sie den Benutzernamen zur Prüfung der Sendeberechtigung einer SMS ein. Maximal 10 Zeichen.

Passwort

Geben Sie das zugehörige Passwort zum Benutzernamen ein. Maximal 10 Zeichen.

CommandCode

Kommando zum SMS-Versand aus dem lokalen Netz. Dieser Wert ist fest 105 und darf nicht verändert werden.

Seq-Num

Die Sequenznummer dient der Zuordnung mehrerer Anfragen gleichzeitig. Die Funktion wird derzeit nicht unterstützt.

Die Sequenznummer besteht aus 2 nummerischen Zeichen von 01 bis 99.

Rufnummer

Rufnummer des SMS-Empfängers mit maximal 40 Zeichen. Internationale Nummern (+49...) sind zulässig.

Nachricht

SMS-Text mit maximal 160 Zeichen

Folgende verbotene Zeichen dürfen im SMS-Text nicht vorkommen:

Trennungszeichen der ersten Kommandoebene

; Trennungszeichen der zweiten Kommandoebene

: Bestimmt das Ende der Nachricht

SMS-Versand aus dem lokalen Netzwerk aktivieren

Wählen Sie "Ja", um SMS aus dem lokalen Netzwerk versenden zu können.

Wählen Sie "Nein", wenn Sie keine SMS aus dem lokalen Netzwerk versenden wollen.

Benutzername

Benutzername, der im Telegramm enthalten sein muss, bevor der Text per SMS versendet wird (siehe oben: "Telegrammformat"). Maximal 10 Zeichen.

Passwort

Passwort, das im Telegramm enthalten sein muss, bevor der Text per SMS versendet wird (siehe oben: "Telegrammformat"). Maximal 10 Zeichen.

Portnummer

TCP/IP-Port, auf dem das SCALANCE M873-0 die TCP/IP-Verbindung zum SMS-Versand entgegen nimmt.

Firewall-Regeln

Damit die TCP/IP-Verbindung zum SMS-Versand aufgebaut werden kann, muss am SCALANCE M873-0 eine Firewall-Regel eingerichtet werden.

Mit "Neu" fügen Sie Quellen ("Von IP") für die TCP/IP-Verbindung zum SMS-Versand hinzu. Mit "Löschen" entfernen Sie Verbindungen.

Von IP (Intern)

Tragen Sie die IP-Adresse der externen Gegenstelle ein, die IP-Pakete zum lokalen Netz senden darf. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Gegenstelle an. 0.0.0.0/0 bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise, siehe Glossar.

Aktionen

Die Klappliste unter Aktionen bezieht sich jeweils auf die TCP/IP-Verbindung der IP-Adresse, die links neben der Klappliste steht. Zur Auswahl stehen drei Möglichkeiten:

- "Erlauben"
  Gibt die TCP/IP-Verbindung für den SMS-Versand frei.
- "Zurückweisen"
  Die Datenpakete werden zurückgewiesen und der Absender erhält eine Information über die Zurückweisung.
- "Verwerfen"
  Die Datenpakete dürfen nicht passieren und werden verworfen. Der Absender erhält keine Information über deren Verbleib.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob das Ereignis protokolliert werden soll (Log = Ja) oder ob die werkseitige Voreinstellung beibehalten wird (Log = Nein).

Das Protokoll wird in das Firewall-Logbuch geschrieben, siehe Kapitel 6.4.

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

Benutzername	User
Passwort	Password
Portnummer	26864
Firewall-Regeln	Nicht aktiv
Von IP	0.0.0.0/0
Aktionen	Erlauben
Log	Nein

Werkseinstellung

Werkseitig hat das SCALANCE M873-0 folgende Einstellungen:

SMS Service Center Rufnummer	-
Alarm SMS Ereignis 1: Schalteingang	Nein (Ausgeschaltet)
Rufnummer	-
Text	-
Alarm SMS Ereignis 2: Keine IP-GPRS-Verbindung	Nein (Ausgeschaltet)
Rufnummer	-
Text	-

9.4 Software-Update

Mit der Update-Funktion können Sie eine neue Betriebssoftware in das SCALANCE M873-0 laden und diese Software aktivieren.

Bei einem sofortigen Update wird die neue Software entpackt. Dieser Vorgang kann einige Minuten dauern. Danach beginnt der eigentliche Update-Vorgang, der durch ein Lauflicht der LEDs angezeigt wird.

Die Einstellungen des SCALANCE M873-0 werden übernommen, sofern diese Einstellungen in der neuen Software-Version noch so wirken, wie vor dem Update.

Abbildung 9-4 Menübefehl "Wartung" > "Update"

Zeitpunkt festlegen

Nein

Update sofort - Die neue Betriebssoftware wird aktiviert, direkt nachdem Sie die Software geladen und auf die Schaltfläche "Absenden" geklickt haben.

Ja

Update zeitgesteuert - Die neue Betriebssoftware wird aktiviert, an dem festgelegten Update Zeitpunkt. Dazu muss die Software zuvor geladen werden.

Update Zeitpunkt festlegen

Wenn Sie das Update zeitgesteuert durchführen lassen wollen, geben Sie den Zeitpunkt an, an dem die neue Betriebssoftware aktiviert werden soll.

Geben Sie Jahr – Monat – Tag – Stunde – Minute an.

Update Datei auswählen

Wählen Sie mit "Durchsuchen" die Datei mit der neuen Firmware aus, z. B.:

M873_v1.024-v1.027.tgz

Laden Sie die Firmware mit "Öffnen" in das Gerät.

Absenden

Mit "Absenden" wird die Firmware entweder sofort oder zum vorgegeben Zeitpunkt aktiviert.

Technische Daten 10

Schnittstellen	Applikations-Schnittstelle	10/100 Base-T (RJ45 plug) Ethernet IEEE802 10/100 Mbit/s
	Service Schnittstelle	USB-A (reserviert für spätere Anwendungen)
Sicherheits-Funktionen		Stateful Inspection Firewall Anti-Spoofing Port Weiterleitung
Weitere Funktionen		DNS Cache, DHCP Server, NTP, Remote Logging, Verbindungsüberwachung, Alarm-SMS
Management		Web-basierte Administrations-Oberfläche,ssh-Konsole
Funkverbindung	Frequenzbänder	UMTS/HSDPA: Triple band, 850 / 1900 / 2100 MHz GSM/GPRS/EDGE: Quad band, 850 / 900 / 1800 / 1900 MHz
	HSDPA	3.6 Mbps, UL 384 kbps UE CAT. [1-6], 11, 12 supported Compressed mode (CM) supported according to 3GPP TS25.212
	UMTS	PS data rate - 384 kbps DL / 384 kbps UL CS data rate - 64 kbps DL / 64 kbps UL
	EDGE (EGPRS)	EDGE Multislot class 12 / EDGE Multislot class 12 Multislot Class 10 Mobile Station Class B PBCCH support Downlink coding schemes - CS 1-4, MCS 1-9 Uplink coding schemes - CS 1-4, MCS 1-9
	GPRS	Multislot Class 10 Full PBCCH support Mobile Station Class B Coding Scheme 1 – 4
	CSD / MTC	V.110, RLP, non-transparent 9.6 kbps
	SMS (TX)	Punkt zu Punkt, MO (abgehend)
	Antennen-anschluss	Impedanz nominal: 50 Ohm, Buchse: SMA
Umwelt-bedingungen	Temperatur-bereich	Betrieb: -20 °C bis +60 °C Lagerung: -40 °C bis +70 °C
	Luftfeuchte	0-95 %, nicht kondensierend
Gehäuse	Ausführung	Hutschienengehäuse
	Material	Kunststoff

	Schutzklasse	IP20
	Abmessungen	114 mm x 45 mm x 99 mm
	Gewicht	ca. 280g
Konformität	CE	Ja
	R&TTE (GSM)	Konform zur Richtlinie 99/05/EC Angewandte Norm: EN 301 511 v.9.0.2
	GSM/EGPRS-Modul	Konform zu GCF, PTCRB
	EMV/ESD	Konform zur Richtlinie 2004/108/EG Angewandte Normen: EN 55022:2006 Klasse A, EN 55024:1998 + A1:2001 + A2:2003, EN 61000-6-2:2001
	Elektrische Sicherheit	Konform zur Richtlinie 2006/95/EG Angewandte Norm: EN 60950-1:11-2006
	Umwelt	Das Gerät entspricht den europäischen Richtlinien ROHS und WEEE.
Spannungs-versorgung	Eingangs-spannung	12 - 60 V DC (24 V DC nominal)
	Leistungs-aufnahme	Typisch 4,4 W bei 12 V Typisch 4,0 W bei 24 V Typisch 5,5 W bei 60 V
	Stromaufnahme	450 mA bei 12 V und 100 mA bei 60 V Iburst = 1,26 A

Verwendete Standards und Zulassungen 11

Hinweis

Die für das Gerät gültigen Zulassungen finden Sie auf dem Gerät aufgedruckt.

11.1 EG-Konformitätserklärung

Kennzeichnung

CE

Angewendete europäische Richtlinien

Bei bestimmungsgemäßer Verwendung entspricht das Produkt den folgenden europäischen Richtlinien:

- Richtlinie 1999/5/EC (R&TTE) des Europäischen Parlaments und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikations-Endeinrichtungen und die gegenseitige Anerkennung ihrer Konformität,
- Richtlinie 2006/95/EG (Niederspannungsrichtlinie) des Europäischen Parlaments und des Rates vom 12. Dezember 2006 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen,
- Richtlinie 2004/108/EC (EMV) des Europäischen Parlaments und des Rates vom 15. Dezember 2004 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit und zur Aufhebung der Richtlinie 89/336/EWG,
- Richtlinie 94/9/EC (ATEX) des Europäischen Parlaments und des Rates vom 23. März 1994 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten für Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen.

Die EG-Konformitätserklärung zu diesem Produkt finden Sie im Internet unter folgender Adresse:

Link zur Konformitätserklärung:
(http://support.automation.siemens.com/WW/view/de/10805878) → Register "Beitragsliste"

Filter: → Beitragsliste → Beitragstyp "Zertifikate" → Zertifikatart: "Konformitätserklärung" → Suchbegriff(e): <Name der Baugruppe>

Richtlinie 1999/5/EC (R&TTE)

Angewandte Normen

- EN301 511: v.9.0.2
- 3GPP TS 51.010-1: v. 5.10.0

Klassifizierung

Telekommunikationsendgerät

Funkgerät

Geräteklasse 1

Richtlinie 2006/95/EC (Niederspannungsrichtlinie)

Angewandte Normen

- EN 60950:2006

Richtlinie 2004/108/EC (EMV)

Angewandte Normen

- EN55022: 2006 Grenzwertklasse A
- EN55024:1998 + A1 : 2001 + A2 : 2003
- EN61000-6-2: 2001

Vorsicht

Das SCALANCE M873-0 ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

Richtlinie 94/9/EC (ATEX)

Zusatzkennzeichnung (Muster)

6NH9741-1AA00, SCALANCE M873-0 GSM/GPRS Router


II 3 G Ex nA IIC T4 Ta= -20°C to 60°C

Angewandte Normen

- EN60079-15 (Schutztyp “n”)

Klassifizierung

Gruppe II, Kategorie 3, Gas Atmosphäre, nichtfunkendes Betriebsmittel, Temperatur Klasse T4, Umgebungstemperaturbereich: -20°C … +60°C

Besondere Nutzungsbedingungen:

1. Das SCALANCE M873-0 muss in einer Schutzumhüllung installiert werden, die einen Schutz gegen das Eindringen von Fremdkörpern und Feuchtigkeit gemäß IP54 bietet; die Schutzumhüllung muss die Anforderungen der EN60079-0 erfüllen und darf nur durch ein Werkzeug zu öffnen sein.

2. Der USB (X1) Anschluss darf nicht verwendet werden.

3. Die Installation des SCALANCE M873-0 muss einen externen Schutz gegen transiente Überspannungen auf der Versorgung bereitstellen, so dass die Spannung an den Versorgungsanschlüssen des SCALANCE M873-0 eine Spannung von 42 V nicht überschreitet.

4. Sofern die Antenne außerhalb der Schutzumhüllung montiert wird, muss die Antenne so montiert und angeschlossen werden, das die IP54 Schutzklasse der Schutzumhüllung erhalten bleibt und sie die Anforderungen gemäß EN60079-0 weiterhin einhält.

11.2 Konformität mit FM, UL und CSA

FM Zertifizierung

Kennzeichnung (Muster)

CLI, DIV2, GP. A,B,C,D T4 Ta= -20°C to 60°C
CLI, Zone 2 IIC, T4 Ta= -20°C to 60°C

Angewandte Normen

- Factory Mutual Approval Standard Class Number 3611

Klassifizierung

Klasse I, Division 2, Gruppe A, B, C, D, 135°C maximale Oberflächentemperatur, Umgebungstemperaturbereich: -20°C … +60°C

Klasse I, Zone 2, Gruppe IIC, 135°C maximale Oberflächentemperatur, Umgebungstemperaturbereich: -20°C … +60°C

Die Zertifikate zur FM Zulassung finden Sie unter:

http://support.automation.siemens.com/WW/view/de/35029750

Filter: → Beitragsliste → Beitragstyp "Zertifikate" → Explosionsschutz

UL/CSA Zertifizierung

Kennzeichnung

Angewandte Normen

- UL 60950, 1st edition
- CSA C22.2 No.60950

11.3 Konformität mit FCC

Kennzeichnung

SCALANCE M873-0
FCC ID: LYHM873-0
contains MC75 FCC ID: QIPMC75

Angewandte Normen

- FCC Part 15
- FCC Part 15.19
- FCC Part 15.21

Vorgeschriebene Benutzerhinweise

FCC Part 15

Das Gerät entspricht den Grenzwerten für digitale Geräte der Klasse A, gemäß den FCC Rules Part 15.

Diese Grenzwerte sind so festgelegt, dass bei ihrer Einhaltung angemessener Schutz gegen schädliche und störende Interferenzen gewährleistet ist, wenn das betreffende Gerät im Wohnbereich installiert ist. Dieses Gerät erzeugt und benutzt Hochfrequenzen und kann diese ausstrahlen.

Wenn dieses Gerät nicht in Übereinstimmung mit den Instruktionen installiert und benutzt wird, kann es störende Interferenzen für den Funkverkehr bewirken. Es kann jedoch nicht garantiert werden, dass es bei bestimmten Installationen, auch wenn diese in Übereinstimmung mit den Instruktionen vorgenommen werden, keine störenden Interferenzen geben kann. Falls dieses Gerät störende Interferenzen beim Radio- oder Fernsehempfang bewirkt, was durch Ein- und Ausschalten des Gerätes ermittelt werden kann, empfehlen wird dem Benutzer, folgende Gegenmaßnahmen zu ergreifen.

- Ändern Sie die Ausrichtung der Empfangsantenne oder installieren Sie diese an anderer Stelle.
- Vergrößern Sie den Abstand zwischen dem SCALANCE M873-0 und dem Radio- oder Fernsehempfänger.
- Schließen Sie das Gerät an eine Netzsteckdose an, die sich in einem anderen Stromkreis befindet als die, an der der Empfänger angeschlossen ist.
- Wenden Sie sich an einen Fachhändler / Installateur oder an einen kompetenten Fachmann für TV und Radioempfang und fragen Sie ihn.

FCC Part 15.19

Dieses Gerät entspricht den Bestimmungen in Part 15 der FCC Rules. Sein Betrieb unterliegt folgenden Bedingungen:

1. Dieses Gerät bewirkt möglicherweise keine schädlichen oder störenden Interferenzen, und

2. dieses Gerät muss empfangene Interferenzen hinnehmen können, auch solche, die ein unerwünschtes Betriebsverhalten bewirken könnten.

FCC Part 15.21

Modifikationen am Gerät, denen dieser Hersteller nicht ausdrücklich zugestimmt hat, können dazu führen, dass der Benutzer nicht mehr befugt ist, das Gerät zu betreiben.

Das SCALANCE M873-0 darf nur mit einer Antenne aus dem Zubehörsortiment des SCALANCE M873-0 betrieben werden.

Ausschließlich Fachpersonal darf das SCALANCE M873-0 und dessen Antenne installieren und warten. Bei Arbeiten an der Antenne oder bei Arbeiten näher als unten angegeben muss der Sender ausgeschaltet sein.

Verwendete FCC ID: QIRMC75 (GSM-Modul)

Dieses Gerät beinhaltet GSM, GPRS Class 12 und EGPRS Class 10-Funktionen im 900 und 1800 MHz Band, die auf den Territorien der USA nicht zu benutzen sind.

Dieses Gerät kann für mobile und fest installierte Anwendungen verwendet werden. Die mit diesem Gerät benutzen internen / externen Antennen müssen mindestens 20 cm von Personen entfernt sein und sie dürfen nicht so platziert oder betrieben werden, dass sie in Verbund mit einer anderen Antenne oder einem anderen Sender arbeiten.

Benutzer und Installateure müssen Installationshinweise für die Antenne und die Bedingungen für den Betrieb der Sendeanlage erhalten, die einzuhalten sind, um der zulässigen HF-Exposition zu genügen. Antennen für das benutzte OEM-Modul dürfen einen Gewinn von 8.4dBi (GSM 1900) und 2.9dBi (GSM 850) bei Betriebskonfiguration für mobile und fest installierte Anwendungen nicht überschreiten. Das Gerät ist zugelassen als Modul zum Einsatz in anderen Geräten.

Glossar

Admin-PC

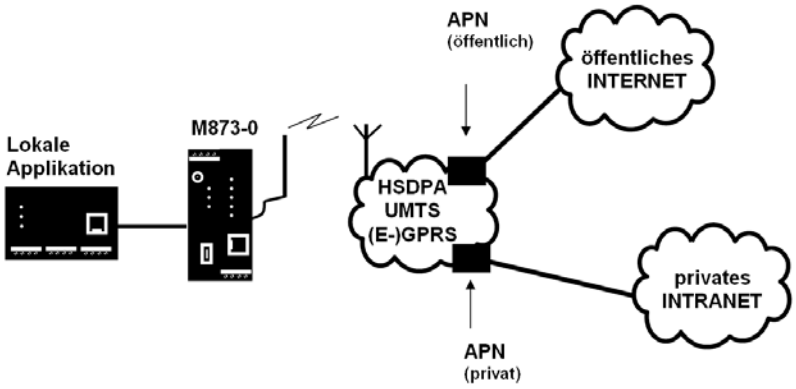
Rechner mit Web-Browser (z. B. MS Internet Explorer ab Version 7 oder Mozilla Firefox ab Version2) angeschlossen an das lokale Netz oder das externe Netz, mit dem die Konfiguration des SCALANCE M873-0 durchgeführt wird. Der Web-Browser muss HTTPS unterstützen. Für die Gerätekonfiguration über SSH wird auf dem Admin-PC ein SSH-Client, z. B, putty benötigt.

AES

Advanced Encryption Standard.
Das NIST (National Institute of Standards and Technology) entwickelt in Zusammenarbeit mit Industrie-Unternehmen seit Jahren den AES-Verschlüsselungsstandard. Diese → symmetrische Verschlüsselung soll den bisherigen DES-Standard ablösen. Der AES-Standard spezifiziert drei verschiedene Schlüsselgrößen mit 128, 192 und 256 Bit. 1997 hatte die NIST die Initiative zu AES gestartet und ihre Bedingungen für den Algorithmus bekannt gegeben. Von den vorgeschlagenen Verschlüsselungsalgorithmen hat die NIST fünf Algorithmen in die engere Wahl gezogen; und zwar die Algorithmen MARS, RC6, Rijndael, Serpent und Twofish. Im Oktober 2000 hat man sich für Rijndael als Verschlüsselungsalgorithmus entschieden.

APN (Access Point Name)

(Zugriffspunktname). Netzübergreifende Verbindungen, z. B. vom GPRS-Netz ins Internet, werden im GPRS-Netz über sogenannte APNs hergestellt.



Ein Endgerät, das eine Verbindung über das GPRS-Netz aufbauen will, gibt durch Angabe des APN an, mit welchem Netz es verbunden werden will: Internet oder privates Firmennetz, das über Standleitung angeschlossen ist.
Der APN bezeichnet den Übergabepunkt zum anderen Netz. Er wird dem Benutzer vom Netzbetreiber mitgeteilt.

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung werden Daten mit einem Schlüssel verschlüsselt und mit einem zweiten Schlüssel wieder entschlüsselt. Beide Schlüssel eignen sich zum Ver- und Entschlüsseln. Einer der Schlüssel wird von seinem Eigentümer geheim gehalten (Privater Schlüssel/Private Key), der andere wird der Öffentlichkeit (Öffentlicher Schlüssel/Public Key), d. h. möglichen Kommunikationspartnern, gegeben.
Eine mit dem öffentlichen Schlüssel verschlüsselte Nachricht kann nur von dem Empfänger entschlüsselt und gelesen werden, der den zugehörigen privaten Schlüssel hat. Eine mit dem privaten Schlüssel verschlüsselte Nachricht kann von jedem Empfänger entschlüsselt werden, der den zugehörigen öffentlichen Schlüssel hat. Die Verschlüsselung mit dem privaten Schlüssel zeigt, dass die Nachricht tatsächlich vom Eigentümer des zugehörigen öffentlichen Schlüssels stammt. Daher spricht man auch von digitaler Signatur, Unterschrift. Asymmetrische Verschlüsselungsverfahren wie RSA sind jedoch langsam und anfällig für bestimmte Angriffe, weshalb sie oft mit einem symmetrischen Verfahren kombiniert werden (→ symmetrische Verschlüsselung). Andererseits sind Konzepte möglich, die die aufwändige Administrierbarkeit von symmetrischen Schlüsseln vermeiden.

CIDR

Classless Inter-Domain Routing
IP-Netzmasken und CIDR sind Notationen, die mehrere IP-Adressen zu einem Adressraum zusammenfassen. Dabei wird ein Bereich von aufeinander folgenden Adressen als ein Netzwerk behandelt.
Das CIDR-Verfahren reduziert die z. B. in Routern gespeicherten Routing-Tabellen durch einen Postfix in der IP-Adresse. Mit diesem Postfix können ein Netz und die darunter liegenden Netze zusammengefasst bezeichnet werden. Die Methode ist in RFC 1518 beschrieben.
Um dem SCALANCE M873-0 einen Bereich von IP-Adressen anzugeben z. B. bei der Konfiguration der Firewall, kann es erforderlich sein, den Adressraum in der CIDR-Schreibweise anzugeben. Die nachfolgende Tabelle zeigt links die IP-Netzmaske, ganz rechts die entsprechende CIDR-Schreibweise.

IP-Netzmaske	binär				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

Beispiel: 192.168.1.0 / 255.255.255.0 entspricht im CIDR: 192.168.1.0/24

Client / Server

In einer Client-Server-Umgebung ist ein Server ein Programm oder Rechner, das/der vom Client-Programm oder Client-Rechner Anfragen entgegennimmt und beantwortet.
Bei Datenkommunikation bezeichnet man auch den Rechner als Client, der eine Verbindung zu einem Server (oder Host) herstellt. D.h. der Client ist der anrufende Rechner, der Server (oder Host) der angerufene.

CSD 9600

CSD (9600) steht für Circuit Switched Data oder Daten-Wählverbindung. Dabei wird eine Verbindung zwischen zwei Teilnehmern (Endpunkten der Verbindung) aufgebaut, ähnlich wie bei einem Telefonat im öffentlichen Fernsprechnetz. Teilnehmer 1 wählt die Rufnummer von Teilnehmer 2. Das Netz signalisiert Teilnehmer 2 den Anruf, Teilnehmer 2 nimmt den Ruf an und das Netz baut die Verbindung auf, bis einer der Teilnehmer die Verbindung wieder beendet.
Im GSM-Netz wird dieser Dienst CSD genannt und erlaubt die Datenübertragung mit 9600 bit/s oder 14400 bit/s, wobei die Übertragung gesichert oder ungesichert stattfindet. Möglich sind Verbindungen GSM Modem zu GSM Modem, Analog Modem zu GSM und ISDN-Modem zu GSM-Modem.

CSQ / RSSI

Der CSQ-Wert ist ein im GSM-Standard festgelegter Wert zur Angabe der Signalqualität. CSQ-Werte korrespondieren zur Empfangsfeldstärke RSSI (= Received Signal Strength Indication):

CSQ	RSSI
< 6	< -101 dBm
6…10	-101…-93 dBm
11…18	-91…-77 dBm
> 18	> 75 dBm
99	nicht eingebucht

Datagramm

Beim Übertragungsprotokoll TCP/IP werden Daten in Form von Datenpaketen, den sog. IP-Datagrammen, versendet. Ein IP-Datagramm hat folgenden Aufbau:

1. IP-Header
2. TCP-/UDP-Header
3. Daten (Payload)

Der IP-Header enthält:

- die IP-Adresse des Absenders (source IP-address)
- die IP-Adresse des Empfängers (destination IP-address)
- die Protokollnummer des Protokolls der nächst höheren Protokollschicht (nach dem OSI-Schichtenmodell)
- die IP-Header Prüfsumme (Checksum) zur Überprüfung der Integrität des Headers beim Empfang.

Der TCP-/UDP-Header enthält folgende Informationen:

- Port des Absenders (source port)
- Port des Empfängers (destination port)
- eine Prüfsumme über den TCP-Header und ein paar Informationen aus dem IP-Header (u. a. Quell- und Ziel-IP-Adresse)

DES / 3DES

Der von IBM stammende und von der NSA überprüfte symmetrische Verschlüsselungsalgorithmus (→ symmetrische Verschlüsselung)
DES wurde 1977 vom amerikanischen National Bureau of Standards, dem Vorgänger des heutigen National Institute of Standards and Technology (NIST), als Standard für amerikanische Regierungsinstitutionen festgelegt. Das es sich hierbei um den ersten standardisierten Verschlüsslungsalgorithmus überhaupt handelte, setzte er sich auch schnell in der Industrie und somit außerhalb Amerikas durch.
DES arbeitet mit einer Schlüssellänge von 56Bit, die heute aufgrund der seit 1977 gestiegenen Rechenleistung der Computer als nicht mehr sicher gilt.
3DES ist eine Variante von DES. Es arbeitet mit 3 mal größeren Schlüsseln, die also 168 Bit lang sind. Sie gilt heute noch als sicher und ist unter anderem auch Teil des IPsec-Standards.

DHCP

Dynamic Host Configuration Protocol (DHCP) übernimmt die automatische dynamische Zuweisung von IP-Adressen und weiteren Parametern in einem Netzwerk. Das Dynamic Host Configuration Protocol verwendet UDP. Es wurde definiert im RFC 2131 und bekam die UDP-Ports 67 und 68 zugewiesen. DHCP arbeitet im Client – Server Verfahren, wobei der Client vom Server die IP-Adressen zugewiesen bekommt.

DNS

Die Adressierung in IP-Netzen erfolgt grundsätzlich über IP-Adressen. Bevorzugt wird im Allgemeinen aber die Adressierung in Form einer Domain-Adresse angegeben (d. h. in der Form www.abc.xyz.de). Erfolgt die Adressierung über die Domain-Adresse, sendet der Absender zunächst die Domain-Adresse an einen Domain Name Server (DNS) und erhält die dazugehörige IP-Adresse zurück. Erst dann adressiert der Absender seine Daten an diese IP-Adresse.

DynDNS-Anbieter

Auch Dynamic DNS-Anbieter. Jeder Rechner, der mit dem Internet verbunden ist, hat eine IP-Adresse (IP = Internet Protocol). Eine IP-Adresse besteht aus 4 maximal dreistelligen Nummern, jeweils durch einen Punkt getrennt. Ist der Rechner über die Telefonleitung per Modem, per ISDN oder auch per ADSL online, wird ihm vom Internet Service Provider dynamisch eine IP-Adresse zugeordnet, d. h. die Adresse wechselt von Sitzung zu Sitzung. Auch wenn der Rechner (z. B. bei einer Flatrate) über 24 Stunden ununterbrochen online ist, wird die IP-Adresse zwischendurch gewechselt.
Soll ein lokaler Rechner über das Internet erreichbar sein, muss seine Adresse der externen Gegenstelle bekannt sein. Nur so kann diese die Verbindung zum lokalen Rechner aufbauen. Wenn die Adresse des lokalen Rechners aber ständig wechselt, ist das nicht möglich. Es sei denn, der Betreiber des lokalen Rechners hat einen Account bei einem DynamicDNS-Anbieter (DNS = Domain Name Server).
Dann kann er bei diesem einen Hostnamen festlegen, unter dem der Rechner künftig erreichbar sein soll, z. B.: www.xyz.abc.de. Zudem stellt der DynamicDNS-Anbieter ein kleines Programm zur Verfügung, das auf dem betreffenden Rechner installiert und ausgeführt werden muss. Bei jeder Internet-Sitzung des lokalen Rechners teilt dieses Tool dem DynamicDNS-Anbieter mit, welche IP-Adresse der Rechner zurzeit hat. Dessen Domain Name Server registriert die aktuelle Zuordnung Hostname - IP-Adresse und teilt diese anderen Domain Name Servern im Internet mit.
Wenn jetzt ein externer Rechner eine Verbindung herstellen will zum lokalen Rechner, der beim DynamicDNS-Anbieter registriert ist, benutzt der externe Rechner den Hostnamen des lokalen Rechners als Adresse. Dadurch wird eine Verbindung hergestellt zum zuständigen DNS (Domain Name Server), um dort die IP-Adresse nachzuschlagen, die diesem Hostnamen zurzeit zugeordnet ist. Die IP-Adresse wird zurück übertragen zum externen Rechner und jetzt von diesem als Zieladresse benutzt. Diese führt jetzt genau zum gewünschten lokalen Rechner.
Allen Internetadressen liegt prinzipiell dieses Verfahren zu Grunde: Zunächst wird eine Verbindung zum DNS hergestellt, um die diesem Hostnamen zugeteilte IP-Adresse zu ermitteln. Ist das geschehen, wird mit dieser „nachgeschlagenen“ IP-Adresse die Verbindung zur gewünschten Gegenstelle, eine beliebige Internetpräsenz aufgebaut.

EDGE

EDGE (= Enhanced Data Rates for GSM Evolution) bezeichnet eine Technik, bei der die verfügbaren Datenraten in GSM-Mobilfunknetzen durch Einführung eines zusätzlichen Modulationsverfahrens erhöht werden. Mit EDGE werden GPRS zu EGPRS (Enhanced GPRS) und HSCSD zu ECSD erweitert.

EGPRS EGPRS steht für "Enhanced General Packet Radio Service " und beschreibt einen auf GPRS beruhenden paketorientierten Datendienst, der durch EDGE-Technologie beschleunigt ist.

Externe Gegenstellen Externe Gegenstellen sind Netzwerkkomponenten im externen Netz, z. B. Web-Server im Internet, Router im Intranet, ein zentraler Firmenserver oder ein Admin-PC.

Externes Netz Externes Netzwerk mit dem das SCALANCE M873-0 über HSDPA, UMTS, EGPRS oder GPRS verbunden ist. Externe Netze sind das Internet oder ein privates Intranet.

GPRS GPRS ist die Abkürzung von "General Packet Radio Service" und ein Datenübertragungssystem von GSM2+ Mobilfunksystemen. GPRS-Systeme nutzen die Basisstationen der GSM-Netze für die Funktechnik und eine eigene Infrastruktur zur Vernetzung und zur Kopplung an andere IP-Netze, wie zum Beispiel dem Internet. Daten werden dabei paket-orientiert vermittelt, wobei das Internet Protokoll (IP) verwendet wird. GPRS stellt Datenraten von bis zu 115,2 KBit/s zur Verfügung.

GSM GSM (= Global System for Mobile Communication) ist ein weltweit verbreiteter Standard für digitale Mobilfunknetze. GSM unterstützt außer dem Sprachdienst zur Telefonie, verschiedene Datendienste, wie Fax, SMS, CSD und GPRS. Abhängig von gesetzlichen Bestimmungen in den verschiedenen Ländern, werden die Frequenzbänder 900 MHz, 1800 MHz oder 850 MHz und 1900 MHz verwendet.

HTTPS HTTPS (=HyperText Transfer Protocol Secure) ist eine Variante des bekannten HTTP, wie es von jedem Web-Browser zur Navigation und zum Datenaustausch im Internet verwendet wird.
Bei HTTPS ist dem ursprünglichen Protokoll eine zusätzliche Komponente zum Datenschutz hinzugefügt. Während bei HTTP Daten ungeschützt in Klartext übertragen werden, werden bei HTTPS Daten erst nach einer Austausch von Sicherheitszertifikaten verschlüsselt übertragen.

IP-Adresse

Jeder Host oder Router im Internet / Intranet hat eine eindeutige IP-Adresse (IP = Internet Protocol). Die IP-Adresse ist 32 Bit (= 4 Byte) lang und wird geschrieben als 4 Zahlen (jeweils im Bereich 0 bis 255), die durch einen Punkt voneinander getrennt sind.
Eine IP-Adresse besteht aus 2 Teilen: der Netzwerk-Adresse und der Host-Adresse.
Alle Hosts eines Netzes haben dieselbe Netzwerk-Adresse, aber unterschiedliche Host-Adressen. Je nach Größe des jeweiligen Netzes - man unterscheidet Netze der Kategorien Class A, B und C - sind die beiden Adressanteile unterschiedlich groß:

	1. Byte	2. Byte	3. Byte	4 Byte
Class A	Netz-Adr.	Host-Adr.		
Class B	Netz-Adr.		Host-Adr.	
Class C	Netz-Adr.			Host-Adr.

Ob eine IP-Adresse ein Gerät in einem Netz der Kategorie Class A, B oder C bezeichnet, ist am ersten Byte der IP-Adresse erkennbar. Folgendes ist festgelegt:

	Wert des 1. Byte	Bytes für die Netz-Adresse	Bytes für die Host-Adresse
Class A	1-126	1	3
Class B	128-191	2	2
Class C	192-223	3	1

Rein rechnerisch kann es nur maximal 126 Class A Netze auf der Welt geben, jedes dieser Netze kann maximal 256 x 256 x 256 Hosts umfassen (3 Bytes Adressraum). Class B Netze können 64 x 256 mal vorkommen und können jeweils bis zu 65.536 Hosts enthalten (2 Bytes Adressraum: 256 x 256). Class C Netze können 32 x 256 x 256 mal vorkommen und können jeweils bis zu 256 Hosts enthalten (1 Byte Adressraum).

IP-Paket

Siehe Datagramm

IPsec

IP security (IPsec) ist ein Standard, der es ermöglicht, bei IP-Datagrammen die Authentizität des Absenders, die Vertraulichkeit und die Integrität der Daten durch Verschlüsselung zu wahren. Die Bestandteile von IPSec sind der Authentication Header (AH), die Encapsulating-Security-Payload (ESP), die Security Association (SA), der Security-Parameter-Index (SPI) und der Internet Key Exchange (IKE).
Zu Beginn der Kommunikation klären die an der Kommunikation beteiligten Rechner das benutzte Verfahren und dessen Implikationen wie z. B. Transport Mode oder Tunnel Mode.
Im Transport Mode wird in jedes IP-Datagramm zwischen IP-Header und TCP- bzw. UDP-Header ein IPSec-Header eingesetzt. Da dadurch der IP-Header unverändert bleibt, ist dieser Modus nur für eine Host- zu-Host-Verbindung geeignet.
Im Tunnel Mode wird dem gesamten IP-Datagramm ein IPSec-Header und ein neuer IP-Header vorangestellt. D. h. das ursprüngliche Datagramm wird insgesamt verschlüsselt in der Payload des neuen Datagramms untergebracht.
Der Tunnel Mode findet beim VPN Anwendung: Die Geräte an den Tunnelenden sorgen für die Ver- bzw. Entschlüsselung der Datagramme, auf der Tunnelstrecke, d. h. auf dem Übertragungsweg über ein öffentliches Netz bleiben die eigentlichen Datagramme vollständig geschützt.

Lokale Applikation

Lokale Applikationen sind Netzwerkkomponenten im lokalen Netz, zum Beispiel einen programmierbare Steuerung, eine Maschine mit Ethernet-Schnittstelle zur Fernüberwachung, ein Notebook bzw. PC oder der Admin-PC.

Lokales Netz

Netzwerk, angeschlossen an der lokalen Schnittstelle des SCALANCE M873-0. Das lokale Netz enthält mindestens eine lokale Applikation.

Lokale Schnittstelle

Schnittstelle des SCALANCE M873-0 zum Anschluss des lokalen Netzes. Die Schnittstelle ist am Gerät mit 10/100-Base-T gekennzeichnet. Es handelt sich um eine Ethernet-Schnittstelle mit 110 Mbit/s oder 100 Mbit/s Datenrate.

NAT (Network Address Translation)

Bei der Network Address Translation (NAT) - oft auch als IP-Masquerading bezeichnet - wird hinter einem einzigen Gerät, dem sog. NAT-Router, ein ganzes Netzwerk „versteckt“. Die internen Rechner im lokalen Netz bleiben mit ihren IP-Adressen verborgen, wenn Sie nach außen über den NAT-Router kommunizieren. Für die Kommunikationspartner außen erscheint nur der NAT-Router mit seiner eigenen IP-Adresse.
Damit interne Rechner dennoch direkt mit externen Rechnern (im Internet) kommunizieren können, muss der NAT-Router die IP-Datagramme verändern, die von internen Rechnern nach außen und von außen zu einem internen Rechner gehen.
Wird ein IP-Datagramm aus dem internen Netz nach außen versendet, verändert der NAT-Router den IP- und den TCP-Header des Datagramms. Er tauscht die Quell-IP-Adresse und den Quell-Port aus gegen die eigene offizielle IP-Adresse und einen eigenen, bisher unbenutzten Port. Dazu führt er eine Tabelle, die die Zuordnung der ursprünglichen mit den neuen Werten herstellt.
Beim Empfang eines Antwort-Datagramms erkennt der NAT-Router anhand des angegebenen Zielports, dass das Datagramm eigentlich für einen internen Rechner bestimmt ist. Mit Hilfe der Tabelle tauscht der NAT-Router die Ziel-IP-Adresse und den Ziel-Port aus und schickt das Datagramm weiter ins interne Netz.

Netzmaske / Subnetz-Maske

Einem Unternehmens-Netzwerk mit Zugang zum Internet wird normalerweise nur eine einzige IP-Adresse offiziell zugeteilt, z. B. 134.76.0.0. Bei dieser Beispiel-Adresse ist am 1. Byte erkennbar, dass es sich bei diesem Unternehmens-Netzwerk um ein Class B Netz handelt, d. h. die letzten 2 Byte können frei zur Host-Adressierung verwendet werden. Das ergibt rein rechnerisch einen Adressraum von 65.536 möglichen Hosts (256 x 256).
Ein so riesiges Netz macht wenig Sinn. Hier entsteht der Bedarf, Subnetze zu bilden. Dazu dient die Subnetz-Maske. Diese ist wie eine IP-Adresse ein 4 Byte langes Feld. Den Bytes, die die Netz-Adresse repräsentieren, ist jeweils der Wert 255 zugewiesen. Das dient vor allem dazu, sich aus dem Host-Adressenbereich einen Teil zu "borgen", um diesen zur Adressierung von Subnetzen zu benutzen. So kann beim Class B Netz (2 Byte für Netzwerk-Adresse, 2 Byte für Host-Adresse) mit Hilfe der Subnetz-Maske 255.255.255.0 das 3. Byte, das eigentlich für Host-Adressierung vorgesehen war, jetzt für Subnetz-Adressierung verwendet werden. Rein rechnerisch können so 256 Subnetze mit jeweils 256 Hosts entstehen.

Port-Nummer

Das Feld Port-Nummer ist ein 2 Byte großes Feld in UDP- und TCP-Headern. Die Vergabe der Port-Nummern dient der Identifikation der verschiedenen Datenströme, die UDP/TCP gleichzeitig abarbeitet. Über diese Port-Nummern erfolgt der gesamte Datenaustausch zwischen UDP/TCP und den Anwendungsprozessen. Die Vergabe der Port-Nummern an Anwendungsprozesse geschieht dynamisch und wahlfrei. Für bestimmte, häufig benutzte Anwendungsprozesse sind feste Port-Nummern vergeben. Diese werden als Assigned Numbers bezeichnet.

PPPoE

Akronym für Point-to-Point Protocol over Ethernet. Basiert auf den Standards PPP und Ethernet. PPPoE ist eine Spezifikation, um Benutzer per Ethernet mit dem Internet zu verbinden über ein gemeinsam benutztes Breitbandmedium wie DSL, Wireless LAN oder Kabel-Modem.

PPTP

Akronym für Point-to-Point Tunneling Protocol. Entwickelt von Microsoft, U.S. Robotics und anderen wurde dieses Protokoll entwickelt, um zwischen zwei VPN-Knoten (→ VPN) über ein öffentliches Netz sicher Daten zu übertragen.

Private Key (privater Schlüssel), Public Key (öffentlicher Schlüssel); Zertifizierung (X.509)

Bei asymmetrischen Verschlüsselungsalgorithmen werden 2 Schlüssel verwendet: ein privater (Private Key) und ein öffentlicher (Public Key). Der öffentliche Schlüssel dient zum Verschlüsseln von Daten, der private Schlüssel zum Entschlüsseln.
Der öffentliche Schlüssel wird vom zukünftigen Empfänger von Daten denen zur Verfügung gestellt, die die Daten verschlüsselt an ihn versenden werden. Der private Schlüssel ist nur im Besitz des Empfängers. Er dient zum Entschlüsseln der empfangenen Daten.
Zertifizierung:
Damit der Benutzer des (zum Verschlüsseln dienenden) öffentlichen Schlüssels sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung: Die Überprüfung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Absenders mit seinem Schlüssel übernimmt eine zertifizierende Stelle (Certification Authority - CA). Dies geschieht nach den Regeln der CA, indem der Absender beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Prüfung signiert die CA den öffentliche Schlüssel des Absenders mit ihrer (digitalen) Unterschrift. Es entsteht ein Zertifikat.
Ein X.509-Zertifikat stellt eine Verbindung zwischen einer Identität in Form eines 'X.500 Distinguished Name' (DN) und einem öffentliche Schlüssel her, die durch die digitale Signatur einer X.509 Certification Authority (CA) beglaubigt wird. Die Signatur - eine Verschlüsselung mit dem Signaturschlüssel - kann mit dem öffentlichem Schlüssel überprüft werden, die die CA dem Zertifikatsinhaber aushändigt.

Protokoll, Übertragungsprotokoll

Geräte, die miteinander kommunizieren, müssen dieselben Regeln dazu verwenden. Sie müssen dieselbe „Sprache sprechen“. Solche Regeln und Standards bezeichnet man als Protokoll bzw. Übertragungsprotokoll. Oft benutzte Protokolle sind z. B. IP, TCP, PPP, HTTP oder SMTP. TCP/IP ist der Oberbegriff für alle auf IP aufbauenden Protokolle.

Service Provider

Anbieter, Firma, Institution, die Nutzern den Zugang zum Internet oder zu einem Online-Dienst

Spoofing, Anti-Spoofing

In der Internet-Terminologie bedeutet Spoofing die Angabe einer falschen Adresse. Durch die falsche Internet-Adresse täuscht jemand vor, ein autorisierter Benutzer zu sein.
Unter Anti-Spoofing versteht man Mechanismen, die Spoofing entdecken oder verhindern.

SSH

SSH (Secure SHell) ist ein Protokoll, das den gesicherten und verschlüsselten Datenaustausch zwischen Rechnern ermöglicht. Verwendet wird Secure SHell zum Fernzugriff auf die Eingabekonsole von LINUX- basierten Maschinen.

Stateful Inspection Firewall

Stateful Inspection Firewall ist eine Methode zur Paketfilterung. Paketfilter lassen IP-Pakete nur dann passieren, wenn dies zuvor durch Firewall-Regeln definiert wurde. In der Firewall-Regel wird folgendes festgelegt,

- welches Protokoll (TCP, UDP, ICMP) passieren darf,
- die erlaubte Quelle der IP-Pakete (Von IP / Von Port)
- das erlaubte Ziel der IP-Pakete (Nach IP / Nach Port)

Gleichfalls wird hier festgelegt, wie mit IP-Pakete verfahren wird, die nicht passieren dürfen, z.B. werden sie verworfen oder zurückgewiesen).
Bei einem einfachen Paketfilter müssen immer zwei Firewall-Regeln für eine Verbindung angelegt werden:

- Eine Regel für die Anfragerichtung von der Quelle zum Ziel und
- eine zweite Regel für die Antwortrichtung vom Ziel zur Quelle.

Anders ist das bei einer Stateful Inspection Firewall. Hier wird nur für die Anfragerichtung von der Quelle zum Ziel eine Firewall-Regel angelegt. Die Firewall-Regel für die Antwortrichtung vom Ziel zur Quelle ergibt sich aus der Analyse der zuvor gesendeten Daten. Die Firewall-Regel für die Antworten wird nach Erhalt der Antworten bzw. nach Ablauf einer kurzen Zeitspanne wieder geschlossen. Antworten dürfen also nur passieren, wenn es zuvor eine Anfrage gab. So kann die Antwortregel nicht für unbefugte Zugriffe benutzt werden. Besondere Verfahren ermöglichen zudem, dass auch UDP- und ICMP-Daten passieren können, obwohl diese Daten zuvor nicht angefordert wurden.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung werden Daten mit dem gleichen Schlüssel ver- und entschlüsselt. Beispiele für symmetrische Verschlüsselungsalgorithmen sind DES und AES. Sie sind schnell, jedoch bei steigender Nutzerzahl nur aufwendig administrierbar.

TCP/IP (Transmission Control Protocol/Internet Protocol

Netzwerkprotokolle, die für die Verbindung zweier Rechner im Internet verwendet werden.
IP ist das Basisprotokoll.
UDP baut auf IP auf und verschickt einzelne Pakete. Diese können beim Empfänger in einer anderen Reihenfolge als der abgeschickten ankommen, oder sie können sogar verloren gehen.
TCP dient zur Sicherung der Verbindung und sorgt beispielsweise dafür, dass die Datenpakete in der richtigen Reihenfolge an die Anwendung weitergegeben werden.
UDP und TCP bringen zusätzlich zu den IP-Adressen Port-Nummern zwischen 1 und 65535 mit, über die die unterschiedlichen Dienste unterschieden werden.
Auf UDP und TCP bauen eine Reihe weiterer Protokolle auf, z. B. HTTP (Hyper Text Transfer Protokoll), HTTPS (Secure Hyper Text Transfer Protokoll), SMTP (Simple Mail Transfer Protokoll), POP3 (Post Office Protokoll, Version 3), DNS (Domain Name Service).
ICMP baut auf IP auf und enthält Kontrollnachrichten.
SMTP ist ein auf TCP basierendes E-Mail-Protokoll.
IKE ist ein auf UDP basierendes IPsec-Protokoll.
ESP ist ein auf IP basierendes IPsec-Protokoll.
Auf einem Windows-PC übernimmt die WINSOCK.DLL (oder WSOCK32.DLL) die Abwicklung der beiden Protokolle.
(→ Datagramm)

UDP

Siehe TCP/IP

UMTS

UMTS (Universal Mobile Telecommunication System) ist ein Mobilfunknetz der 3. Generation, das deutlich höhere Datenübertragungsraten ermöglicht, als die GSM-Netze der 2. Generation. UMTS bietet neben der Sprachübertragung, IP-basierte Datenübertragung und SMS Übertragung auch die Möglichkeit zu Übertragung von Videoanwendungen.
Mit Ausnahme des nordamerikanisches Raums verwendet UMTS ein Frequenzband bei 2100 MHz. In Nordamerika werden die Frequenzbänder bei 850 MHz und 1900 MHz genutzt, die auch für GSM-Netze verwendet werden.

VPN (Virtuelles Privates Netzwerk)

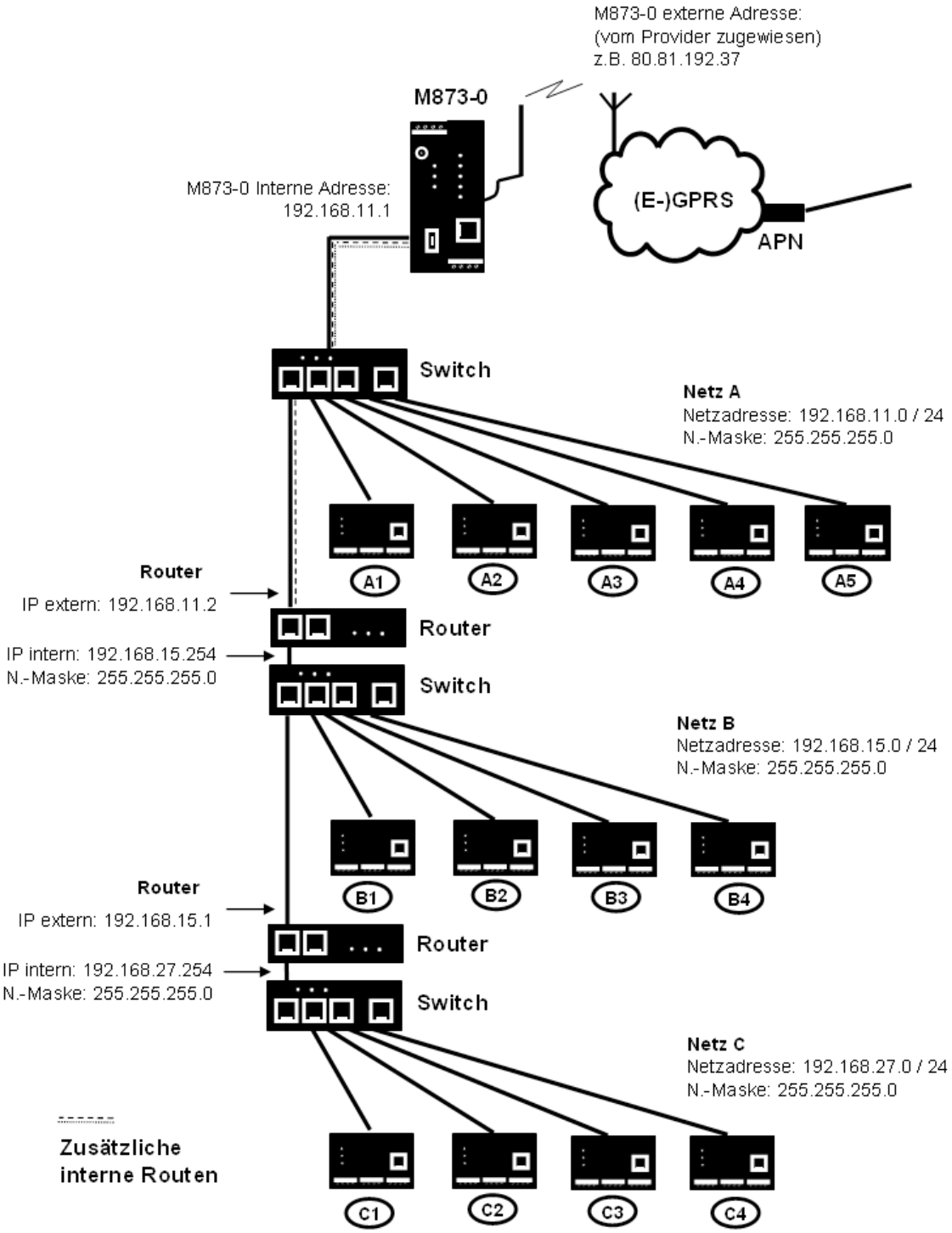
Ein Virtuelles Privates Netzwerk (VPN) schließt mehrere voneinander getrennte private Netzwerke (Teilnetze) über ein öffentliches Netz, z. B. das Internet, zu einem gemeinsamen Netzwerk zusammen. Durch Verwendung kryptographischer Protokolle wird dabei die Vertraulichkeit und Authentizität gewahrt. Ein VPN bietet somit eine kostengünstige Alternative gegenüber Standleitungen, wenn es darum geht, ein überregionales Firmennetz aufzubauen.

X.509-Zertifikat

Eine Art „Siegel“, welches die Echtheit eines öffentlichen Schlüssels (→ asymmetrische Verschlüsselung) und zugehöriger Daten belegt. Damit der Benutzer eines zum Verschlüsseln dienenden öffentlichen Schlüssels sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von seinem tatsächlichen Aussteller und damit der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung. Diese Beglaubigung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Ausstellers mit seinem Schlüssel übernimmt eine zertifizierende Stelle (Certification Authority - CA). Dies geschieht nach den Regeln der CA, indem der Aussteller des öffentlichen Schlüssels beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Überprüfung signiert die CA den öffentlichen Schlüssel mit ihrer (digitalen) Unterschrift, ihrer Signatur. Es entsteht ein Zertifikat.
Ein X.509(v3) Zertifikat beinhaltet also einen öffentlichen Schlüssel, Informationen über den Schlüsseleigentümer (angegeben als Distinguished Name (DN)), erlaubte Verwendungszwecke usw. und der Signatur der CA.
Die Signatur entsteht wie folgt: Aus der Bitfolge des öffentlichen Schlüssels, den Daten über seinen Inhaber und aus weiteren Daten erzeugt die CA eine individuelle Bitfolge, die bis zu 160 Bit lang sein kann, den sog. HASH-Wert. Diesen verschlüsselt die CA mit ihrem privaten Schlüssel und fügt ihn dem Zertifikat hinzu. Durch die Verschlüsselung mit dem privaten Schlüssel der CA ist die Echtheit belegt, d. h. die verschlüsselte HASH-Zeichenfolge ist die digitale Unterschrift der CA, ihre Signatur. Sollten die Daten des Zertifikats missbräuchlich geändert werden, stimmt dieser HASH-Wert nicht mehr, das Zertifikat ist dann wertlos.
Der HASH-Wert wird auch als Fingerabdruck bezeichnet. Da er mit dem privaten Schlüssel der CA verschlüsselt ist, kann jeder, der den zugehörigen öffentlichen Schlüssel besitzt, die Bitfolge entschlüsseln und damit die Echtheit dieses Fingerabdrucks bzw. dieser Unterschrift überprüfen.
Durch die Heranziehung von Beglaubigungsstellen ist es möglich, dass nicht jeder Schlüsseleigentümer den anderen kennen muss, sondern nur die benutzte Beglaubigungsstelle. Die zusätzlichen Informationen zu dem Schlüssel vereinfachen zudem die Administrierbarkeit des Schlüssels.
X.509-Zertifikate kommen z.B. bei Email Verschlüsselung mittels S/MIME oder IPsec zum Einsatz.

Zusätzliche interne Routen

Die nachfolgende Skizze zeigt, wie in einem lokalen Netzwerk mit Subnetzen die IP-Adressen verteilt sein könnten, welche Netzwerk-Adressen daraus resultieren und wie die Angabe einer zusätzlichen internen Route lauten könnte.



Netz A ist an das SCALANCE M873-0 angeschlossen und über dieses mit einem entfernten Netz verbunden. Zusätzliche interne Routen zeigen den Weg zu weiteren Netzen (Netz B, C), die über Gateways (Router) miteinander verbunden sind. Für das SCALANCE M873-0 sind bei dem gezeigten Beispiel die Netze B und C beide über das Gateway 192.168.11.2 und die Netzwerkadresse 192.168.11.0/24 erreichbar.

Netz A					
Rechner	A1	A2	A3	A4	A5
IP-Adresse	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Netz B					
Rechner	B1	B2	B3	B4	**Zusätzliche interne Routen:** Netzwerk: 192.168.15.0/24 Gateway: 192.168.11.2 Netzwerk: 192.168.27.0/24 Gateway: 192.168.11.2
IP-Adresse	192.168.15.3	192.168.15.4	192.168.15.5	192.168.15.6	
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	
Netz C					
Rechner	C1	C2	C3	C4	
IP-Adresse	192.168.27.3	192.168.27.4	192.168.27.5	192.168.27.6	
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	