TAINY IQ-LTE
TAINY IQ-LTE 6E

Anwenderhandbuch

Dr. Neuhaus

Sagemcom Dr. Neuhaus GmbH

Papenreye 65

22453 Hamburg

Deutschland

Internet: www.neuhaus.de

Internet: www.sagemcom.com/de/smart-city/dr-neuhaus/

Technische Änderungen vorbehalten.

Alle Lieferungen und Leistungen erbringt die Sagemcom Dr. Neuhaus GmbH auf der Grundlage der allgemeinen Geschäftsbedingungen der Sagemcom Dr. Neuhaus GmbH in der jeweils aktuellen Fassung. Alle Angaben basieren auf Herstellerangaben. Keine Gewähr oder Haftung bei fehlerhaften und unterbliebenen Eintragungen. Die Beschreibungen der Spezifikationen in diesem Handbuch stellen keinen Vertrag da.

Produkt-Nr.:	3202
Dok.-Nr.:	3202AD011 Version 1.10 / November 2019
Kompatibel:	ab Firmware Version 3.007

Inhaltsverzeichnis

1 Einleitung

1.1 Produktübersicht

Die Mobilfunkrouter TAINY IQ-LTE und TAINY IQ-LTE 6E sind für den industriellen Einsatz konzipiert und bietet eine Vielfalt an Funktionen. Das vorliegende Handbuch beschreibt die diversen Einsatzszenarien für TAINY IQ-LTE sowie die Installation und Konfiguration des Routers.

Daten

2G/3G/4G

2 x Ethernet LAN/WAN Variante TAINY IQ-LTE

1 x Ethernet WAN und 5 x Ethernet LAN Variante TAINY IQ-LTE 6E

IPv4 (TAINY IQ-LTE und TAINY IQ-LTE 6E)

IPv6 (***nur TAINY IQ-LTE***)

Stromversorgung 24 V_{DC}

Drahtlose WAN-Verbindung

TAINY IQ-LTE bietet eine drahtlose Verbindung zum Internet oder zu einem privaten Netzwerk.

TAINY IQ-LTE kann diese Verbindung an jedem Ort herstellen, an dem ein UMTS-Netz (Universal Mobile Telecommunication System = Mobilfunk-netz 3. Generation), ein LTE-Netz (Long Term Evolution = Mobilfunknetz 4. Generation) oder ein GSM-Netz (Global System for Mobile Communication = Mobilfunknetz) verfügbar ist, das IP-basierte Datendienste bereitstellt. Bei UMTS sind dies HSDPA (High Speed Downlink Packet Access), HSUPA (High Speed Uplink Packet Access) oder der UMTS-Daten-Service. Bei GSM sind dies EGPRS (Enhanced General Packet Radio Service = EDGE) oder GPRS (General Packet Radio Service).

HSDPA und HSUPA sind im Folgenden unter dem Begriff HSPA+ zusammengefasst.

WAN-Verbindung über Kabel

TAINY IQ-LTE kann eine WAN-Verbindung auch über Ethernet-Kabel herstellen, vorausgesetzt, es ist an einen Router mit WAN-Zugang oder ein DSL-Modem angeschlossen.

TAINY IQ-LTE verfügt über 2 Ethernet-Ports, über die es lokal angeschlossene Applikationen oder ganze Netzwerke mit dem Internet verbindet. Dazu verwendet TAINY IQ-LTE kabellose oder kabelgebunden IP-Verbindungen. Möglich ist auch die direkte Verbindung mit einem Intranet, an das wiederum die externen Gegenstellen angeschlossen sind.

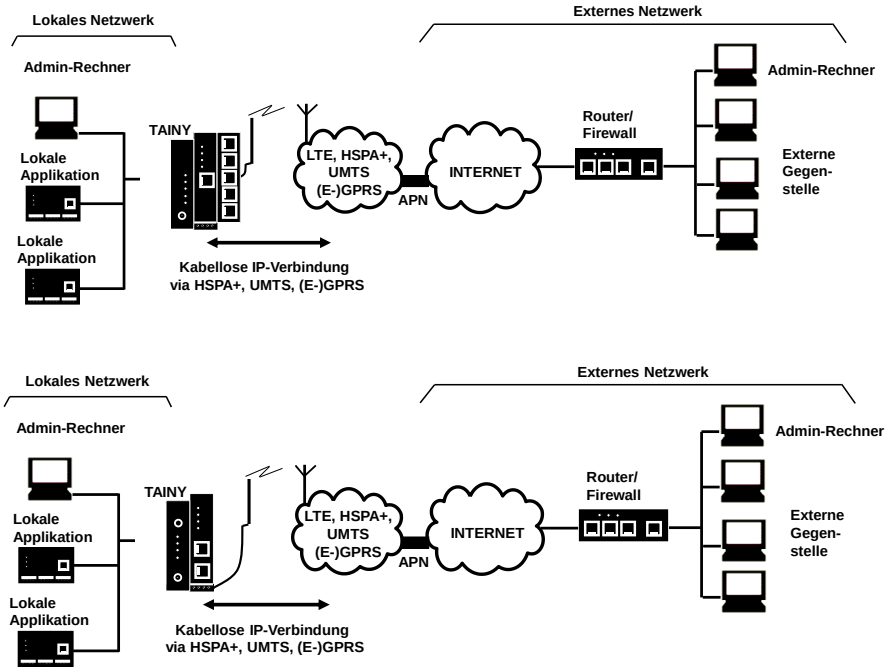
TAINY IQ-LTE kann über eine drahtlose oder kabelgebundene IP-Verbindung ein VPN (Virtual Private Network) zwischen einer lokal angeschlossenen Applikation/Netzwerk und einem externen Netzwerk herstellen. Es schützt diese Verbindung mit IPsec (Internet Protocol Security) vor dem Zugriff Dritter.

Dual SIM

Mit 2 SIM-Karten-Einschüben ausgestattet, ermöglicht TAINY IQ-LTE den alternativen Betrieb mit einer zweiten SIM-Karte, z. B. eines zweiten Betreibers, der die Kommunikation übernimmt, sollte die Verbindung über die erste SIM-Karte unterbrochen sein.

1.2 Begriffe

In diesem Abschnitt werden die, in diesem Handbuch am häufigsten verwendeten Begriffe kurz erläutert.



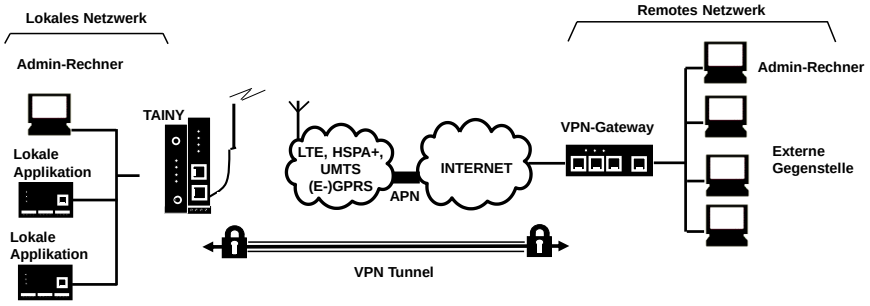
Lokales Netz	Das an die lokale Schnittstelle des TAINY IQ-LTE angeschlossene Netz. Das lokale Netz enthält mindestens eine lokale Applikation.
Lokale Schnittstellen ETH 0, ETH 1 (10/100-Base-T)	Schnittstellen des TAINY IQ-LTE zum Anschluss des lokalen Netzes. Die Schnittstellen sind am Gerät gekennzeichnet als ETH 0 bis ETH 1 (10/100 Base-T). Die Ethernet-Schnittstellen verfügen über Datenübertragungsraten von 10 MBits oder 100 MBits (Autosensing-Funktion MDI/MDIX). Sie können ETH0 und ETH1 als separate LAN-Netzwerkeschnittstellen verwenden oder ETH0 als kabelgebundene WAN-Verbindung (siehe Kapitel 6.5). Zwischen dem Netzwerk auf ETH0 und ETH1 wird intern geroutet.
Lokale Schnittstellen ETH 0, ETH 1, ETH 2, ETH 3, ETH 4, ETH 5 (10/100-Base-T)	Schnittstellen des TAINY IQ-LTE 6E zum Anschluss des lokalen Netzes. Die Schnittstellen sind am Gerät gekennzeichnet als ETH 0 bis ETH 5 (10/100 Base-T). Die Ethernet-Schnittstellen verfügen über Datenübertragungsraten von 10 MBits oder 100 MBits (Autosensing MDI/MDIX). Während ETH 0 direkt mit der Router-Funktion des TAINY iQ verbunden ist, sind ETH 1 bis ETH 5 über einen Switch mit der Router-Funktion verbunden. Sie können Daten zwischen ETH 0 und allen anderen Ports senden (siehe Kapitel 9.3) oder Sie nutzen ETH 0 als kabelgebundene WAN-Verbindung (siehe Kapitel 6.5). ETH 1 bis ETH 5 können zu VLANs gruppiert werden.
Lokale Applikation	Lokale Applikationen sind Netzwerkkomponenten im lokalen Netz, wie z. B. eine programmierbare Steuerung, eine Maschine mit Ethernet-Schnittstelle zur Fernüberwachung, ein Notebook oder Admin-Rechner.

Admin-Rechner	Rechner mit Webbrowser (z. B. Windows Internet Explorer ab Version 11, Mozilla Firefox ab Version 37 oder Chrome ab Version 64 oder neuer), der an das lokale Netz oder das externe Netz angeschlossen ist und mit dem die Konfiguration des TAINY IQ-LTE durchgeführt wird. Der Webbrowser muss HTTPS unterstützen.
Externes Netz	Das externe Netzwerk, mit dem TAINY IQ-LTE über HSPA+, UMTS, EGPRS oder GPRS verbunden ist. Externe Netze sind das Internet oder ein privates Intranet.
Externe Gegenstellen	Externe Gegenstellen sind Netzwerkkomponenten im externen Netz, z. B. Webserver im Internet, Router im Intranet, der zentrale Server eines Unternehmens, ein Admin-Rechner und vieles mehr.
(E-)GPRS	EGPRS oder GPRS, je nach Verfügbarkeit der Dienste.
VPN-Gateway	Komponente des externen Remote-Netzwerks, das DM-VPN und IPsec unterstützt und mit TAINY IQ-LTE kompatibel ist.
Remote Network	Externes Netz, mit dem TAINY IQ-LTE eine VPN-Verbindung aufbaut.
Mobilfunknetz	Infrastruktur und Technologie zur drahtlosen mobilen Sprach- und Datenkommunikation. TAINY IQ-LTE ist zum Einsatz für das LTE-, UMTS-Mobilfunknetz und GSM- Mobilfunknetze geeignet.
Zertifikatsverwaltung	Verwaltung aller TAINY IQ-LTE -Zertifikate sowie der externen CA-Zertifikate. Möglichkeit zum Herunterladen, Export und Mailen von Zertifikaten sowie zur Erstellung neuer Geräteschlüssel.

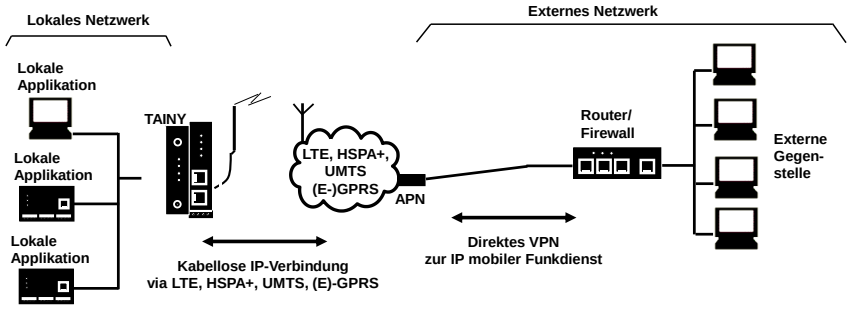
1.3 Verschiedene Einsatz-Szenarien

In diesem Kapitel werden mögliche Einsatzszenarien für TAINY IQ-LTE beschrieben.

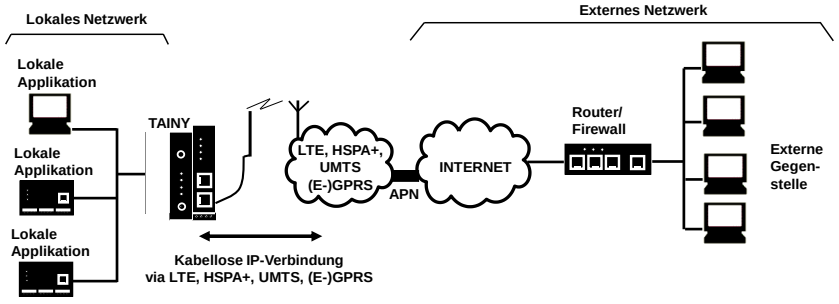
Szenario 1: Virtual Private Network (VPN) mit IPsec



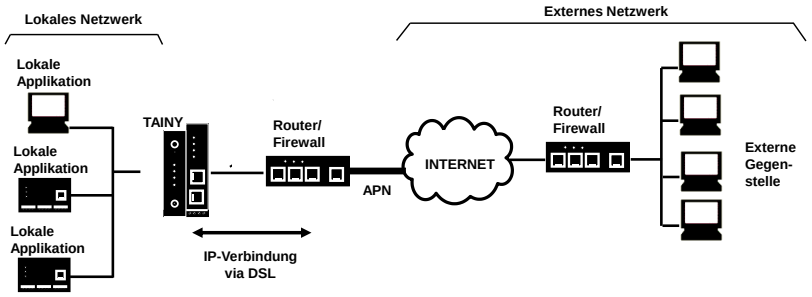
Szenario 2: Verbindung über HSPA+, UMTS, EGPRS oder GPRS oder LTE oder DSL und ein direktes VPN zum externen Netz



Szenario 3: Verbindung über HSPA+, UMTS, EGPRS oder GPRS oder LTE oder DSL und das Internet zum externen Netz

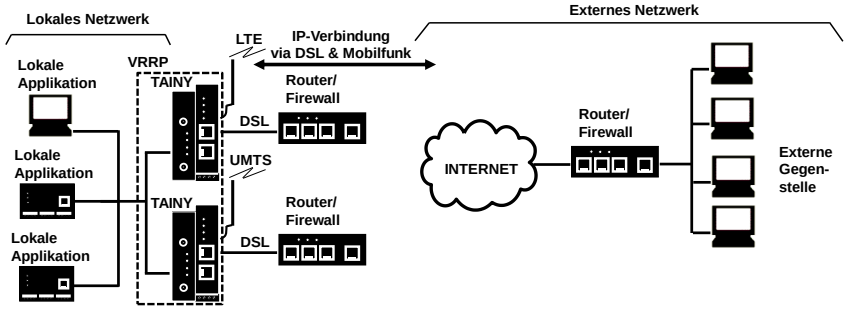


Szenario 4: Verbindung über DSL und Internet zu einem externen Netz



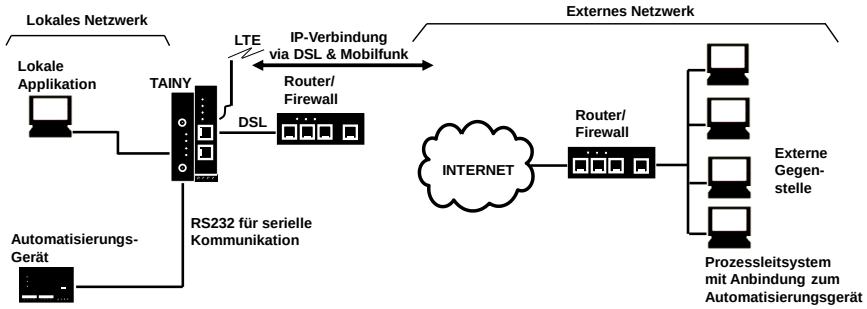
Lokale Applikationen könnten z. B. eine programmierbare Steuerung, eine Maschine mit Ethernet-Schnittstelle zur Fernüberwachung oder ein Notebook oder Rechner sein. Diese Applikationen nutzen TAINY IQ-LTE-LTE, um Zugriff auf ein externes Netz zu erhalten, als ob sie direkt vor Ort an das externe Netz angeschlossen wären.

Szenario 5 Verbindung über DSL und/oder Mobilfunk durch das Internet zu einem externen Netz & Redundanz durch VRRP



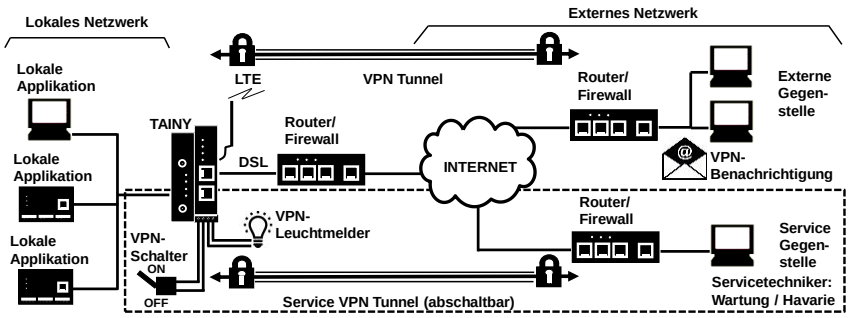
Bietet maximale Ausfallsicherheit:

Szenario 6:



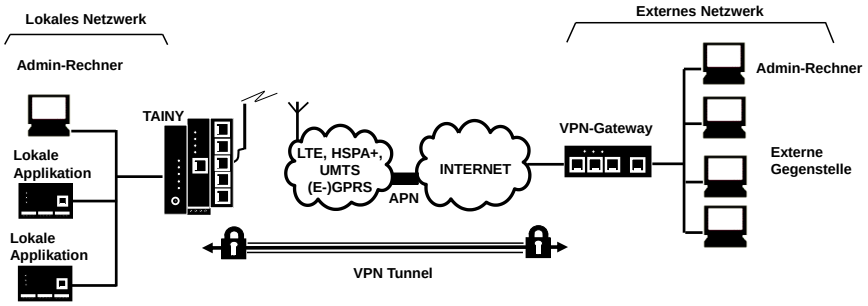
Serielle Kommunikation

Szenario 7: IPsec-VPN

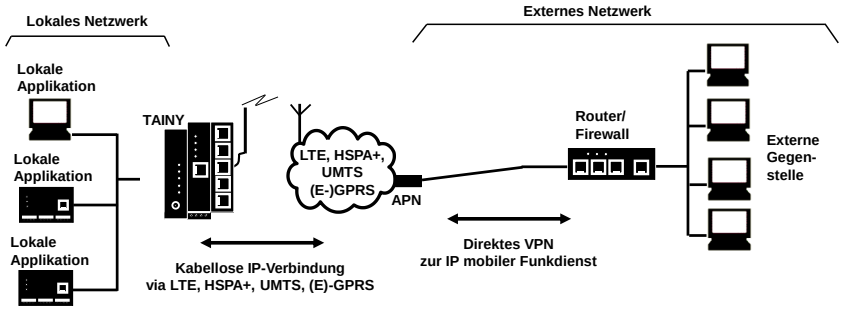


IPsec-VPN: Dauerhafte VPN-Verbindung und abschaltbarer Service-VPN-Zugang (Schaltbar über Digitaleingang & Benachrichtigung durch Leuchtmelder und E-Mail)

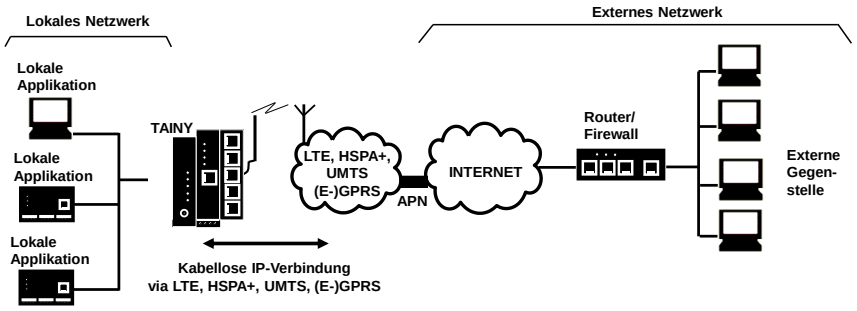
Szenario 8: Virtual Private Network (VPN) mit IPsec



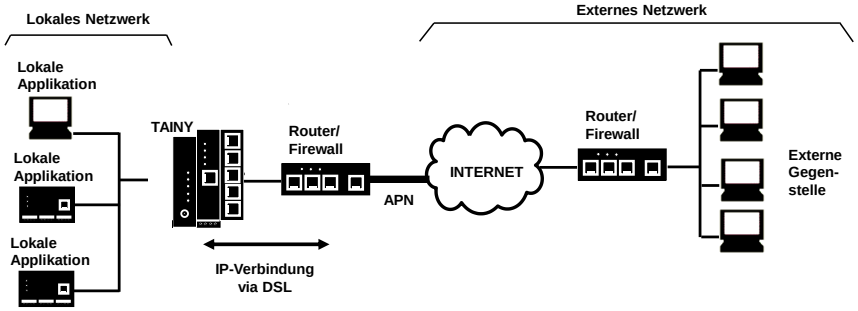
Szenario 9: Verbindung über HSPA+, UMTS, EGPRS oder GPRS oder LTE oder DSL und ein direktes VPN zum externen Netz



Szenario 10: Verbindung über HSPA+, UMTS, EGPRS oder GPRS oder LTE oder DSL und das Internet zum externen Netz

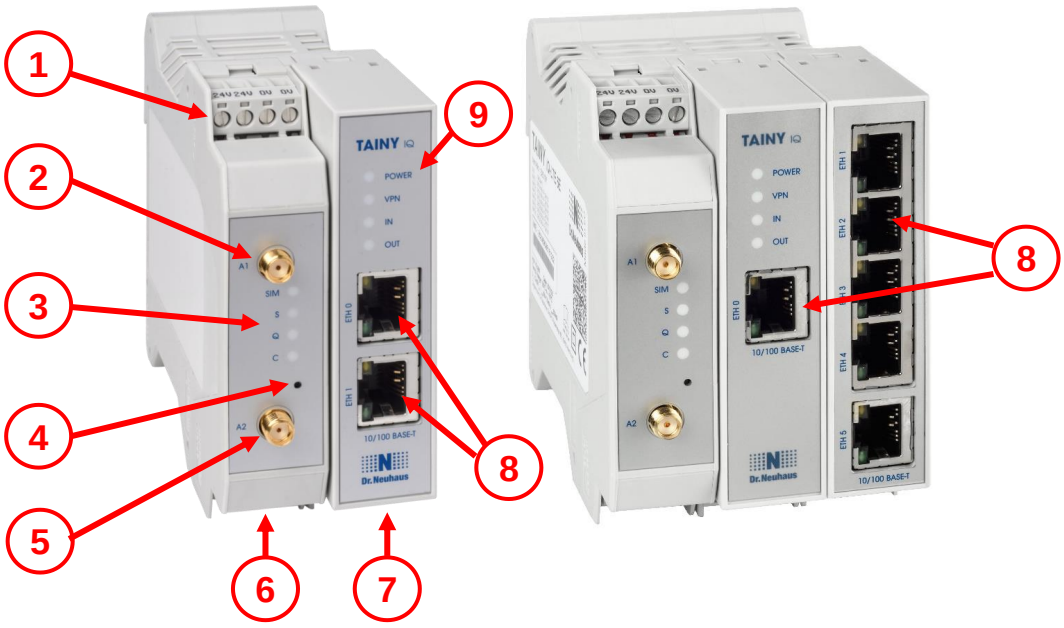


Szenario 11: Verbindung über DSL und Internet zu einem externen Netz



Lokale Applikationen könnten z. B. eine programmierbare Steuerung, eine Maschine mit Ethernet-Schnittstelle zur Fernüberwachung oder ein Notebook oder Rechner sein. Diese Applikationen nutzen TAINY iQ, um Zugriff auf ein externes Netz zu erhalten, als ob sie direkt vor Ort an das externe Netz angeschlossen wären.

1.4 Bedienelemente



1	24V Spannungsversorgungs-Anschluss
2, 5	MIMO-Antennensystem
3, 9	Signalleuchten
4	Service-Taster
6	RS232-Schnittstelle
7	Digital Eingabe/Ausgabe
8	Ethernet-Ports

1.5 Funktionsüberblick

Die folgende Aufzählung gibt einen Überblick zu den wichtigsten Funktionen und Besonderheiten des TAINY IQ-LTE.

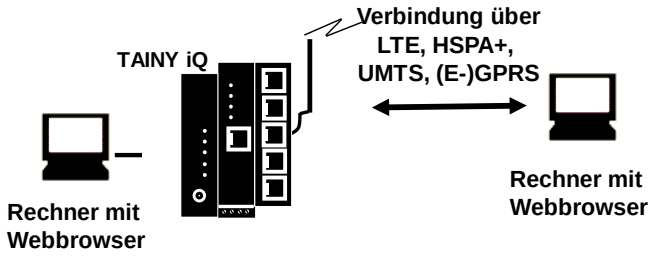
Sie benötigen das Wissen des Anwenderhandbuchs um den Mobilfunkrouter korrekt in Betrieb nehmen und für das jeweilige Einsatzszenario korrekt konfigurieren zu können.

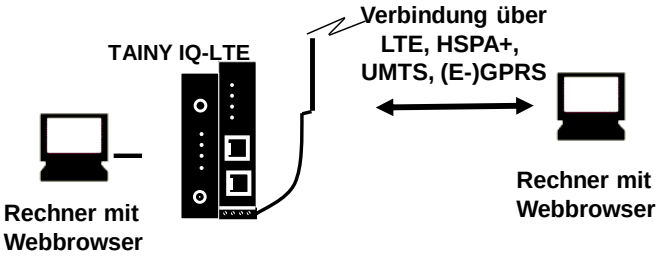
Beachten Sie außerdem dringend die Sicherheitshinweise im vorliegenden Anwenderhandbuch, da ein Zuwiderhandeln schwerwiegende Folgen nicht nur für den Betrieb des Routers sondern auch den Anwender haben können.

Konfiguration

Die Konfiguration des Gerätes erfolgt über eine Benutzeroberfläche, die sich mit einem Webbrowser anzeigen lässt. Der Zugriff kann über folgende Wege stattfinden:

- Lokale Schnittstelle
- LTE, HSPA+, UMTS, EGPRS, GPRS





Allgemein

- Web-Konfigurationsoberfläche auf Englisch und Deutsch mit einstellbarem Port (HTTPS)
- Export und Import der Router-Konfiguration, Reset auf Werkseinstellung, Setzen von individuellen Widerherstellungspunkten
- Versand von E-Mails (event- oder zeitabhängig), die Event- oder Geräteinformationen enthalten (SMTP)
- SNMPv3 (Auslesen des Gerätestatus)
- SSH-Zugriff
- CA-Zertifikate und Gegenstellenzertifikate
- Benutzer-Gruppen mit konfigurierbaren Berechtigungen sowie unterschiedliche Wege der Benutzer-Authentifizierung: Lokal, RADIUS, TACACS+
- Exportierbares Logbuch mit einstellbaren Log-Aufzeichungslevel
- Integrierte Netzwerktools: Ping, Traceroute, NSlookup
- Staus Informationen, z.B.: Feldstärke, WAN-IP-Adresse, verbrauchtes Datenvolumen, VPN-Status

WAN-Anbindung

- WAN-Anbindung über DSL und/oder Mobilfunk möglich sowie 2 Mobilfunkanbieter (Dual SIM)
- Höchste Ausfallsicherheit in Kombination mit VRRP (Redundante Kommunikationswege + Geräteredundanz)

LAN-Funktionen

- Zuordnung mehrerer LAN-IP-Adressen möglich (auch unterschiedliche Netze)
- Modus: "Automatisch", "10M/Halbduplex", „10M/Vollduplex, „100M/Halbduplex“, „100M/Vollduplex“
- DNS-Server
- DHCP-Server
  - Dynamischer IP-Adressbereich
  - Statische DHCP-Zuordnungen
- DHCP-Relay
- VRRP (Virtual Router Redundanz Protocol) für den Einsatz von Redundanzgeräten
  - VRRP-ID-Zuweisung
  - Statische/dynamische VRRP-Prioritäten

VPN-Funktionen

- IPsec IKEv1 (maximal 10 gleichzeitige Tunnelverbindungen garantiert)
  - Server oder Client
  - Main- & Aggressive-Mode
  - Authentifizierungsmodi: "Pre-Shared-Key", "Gegenstellenzertifikat", "CA-Zertifikat"
  - Verschlüsselungsverfahren: "3DES", "AES-128", "AES-192", "AES-256"
  - HASH-Verfahren: "MD5", "SHA-1", "SAH-256", "SAH-384", "SAH-512"
  - NAT-Traversal
  - Dead Peer Detection (DPD)
- DM-VPN (Dynamic Multipoint VPN)
  - GRE
  - NHRP

Firewall-Funktionen

- Paketfilterregeln einzeln einstellbar für LAN-, WAN-, VPN-Schnittstelle
  - Datenpakete von Adressbereichen/Einzeladressen „Akzeptieren“/“Verwerfen“/“Abweisen“
  - Klassifizierung der Filtereinstellungen nach Protokoll: TCP/UDP/ICMP
- Regeln für Fernzugang einzeln einstellbar für WAN-, VPN-Schnittstelle
  - Fernzugang von Adressbereichen/Einzeladressen „Akzeptieren“/“Verwerfen“/“Abweisen“
  - Klassifizierung der Fernzugänge nach Dienst: HTTPS/SNMP/SSH/ICMP
- Portweiterleitung
  - Portweiterleitung von Adressbereichen/Einzeladressen zu Ziel-Adresse
  - Port-Umsetzung
  - Klassifizierung der Portweiterleitung nach Protokoll: TCP/UDP
  - Unbekannter Datenverkehr kann an bestimmte Zieladresse weitergeleitet werden (Exposed Host)

MAC-Tabelle

- MAC-Adresse kann bestimmtem Ethernet-Port zugewiesen werden

Protokollierung im separaten Firewall-Log (Auswertung des gesamten Datenverkehrs)

2 Sicherheit

TAINY IQ-LTE erfüllt die allgemeinen Anforderungen der DIN EN 62368-1, Einrichtungen der Telekommunikation – Sicherheit.

Für eine sichere Inbetriebnahme beachten Sie bitte das aktuelle Datenblatt und die Dokumentation Ihres Produktes.

Sie können alle relevanten Dokumentationen und zusätzliche Informationen zu Ihrem Produkt auf www.sagemcom.com einsehen.

2.1 Bestimmungsgemäßer Gebrauch

Das Gerät darf nur gemäß dem in diesem Handbuch beschriebenen Gebrauch und in Übereinstimmung mit den technischen Daten (siehe auch Kapitel 19) verwendet werden.

Das Gerät darf nur für die in diesem Dokument und im Datenblatt genannten Applikationen genutzt werden. Ordnungsgemäßer Transport, Lagerung, Installation, Inbetriebnahme und Bedienung sichern einen fehlerfreien und zuverlässigen Betrieb des Produktes.

2.2 Nicht bestimmungsmäßer Gebrauch

Verwenden Sie TAINY IQ-LTE niemals ohne ein sicheres Back-up-Gerät, wenn Sie es für eine Applikation nutzen, deren Fehlfunktion zu Sachschaden, Verletzungen oder Tod führen können.

2.3 Qualifikationen Fachpersonal

Das Gerät darf nur von einer ausgebildeten Elektrofachkraft montiert, installiert, betrieben und demontiert werden. Eine Elektrofachkraft besitzt aufgrund ihrer fachlichen Ausbildung ausreichend Kenntnisse und Erfahrungen hinsichtlich

- des Einschaltens, Ausschaltens, Freischaltens, Erdens und Kurzschließens von elektrischen Stromkreisen und elektrischen Geräten,
- der ordnungsgemäßen Anwendung und Wartung von Sicherheits- und Schutzeinrichtungen entsprechend den geltenden Sicherheitsanforderungen,
- der Notversorgung von Verletzten.

2.4 Klassifizierung der Sicherheitshinweise

Dieses Handbuch enthält Hinweise und Anweisungen, die Sie zu Ihrer persönlichen Sicherheit und zum Schutz vor Sachschäden unbedingt befolgen sollten. Hinweise, bei deren Nichtbefolgung die Sicherheit von Leib und Leben gefährdet ist, sind mit einem Warndreieck versehen. Hinweise bei deren Nichtbefolgung Sachschäden entstehen, sind nicht mit einem Warndreieck versehen. Die Warnhinweise sind in der folgenden Staffelung gemäß des Gefährdungspotenzials aufgeführt:

Gefahr

Beschreibt eine unmittelbar gefährliche Situation, die – sofern sie nicht vermieden wird – zu schweren Verletzungen oder zum Tod führen wird.

Warnung

Beschreibt eine möglicherweise gefährliche Situation, die – sofern sie nicht vermieden wird – zu schweren Verletzungen oder Tod führen kann.

Vorsicht

Beschreibt eine möglicherweise gefährliche Situation, die – sofern sie nicht vermieden wird – zu leichten Verletzungen führen kann.

Achtung

Beschreibt eine möglicherweise gefährliche Situation, die – sofern sie nicht vermieden wird – zu Schäden am Gerät oder Datenverlust führen kann.

Hinweis

Beschreibt eine möglicherweise gefährliche Situation, die – sofern sie nicht vermieden wird bzw. der Hinweis nicht eingehalten wird – zu ungewollten Ergebnissen führen kann.

Tipp

Hilfestellungen und Hinweise für eine schnellere und leichtere Installation sowie einen einfacheren und verbesserten Betrieb des Gerätes.

Treten mehrere Gefahrenebenen gleichzeitig auf, gilt immer der Hinweis mit dem höchsten Gefährdungspotenzial. Weist ein Hinweis mit Warndreieck auf Personenschäden hin, ist davon auszugehen, dass auch Sachschaden entsteht.

2.5 Sicherheitshinweise

TAINY IQ-LTE erfüllt die allgemeinen Anforderungen der DIN EN EN62368-1, Audio and Video Information and Communication technology equipment – part1: Safety requirements.

Lesen Sie dieses Anwenderhandbuch sorgfältig vor der Installation, der Inbetriebnahme und dem Gebrauch des Gerätes durch.

Allgemein

Gefahr

Verletzungsgefahr durch elektrischen Schock

- Niemals ein defektes Gerät installieren oder betreiben.
- Niemals das Gerät installieren oder betreiben, wenn die angeschlossenen Kabel beschädigt sind.
- Niemals das Gerät an defekte Kabel anschließen.
- Das Gerät niemals im Freien installieren oder betreiben.
- Das Gerät niemals in einer feuchten Umgebung installieren oder betreiben.
- Das Gerät niemals anders als zum bestimmungsgemäßen Gebrauch verwenden.
- Das Gerät außer Reichweite von Kindern aufbewahren.

Elektrofachkraft

Gefahr

Verletzungsgefahr durch elektrischen Schock und Unwissenheit

- Die Installation und der Betrieb des Gerätes darf nur von einer Elektrofachkraft durchgeführt werden.
- Auch die Installation sämtlicher angeschlossener Geräte und der Antenne darf nur durch eine Elektrofachkraft durchgeführt werden.
- Das Handbuch vor Installation und Inbetriebnahme lesen.
- Die Sicherheitshinweise müssen jederzeit befolgt werden.
- Stellen Sie sicher, dass das Gerät galvanisch isoliert ist, bevor Sie die SIM-Karte einstecken.

Bestimmungsgemäßer Gebrauch

Warnung

Gefahr von Personenschaden und Geräteschaden

- Gerät nur bestimmungsgemäß nutzen.
- Gerät nur in Übereinstimmung mit den elektrischen und technischen Daten, wie auf dem Datenblatt und im Kapitel Technische Daten beschrieben, betreiben.
- Gerät nur gemäß den Beschreibungen in diesem Handbuch montieren bzw. demontieren.
- Gerät mit großer Sorgfalt transportieren und lagern.

Umgang mit Kabeln

Warnung

Gefahr von elektrischem Schock durch falschen Umgang mit Kabeln

- Netzkabel immer am Stecker, niemals am Kabel aus der Steckdose ziehen.
- Niemals Kabel ohne Kantenschutz über scharfe Ecken oder Kanten führen.
- Einen ausreichenden Entlastungszug für die Kabel sicherstellen.

Antennenmontage

Achtung

Gefahr von verringerter Übertragung und Empfang

- Beim Führen des Antennenkabels den Biegeradius beachten.
- Der minimale Biegeradius für Kabel darf niemals die folgenden Werte unterschreiten:
  - Statische Kabel: 5-facher eigener Durchmesser
  - Dynamische Kabel: 15-facher eigener Durchmesser

HF-Exposition (hochfrequente elektromagnetische Felder)

Warnung

Gefahr von Störung und Beschädigung anderer Geräte durch Funksender

- Niemals das Gerät in einer Umgebung nutzen, in der der Betrieb von Funksendern untersagt ist.
- Menschen mit Hörgeräten oder Herzschrittmachern dürfen nicht in die Nähe des Gerätes gelangen. Im Zweifel fragen Sie Ihren Arzt oder den Hersteller des medizinischen Gerätes um Rat.
- Die internen und externen Antennen des Gerätes dürfen nur mit einem Mindestabstand von 20 cm von Menschen entfernt installiert und betrieben werden.

Warnung

Gefahr von Sachschaden und Datenverlust durch Entmagnetisierung

- Keine Disketten, Kreditkarten oder andere magnetische Datenträger in der Nähe des Gerätes lagern.

Vorsicht

Gefahr von Rechtsbruch und Störung anderer Transmitter

- Beachten Sie die gesetzliche Begrenzung für elektromagnetische Felder (0 Hertz bis 300 Gigahertz) in öffentlichen Räumen, wenn eine Richtantenne verwendet wird. Details siehe Empfehlungen des EU Rates 199/519/EG vom 12. Juli 1999.
- Die internen und externen Antennen des Gerätes dürfen nur mit einem Mindestabstand von 20 cm von Menschen entfernt installiert und betrieben werden.
- Die Antennen müssen so installiert und betrieben werden, dass sie nicht mit anderen Antennen oder Transmittern interagieren.

Externe Stromversorgung

Warnung

Gefahr von Geräteschaden durch falsche Stromversorgung

- Nur Stromversorgung verwenden, die konform mit der Richtlinie DIN EN62368-1 Annex Q ist.
- Die Ausgangsspannung der Stromversorgung darf 60 V_{DC} nicht überschreiten.
- Die Leistung der externen Stromversorgung muss kurzschlussfest sein.

Warnung

Gefahr von Geräteschaden durch fehlerhaften Anschluss an Batterie

- Sicherstellen, dass sich zwischen dem Gerät und der Batterie bzw. aufladbaren Batterie eine allpolige Abschalteinrichtung (Batteriehauptschalter) mit ausreichender Trennungskapazität und eine Sicherung mit ausreichender Trennungskapazität (Sicherung Batterie 32 V, 3 A) befindet.

Warnung

Gefahr von Geräteschaden durch unzulässige Stromzufuhr

- Nur Stromversorgungsgeräte verwenden, die mit der Richtlinie IEV/EN 62368-1 Annex Q „Limited Power Source“ konform sind.
- Die externe Stromversorgung muss außerdem die Anforderungen für NEC Class 2 circuit as defined in the National Electric Code (ANSI/NFPA 70) erfüllen.

–

Schalteingang und Schaltausgang

Warnung

Gefahr von Verletzungen und Sachschaden durch unzulässige Spannung

- Der Schalteingang und der Schaltausgang sind gegen die anderen Anschlüsse des TAINY IQ-LTE elektrisch isoliert. Wenn die an TAINY IQ-LTE angeschlossene Fremdanlage ein Signal des Schalteingangs und des Schaltausgangs mit einem Signal der Stromversorgung des TAINY IQ-LTE (galvanisch) verbindet, darf die Spannung der einzelnen Signale des Schalteingangs und des Schaltausgangs sowie der Stromversorgung 60 V nicht überschreiten.

Vorsicht: Gebühren

Vorsicht

Gefahr von zusätzlichen Gebühren

- Bedenken Sie, dass der Austausch von Datenpaketen, unabhängig davon, ob die Verbindung zu einer Gegenstelle beständig besteht oder neu aufgebaut wird, Gebühren verursacht.
- Erfolglose Verbindungsaufbauversuche zu falschen Adressen oder abgeschalteten Gegenstellen können ebenfalls Gebühren verursachen.

Firmware with open source GPL/LGPL

The firmware for TAINY IQ-LTE contains open source software under GPL/LGPL conditions. We provide you with the source code in accordance with Section 3b of GPL and Section 6b of LGPL. You can find the source code on our webpage, www.neuhaus.de.

As an alternative, you can also request the source code from us on CD-ROM. Send your email to Kundendienst@neuhaus.de. Please enter "Open Source iQ" in the subject line of your email so that we can easily filter out your message.

The license conditions for the open source software can be found in the source code on the product CD.

Firmware with OpenBSD

The firmware of the TAINY IQ-LTE contains parts from the OpenBSD software. Whenever OpenBSD software is used, the following copyright note must be reproduced:

```
* 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.
```

3 Installation

3.1 Schritt für Schritt

Bitte lesen Sie immer sorgfältig die genannten Kapitel. Dieser Abschnitt ist keine Kurzanleitung oder gar ein Ersatz für die gesamte Anleitung.

TAINY IQ-LTE wird in den folgenden Schritten in Betrieb genommen:

Schritt		Kapitel
1.	Machen Sie sich zuerst mit den Voraussetzungen für den Betrieb des TAINY IQ-LTE vertraut.	1
2.	Lesen Sie unbedingt vor der Installation die Sicherheitshinweise und die Anweisungen in diesem Handbuch sorgfältig durch. Gehen Sie sicher, diese vollständig verstanden zu haben.	2,3
3.	Machen Sie sich vor der Installation unbedingt mit den Bedienelementen, den Anschlüssen und Statusanzeigen für den Betrieb des TAINY IQ-LTE vertraut.	3.2
4.	Trennen Sie TAINY IQ-LTE von der Stromversorgung.	3.3
5.	Verbinden Sie den Webbrowser Ihres Rechners mit einer der lokalen Schnittstellen (10/100 BASE-T) des TAINY IQ-LTE.	4.4
6.	Geben Sie die PIN (persönliche Identifikationsnummer) Ihrer SIM-Karte(n) auf der Benutzeroberfläche des TAINY IQ-LTE ein.	6.4
7.	Führen Sie die SIM-Karte(n) in das Gerät ein.	3.11
8.	Schließen Sie die Antenne an.	3.6
9.	Schließen Sie TAINY IQ-LTE an die Stromversorgung an.	3.3
10.	Richten Sie TAINY IQ-LTE gemäß Ihren Anforderungen ein.	4 bis 15
11.	Schließen Sie Ihre lokale Applikation an.	3.4

3.2 Voraussetzungen und Informationen

Um TAINY IQ-LTE in Betrieb nehmen zu können, müssen die folgenden Informationen zur Verfügung stehen und die folgenden Bedingungen erfüllt sein:

Antennen	Eine oder zwei Antennen wie in Kapitel 3.6 beschrieben
Stromversorgung	Installation für 24 V: siehe Kapitel 3.3
SIM-Karte	Eine SIM-Karte des ausgewählten GSM-Netzbetreibers
PIN	Die PIN-Nummer der SIM-Karte
Aktivierung von HSPA+/UMTS EGPRS/GPRS	Der Netzbetreiber muss die folgenden Dienste auf Ihrer SIM-Karte freigeschaltet haben: LTE, HSPA+, UMTS-Daten und/oder EGPRS oder GPRS. Die folgenden Zugangsdaten müssen bekannt sein: - Name des Zugangspunktes (Access Point Name – APN) - Benutzername - Passwort

3.3 Anschluss an 24V/0V Versorgung

Bitte Lessen Sie die Sicherheitshinweise vor der Installation sorgfältig durch.

TAINY IQ-LTE wird mit Gleichstrom von 12 bis 60 V_{DC} betrieben, nominal 24 V_{DC}.

Die externe Stromzufuhr wird an die beiden Anschlussklemmen auf der linken Seite des Gerätes angeschlossen.

Der Stromverbrauch beträgt ungefähr 450 mA bei 12 V und 100 mA bei 60 V (I_{Burst}>1.26 A).

Warnung

Gefahr von Verletzungen und Sachschaden durch unzulässige Spannung

- Der Schalteingang und der Schaltausgang sind gegen die anderen Anschlüsse des TAINY IQ-LTE elektrisch isoliert. Wenn die an TAINY IQ-LTE angeschlossene Fremdanlage ein Signal des Schalteingangs und des Schaltausgangs mit einem Signal der Stromversorgung des TAINY IQ-LTE (galvanisch) verbindet, darf die Spannung der einzelnen Signale des Schalteingangs und des Schaltausgangs sowie der Stromversorgung 60 V nicht überschreiten.

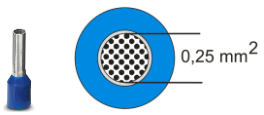
Anschlussklemmen

1. Um eine verlässliche und berührungssichere Verbindung herzustellen, ziehen Sie die Isolation des Kabels ab, wie in der folgenden Tabelle beschrieben.
2. Verwenden Sie Aderendhülsen für flexible Kabel.
3. Verschließen Sie ungenutzte Anschlussklemmen.

Querschnitt steif/flexibel	0,2–2,5 mm²
AWG (American wire gauge)	24–14
Isolation auf folgende Länge entfernen L	7 mm
Vorgegebenes Drehmoment	0,5–0,6 Nm/ 4,4–5,3 lb in

Maximal zulässiger Querschnitt für flexible Kabel mit Aderendhülsen **ohne** Kunststoffhülle: 2,5 mm².

Maximal zulässiger Querschnitt für flexible Kabel mit Aderendhülsen **mit** Kunststoffhülle: 0,25 mm².



3.4 Ethernet-Ports (ETH0, ETH1, ETH2, ETH3, ETH4, ETH5)

An die Ethernet-Ports ETH1 bis ETH5 (10/100 Base-T) der 6E-Variante und ETH1 der E2-Variante wird das lokale Netz mit den lokalen Applikationen angeschlossen, wie z.B.: programmierbare Steuerungen, Maschinen mit Ethernet-Schnittstelle zur Fernüberwachung, ein Notebook oder Rechner.

TAINY iQ dient zwischen den verfügbaren Schnittstellen als Schalter.

Zum Einrichten des TAINY iQ schließen Sie hier den Admin-Rechner mit Webbrowser an.

Der Ethernet-Port ETH0 ist eigentlich dafür vorgesehen, eine kabelgebundene WAN-DSL/LAN-Verbindung herzustellen, allerdings kann er auch als zusätzlicher Port zum Anschluss des lokalen Netzes mit lokalen Applikationen verwendet werden, siehe Kapitel 9.3.

Verwenden Sie CAT5-Kabel. Alle Schnittstellen unterstützen Auto-negotation. Daher wird automatisch erkannt, ob eine Übertragungs-geschwindigkeit von 10 MBit/s oder 100 MBit/s im Ethernet genutzt wird und ob ein Cross-Over oder Eins-zu-eins-Kabel verwendet wird.

3.5 Ethernet-Ports (ETH0 und ETH1)

An den Ethernet-Port ETH1 (10/100 Base-T) wird das lokale Netz mit den lokalen Applikationen angeschlossen, wie z.B.: programmierbare Steuerungen, Maschinen mit Ethernet-Schnittstelle zur Fernüberwachung, ein Notebook oder Rechner.

TAINY IQ-LTE dient zwischen den verfügbaren Schnittstellen als Schalter.

Zum Einrichten des TAINY IQ-LTE schließen Sie hier den Admin-Rechner mit Webbrowser an.

Der Ethernet-Port ETH0 ist eigentlich dafür vorgesehen, eine kabelgebundene WAN-DSL/LAN-Verbindung herzustellen, allerdings kann er auch als zusätzlicher Port zum Anschluss des lokalen Netzes mit lokalen Applikationen verwendet werden, siehe Kapitel 9.3.

Verwenden Sie CAT5-Kabel. Alle Schnittstellen unterstützen Auto-negotiation. Daher wird automatisch erkannt, ob eine Übertragungs-geschwindigkeit von 10 MBit/s oder 100 MBit/s im Ethernet genutzt wird und ob ein Cross-Over oder Eins-zu-eins-Kabel verwendet wird.

3.6 Antennenanschluss

2

TAINY IQ-LTE verfügt über zwei MIMO-Antennenbuchsen des Typs SMA zum Anschluss der Antenne.

Stellen Sie sicher, dass während des Betriebs immer eine Antenne an TAINY IQ-LTE angeschlossen ist.

Anforderungen an die Antenne:

Passiv, azimutal omnidirektional, vertikale Polarisation, Gewinn < 1,5 dBi, VSWR < 2,0:1, Impedanz 50 Ω, angepasst für die genutzten Frequenzbänder. In Kapitel 19 finden Sie eine Liste der unterstützten Frequenzbänder.

Welche Frequenzbänder am Einsatzort tatsächlich genutzt werden, ist abhängig vom Land und dem Netzbetreiber. Erfragen Sie diese Informationen beim Netzbetreiber.

Vorsicht

Gefahr von Sachschaden und Störung anderer Geräte

- Verwenden Sie ausschließlich Antennen aus dem Zubehörsortiment des TAINY IQ-LTE: Diese Antennen sind von uns getestet und verfügen über alle beschriebenen Produkteigenschaften.

Achtung

Gefahr von verminderter Datenübertragung und Empfang

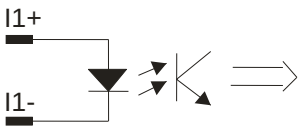
- Bei der Montage sollte ein ausreichend gute Signalqualität sichergestellt werden (CSQ > 11).
- Beachten Sie dazu die Signalleuchten des TAINY IQ-LTE oder die Benutzeroberfläche Status-Übersicht, siehe Kapitel 4.1.
- Stellen Sie sicher, dass sich keine großen Metallobjekte, wie z. B. Stahlbeton, in der Nähe der Antenne befinden.
- Lesen Sie die Montageanleitung und das Benutzerhandbuch der verwendeten Antenne vor der Montage sorgfältig durch.

3.7 Digital Eingabe/Ausgabe

Digital Eingabe

6

TAINY IQ-LTE besitzt einen Schalteingang. Die Anschlussklemmen sind gekennzeichnet mit I1+/I1-.



U_{In} = 5…30 V; An: $U_{In} \geq$ 5 V; Aus: $U_{In} \leq$ 1,2 V

Dieser Port ist der Schalteingang. Für die WAN-Setup-Betriebsregeln siehe Kapitel 6.3.

Warnung:

Gefahr von Verletzung und Sachschaden durch unzulässige Spannung

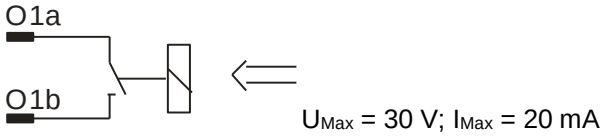
- Der Schalteingang und der Schaltausgang sind gegen die anderen Anschlüsse des TAINY IQ-LTE elektrisch isoliert. Wenn die an TAINY IQ-LTE angeschlossene Fremdanlage ein Signal

	des Schalteingangs und des Schaltausgangs mit einem Signal der Stromversorgung des TAINY IQ-LTE (galvanisch) verbindet, darf die Spannung der einzelnen Signale des Schalteingangs und des Schaltausgangs sowie der Stromversorgung 60 V nicht überschreiten.

Schaltausgang O1a/O1b

6

TAINY IQ-LTE besitzt einen Schaltausgang. Die Anschlussklemmen sind gekennzeichnet: O1a/O1b.



Dieser Port ist der Schaltausgang. Für die WAN-Setup- Betriebsregeln siehe Kapitel 6.3. Ist der Schaltausgang aktiviert, ist der Schalter geschlossen.

Warnung

Gefahr von Verletzung und Sachschaden durch unzulässige Spannung

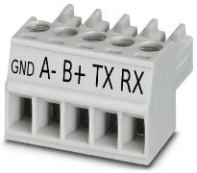
- Der Schalteingang und der Schaltausgang sind gegen die anderen Anschlüsse des TAINY IQ-LTE elektrisch isoliert. Wenn die an TAINY IQ-LTE angeschlossene Fremdanlage ein Signal des Schalteingangs und des Schaltausgangs mit einem Signal der Stromversorgung des TAINY IQ-LTE (galvanisch) verbindet, darf die Spannung der einzelnen Signale des Schalteingangs und des Schaltausgangs sowie der Stromversorgung 60 V nicht überschreiten.

3.8 Serielle RS232 Schnittstelle

RS232

5

TAINY IQ-LTE besitzt eine RS232 Schnittstelle mit folgender Stecker Belegung:



TX	Transmit Data	Leitung für ausgehende (von DTE gesendete) Daten (negative Logik)
RX	Receive Data	Leitung für eingehende (von DTE zu empfangende) Daten (negative Logik).
A-	Data (A-)	**RS485 Schnittstelle ! Diese Funktion wird derzeit nicht unterstützt**
B+	Data (B+)	**RS485 Schnittstelle ! Diese Funktion wird derzeit nicht unterstützt**
GND	Ground	Gemeinsame Masse Verbindung

3.9 Signalleuchten

Signalleuchten TAINY IQ-LTE ist ausgestattet mit einer Reihe von Signalleuchten, die den Betriebszustand anzeigen.

Stromversorgungssignal

LED	Status	Bedeutung
POWER	Immer AUS	Keine Netzspannung vorhanden oder defekt
	Immer AN	In Betrieb

WAN-Status-Signal

LED	Status	Bedeutung
SIM	Konstant AUS	Keine SIM-Karte aktiv
	Konstant AN	SIM-Karte 1 aktiv
	Blinkend	SIM-Karte 2 aktiv
S (Status)	Blinkend	Nicht im mobilen Funknetz registriert
	Konstant AN	WAN-IP-Verbindung vorhanden (Mobil oder Ethernet)
Q (Qualität)	Blinkt langsam	Wählt sich ins GMS-Netz ein
	Blinkt 1-mal mit Intervall	Feldstärke schwach
	Blinkt 2-mal mit Intervall	Feldstärke mittelmäßig
	Blinkt 3-mal mit Intervall	Feldstärke gut
	Konstant AN	Feldstärke sehr gut
	Konstant AUS	Feldstärke nicht vorhanden
C (Verbindung)	Immer AUS	Keine Verbindung
	Blinkt 1-mal mit Intervall	GPRS-/EDGE-Verbindung
	Blinkt 2-mal mit Intervall	LTE/UMTS-Verbindung
	Blinkt 3-mal mit Intervall	LAN-Verbindung

VPN- und IO-Status-Signal

LED	Status	Bedeutung
VPN	Konstant AUS	Kein VPN-Tunnel aufgebaut
	Konstant AN	Ein oder mehrere VPN-Tunnel aufgebaut
IN	Konstant AUS	Eingang nicht aktiviert
	Konstant AN	Eingang aktiviert
OUT	Konstant AUS	Ausgang nicht aktiviert
	Konstant AN	Ausgang aktiviert

Ethernet-Ports-Status-Signale

Jeder Ethernet-Port ETH ist mit einer gelben und einer grünen LED ausgestattet, die den Betriebsstatus des Ports anzeigt.

LED	Status	Bedeutung
Grün	Konstant AN	Link hergestellt
	Konstant AUS	Kein Link hergestellt
Gelb	Blinkt	Daten werden übermittelt

3.10 Servicetaster

An der Vorderseite des TAINY IQ-LTE befindet sich ein kleines Loch, in dem sich ein Taster befindet. Benutzen Sie einen dünnen Gegenstand, z. B. eine aufgebogene Büroklammer, um den Taster zu drücken.

➲ Wenn Sie den Taster während des Betriebs länger als 5 Sekunden drücken, wird TAINY IQ-LTE auf die Werkseinstellung zurückgesetzt.

3.11 SIM-Karten-Halter

Achtung

Bevor Sie die SIM-Karte einschieben, geben Sie die PIN-Nummer der SIM-Karte in die Benutzeroberfläche des TAINY IQ-LTE ein, siehe Kapitel 6.4.

1. Nachdem Sie die PIN der SIM-Karte eingegeben haben, trennen Sie TAINY IQ-LTE komplett von der Stromversorgung.

2. Die Schubfächer für die SIM-Karte(n) befinden sich auf der Rückseite des Gerätes. Direkt neben jedem Schubfach befindet sich im Gehäuse ein kleiner gelber Taster. Drücken Sie auf den Taster mit einem spitzen Gegenstand wie z. B. einem Bleistift.

   Drücken Sie solange auf den Taster, bis der SIM-Karten-Halter aus dem Gehäuse kommt.

3. Platzieren Sie die SIM-Karte so in das Schubfach, dass die goldbeschichteten Kontakte sichtbar bleiben.

4. Schieben Sie das Schubfach mit der SIM-Karte komplett in das Gehäuse zurück und nehmen das Gerät wieder in Betrieb.

Vorsicht

Gefahr von Beschädigung oder Verlust der SIM-Karte oder des Gerätes

- Schieben oder entfernen Sie die SIM-Karte unter keinen Umständen während des Betriebs in das bzw. aus dem Gerät.

3.12 Montage

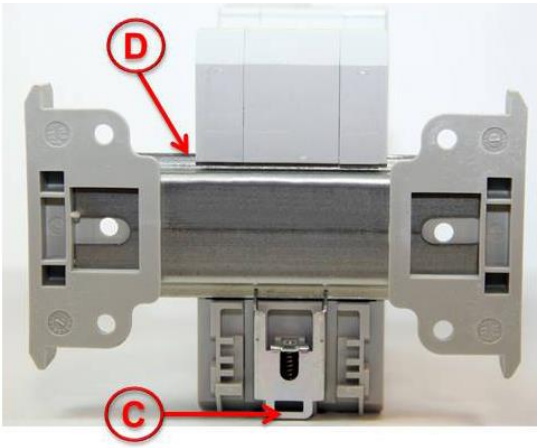
TAINY IQ-LTE ist zur Montage auf einer Hutschiene in Übereinstimmung mit DIN EN 50022 (3,5mm x 7,5mm) geeignet.
Die entsprechende Halterung befindet sich auf der Rückseite des Gerätes.

Warnung

Gefahr von Verletzung oder Sachschaden durch spannungsführende Bauteile

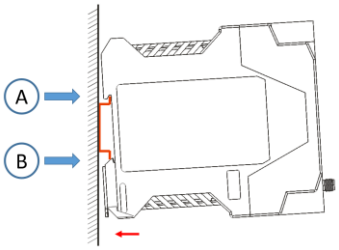
- Decken Sie nach der Installation des TAINY IQ-LTE den Bereich der Anschlussklemmen (digitale Eingabe und Ausgabe oder 24-V-Anschlussklemmen) ab, um eine unbeabsichtigte Berührung der spannungsführenden Bauteile zu verhindern.
- Verhindern Sie das Eindringen von Fremdkörpern wie z. B. Schrauben, Papierklammern oder andere metallischen Gegenständen.

Auf der Rückseite hat TAINY IQ-LTE eine Einbuchtung (D), die oben in die Hutschiene eingehängt wird. Mit einem Metall-verschluss (C) wird das TAINY IQ-LTE unten an der Hutschiene befestigt.
Ziehen Sie die Verschlüsse mit einem Schraubendreher nach unten, um sie wieder zu lösen.



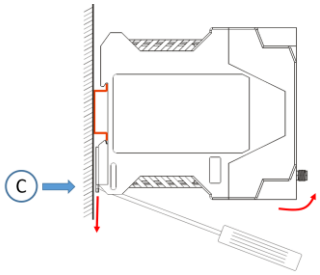
Montage:

Haken Sie TAINY IQ-LTE oben auf der Hutschiene ein (A). Drücken Sie den unteren Teil von TAINY IQ-LTE vorsichtig gegen die Hutschiene (B), bis es dort einrastet.



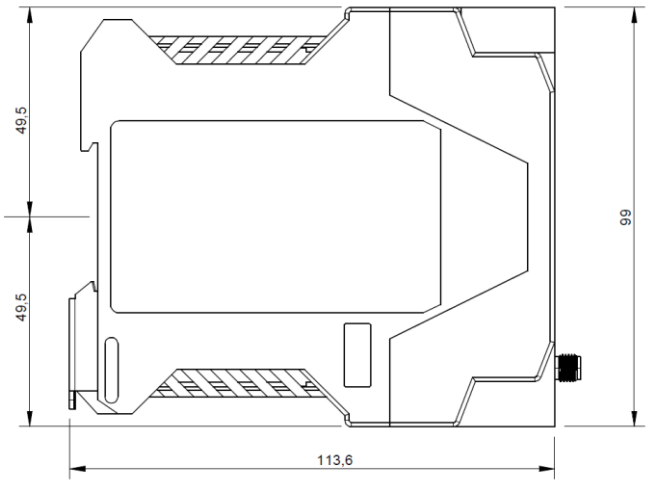
Demontage:

Verwenden Sie einen Flachkopf-Schraubendreher, um zuerst die rechte Befestigung des TAINY IQ-LTE von der Hutschiene (C) zu lösen.



Montage:

Position der Hutschiene:



[mm]

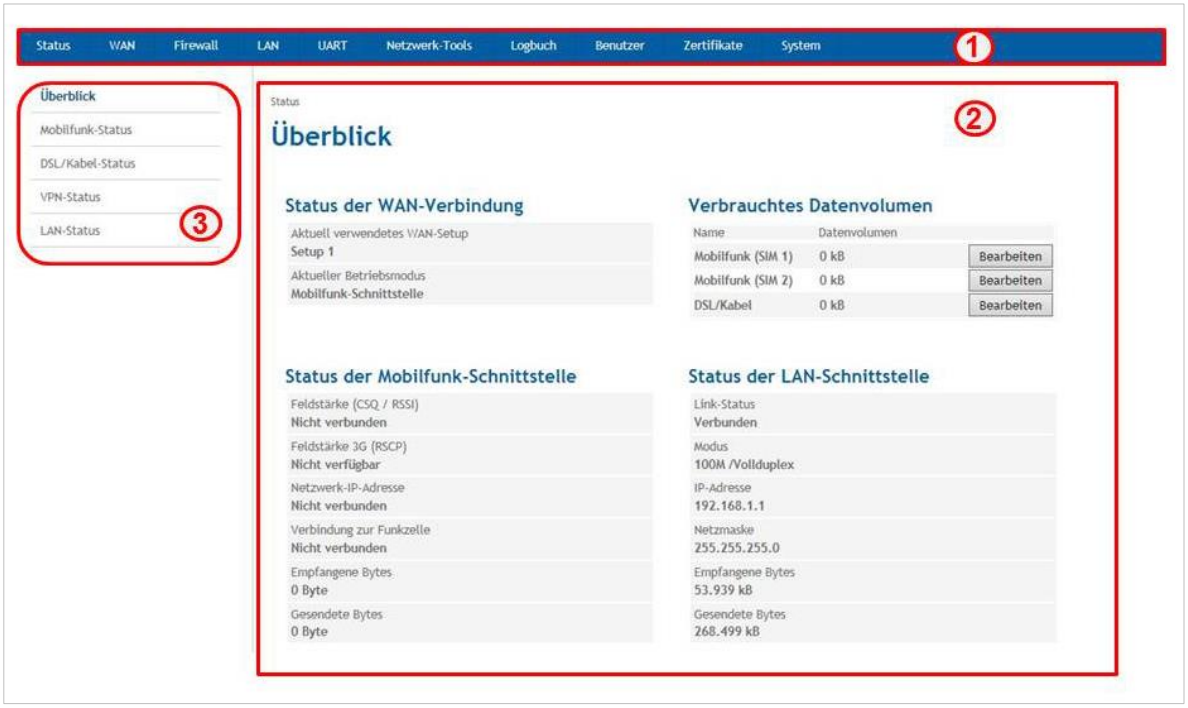
4 Konfiguration

4.1 Überblick Benutzeroberfläche

Die Konfiguration des TAINY IQ-LTE wird in den verschiedenen Registern der Benutzeroberfläche vorgenommen. Jedes Register ist gleich aufgebaut: Registerleiste (1), Menü (3) und Dialogbox (2).

Aus Illustrationsgründen wird das in der linken Textspalte abgebildete Menü nur jeweils mit dem gerade beschriebenen Register abgebildet.

Beachten Sie außerdem, dass einige der in der Dialogbox gezeigten Konfigurationsmöglichkeiten von Produktvariante zu Produktvariante unterschiedlich sein können. Die zutreffenden Varianten sind in der linken Textspalte entsprechend aufgeführt.



Tipp

Beachten Sie, dass die Namen, die Sie in die Felder `Name` eingeben, z. B. für ein neues Netzwerk, 20 Zeichen nicht überschreiten.

4.2 Übersicht

Die Konfigurationen der Funktionen des TAINY IQ-LTE werden lokal oder remote über die webbasierte Benutzeroberfläche des TAINY IQ-LTE ausgeführt.

Remote-Konfiguration

Der Remote-Zugriff auf den Webserver wird entweder durch bestimmte Einstellungen der Firewall oder die Standardeinstellung des VPN-Tunnels über HTTPS möglich.

Konfiguration über die lokale Schnittstelle

Folgende Voraussetzungen zur Erstkonfiguration über die lokale Schnittstelle müssen erfüllt sein:

- Der Rechner (Admin PC), mit dem die Konfiguration ausgeführt wird, muss entweder
  - direkt an einen der Ethernet-Ports des TAINY IQ-LTE mittels Netzkabel angeschlossen sein

  oder
  - über das lokale Netz direkten Zugriff auf TAINY IQ-LTE haben.

- Standardmäßig ist der LAN Port ETH1 des TAINY IQ-LTE Teil des lokalen Netzwerks mit der IP-Adresse 192.168.1.1 und Subnetzmaske 255.255.255.0

Nehmen Sie die folgenden Einstellungen an Ihrem Rechner vor:

- 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 192.168.1.x** verwenden, außer den Adressen 192.168.1.0, 192.168.1.1 und 192.168.1.255.

- Wenn Sie mit dem Admin-PC über TAINY IQ-LTE auch auf ein externes Netz zugreifen wollen, sind zusätzlich die folgenden Einstellungen erforderlich:

  Standardgateway: **192.168.1.1**

  Bevorzugter DNS-Server: **Adresse des Domain-Name-Servers**

Siehe Kapitel 9.3, falls ETH0 auch als LAN-Port verwendet werden soll.

4.3 Zulässige Zeichen für Benutzernamen, Passwörter und weitere Eingaben

Zulässige Zeichen

Die folgenden ASCII-Zeichen sind für Benutzernamen, Passwörter, Hostnamen, APN und PIN zulässig:

Benutzer-namen und Passwörter	# @ ~ % $, * ' = ! + - \ / ? ( ) { } . : ; [ ] _ | 0 1 2 3 4 5 6 7 8 9 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
Hostnamen und APN	. - 0 1 2 3 4 5 6 7 8 9 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
PIN	Für PIN-Eingaben werden nur numerische Eingaben unterstützt. 0 1 2 3 4 5 6 7 8 9

Einige Parameter erlauben weitere Sonderzeichen.

4.4 Konfigurationsverbindung herstellen

Webbrowser einrichten

Gehen Sie wie folgt vor:

Starten Sie den Webbrowser (z.B. MS Internet Explorer ab Version 11, Mozilla Firefox ab Version 37 oder Chrome ab Version 64).

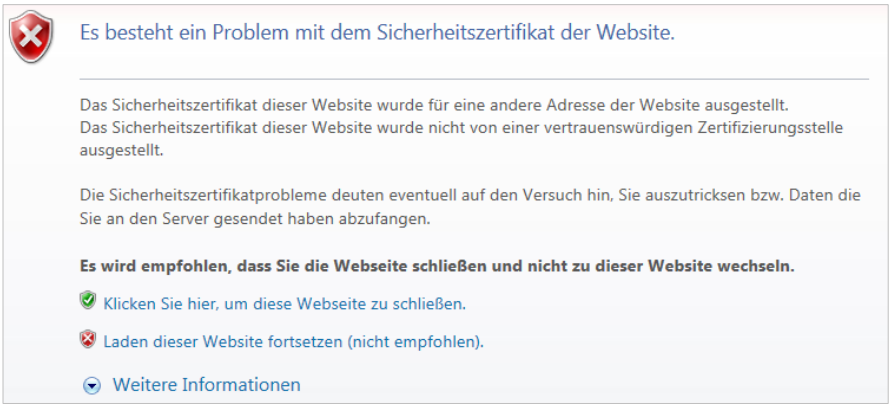
Startseite des TAINY IQ-LTE öffnen

Geben Sie die vollständige Adresse des TAINY IQ-LTE in die Adresszeile des Browsers ein.

Werkseinstellung lautet: https://192.168.1.1

Ergebnis: Es erscheint ein Sicherheitshinweis.
Für den Internet Explorer 7 zum Beispiel der folgende:

Sicherheitshinweis bestätigen



Bestätigen Sie den Sicherheitshinweis mit „Laden dieser Webseite fortsetzen …“.

Tipp

Da das Gerät nur über einen verschlüsselten Zugriff administriert werden kann, wird es mit einem selbstsignierten Zertifikat geliefert. Befindet sich auf dem Zertifikat eine dem Betriebssystem unbekannte Signatur, wird ein Sicherheitshinweis generiert. Sie können sich das Zertifikat anzeigen lassen.

Es muss deutlich aus dem Zertifikat hervorgehen, dass es für Sagemcom Dr. Neuhaus GmbH ausgestellt wurde. Da die Web-Benutzeroberfläche über eine IP-Adresse und nicht über einen Namen adressiert wird, ist der Name im Sicherheitszertifikat ein anderer als im Zertifikat.

Geben jetzt den Benutzernamen und das Passwort ein, um sich anzumelden.

Benutzername und Passwort eingeben

Die Werkseinstellungen sind:

Benutzername:	**admin**
Passwort:	**<Seriennummer des Gerätes>**
Beispiel	*15044201*

Tipp

Sie sollten nach dem ersten Einloggen dringend das Passwort ändern. Die Werkseinstellungen sind weitläufig bekannt und bieten somit keinen ausreichenden Schutz. Lesen Sie in Kapitel 13, wie das Passwort geändert wird.

Drücken Sie auf „**Einloggen**“, um die Startseite zu öffnen.

Tipp

Um sich erfolgreich am TAINY IQ-LTE anzumelden, aktivieren Sie die Cookies Ihres Browsers.

Tipp

Es erscheint im Anmeldedialog ein Auswahlmenü für die Anmeldung über TACACS+ / Radius oder für eine normale lokale Anmeldung, die auch bei der Inbetriebnahme genutzt wird.

Weitere Informationen zur Anmeldung über TACACS+ siehe Kapitel 13.2 und Glossar sowie Kapitel 13.3 und Glossar.

Die Startseite wird angezeigt	Nach der Eingabe des Benutzernamens und des Passworts erscheint die Startseite des TAINY IQ-LTE im Webbrowser. Sie sehen eine Status-Übersicht zum Betrieb des Gerätes, Details siehe Kapitel 5.

4.5 Konfigurationsverbindung beenden

Log-out	Drücken Sie auf den *Log-out*-Button oben rechts im Fenster, um sich manuell abzumelden. Die Konfigurationsverbindung zu TAINY IQ-LTE ist damit beendet. Der Webserver kehrt zum Startbildschirm zurück. Um die Konfigurationsverbindung wieder herzustellen, geben Sie Ihren Benutzernamen und das Passwort wie in 4.4 beschrieben erneut ein.

5 Status

5.1 Status-Überblick abfragen

Überblick

Öffnen Sie das Register **`Status`** und wählen Sie im Menü „**`Überblick`**“.

Nach dem erfolgreichen Einloggen in die Web-Benutzeroberfläche wählen Sie das Register **`Status`** aus. Es wird ein Überblick zum aktuellen Betriebsstatus des TAINY IQ-LTE angezeigt. Im Detail sind es die Status zu:

- WAN-Verbindung
- Mobilfunk-Schnittstelle
- Verbrauchtes Datenvolumen
- DSL/Kabel-Schnittstelle
- Aktivierte LAN-Schnittstelle

Tipp

Die angezeigten Werte werden automatisch von TAINY IQ-LTE aktualisiert.

`Feldstärke:` Gibt die Stärke des empfangenen Signals des Mobilfunknetzes als CSQ-Wert (siehe Glossar) und RSSI-Wert wieder.

`Empfangene Bytes/Gesendete Bytes:` Anzahl der seit Verbindungsaufbau empfangenen und gesendeten Bytes an. Wird die Verbindung neu aufgebaut, wird der Zähler zurückgesetzt.

`Netzwerk-IP-Adressen:` Angezeigt werden die vom Provider bereitgestellte IPv4 und falls zugeteilt die IPv6 Adresse

Verbrauchtes Datenvolumen

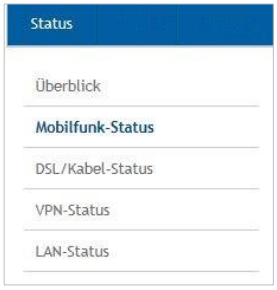
Legt fest, in welchem Intervall der Wert des verbrauchten Datenvolumens auf Null zurückgesetzt wird. Werkseitig ist monatlich eingestellt (zu jedem Ersten eines Monats). Um das Intervall zu ändern, wählen Sie die gewünschte Option aus der Liste „`Rücksetzmodus`“ aus.

Um den Wert sofort auf Null zu setzen, drücken Sie „**`Zurücksetzen`**“ unter „`Jetzt Zurücksetzen`“.

5.2 Mobilfunknetz-Status abfragen

Status Mobilfunknetz

Öffnen Sie das Register **`Status`** und wählen Sie im Menü „**`Mobilfunk`**“.



Hier finden Sie Informationen zu Signalstärke, Signalqualität, zum genutzten Mobilfunknetz, zur SIM-Karte und zum im TAINY IQ-LTE eingebauten Mobilfunk-Modul.

Informationen zu CSQ, LAC (Cell ID), IMCI, ICCID, IMEI siehe Glossar.

Tipp

Die angezeigten Werte werden automatisch von TAINY IQ-LTE aktualisiert.

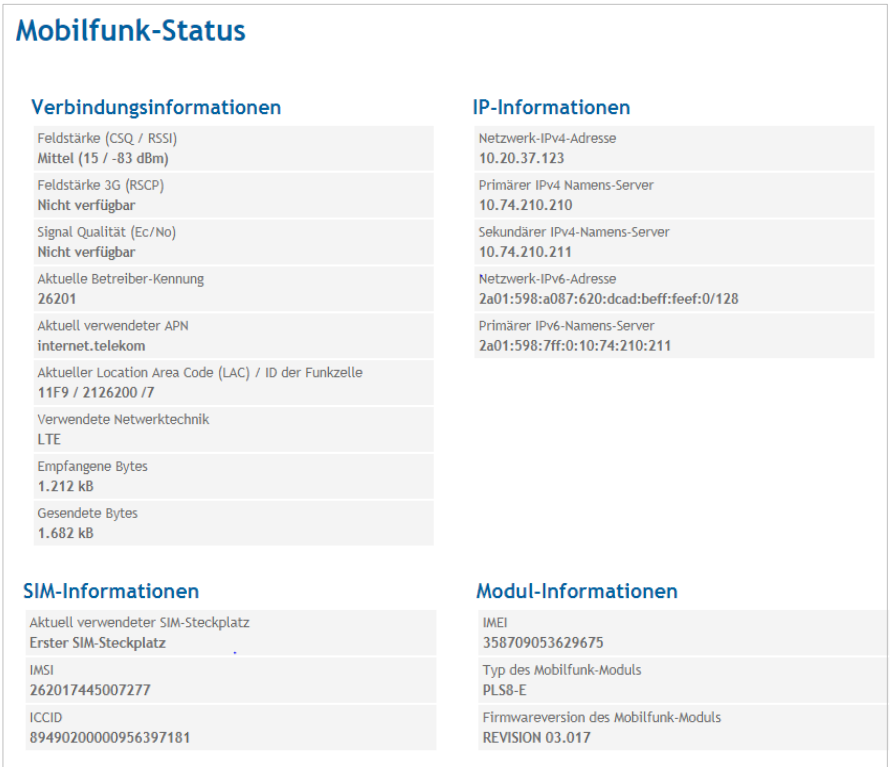
`Empfangene Bytes/Gesendete Bytes:` Anzahl der seit Verbindungsaufbau empfangenen und gesendeten Bytes. Wird die Verbindung neu aufgebaut, wird der Zähler zurückgesetzt.

`Typ des Mobilfunk-Moduls/Firmware Version des Mobilfunk-Moduls:`

TAINY IQ-LTE ist mit einem Mobilfunk-Modul ausgestattet, das als Funkschnittstelle dient. Es übernimmt die gesamte Kommunikation über das Funknetzwerk.

Außerdem wird die **`Firmware Version des Mobilfunk-Moduls`** angezeigt.

Beispiel Darstellung des Mobilfunk Status



IP-Informationen

Netzwerk-IPv4-Adressen und Netzwerk-IPv6-Adressen:

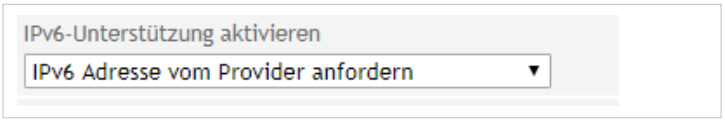
Angezeigt werden die vom Provider bereitgestellte IPv4 Adresse und falls zugeteilt die IPv6 Adresse mit den zugehörigen Namens-Server für IPv4 und IPv6.

Hinweis

Die Zuteilung einer IPv6 Adresse ist abhänig davon, ob der verwendete Internet Provider die Vergabe von IPv6 Adressen im Mobilen Datennetz unterstützt.

Die Erreichbarkeit mit IPv6 aus dem Internet ist abhängig vom Mobilfunkbetreiber und den abgeschlossenen Vertrag mit dem Betreiber. Mobilfunkbetreiber können private APN (access point name) für die Verwendung von ausgehenden und eingehenden IPv6 Verbindungen voraussetzen.

Außerdem muss bei den Mobilfunk Einstellungen die IPv6-Unterstützung aktiviert werden.



Mit der Einstellung IPv6 Adresse vom Provider anfordern wird diese Funktion bereit gestellt.

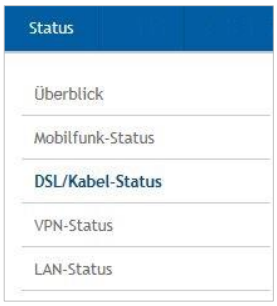
Falls keine IPv6 Adresse bezogen wurde, entfällt die Anzeige für IPv6 Adresse.

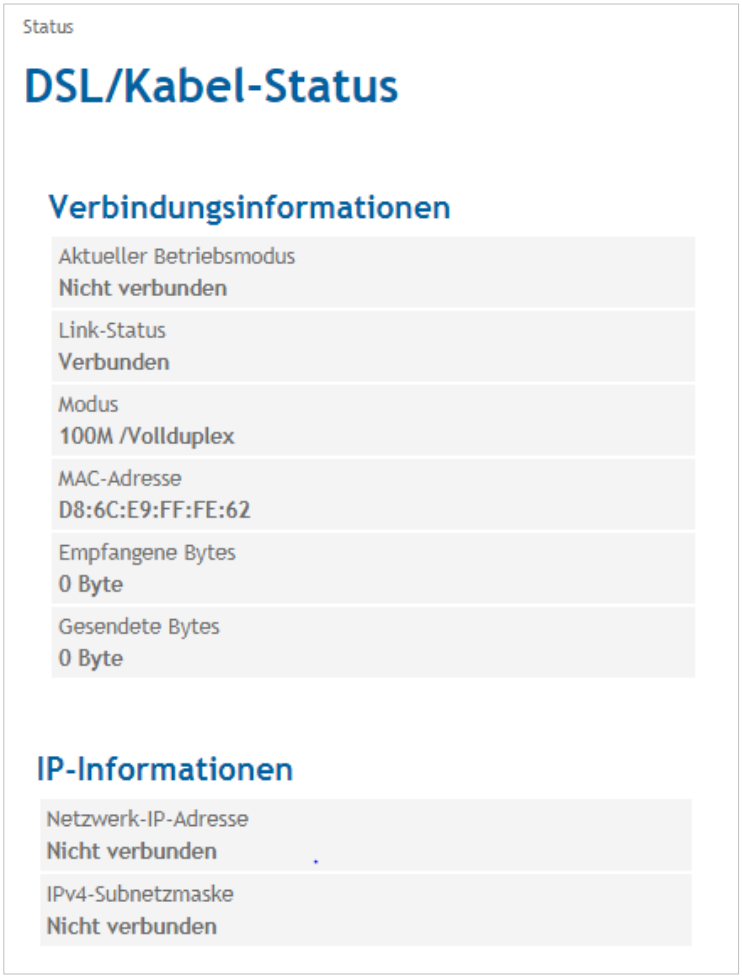
Der Provider muss die Vergabe von IPv6 Adressen unterstützen!

5.3 DSL/Kabel-Status abfragen

DSL/Kabel-Status

Öffnen Sie das Register **Status** und wählen Sie im Menü „**DSL/Kabel-Status**“.





IP-Informationen

Netzwerk-IPv4-Adressen und Netzwerk-IPv6-Adressen:

Angezeigt werden die vom Provider bereitgestellte IPv4 Adresse und falls zugeteilt die IPv6 Adresse mit den zugehörigen Namens-Server für IPv4 und IPv6

Status und Einstellungen der WAN-Verbindung, sofern diese über eine kabelgebundene DSL/Kabel-Verbindung hergestellt wurde.

Empfangene Bytes/Gesendete Bytes: Anzahl der seit Verbindungsaufbau empfangenen und gesendeten Bytes. Wird die Verbindung neu aufgebaut, wird der Zähler zurückgesetzt.

Netzwerk-IP-Adressen: Angezeigt wird die vom Provider bereitgestellte IPv4 und falls zugeteilt die IPv6 Adresse

Beispielanzeige mit dem Bezug einer IPv6 Adresse auf der DSL/Kabel-Schnittstelle:

Die Darstellung zeigt den Bezug einer IPv4 und einer IPv6 Adresse auf der DSL/Kabel-Schnittstelle

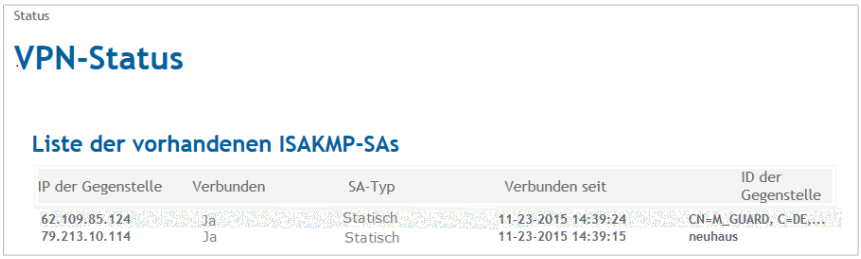
Es muss beachtet werden dass die Einstellung Betriebsmodus der WAN-Schnittstelle als zusätzliche LAN-Schnittstelle aktiviert wurde.

Unter den WAN-Setup-Einstellungen muss der Betriebsmodus des WAN-Setups beide Schnittstellen oder mindestens die DSL/Kabel-Schnittstelle eingestellt werden.

5.4 VPN-Status abfragen

VPN-Status

Öffnen Sie das Register **`Status`** und wählen Sie im Menü „**`VPN-Status`**“.



Liste aller vorhandenen ISAKMP-SAs (= Security Associations, Sicherheits-Verbindungen).

`IP der Gegenstelle`: IP-Adresse des anderen Teilnehmers.

`Verbunden`: „`Ja`“ = Verbindung steht oder „`Nein`“ = Verbindung konnte nicht hergestellt werden.

`SA-Typ`: Typ der Sicherheitsverbindung. Legt die Konventionen (Verbindung) fest, die die beiden miteinander kommunizierenden Teilnehmer innerhalb des sicheren Netzwerks nutzen.

> **`Statisch:`** Verbindung wurde von TAINY IQ-LTE konfiguriert und hergestellt.
>
> **`Dynamisch:`** Verbindung wurde von dem anderen externen Teilnehmer hergestellt.

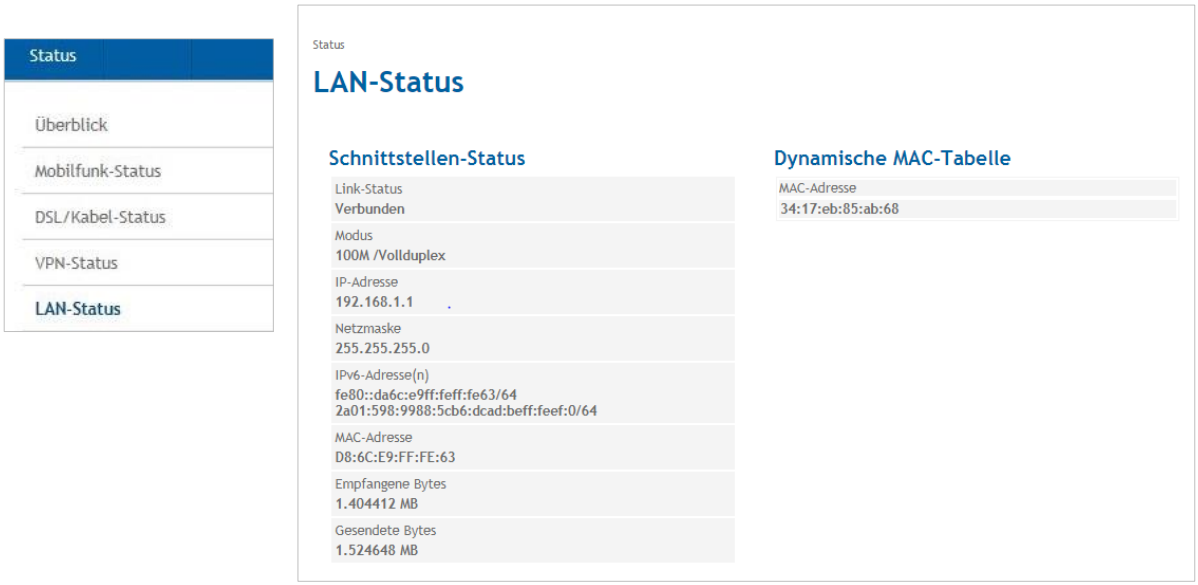
`Verbunden seit`: Zeitstempel der Verbindung.

`ID der Gegenstelle`: Identifikator des anderen Teilnehmers.

5.5 LAN-Status abfragen

LAN-Status

Öffnen Sie das Register **Status** und wählen Sie im Menü „**LAN-Status**“.



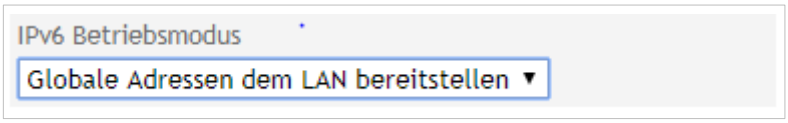
Schnittstellen-Status

IP-Adresse, Netzmaske und MAC-Adresse, die der Schnittstelle zugeordnet sind.

Empfangene Bytes/Gesendete Bytes: Anzahl der seit Verbindungsaufbau empfangenen und gesendeten Bytes. Wird die Verbindung neu aufgebaut, wird der Zähler zurückgesetzt.

Netzwerk-IP-Adressen: Angezeigt wird die vom Provider bereitgestellte IPv6 Adresse und die Link Lokale IPv6 Adresse beginnend mit fe80.

Die IPv6 Adresse(n) werden nur angezeigt, wenn unter der Einstellung LAN-Schnittstelle der IPv6 Betriebsmodus aktiviert wurde



Dynamische MAC-Tabelle

MAC-Adresse(n) der angeschlossenen Clients oder statische MAC-Tabelle.

DHCP-Clients

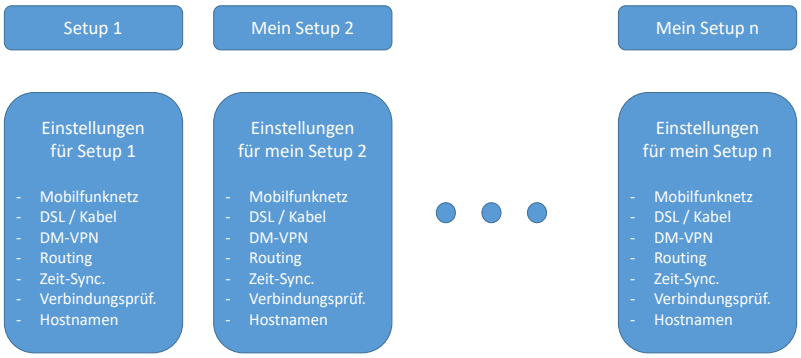
LAN-Geräte, die eine IP-Adresse vom TAINY IQ-LTE-DHCP-Server abgerufen haben, sofern dieser Server aktiviert ist (siehe Kapitel 8 und Kapitel 9). Für jedes Gerät wird die zugeordnete IP-Adresse, die MAC-Adresse, der Hostname und der Status angezeigt.

6 WAN-Einstellungen

6.1 Auswahl des Standard-WAN-Setups

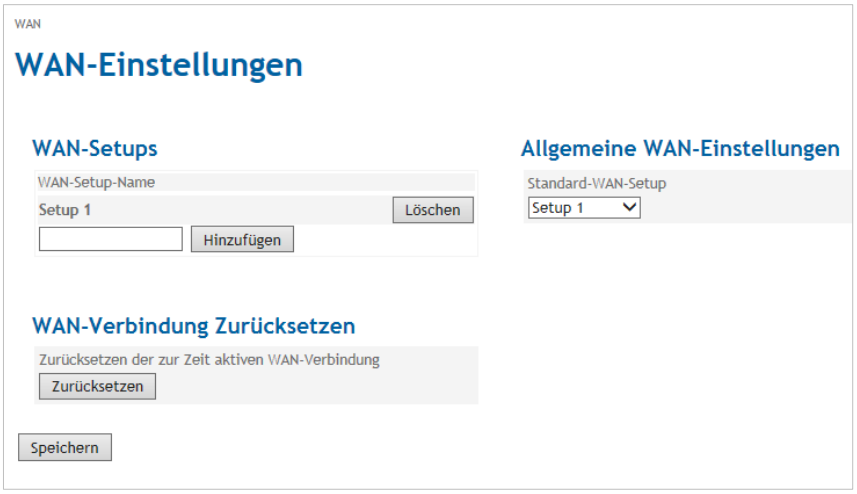
WAN-Einstellungen

Ein WAN-Setup, z. B. Setup 1, umfasst eine Gruppe von WAN-Schnittstellen mit entsprechenden Einstellungen, siehe Abbildung.



Sie können mehrere WAN-Setups mit unterschiedlichen Einstellungen erstellen und eines der Setups als Standardeinstellung auswählen.

Öffnen Sie das Register **WAN** und wählen Sie im Menü „**WAN-Einstellungen**“.



WAN-Verbindung zurücksetzen

In diesem Register können Sie weitere WAN-Setups erstellen, die Standard-Einstellung auswählen oder die eingestellte WAN-Verbindung zurücksetzen.

Allgemeine WAN-Einstellungen

In dieser Spalte sehen Sie das aktuell von TAINY IQ-LTE genutzte WAN-Setup. Dieses wird standardmäßig verwendet, sobald TAINY IQ-LTE neu gestartet wird.

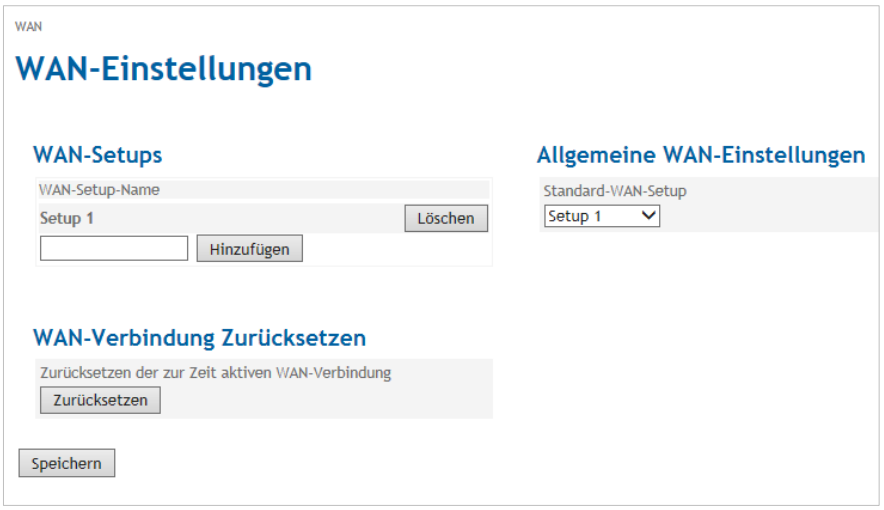
Um das eingestellte WAN-Setup zu ändern, wählen Sie ein anderes WAN-Setup aus der Liste **Standard-WAN-Setup** aus und speichern dieses mit „Speichern“. Das neu ausgewählte Setup ist sofort aktiviert.

Erstellung eines neuen WAN-Setups siehe Kapitel 6.2.

6.2 Anzeigen, Hinzufügen, Löschen von WAN-Setups

WAN-Setup

Öffnen Sie das Register **WAN** und wählen Sie im Menü „**WAN-Einstellungen**“.



Setup 1
(oder neues Setup erstellen)

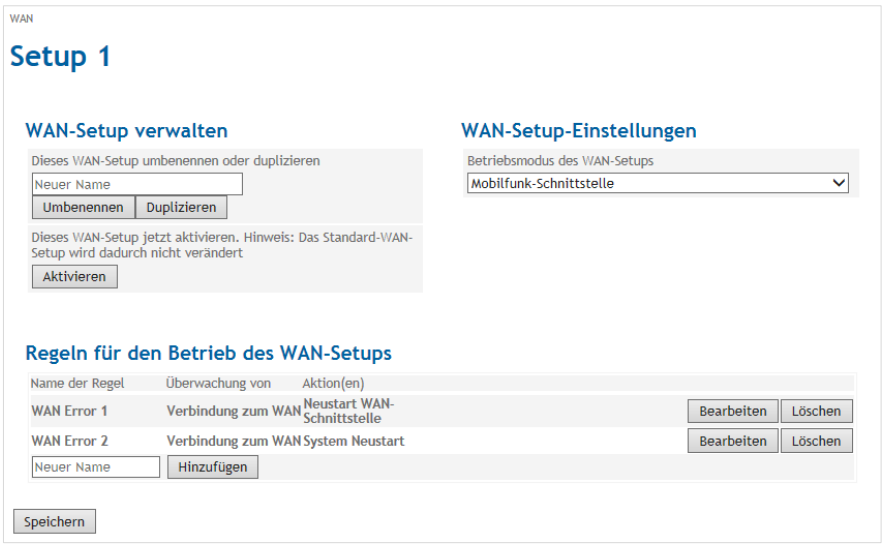
WAN-Setups

Alle bestehenden WAN-Setups sind in dieser Spalte aufgeführt.

Sie können WAN-Setups neu hinzufügen oder löschen.

Um ein neues WAN-Setup hinzuzufügen, geben Sie einen Namen für das neue Setup in das Feld unter „Setup 1“ ein und drücken Sie „Hinzufügen“.

Das neue WAN-Setup erscheint in der Liste und links im Menü.



WAN-Setup verwalten

Unter WAN-Setup verwalten können Sie die Setups **umbenennen**, **duplizieren** und **aktivieren**.

Umbenennen

Um die Benennung eines vorhandenen Setups zu ändern, wählen Sie das entsprechende Setup im Menü aus. Tragen Sie jetzt den neuen Namen unter WAN-Setup verwalten ein und bestätigen Sie dieses mit „**Umbenennen**“.

Duplizieren

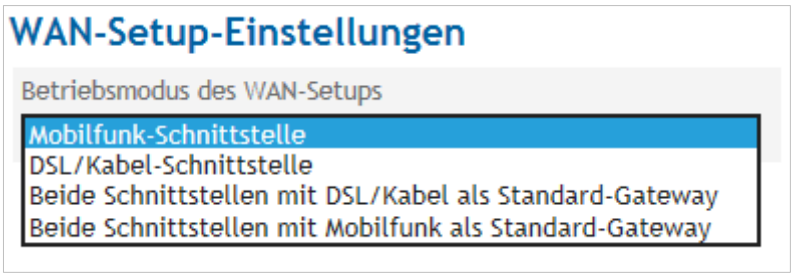
Um ein neues Setup zu erstellen, das weitestgehend über die gleichen Einstellungen verfügt wie ein schon vorhandenes Setup, können Sie dieses duplizieren. Wählen Sie im Menü links das Setup aus, das Sie duplizieren möchten und geben Sie unter „WAN-Setup verwalten“ den Namen des neuen Setups ein und drücken Sie „**Duplizieren**“.

Das neu angelegte Setup erscheint jetzt links in der Menüleiste und Sie können die Änderungen/Einstellungen für das duplizierte Setup vornehmen wie in diesem Handbuch beschrieben.

Um ein WAN Setup zu aktivieren, wählen Sie das Setup im Menü aus und drücken Sie „**Aktivieren**“.

Betriebsmodus des WAN-Setups

Wählen Sie eine Schnittstelle aus (Mobilfunk oder DSL/Kabel), die für den Aufbau der WAN-Verbindung zuständig ist. Oder Sie wählen die Optionen „Beide Schnittstellen ...“ aus. In diesem Fall müssen Sie die Schnittstellen DSL/Kabel oder Mobilfunk priorisieren und festlegen, welche Schnittstelle zuerst angefragt wird, um die Verbindung aufzubauen. Sollte diese nicht reagieren, übernimmt die andere Schnittstelle den Aufbau der WAN-Verbindung.



Tipp

Soll der ETH0-Port als LAN-Port genutzt werden, müssen Sie die Option „Beide Schnittstellen mit Mobilfunk als Standard-Gateway“ auswählen, andernfalls wird der ETH0-Port deaktiviert.

Zusätzlich zur Festlegung der „Regeln für den Betrieb des WAN-Setups“ und den Betriebsmodus der WAN-Setup-Einstellungen, können Sie für jedes einzelne WAN-Setup die folgenden Einstellungen vornehmen:

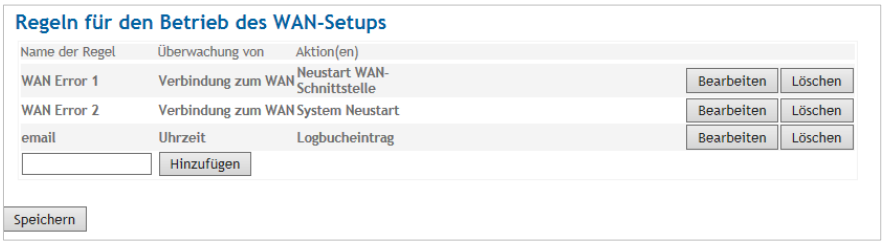
- Mobilfunk-Schnittstelle
- DSL/Kabel-Schnittstelle
- DM-VPN
- IPsec-Tunnel
- Routing
- Zeitsynchronistation
- Verbindungsprüfung
- Hostnamen
- DDNS

6.3 Konfiguration der Regeln für den Betrieb des WAN-Setups

Regeln für den Betrieb des WAN-Setups

Legen Sie das Verhalten des TAINY IQ-LTE im Falle einer in der WAN-Verbindung auftretenden Störung fest, z.B. bei Verlust der Verbindung oder bei einem Umschaltvorgang am Port.

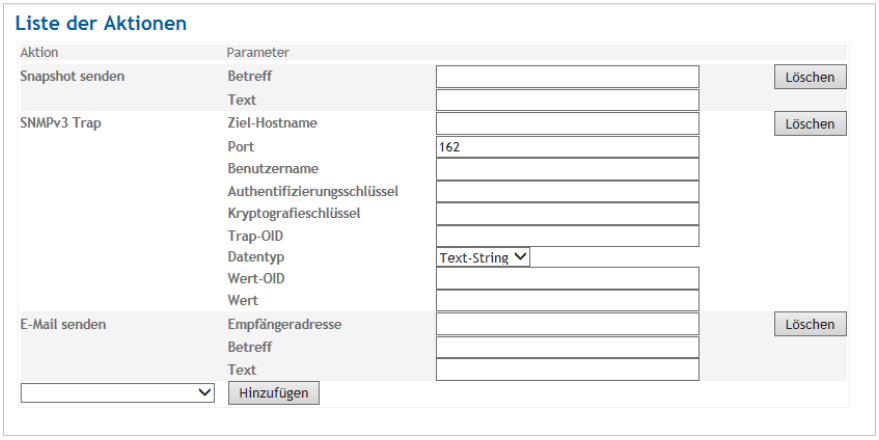
Fügen Sie neue Regeln für das WAN-Setup hinzu, bearbeiten oder löschen Sie bestehende Regeln.



Um eine neue Regel hinzuzufügen, geben Sie einen Namen für die Regel ein und drücken auf „`Hinzufügen`“. Die neue Regel erscheint in der Liste.

Um eine bestehende Regel zu ändern, drücken Sie „`Bearbeiten`“ hinter der betreffenden Regel in der Liste, die geändert werden soll.

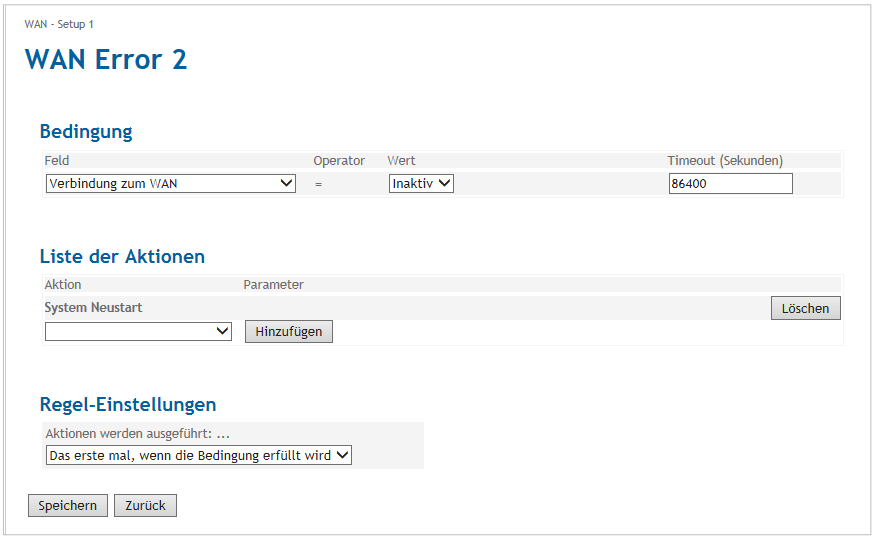
Wählen Sie die gewünschte Aktion aus der Liste „`Liste der Aktionen`“ aus, z.B. `Snapshot senden`/`E-Mail senden`/`SNMPv3-Trap`.



Sie finden Erläuterungen zu den Parametern in den Tabellen: *„Wählbare Bedingungen“*, *„Wählbare Aktionen“* und *„Wählbare Regeln“*.

WAN Error 2

(neue Regeln erstellen)



Wählen Sie zunächst die **Bedingung,** auf die die Regel angewendet werden soll, dann die **Aktion,** die ausgeführt werden soll, und abschließend die **Regel-Einstellung** für die Aktion.

Beispiel:

Bedingung:	*Die Verbindung zu WAN ist 3600 Sekunden inaktiv*.
Aktion:	*Neustart der WAN-Schnittstelle.*
Regel-Einstellung:	*Periodisch, alle 300 Sekunden*, *bis die Bedingung erfüllt ist.*

Ist die WAN-Verbindung für 3600 Sekunden inaktiv, versucht TAINY IQ-LTE die WAN-Schnittstelle neu zu starten. Dieses wird periodisch alle 300 Sekunden wiederholt und zwar solange, bis die WAN-Verbindung nicht länger inaktiv ist.

Wählbare Bedingungen

Bedingung	Parameter	Aktion wird ausgelöst …
Allgemein		
Ohne Bedingung	Timeout	… wenn das Timeout abgelaufen ist.
Verbindung zum WAN	Operator/ Value/ Timeout	… wenn die Verbindung zu WAN im definierten Zeitraum (Timeout) aktiv oder inaktiv ist.
Schalteingang	Operator/ Value/ Timeout	… wenn der Schalteingang im definierten Zeitraum (Timeout) aktiv oder inaktiv ist.
Verbindungsprüfung		
Prüfung erfolgreich	n/a	… wenn Verbindungsprüfung erfolgreich
Prüfung fehlgeschlagen	n/a	… wenn Verbindungsprüfung fehlgeschlagen.
Verlorene Pakete (%)	Operator/ Value/ Timeout	… wenn der Prozentsatz der verlorenen Datenpakete gleich, höher oder niedriger als der definierte Wert oder innerhalb der definierten Zeitspanne (Timeout) ist. Es wird nur der Datenaustausch der Verbindungsprüfung einbezogen.
Durchschnittliche Antwortzeit (ms)	Operator/ Value/ Timeout	… wenn die durchschnittliche Antwortzeit gleich, höher oder niedriger als der definierte Wert oder innerhalb der definierten Zeitspanne (Timeout) liegt. Es wird nur der Datenaustausch der Verbindungsprüfung einbezogen.
WAN-Datenvolumen		
Datenvolumen SIM 1 (kB)	Zähler Value Mobil	… wenn der Wert gleich, höher oder niedriger als der eingegebene Wert oder innerhalb der definierten Zeitspanne (Timeout) ist.
Datenvolumen SIM 2 (kB)	Zähler Value Mobil	… wenn der Wert gleich, höher oder niedriger als der eingegebene Wert oder innerhalb der definierten Zeitspanne (Timeout) ist.
Datenvolumen DSL/Kabel (kB)	Zähler Value DSL/Kabel	… wenn der Wert gleich, höher oder niedriger als der eingegebene Wert oder innerhalb der definierten Zeitspanne (Timeout) ist.
Mobilfunk-Verbindung		
Feldstärke (CSQ)	Operator/ Value/ Timeout	… wenn der Wert gleich, höher oder niedriger als der eingegebene Wert oder innerhalb der definierten Zeitspanne (Timeout) ist.
Feldstärke (RSSI (dBm))	Operator/ Value/ Timeout	… wenn der Wert gleich, höher oder niedriger als der eingegebene Wert oder innerhalb der definierten Zeitspanne (Timeout) ist.
Feldstärke 3G (RSCP (dBm))	Operator/ Value/ Timeout	… wenn der Wert gleich, höher oder niedriger als der eingegebene Wert oder innerhalb der definierten Zeitspanne (Timeout) ist.
Signal-Qualität (Ec/No (dBm))	Operator/ Value/ Timeout	… wenn der Wert gleich, höher oder niedriger als der eingegebene Wert oder innerhalb der definierten Zeitspanne (Timeout) ist.
DM-VPN		
Kein Standard-Gateway verfügbar	n/a	… wenn keines der für den Dynamic-Multipoint-VPN konfigurierten Standard-Gateways erreichbar ist.
Dead Peer Detection (DPD)	n/a	… wenn die Dead Peer Detection (DPD) fehlschlägt.

Bedingung	Parameter	Aktion wird ausgelöst …
Timeout der IPsec-Phase 1	n/a	Aktion wird im Fall der IPsec-Phase 1 Timeout gestartet.
Verbindung mit VPN	Operator/ Value/ Timeout	Aktion wird gestartet, wenn die Verbindung zu VPN für den definierten Zeitraum (Timeout) aktiv oder inaktiv ist.
Zeit		
Systemlaufzeit (Sekunden)	n/a	… wenn der Wert der Systemlaufzeit gleich, höher oder niedriger als der eingegebene Wert oder innerhalb der definierten Zeitspanne (Timeout) ist.
Uhrzeit	Value	… zum Zeitpunkt der Eingabe (hh:mm:ss)
Sichere Zeitbasis	Operator/ Value/ Timeout	… wenn die sichere Zeitbasis des TAINY IQ-LTE innerhalb des definierten Zeitraums (Timeout) aktiv oder inaktiv ist. Die verlässliche Normalzeit ist solange aktiv, wie die letzte erfolgreiche NTP-Synchronistation nicht älter als 48 Stunden ist.
LAN-Link-Status		
ETH 1 verbunden	n/a	... sobald ein Netzwerkkabel in Schnittstelle ETH1 gesteckt wird.
ETH 1 getrennt	n/a	... sobald ein Netzwerkkabel aus der Schnittstelle ETH1 entfernt wird.
Per Regel beeinflussbare Zähler		
Zähler 1…5	Operator/ Value/ Timeout	... wenn der Zähler gleich, höher oder niedriger als der eingegebene Wert oder innerhalb der definierten Zeitspanne (Timeout) ist.

Wählbare Aktionen

Aktion	Parameter	Beschreibung
System-Neustart	n/a	TAINY IQ-LTE führt einen System- Neustart durch
Wechsel des WAN-Setups	WAN-Setup-Name	TAINY IQ-LTE wechselt zu dem WAN-Setup, das vom Parameter vorgegeben ist.
Neustart WAN-Schnittstelle	n/a	Die WAN-Schnittstelle wird neu gestartet und die Verbindung erneut aufgebaut gemäß der Vorgaben des als Standard eingestellten WAN-Setups.
Neustart VPN	n/a	Der VPN-Dienst wird neu gestartet, die VPN-Verbindung wird eingestellt und wieder-hergestellt gemäß dem Setup.
Logbucheintrag	Log Level Ereignistext	Ein Eintrag ins Logbuch mit konfiguriertem Text. Log Level, wird generiert.
SNMPv3-Trap	Ziel Adresse/Ziel/ Benutzername/ Passwort/ Authentifizierungs schlüssel/ Verschlüsselungs-schlüssel/ Trap-OID/ Datentyp/ Wert-OID/Wert	Wenn eine der oben genannten Bedingungen zutrifft, wird ein SNMPv3-Trap versendet. ***Beachten:*** Die Empfänger-adresse wird auf dem Register Geräte-Informationen im Menü Geräte-Information konfiguriert.

Aktion	Parameter	Beschreibung
E-Mail senden	Empfänger-adresse/ Betreff/Text	Eine E-Mail wird gesendet
Snapshot senden	Betreff/Text	Ein Snapshot wird per E-Mail gesendet. ***Beachten:*** Die Empfänger-adresse wird im Register System im Menü Geräte Informationen konfiguriert.
Schaltausgang	Output-Status	Der Schaltausgang ist gemäß des im Parameter konfigurierten Status gesetzt.
Zähler inkrementieren/ hochsetzen	Zähler	Der ausgewählte Zähler (1…5) wird um 1 hochgesetzt.
Zähler dekrementieren	Zähler	Der ausgewählte Zähler (1...5) wird um 1 heruntergesetzt.
Zähler setzen	Zähler Wert	Der ausgewählte Zähler (1...5) wird auf den Wert gesetzt, der im Parameter vorgegeben ist.

Wählbare Regeln

Regel	Parameter	Beschreibung
Immer wenn die Bedingung erfüllt ist.	n/a	Die Aktion wird ausgeführt, sobald die Bedingung von nicht erfüllt zu erfüllt wechselt.
Die Bedingung ist zum ersten Mal erfüllt.	n/a	Die Aktion wird zum ersten Mal ausgeführt, nachdem das Gerät in Betrieb genommen wurde oder die Regel im System gespeichert ist.
Periodisch solange, bis die Regel erfüllt ist.	Wartezeit	Die Aktion wird solange durchgeführt, wie die Bedingung erfüllt ist. Die nächste Aktion wird erst nach Ablauf der Wartezeit durchgeführt.

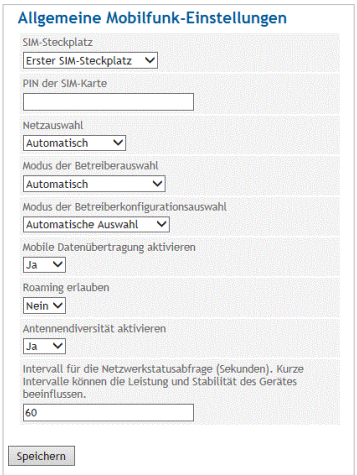
6.4 Konfigurieren der WAN-Mobilfunk-Schnittstelle

Mobilfunk

Öffnen Sie das Register **WAN** und wählen Sie im Menü „**Mobilfunk**“.

Allgemeine Mobilfunk-Einstellungen

Wählen Sie den gewünschten SIM-Karten-Steckplatz aus und setzen Sie die für die SIM-Karte gewünschten Parameter.



SIM-PIN: Geben Sie die PIN der im ausgewählten SIM-Steckplatz befindlichen SIM-Karte ein.

Netzauswahl: Wählen Sie aus, wie oft sich das TAINY IQ-LTE automatisch am fortschrittlichsten Netzwerk anmelden soll, ob dieses unterstützt wird und erreichbar ist:

Modus der Betreiber-auswahl:	Wählen Sie die Liste der erlaubten Netzwerkbetreiber aus, die bei der Suche nach einem Netzwerk angewendet werden soll: `Automatisch`: TAINY IQ-LTE sucht automatisch nach dem besten Netz und versucht, sich dort anzumelden. `SIM-Karten Liste`: TAINY IQ-LTE verbindet sich nur mit den Netzanbietern, die auf der SIM-Karte gespeichert sind.

Benutzerdefinierte Liste: TAINY IQ-LTE verbindet sich nur mit Netzen, die auf der `Liste der erlaubten Betreiber` aufgeführt sind. Auf diese Liste setzen Sie die von Ihnen bevorzugten Betreiber. TAINY IQ-LTE fragt die Betreiber gemäß Reihenfolge von oben nach unten an. Drücken Sie „`Hoch`“, um die Reihenfolge zu verändern.

Modus der Betreiber-konfigurations-auswahl:	Wählen Sie den Zugangsparameter: • Automatische Auswahl, wenn Betreiber-ID auf der SIM-Karte gespeichert (siehe automatische Betreiber-Konfiguration) • Manuelle Auswahl, wenn feste Einstellungen (siehe manuelle Betreiber-Konfiguration)
Mobile Datenüber-tragung aktivieren:	Aktiviert/Deaktiviert die Kommunikation mit dieser SIM-Karte über die Mobilfunk-Schnittstelle. Das Gerät meldet sich am Netz, jedoch nicht am Datenservice an.
Roaming erlauben:	Aktiviert/Deaktiviert Roaming.
Intervall für die Netzwerk-statusabfrage:	Intervall der Aktualisierung der Qualitätsdaten der Mobilfunkverbindung (Wertebereich: 5 – 300 Sekunden)

`Liste der Betreiber-Konfiguration`

Diese Liste ist nur sichtbar, wenn der „`Modus der Betreiberkonfigurationsauswahl`“ auf „`Automatisch`“ gesetzt ist.

Die Liste führt auf, welche Zugangskonfigurationen für welchen Netzbetreiber TAINY IQ-LTE gespeichert hat.

Um eine neue Betreiberkonfiguration hinzuzufügen, tragen Sie den Namen der Betreiberkonfiguration in das Feld ein und drücken Sie „`Hinzufügen`“.

Um eine bestehende Konfiguration einzusehen oder zu ändern, drücken Sie „`Bearbeiten`“ hinter der entsprechenden Konfiguration.

Um einen Betreiber zu löschen, drücken Sie „`Löschen`“ in der entsprechenden Zeile.

Betreiber Konfiguration (für automatische Auswahl)

Nur zutreffend, wenn der `Modus der Betreiberkonfiguration` auf „`Automatische Auswahl`“ gesetzt ist.

TAINY IQ-LTE liest die Betreiber-ID auf der aktivierten SIM-Karte und wählt die vordefinierte Betreiberkonfiguration für die Betreiber-ID aus.

Die Betreiberkonfiguration wird für den Zugang zum IP-Daten-Dienst (GPRS, EDGE or HSPA+) benötigt.

Betreiber-ID: Mithilfe dieser ID wird die richtige Betreiberkonfiguration der verwendeten SIM-Karte zugeordnet. TAINY IQ-LTE liest die Betreiber-ID auf der SIM-Karte (Teil des IMSI) und wählt aus der Liste der Betreiberkonfigurationen den passenden Eintrag aus.

Stimmen die Betreiber-ID auf der SIM-Karte und auf der Betreiberliste überein, wird die entsprechende Betreiberkonfiguration zur Anmeldung am IP-Daten-Dienst verwendet.

Tipp

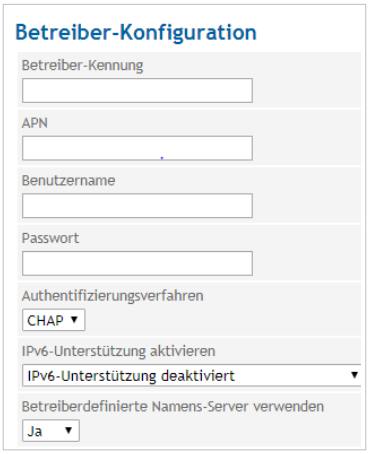
Die Betreiber ID besteht aus den ersten 5 Ziffern der IMSI; welche bei eingelegter SIM auf der Mobilfunkt-Status Seite zu finden ist. Oder in den Infomationsdokumenten Ihres UMTS- oder GSM/GPRS- Anbieters sowie auf dessen Homepage. Sie können auch die Anbieter- Hotline (Kwan Interface Keyword: MCC/MNC) kontaktieren.

Betreiber-konfiguration (für manuelle Konfiguration)

Nur zutreffend, wenn der `Modus der Betreiberkonfigurations-auswahl` auf „`Manuell`“ gesetzt ist.

Die Betreiberkonfiguration wird für den Zugang zum IP-Daten-Dienst (GPRS, EDGE or HSPA+) benötigt.

Unabhängig von der Betreiber-ID auf der SIM-Karte wird die eingegebene Betreiberkonfiguration verwendet.



Parameter der Betreiberkonfiguration

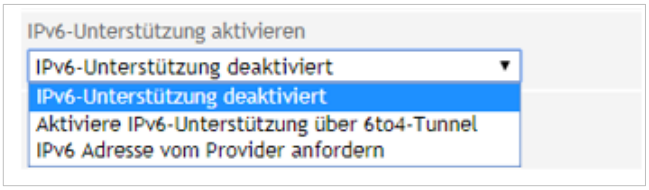
Geben Sie den **APN**, den **Benutzernamen** und das **Passwort** ein. Diese Angaben finden Sie in den Dokumenten des Mobilfunknetz-betreibers, auf dessen Homepage oder Sie fragen bei dessen Hotline nach.

Manche Mobilfunknetzbetreiber verwenden weder Benutzername noch Passwort als Zugangskontrolle zum Netz. In diesem Fall tragen Sie in die entsprechenden Felder *Gast* ein.

Um sich beim kabellosen Daten-Service (HSPA+, UMTS, EGPRS oder GPRS) anzumelden, sind zwei verschiedene **Authentifizierungs-methoden** (PAP und CHAP) denkbar. Für gewöhnlich wird die Methode automatisch ausgewählt. Ist keine bestimmte Methode vorgegeben, wählen Sie manuell aus, entweder PAP oder CHAP.

IPv6

IPv6-Unterstützung aktivieren



Sie können einstellen ob vom Mobilfunk-Provider eine IPv6 Adresse angefordert werden soll. Wählen Sie „IPv6 Adresse vom Provider anfordern“.

Falls eine IPv6-Adresse **nicht** benötigt wird, wählen Sie die Einstellung „IPv6-Unterstützung deaktivieren“ aus.

Die IPv6-Adressen vom Mobilfunk-Provider sind im Normalfall weltweit eindeutige Adressen. Das TANY IQ stellt daraufhin IPv6 Adressen in seinem Lokalen Netzwerk zur Verfügung. Client Rechner angeschlossen an der LAN-Schnittstelle, erhalten so die Möglichkeit zusätzlich zur einer IPv4-Adresse auch über die zugewiesene IPv6-Adresse Verbindungen in das Internet aufzubauen.

Um die IPv6-Adressen an der LAN-Schnittstelle den Client Computern zur Verfügung zu stellen, muss unter LAN-Schnittstelle der IPv6-Betriebsmodus auf „Globale Adressen dem LAN bereitstellen“ gewählt werden.

Hinweis

Die Zuteilung einer IPv6-Adresse im Mobilfunknetz ist abhängig davon, ob der verwendete Internet Mobilfunkbetreiber die Vergabe von IPv6 Adressen im Mobilen Datennetz unterstützt.

Die Erreichbarkeit mit IPv6 aus dem Internet ist abhängig vom Mobilfunkbetreiber und den abgeschlossenen Vertrag mit dem Betreiber. Mobilfunkbetreiber können private APN (access point name) für die Verwendung von ausgehenden und eingehenden IPv6 Verbindungen voraussetzen.

Auf der Webseite „Mobilfunk-Status“ können sie sehen ob eine IPv6 Adresse bezogen wurde. Falls dem so ist erscheint dort ein Zusätzlicher Eintrag mit dem Hinweis Netzwerk-IPv6-Adresse und Primärer IPv6-Namens-Server. Zusätzlich wird im Normalfall auch ein IPv6-Namens Server vom

Mobilfunk-Provider bezogen. Damit erhält das TAINY IQ die Möglichkeit Hostnamen in IPv6-Zieladressen aufzulösen.

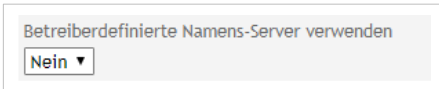
6to4 Tunnel

Mit der Einstellung „Aktiviere IPv6-Unterstützung über 6to4-Tunnel“ können IPv6 Netzwerke bzw. IPv6-Verbindungen an der LAN-Schnittstelle über einen IPv4-Tunnel über das Mobilfunknetz betrieben werden, falls der Mobilfunk-Provider keine IPv6-Adresse über Mobilfunk bereitstellt.

Mit einem 6to4-Tunnel lassen sich IPv6-Pakete über IPv4 transportieren.

Auf der Webseite „LAN-Status“ können sie unter dem Eintrag IPv6-Adresse(n) sehen ob eine IPv6-Adresse über den 6to4-Tunnel bereitgestellt wurde.

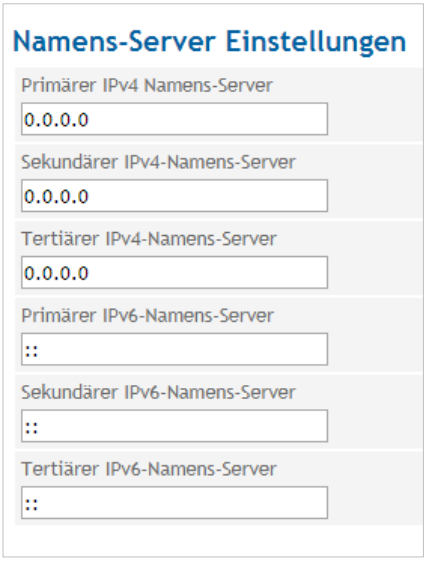
Namens-Server Konfiguration



Namens-Server wie vom Betreiber definiert konfigurieren.

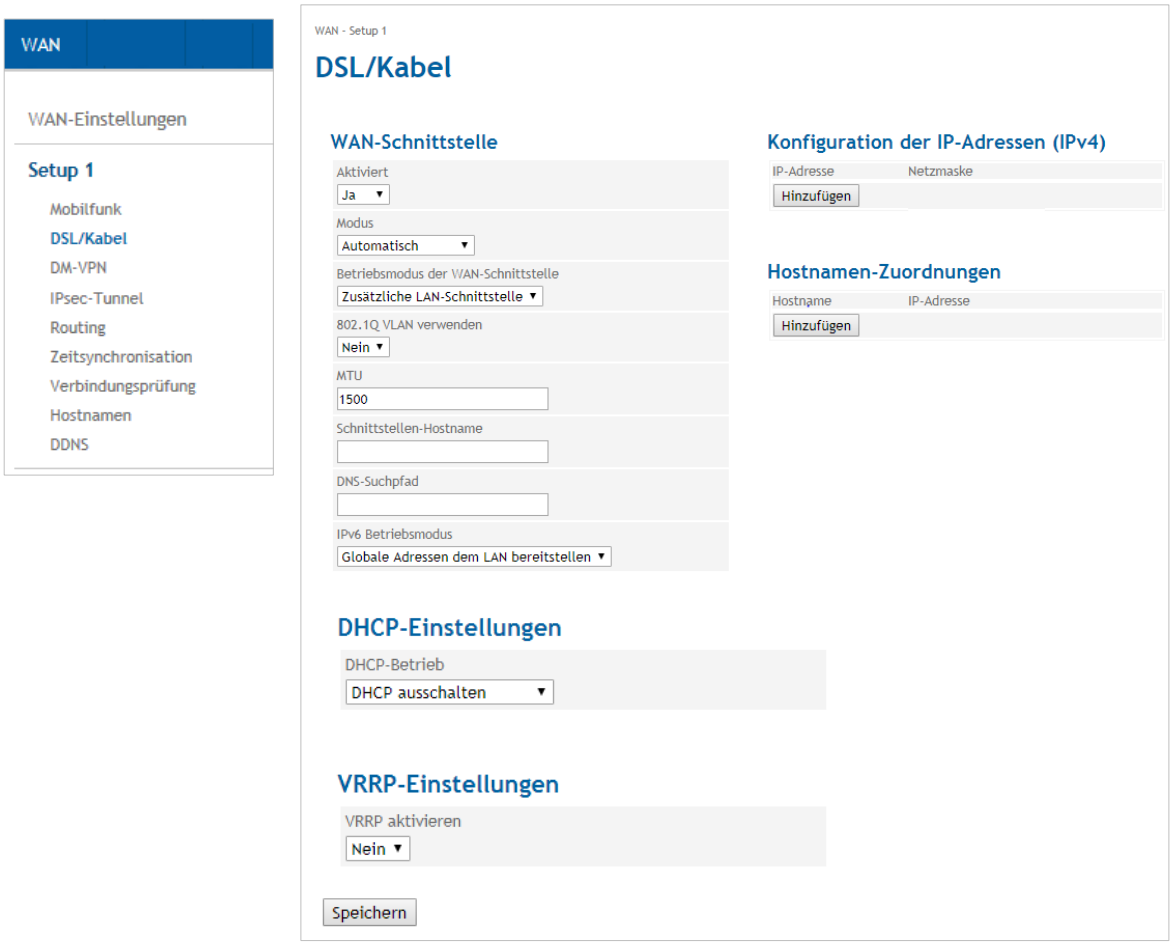
Wählen Sie „Ja“, wenn die vom Betreiber angebotenen Namens-Server verwendet werden sollen. Wählen Sie „Nein“, um bis zu 6 IPv4 und IPv6 Namens-Server manuell zu bestimmen.

Sie könne IPv4 und IPv6 Namens Server angeben.



6.5 Konfiguration der WAN-DSL/Kabel-Schnittstelle

DSL/Kabel



`WAN-Schnittstelle`

Um die WAN-Kommunikation über eine Ethernet-Kommunikation herzustellen, müssen die folgenden Parameter für die folgenden Einstellungen gesetzt werden:

Wählen Sie den korrekten **`Betriebsmodus der WAN-Schnittstelle`** in der Liste aus:

- Wählen Sie PPPoE, um TAINY IQ-LTE mit einem DSL-Modem mit einer PPPoE-logischen Schnittstelle zu verbinden,
- Wählen Sie DHCP, um TAINY IQ-LTE mit Routern zu verbinden.
- Wählen Sie PPPoE > DHCP oder DHCP > PPPoE, wenn TAINY IQ-LTE automatisch die korrekte logische Schnittstelle auswählen soll. Mit PPPoE > DHCP wird es erst versuchen, sich mit PPPoE zu verbinden. Schlägt dies fehl, wird es DHCP versuchen.
  Mit DHCP > PPPoE wird TAINY IQ-LTE genau den umgekehrten Weg versuchen.
- Im Falle einer PPPoE-Verbindung geben Sie den Benutzernamen und das Passwort ein.

  Es ist möglich, den `Modus` der Schnittstelle zu ändern. Wählen Sie den benötigten Modus aus der Liste `Modus` aus:

- `Automatisch`
- `100M Vollduplex` oder `100M Halbduplex`

- `10M Vollduplex` oder `10M Halbduplex`

Um die Schnittstelle zu deaktivieren, setzen Sie **`Aktiviert`** auf „`Nein`“.

`MTU`

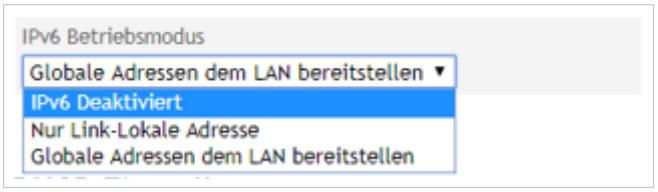
Geben Sie einen Wert für die MTU (Maximum Transmission Unit) ein, um die maximale Größe eines IP-Paketes festzulegen.

`VLAN-Tags (802.1Q) verwenden`

Wählen Sie „`Ja`“, wenn die `VLAN-Tags` über diese physikalische Schnittstelle an die angeschlossenen Anwendungen weitergeleitet werden sollen. Andernfalls werden die `VLAN-Tags` von der ausgehenden Kommunikation entfernt.

`IPv6-Betriebsmodus`

`IPv6 im lokalen Netzwerk`



Sie können einstellen ob die Globale IPv6-Adresse vom Mobilfunk-Provider oder dem 6to4-Tunnel dem lokalen Netzwerk an der LAN-Schnittstelle zur Verfügung gestellt werden soll.

Fall an der LAN-Schnittstelle IPv6-Adressen zur Verfügung gestellt werden sollen, wählen sie die Einstellung „Globale Adressen dem LAN bereitstellen“ aus. Bei dieser Einstellung können die im LAN angeschlossenen Computer mit „Neighbor Discovery Protocol“ weltweit eindeutige IPv6-Adressen vom TAINY IQ beziehen.

Falls eine IPv6-Adresse **nicht** benötigt wird, wählen Sie die Einstellung „IPv6-Deaktiviert“ aus.

Mit der Einstellung „Nur Link-Lokale Adresse“ wird dem lokalen Netzwerk an der LAN-Schnittstelle nur die innerhalb abgeschlossener Netzwerksegmente gültig Link-Lokale Adresse vom TAINY IQ angezeigt.

Das Formatpräfix der Link-Lokalen Adresse lautet „ fe80::/64“

Auf der Webseite „LAN-Status“ können sie unter dem Eintrag IPv6-Adresse(n) sehen welche IPv6-Adresse(n) eingestellt wurde.

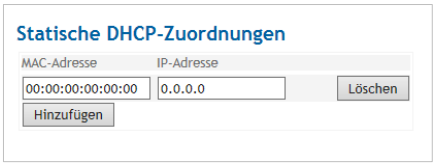
`DHCP-Einstellungen`

`DHCP-Betrieb`

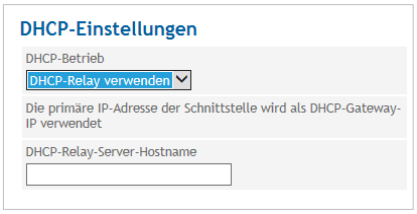
TAINY IQ-LTE bietet eine DHCP-Server-Funktion oder eine DHCP-Relais-Funktion.

Ist die DHCP-Server-Funktion aktiviert, ordnet TAINY IQ-LTE selbst den an die LAN-Schnittstelle angeschlossenen Anwendungen IP-Adressen zu. Definieren Sie den Bereich, aus dem die zu-zuordnenden IP-Adressen

stammen sollen und/ oder definieren Sie statische Zuordnungen von Client MAC-Adresse zur IP-Adresse



Ist die DHCP-Relais-Funktion aktiviert, leitet TAINY IQ-LTE die DHCP- Anfrage der an die LAN-Schnittstelle angeschlossenen Anwendung an einen remoten DHCP-Relais-Server weiter, der die IP-Adressen zur Verfügung stellt. Geben Sie den Hostnamen oder die IP-Adresse des DHCP-Relais-Servers ein.



VRRP-Einstellungen

VRRP (Virtual Router Redundancy Protocol) nutzt eine Reihe von TAINY IQ-LTEs, um die Verfügbarkeit wichtiger Gateways innerhalb des Netzwerks sicherzustellen.

Um die VRRP-Einstellungen konfigurieren zu können, setzen Sie `VRRP-Einstellungen aktivieren` auf „`Ja`“.

Virtual-Router-ID

ID der Gruppe der verwendeten TAINY IQ-LTEs.

VRRP-Basis-Priorität

Legt fest, welcher TAINY IQ-LTE als Master dient und welcher als Back-up. Der TAINY IQ-LTE mit der höchsten Priorität ist der Master. Geben Sie Werte zwischen 1 (niedrigste Priorität) und 254 (höchste Priorität) ein. Die VRRP-Priorität kann automatisch an einen neuen Wert angepasst werden.

VRRP-Priorität anpassen

Im Fall einer aktivierten WAN- oder VPN-Verbindung.

Liste der VRRP-IP-Adressen

IP-Adressen der VRRP (TAINY IQ-LTEs)

Konfiguration der IP-Adressen/ Hostnamen, Zuordnung	**Hostnamen, IP-Adressen:** TAINY IQ-LTE ermöglicht es, IP-Adressen von Remote-Rechnern Hostnamen zuzuordnen. Wird diese Funktion genutzt, sprechen die an der LAN-Schnittstelle des TAINY IQ-LTE angeschlossen Applikationen die Remote-Rechner mit den hier eingetragenen Hostnamen an. Die Funktionen des TAINY IQ-LTE nutzen ebenfalls dieses Feature (z.B. NTP).

DSL/Kabel

Öffnen Sie das Register **WAN** und wählen im Menü „**DSL/Kabel**“.

WAN-Schnittstelle

Um eine WAN-Kommunikation über eine kabelgebundene Ethernet-Verbindung aufzubauen, müssen die folgenden Parameter gesetzt werden:

Wählen Sie den korrekten „Betriebsmodus der WAN-Schnittstelle“ aus der Liste:

- Um TAINY IQ-LTE an ein DSL-Modem mit einer PPPoE-logischen Schnittstelle anzuschließen, Betriebsmodus der WAN-Schnittstelle wählen Sie PPPoE.
- Um TAINY IQ-LTE an einen Router anzuschließen, wählen Sie DHCP.

Soll TAINY IQ-LTE automatisch die logische Schnittstelle auswählen, wählen Sie PPPoE > DHCP oder DHCP > PPPoE.

Mit PPPoE > DHCP wird zuerst versucht, sich mit PPPoE zu verbinden. Schlägt dieses fehl, wird die Verbindung zu DHCP versucht.

Mit DHCP > PPPoE wird der entgegengesetzte Weg versucht.

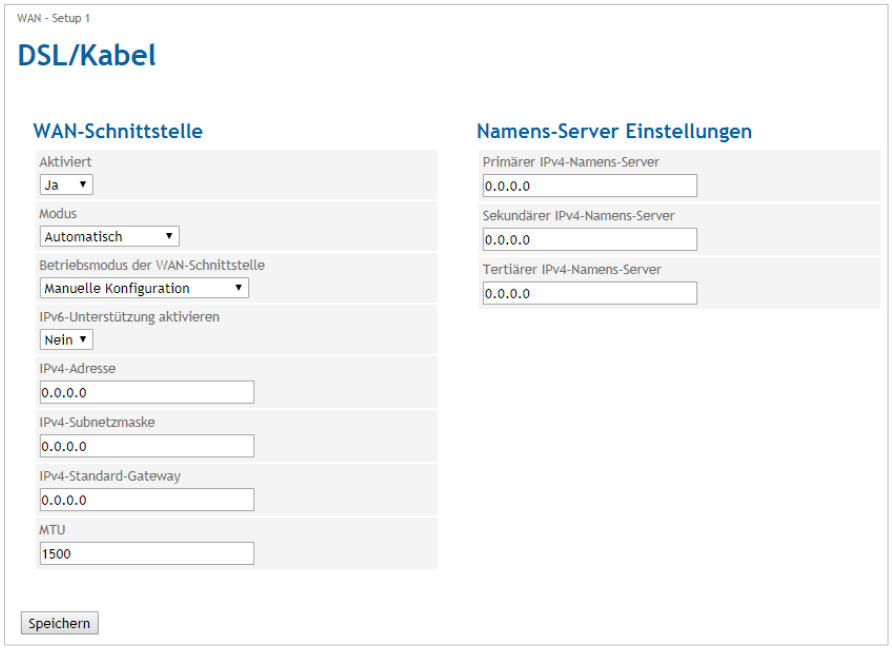
Im Falle einer PPPoE-Verbindung geben Sie den Benutzernamen und das Passwort ein.

Betriebsmodus der WAN-Schnittstelle

Manuelle Konfiguration

Für die Manuelle Konfiguration wählen sie die Einstellung unter Betriebsmodus der WAN-Schnittstelle „Manuelle Konfiguration“ aus.

Hier habe sie die Möglichkeit die WAN-Schnittstelle manuell zu konfigurieren:



IPv4-Adresse Geben Sie hier eine IPv4 Adresse für die WAN-Schnittstelle an

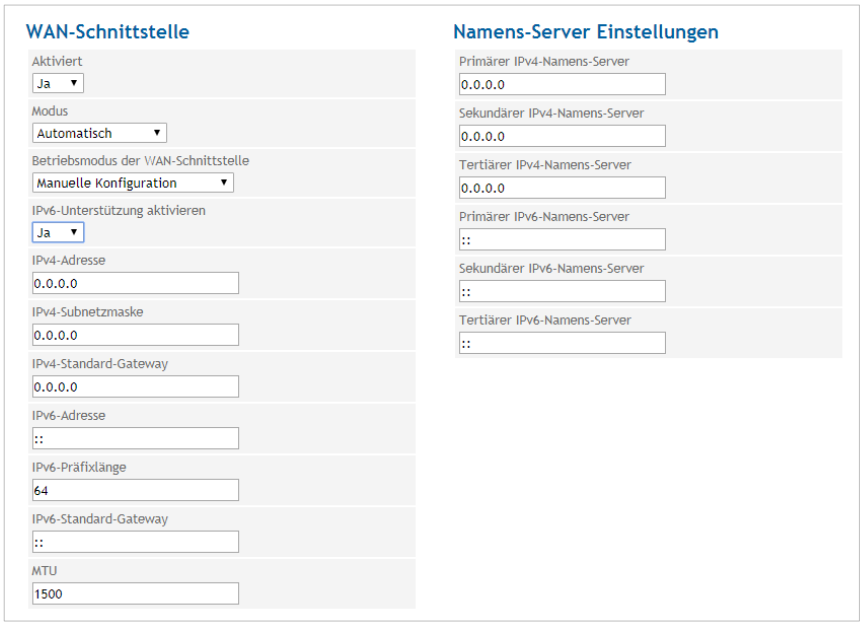
IPv4-Subnetzmaske Geben sie hier eine IPv4 Subnetzmaske für die WAN-Schnittstelle an

IPv4-Gateway Geben sie hier die IPv4 Gateway Adresse an über die das TAINY IQ die IPv4 Datenpakete weiterleitet

MTU Hier können Änderungen an der Maximum Transmission Unit (MAC-Layer) bei Bedarf vorgenommen werden.

IPv6-Unterstützung aktivieren

Hier habe sie die Möglichkeit zusätzlich zur IPv4 Konfiguration auch IPv6 zu konfigurieren. Dafür wählen Sie im Menü „IPv6-Unterstützung aktivieren“ „Ja“ aus.



IPv4-Adresse Geben Sie hier eine IPv4 Adresse für die WAN-Schnittstelle an

IPv4-Subnetzmaske Geben sie hier eine IPv4 Subnetzmaske für die WAN-Schnittstelle an

IPv4-Gateway Geben sie hier die IPv4 Gateway Adresse an über die das TAINY IQ die IPv4 Datenpakete weiterleitet

IPv6-Adresse Geben sie hier eine IPv6 Adresse für die WAN-Schnittstelle an

IPv6-Prefixlänge Geben sie hier die IPv6 Prefixlänge an. Z.B. 64

IPv6-Gateway Geben sie hier die IPv6 Gateway Adresse an über die das TAINY IQ IPv6 Datenpakete weiterleitet

IPv4-Namens-Server Tragen sie einen IPv4 Namens-Server für die Auflösung von Hostnamen zu IPv4 Adressen ein

IPv6-Namens-Server Tragen sie einen IPv6 Namens-Server für die Auflösung von Hostnamen zu IPv6 Adressen ein

MTU Hier können Änderungen an der Maximum Transmission Unit (MAC-Layer) bei Bedarf vorgenommen werden.

6.6 Konfiguration Dynamic-Multipoint-VPN

DM-VPN

Öffnen Sie das Register **WAN** und wählen Sie im Menü „**DM-VPN**“.

DM-VPN-Netzwerke

Netzwerk-Definition der bestehenden Netzwerke (siehe nächste Seite).

Allgemeine DM-VPN-Einstellungen/ Liste der möglichen Standard-Gateways

Wählen Sie „Ja“, um den „Datenverkehr über ein Standard-Gateway in einem DM-VPN-Netzwerk zu routen“. Der Standard-Gateway muss in der „Liste der möglichen Standard-Gateways“ stehen.

Wählen Sie „Ja“, wenn TAINY IQ-LTE die „Erreichbarkeit des Standard-Gateways mit IMCP Echo Request (Pings) überwachen“ soll. Ist ein Gateway nicht erreichbar, wird automatisch auf den nächsten verfügbaren Gateway gewechselt.

DM-VPN-Netzwerke hinzufügen

Um ein neues DM-VPN-Netzwerk hinzuzufügen, geben Sie die Namen für das Netzwerk ein und drücken Sie auf „Hinzufügen“. Definieren Sie die Merkmale für das neue Netzwerk.

GRE-Einstellungen

Lokale IP-Adresse	Geben Sie die IP-Adresse des TAINY IQ-LTE innerhalb des VPN ein. Die IP-Adresse wird vom Betreiber des DM-VPN zur Verfügung gestellt.
Subnetzmaske	Geben Sie die Kennung des Subnetzes des DM-VPN ein. Die Subnetzmaske wird vom Betreiber des DM-VPN zur Verfügung gestellt.
MTU	Geben Sie eine MTU (Maximum Transmission Unit) ein, um die maximale Größe eines IP-Paketes, das im DM-VPN genutzt wird, zu begrenzen. Dieser Wert kann von der in Kapitel 9.1definierte MTU-Größen abweichen. Bitte beachten Sie, dass das GRE-Protokoll die Größe des Daten-Paketes ansteigen lässt.

NHRP-Einstellungen

Betriebs-modus	Wählen Sie aus, ob TAINY IQ-LTE als NHRP-Spoke oder -Hub dient. Beachten Sie, dass sich nur ein Hub in der DM-VPN befinden darf.
Dauer der Gültigkeit der Regis-trierung (in Sekunden)	Nur zutreffend im Betriebsmodus „**Spoke**“: Die Dauer der Gültigkeit der Registrierung definiert den Zeitraum (in Sekunden), den der nächste Next-Hop-Server die Adress-Information behält.
Next-Hop-Server NBMA Hostname	Nur zutreffend im Betriebsmodus „**Spoke**“: Geben Sie die WAN-IP-Adresse des Next-Hop-Servers NBMA ein.
Next-Hop-Server Protokoll-Adresse	Nur zutreffend im Betriebsmodus „**Spoke**“: Geben Sie die DM-VPN-IP-Adresse des Next-Hop-Servers NBMA ein.
Unterstütz-ung für Multicast-Pakete	Aktiviert/Deaktiviert die Verteilung von Multicast-Paketen im DM-VPN.
Authenti-fizierung verwenden	Wählen Sie „Ja“, wenn TAINY IQ-LTE sich eigenständig an der remoten NHRP-Station authentifizieren soll. Geben Sie dazu den Authentifizierungsschlüssel ein.
NHRP-Purge deaktivieren	Ist „Nein“ ausgewählt, sendet TAINY IQ-LTE im Betriebsmodus Spoke nach der (Re-)Registrierung eine Aufforderung an den Hub zur Reinigung der vormals gespeicherten Routing-Daten des TAINY IQ-LTE (Standard-Implementierung). Ist „Ja“ ausgewählt, wird diese Aufforderung nicht gesendet.

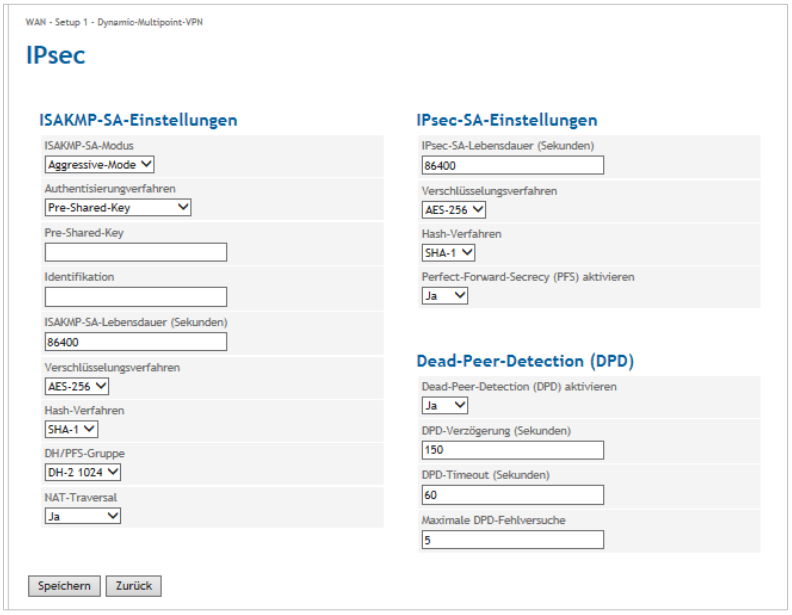
6.7 Konfiguration des IPsec für Dynamic-Multipoint-VPN

Öffnen Sie das Register **WAN** und wählen Sie im Menü „**DM-VPN**“.

IPsec

Der DM-VPN verfügt weder über eine eigene Verschlüsselung noch über einen Authentifizierungsmechanismus. Jedoch ermöglicht die IPsec-Technologie, diese Features hinzuzufügen.

Wählen Sie „`Ja`“, wenn die `Kommunikation mit IPsec geschützt` werden soll und drücken Sie auf „`Einstellungen`“.



Ist die IPsec-Funktion aktiviert, wird jeder dynamisch aufgebaute GRE-Tunnel durch den entsprechenden IPsec-Tunnel geschützt, der ebenfalls dynamisch aufgebaut wird.

`ISAKMP-SA-Einstellungen`

Die ISAKMP-SA-Einstellungen definieren das Prozedere und Paketformat zum Aufbau, Passieren, Modifizieren und Löschen der Sicherheits-verbindungen Security Associations (SA) für die IPsec-Tunnel.

`IPsec-SA-Einstellungen`

Die IPsec-SA-Einstellungen definieren die Timeouts, Verschlüsselungs-methoden, Paketformate etc. der Sicherheitsverbindung Security Association (SA) der IPsec-Tunnel.

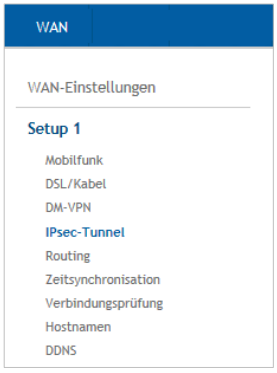
Aktiviert/Deaktiviert außerdem die Dead-Peer-Detection-(DPD-)Funktion.

Die Einstellungen, die auf ISAKMP-SA- und IPsec-SA-Einstellungen Anwendung finden, müssen sowohl mit dem Administrator der Gegenstelle als auch dem von DM-VPN abgestimmt sein. Die Einstellungen aller Kommunikationspartner TAINY IQ-LTE in diesem DM-VPN sollten möglichst gleich sein.

6.8 Konfiguration der IPsec-Tunnel

IPsec-Tunnel

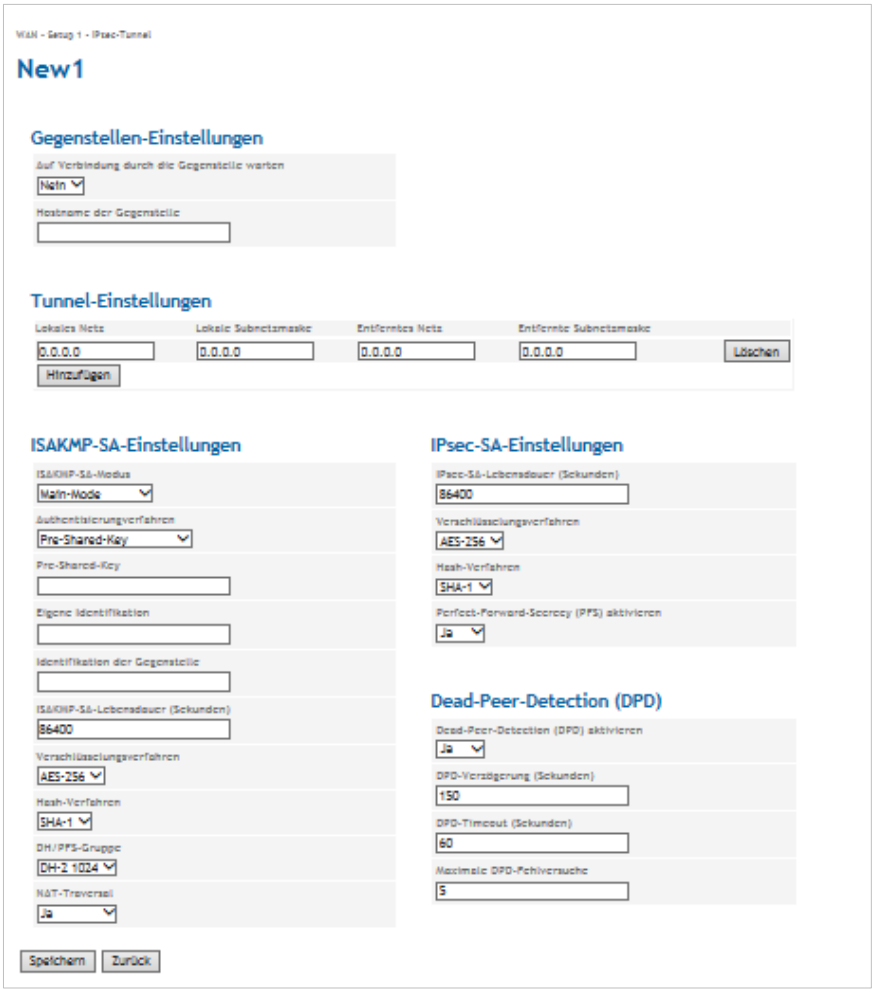
Öffnen Sie das Register **WAN** und wählen Sie im Menü „**IPsec-Tunnel**“.



Alle konfigurierten `IPsec-Hosts` sind in dieser Ansicht aufgeführt. Angegeben sind: `Name`, `Gegenstelle` und die `Anzahl der Tunnel`.

Zur Bearbeitung eines IPsec-Tunnels drücken Sie „`Bearbeiten`“ in der entsprechenden Zeile.

Um einen neuen IPsec-Host zu erstellen, geben Sie den Namen des Hosts ein und drücken Sie „`Hinzufügen`“.



Setzen Sie die folgenden Parameter, um einen bestehenden IPsec-Tunnel zu ändern oder einen neuen zu konfigurieren:

Gegenstellen-Einstellungen

Setzen Sie den Parameter **`Auf Verbindung durch die Gegenstelle warten`** auf „`Ja`“, stellen Sie sicher, dass die Gegenstelle durchgehend erreichbar ist und auf Pings antwortet.

Geben Sie den `Hostnamen der Gegenstelle` ein.

Tunnel-Einstellungen

Tunnel-Einstellungen einsehen, hinzufügen oder löschen.

Um neue Tunnel-Einstellungen hinzuzufügen, sind die folgenden Parameter erforderlich:

IPs des **`Lokalen Netzes`** und der **`Lokalen Subnetzmaske`**, die TAINY IQ-LTE verwendet, um eine Verbindung zum Remote-Netzwerk herzustellen.

Sowie die eigentlichen IPs des **`Entfernten Netzes`** und der **`Entfernten Subnetzmaske`**.

Sie können die Felder auch leer lassen.

ISAKMP-SA-Einstellungen

ISAKMP-SA-Modus

ISAKMP (Internet Security Association and Key Management) baut die Sicherheitsverbindung SA (Security Association) für den Schlüsselaustausch zwischen TAINY IQ-LTE und dem VPN-Gateway des Netzwerks der Gegenstellen auf.

Wählen Sie entweder `Main Mode` oder `Aggressive Mode`.

`Main Mode` schützt die identifizierten Peers in jedem Fall, während `Aggressive Mode` die identifizierten Peers nicht schützt.

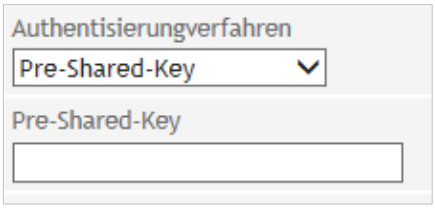
Authentifizierungsverfahren

Um die in diesem Abschnitt beschrieben nötigen Einstellungen vornehmen zu können, müssen Sie sicherstellen, dass die erforderlichen Zertifikate schon auf TAINY IQ-LTE vorhanden sind (siehe Kapitel 14 für weitere Informationen zu Zertifikaten).

Wählen Sie das bevorzugte **Authentifizierungsverfahren** aus den drei Optionen aus:

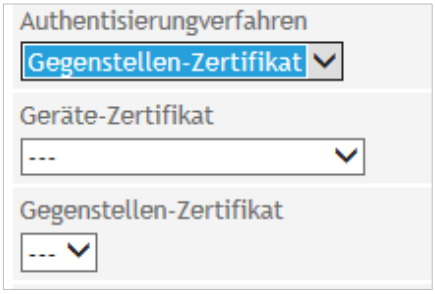
Pre-Shared-Key

Wählen Sie Pre-Shared-Key aus, geben Sie ein Passwort in das Feld Pre-Shared-Key ein.



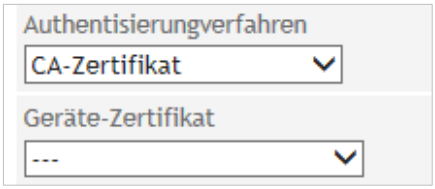
Remote-Zertifikat

Wählen Sie „Gegenstellen-Zertifikat“ aus, wählen Sie dazu das gewünschte **Geräte-Zertifikat** und abschließend das entsprechende **Gegenstellen-Zertifikat**.



CA-Zertifikat

Wählen Sie CA-Zertifikat aus, wählen Sie dazu das gewünschte **Geräte-Zertifikat** aus.



Eigene/Gegenstelle Identifikation

Geben Sie die IDs für die lokale und die ISAKMP-Sicherheitsverbindung der Gegenstellen ein.

ISAKMP-SA-Lebensdauer (in Sekunden)

Geben Sie die Gültigkeit der ISAKMP (Internet Security Association und Key Management) in Sekunden ein. Der Wert kann zwischen 1 Sekunde und 24 Stunden liegen.

Verschlüsselungsverfahren

Wählen Sie das benötigte Verschlüsselungsverfahren (Algorithmus) aus:

AES oder 3DES.

Hash-Verfahren

Wählen Sie den zu verwendenden Hash-Algorithmus.

DH/PFS-Gruppe

Wählen Sie die DH-(Dynamic Host)/PFS-(Perfect Forward Secrecy)Gruppe, die Sie mit dem Administrator des Netzwerks der Gegenstelle zum Austausch der Schlüssel vereinbart haben.

NAT-Traversal

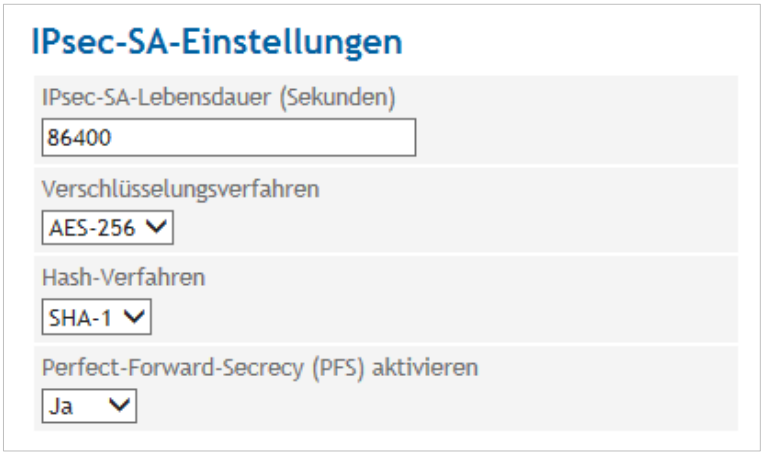
Wählen Sie:

„Ja“, um NAT-Traversal einzurichten und zu nutzen, sobald die Verbindung hergestellt ist.

„Nein“: NAT-Traversal wird nicht eingerichtet, sobald eine Verbindung hergestellt ist.

„Erzwingen“: NAT-Traversal wird in jedem Fall genutzt.

IPsec-SA-Einstellungen



IPsec (Internet Protocol Security) stellt die eigentliche Sicherheitsverbindung SA (Security Association) für die Verbindung zwischen TAINY IQ-LTE und dem Netzwerk der Gegenstelle her.

IPsec-SA-Lebensdauer (Sekunden)

Geben Sie die Gültigkeit des Internet Protocol Security in Sekunden ein. Der Wert kann zwischen 1 Sekunde und 24 Stunden liegen.

Verschlüsselungsverfahren

Wählen Sie das benötigte Verschlüsselungsverfahren (Algorithmus) aus:

„AES“ oder „3DES“.

Hash-Verfahren

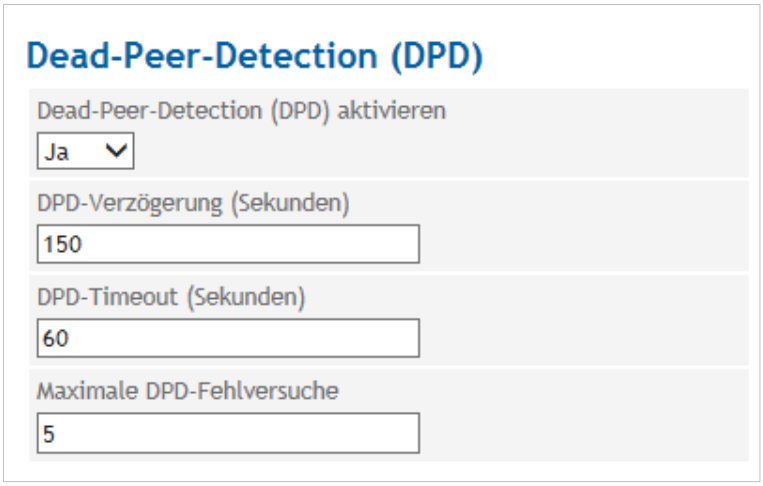
Wählen Sie das verwendete Hash-Verfahren aus.

Aktivieren des Perfect Forward Secrecy (PFS)

Wenn auf „Ja“ gesetzt, wird ein neuer Session-Key generiert (DH-Key-Exchange), sobald die ISAKMP-SA für die IPsec-SA-Sicherheitsverbindung eingerichtet ist.

Wenn auf „Nein“ gesetzt, wird die ISAKMP-SA wieder genutzt.

Dead-Peer-Detection (DPD)



Die Dead-Peer-Detection erkennt, ob die IPsec-Verbindung zwischen zwei Netzwerken noch gültig ist oder die Verbindung neu aufgebaut werden muss. Die Funktion setzt allerdings voraus, dass sie auf beiden Seiten unterstützt wird.

Vorsicht

Gefahr von zusätzlichen Kosten

Bedingt durch das Versenden von DPD-Anfragen und den Gebrauch von NAT-Traversal erhöht sich die Anzahl der gesendeten und empfangenen Daten. Abhängig von den gewählten Einstellungen kann das zu einem zusätzlichen Datenvolumen von 5 MB pro Monat führen. Das wiederum kann zusätzliche Kosten verursachen.

Dead-Peer-Detection aktivieren

Wählen Sie „Ja“, um die Funktion nutzen zu können. TAINY IQ-LTE erkennt jetzt die Gültigkeit einer Verbindung unabhängig von der Datenübertragung.

Wählen Sie „Nein“, um die Funktion abzustellen.

DPD-Verzögerung

Zeitspanne in Sekunden, innerhalb derer die DPD-Aufforderungen gesendet werden.

DPD-Timeout

Zeitspanne (in Sekunden), nach deren Ablauf die DPD-Anfrage als fehlgeschlagen gilt, wenn keine Antwort erhalten wurde. Dieses ist auch das Intervall, in dem die nächste Anfrage gesendet wird, bis die Verbindung endgültig unterbrochen wird.

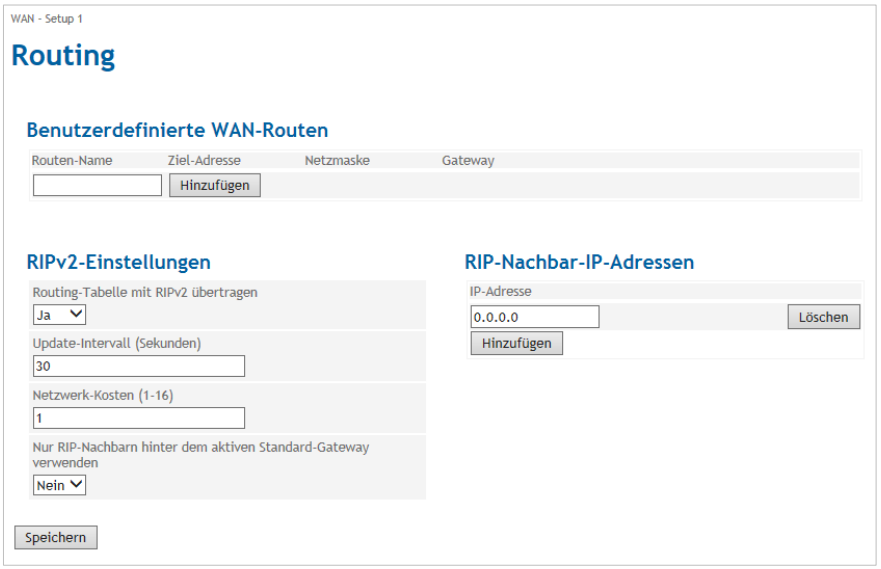
Maximale DPD-Fehlversuche

Anzahl der zulässigen Fehlversuche, bis die IPsec-Verbindung als unterbrochen erkannt wird.

6.9 Konfiguration benutzerdefinierter WAN-Routes und RIPv2

Routing

Öffnen Sie das Register **WAN** und wählen Sie im Menü „**Routing**“.



Benutzer-definierte WAN-Routen

Wählen Sie die logische Schnittstelle aus, über die der Datenverkehr von und zu der Gegenstelle über WAN geleitet werden soll:

- Über die DSL/Kabel-Verbindung
- Über eine Mobilfunk-Verbindung
- Über IP-Gateway

Geben Sie die IP-Adresse der Gegenstelle sowie der entsprechenden Netzmaske ein.

RIPv2-Einstellungen

Das RIPv2-Protokoll wird verwendet, um die konfigurierten LAN-Routing-Tabellen wiederholt zu festgesetzten Intervallen an die Gegenstelle zu übertragen.

Bieten zwei Router (z. B. TAINY IQ-LTE) die gleiche Route, können Sie die Router priorisieren. Geben Sie einen niedrigeren Wert für die **Netzwerk-Kosten** für einen der Router ein. Dieser Router wird priorisiert.

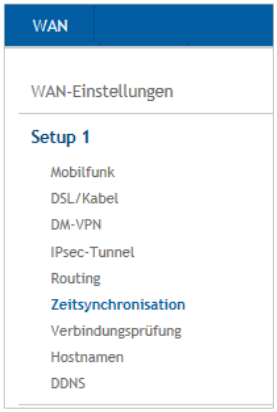
Wählen Sie „Ja“, wenn **nur** der **RIP-Nachbar hinter dem aktiven Standard-Gateway** genutzt werden soll. TAINY IQ-LTE wird die Routing-Tabellen nur über diesen Gateway übermitteln.

RIP-Nachbar-IP-Adresse

Geben Sie die IP-Adresse der Gegenstelle ein, an die die Routing-Tabellen gesendet werden sollen.

6.10 Konfiguration der Zeitsynchronisation, NTP-Einstellungen

Zeitsynchronisation



Öffnen Sie das Register **WAN** und wählen Sie im Menü „**Zeitsynchronisation**“.

NTP-Einstellungen

TAINY IQ-LTE bezieht seine Systemzeit von einem Zeit-Server via NTP (= *Network Time Protocol*). Es gibt eine ganze Reihe von Zeit-Servern im Internet, die verwendet werden können, um die aktuelle Zeit via NTP zu beziehen.

NTP-Server 1…3

Sie können bis zu 3 Zeit-Server angeben. Geben Sie entweder deren Hostname oder deren IP-Adresse ein.

Intervall der Synchronisation

Wählen Sie ein Intervall aus, zu dem der NTP-Server die tatsächlichen Zeitstempel abfragt.

NTP-Server-Funktion für das lokale Netz bereitstellen

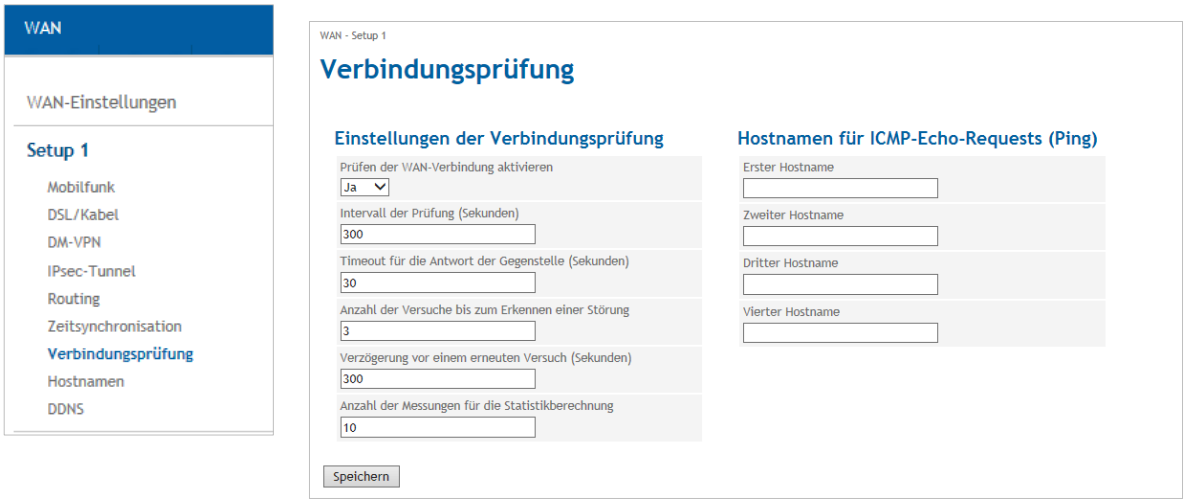
TAINY IQ-LTE kann selbst als NTP-Zeit-Server für die an die lokale Schnittstelle angeschlossenen Applikationen dienen. Um diese Funktion zu aktivieren, wählen Sie „Ja“ aus.

Der NTP-Zeit-Server des TAINY IQ-LTE kann über die für TAINY IQ-LTE gesetzte IP-Adresse erreicht werden.

6.11 Konfiguration Verbindungsprüfung

Verbindungsprüfung

Öffnen Sie das Register **WAN** und wählen Sie im Menü „**Verbindungsprüfung**“.



Mit der Funktion Verbindungsprüfung kontrolliert TAINY IQ-LTE seine Verbindungen zu UMTS/GPRS und den angeschlossenen externen Netzwerken, wie das Internet oder ein Intranet. Dazu sendet TAINY IQ-LTE in regelmäßigen Intervallen Ping-Pakete (ICMP) an bis zu 4 Gegenstellen.

Einstellungen der Verbindungsprüfung

Prüfen der WAN-Verbindung aktivieren

Wählen Sie „Ja“, um die Verbindungsprüfung zu aktivieren.

Intervall der Prüfung (Sekunden)

Legt das Intervall fest, zu dem die Verbindungsprüfung durchgeführt wird.

Timeout für die Antwort der Gegenstelle (Sekunden)

Legt die Antwortzeit des Timeouts fest. Erhält TAINY IQ-LTE innerhalb dieser Zeitspanne die ICMP-Ping-Antworten der Gegenstelle, war die Überprüfung erfolgreich.

Anzahl der Versuche bis zum Erkennen einer Störung

Legt die Anzahl der Wiederholung fest, bis ein Fehler entdeckt wird. Erhält TAINY IQ-LTE nicht innerhalb des Timeouts der Antwortzeit eine ICMP-Ping-Antwort, wird die Überprüfung gemäß der festgelegten Anzahl der Wiederholungen durchgeführt. Sind alle Wiederholungen fehlgeschlagen, gilt die Überprüfung als fehlgeschlagen.

Verzögerung vor einem erneuten Versuch (Sekunden)

Legt die Verzögerung zwischen den Wiederholungen fest.

Anzahl der Messungen für die Statistikberechnung

Bestimmt die Anzahl der Stichproben, die für die Kalkulation eines Durchschnittwertes genommen werden.

Hostnamen für ICMP-Echo-Requests (Ping)

Erster…Vierter Hostname

Geben Sie bis zu vier Gegenstellen ein, die TAINY IQ-LTE pingen kann. Die Gegenstellen müssen durchgehend verfügbar sein und auf die ICMP-Pakete antworten.

Tipp

Stellen Sie sicher, dass die Gegenstelle nicht mit Anfragen „überlastet“ wird.

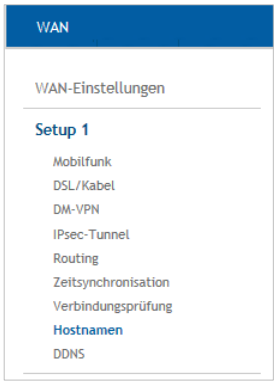
Tipp

Soll mit der Verbindungsüberwachung ein VPN Tunnel überwacht werden, sollte nur die VPN-Gegenstelle als ICMP Ziel angegeben werden.
Bei Angabe weiterer Hosts, welche auf die ICMP Requests antworten, wird sonst der Ausfall des Tunnels nicht erkannt.

6.12 Hostnamen remoten IP-Adressen zuordnen

Hostnamen

Öffnen Sie das Register **WAN** und wählen Sie im Menü „**Hostnamen**“.



Mit dieser Funktion können IP-Adressen von Gegenstellen Hostnamen zugeordnet werden. Diese Funktion lässt die an die LAN-Schnittstellen des TAINY IQ-LTE angeschlossenen Applikationen die Gegenstellen mit den hier angegebenen Hostnamen ansprechen.
TAINY IQ-LTE-Funktionen (z. B. NTP) können dieses Feature auch nutzen.

Die hier konfigurierten Hostnamen sind nur für das ausgewählte WAN-Setup gültig. Hostnamen, die unabhängig von dem WAN-Setup sind, können im Abschnitt LAN eingegeben werden, siehe Kapite8.

6.13 Dynamisches DNS (DDNS)

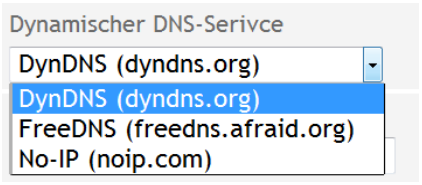
DDNS

Öffnen Sie das Register **WAN** und wählen Sie im Menü „**DDNS**“.

TAINY IQ-LTE verwendet DynDNS-Services, um mittels des DynDNS-Hostnamen ansprechbar zu sein. Sie können diese Funktion aktivieren oder deaktivieren.

Dynamischer DNS-Service

Wählen Sie eine der drei unterstützten Funktionen aus:



Benutzername Passwort

Geben Sie den Benutzername und das Passwort ein, um auf den ausgewählten DynDNS-Service zuzugreifen.

Dynamischer DNS-Hostname

Geben Sie den Hostnamen ein, mit dem TAINY IQ-LTE angesprochen wird (verfügbar beim DynDNS-Service).

SSL verwenden

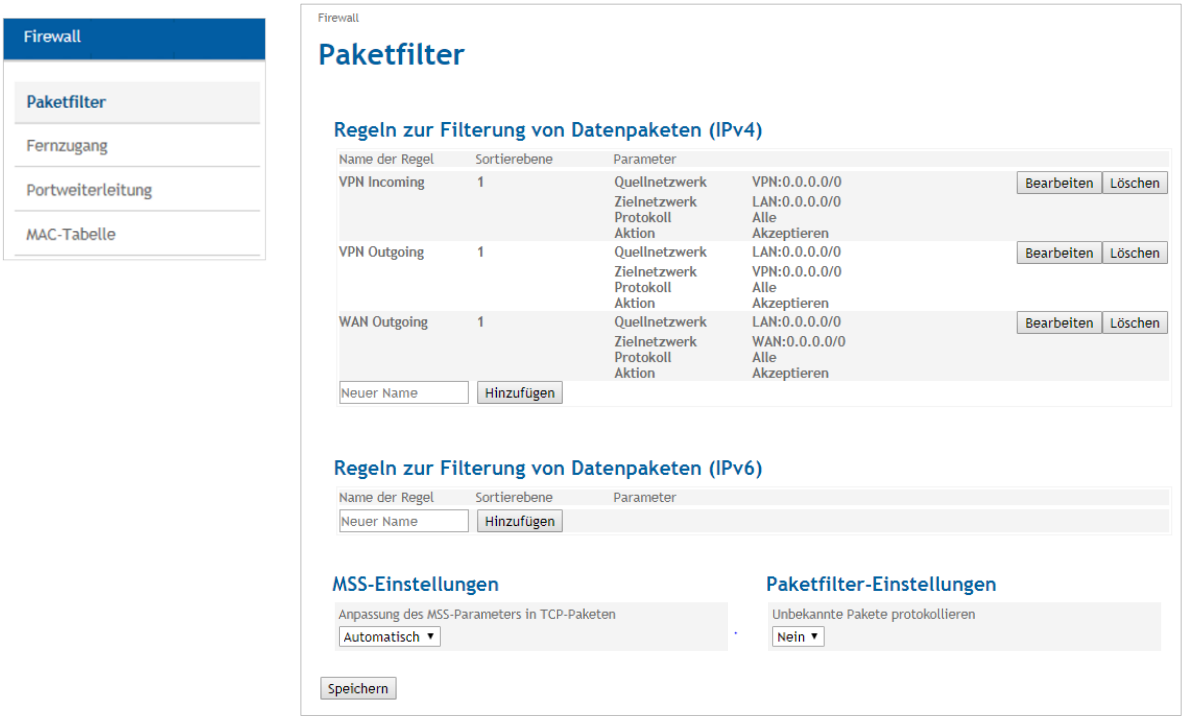
Legen Sie fest, ob die Verbindung zum DynDNS-Service SSL-geschützt sein soll.

7 Firewall-Einstellungen

7.1 Konfiguration der Paketfilter

Paketfilter

Öffnen Sie das Register **`Firewall`** und wählen Sie im Menü „**`Paketfilter`**“.



`Paketfilter IPv4 und IPv6`

Es ist möglich, über die Firewall-Einstellungen IPv4 und IPv6 Netzwerke Zugang zu erlauben.

Sind keine Regeln für die Paketfilter eingerichtet, unterbindet die Firewall jeglichen Datenverkehr, der durch TAINY IQ-LTE fließt, wie z.B. von LAN zu WAN oder LAN zu LAN. Nur der interne Datenverkehr, der sich ausschließlich innerhalb TAINY IQ-LTE bewegt, wie beispielsweise für die Konfiguration, ist nicht blockiert.

Standardmäßig sind drei Regeln für Paketfilter eingerichtet (VPN-Eingang, VPN-Ausgang und WAN-Ausgang).

Paketfilter können definiert werden, um Datenverkehr von einer bestimmten Datenquelle zu einem bestimmten Datenziel und umgekehrt zu senden.

`Regeln zur Filterung von Datenpaketen (IPv4)`

Hier werden die Einstellung für den IPv4 basierenden Datenverkehr vorgenommen.

Um einen Paketfilter einzurichten eben Sie einen **`Namen`** für die neue Regel in das Feld in diesem Bereich ein und drücken Sie „**`Hinzufügen`**“.

`Paketfilter-Einstellungen`

Setzen Sie „**`Unbekannte Pakete protokollieren`**“ auf „`Ja`“, damit unbekannte Datenpakete in den Logbüchern protokolliert und angezeigt werden.

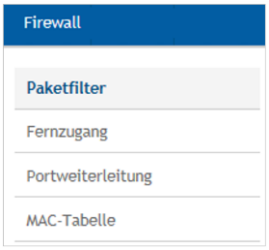
MSS-Einstellungen

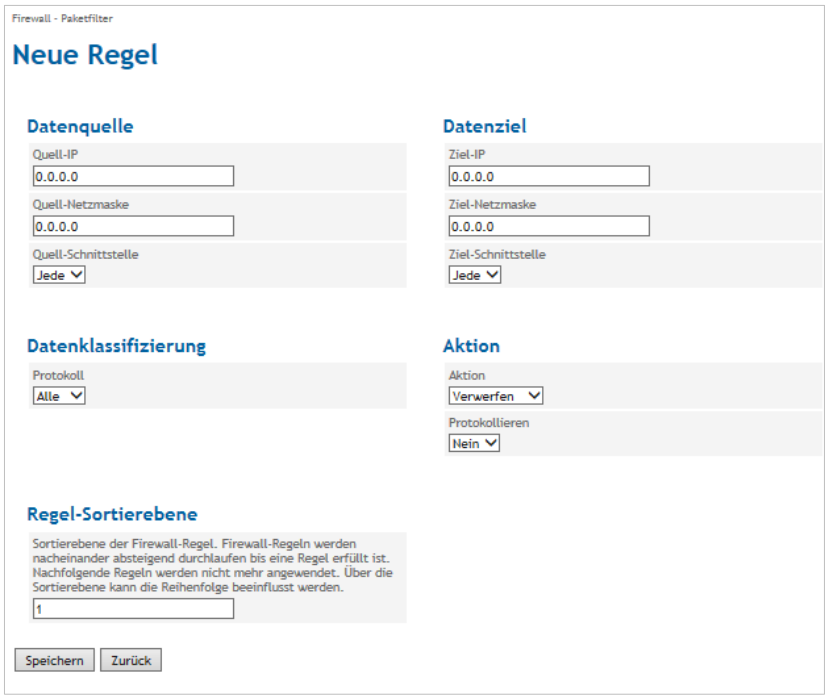
Wählen Sie ob der `MSS` (Maximum Segment Size) `Parameter` in `TCP-Paketen` `manuell` oder `automatisch` angepasst oder `deaktivier` wird.

Wählen Sie die Option manuell tragen Sie den `MSS-Wert` der Größe ein.

Regeln definieren

IPv4





Datenquelle

Geben Sie die IP-Adresse und Netzmaske der Applikation ein, die Daten senden sollen. Definieren Sie die „**`Quell-Schnittstelle`**“, mit der die Datenquelle verbunden ist (WAN, LAN, DM-VPN oder Alle).

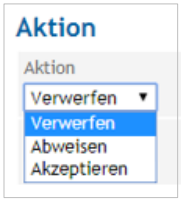
Datenziel

Geben Sie die IP-Adresse und Netzmaske der Applikation ein, die Daten erhalten sollen. Definieren Sie die „**`Ziel-Schnittstelle`**“, mit der das Datenziel verbunden ist (WAN, LAN, DM-VPN oder Alle).

Datenklassifi-zierung

Legen Sie fest, ob nur ein bestimmtes Datenprotokoll den Paketfilter passieren darf (TCP, UDP, ICMP oder Alle).

Aktion



Legen Sie fest, wie mit den Daten aus dieser Datenquelle verfahren werden soll: `Akzeptieren`, `Verwerfen` oder `Abweisen`.

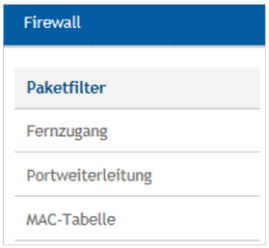
Setzen Sie diese Einstellung auf „`Ja`“, wird jedesmal, wenn die Bedingungen dieser Regel erfüllt sind, ein Eintrag in das Firewall-Logbuch vorgenommen. Diese Einträge können mittels Snapshot abgerufen werden (siehe Kapitel 15.6).

Um jede Aktion zu `protokollieren`, wählen Sie „`Ja`“.

Regel-Sortierebene

Bezeichnet die Sortierebene der Firewall-Regeln. Firewall-Regeln werden sequenziell verarbeitet in absteigender Reihenfolge, bis eine passende Regel gefunden ist. Die nachfolgenden Regeln finden danach keine Anwendung mehr. Die Reihenfolge der Regeln wird durch die Sortierebene beeinflusst. Die Ebene 1 wird zuerst bearbeitet, dann Ebene 2 usw.

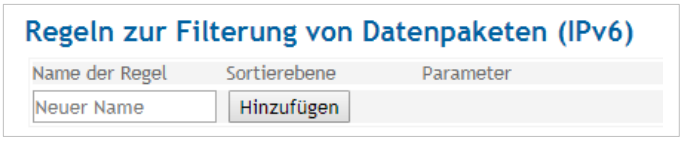
Regeln zur Filterung von Datenpaketen (IPv6)



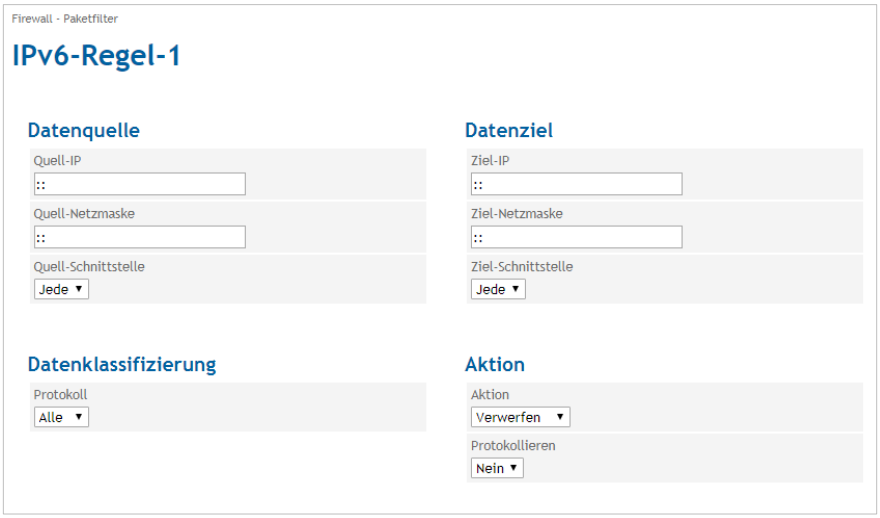
IPv6

Hier werden die Einstellung für den IPv6 basierenden Datenverkehr vorgenommen.

Um einen Paketfilter einzurichten eben Sie einen **Namen** für die neue Regel in das Feld in diesem Bereich ein und drücken Sie „**Hinzufügen**“.



Als Beispiel wir die Regel „IPv6-Regel-1“ angelegt:



Datenquelle

Geben Sie die IPv6-Adresse und IPv6-Netzmaske der Applikation ein, die Daten senden sollen. Definieren Sie die „**Quell-Schnittstelle**“, mit der die Datenquelle verbunden ist (WAN, LAN oder Jede).

Datenziel

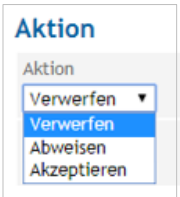
Geben Sie die IPv6-Adresse und IPv6-Netzmaske der Applikation ein, die Daten erhalten sollen. Definieren Sie die „**Ziel-Schnittstelle**“, mit der das Datenziel verbunden ist (WAN, LAN oder Jede).

Datenklassifizierung

Legen Sie fest, ob nur ein bestimmtes Datenprotokoll den Paketfilter passieren darf (TCP, UDP, ICMP oder Alle).

Aktion

Legen Sie fest, wie mit den Daten aus dieser Datenquelle verfahren werden soll: `Akzeptieren`, `Verwerfen` oder `Abweisen`.



Setzen Sie diese Einstellung auf „Ja“, wird jedes Mal, wenn die Bedingungen dieser Regel erfüllt sind, ein Eintrag in das Firewall-Logbuch vorgenommen. Diese Einträge können mittels Snapshot abgerufen werden (siehe Kapitel 15.6).

Um jede Aktion zu protokollieren, wählen Sie „Ja“.

Regel-Sortierebene

Bezeichnet die Sortierebene der Firewall-Regeln. Firewall-Regeln werden sequenziell verarbeitet in absteigender Reihenfolge, bis eine passende Regel gefunden ist. Die nachfolgenden Regeln finden danach keine Anwendung mehr. Die Reihenfolge der Regeln wird durch die Sortierebene beeinflusst. Die Ebene 1 wird zuerst bearbeitet, dann Ebene 2 usw.

Anwendungs-beispiele IPv6 Firewall-Regeln

Für „Alles erlauben“ reicht der Eintrag :: Datenquelle und Datenziel

Ganze netzte den Zugriff erlauben:

Datenquelle:

Quell-IP:

2a01:0598:990e:66bf:0000:0000:0000:0000

Quell-Netzwerkmaske:

ffff:ffff:ffff:ffff:0000:0000:0000:0000

Datenziel: (erlaubt an alle Rechner im lokalen Netzwerk)

Ziel-IP:

0000:0000:0000:0000:0000:0000:0000:0000

Ziel-Netzwerkmaske:

0000:0000:0000:0000:0000:0000:0000:0000

Oder Ziel-IP ::, Ziel-Netzwerkmaske ::

IPv6 Traffic nur an einen Rechner im LAN erlauben:

Ziel-IP:

2a01:598:990e:66bf:dcad:beff:feef:aaaa

Ziel-Netzwerkmaske:

ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Von dem Prefix (Netz-ID) 2a01:598:990e:66bf alle Rechner der Zugriff erlauben

Ziel-IP:

2a01:598:990e:66bf:ffff:ffff:ffff:ffff

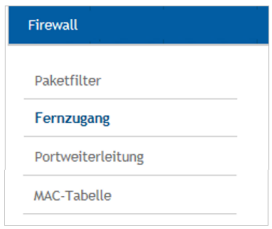
Ziel-Netzwerkmaske:

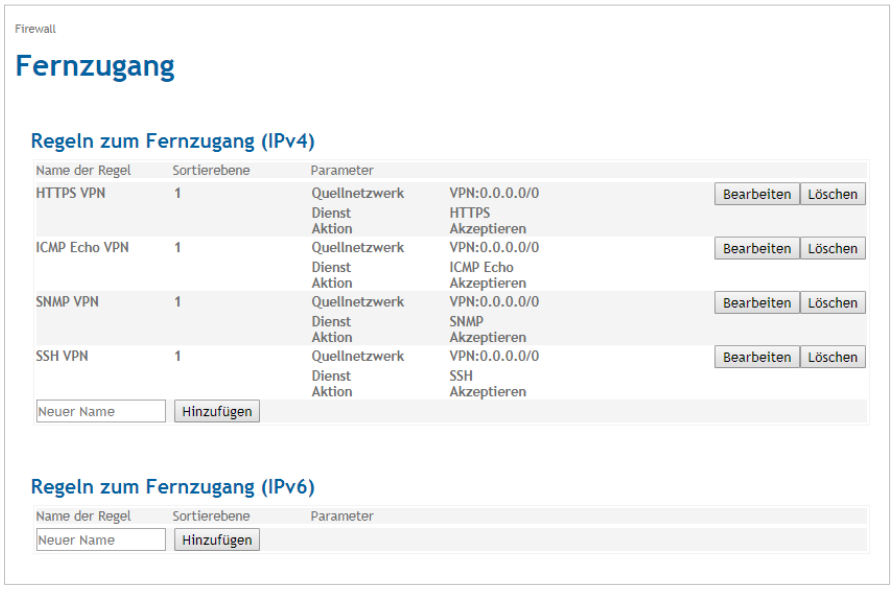
ffff:ffff:ffff:ffff:: ist wie ffff:ffff:ffff:ffff:0000:0000:0000:0000

7.2 Konfiguration Fernzugang

Fernzugang

Öffnen Sie das Register **`Firewall`** und wählen Sie im Menü „**`Fernzugang`**“.



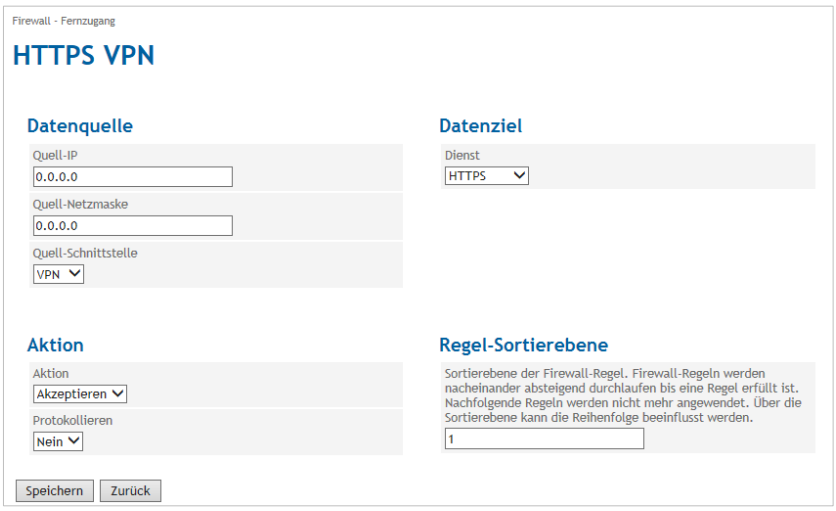


Es ist möglich, über die Firewall-Einstellungen den Fernzugang für Dienste wie HTTP, SSH, ICMP oder SNMP für IPv4 und IPv6 Netzwerke zu erlauben.

Regeln für Fernzugang definieren

Um einen neuen Fernzugang einzurichten oder die Regeln für einen bestehenden Fernzugang zu ändern, drücken Sie „**`Hinzufügen`**“ (hier erst den Namen für den neuen Zugang eintragen) oder „**`Bearbeiten`**“.

`HTTPS-VPN`



`Datenquelle`

Geben Sie die IP-Adresse und die Netzmaske der Applikation ein, die Daten senden soll.

Definieren Sie die **`Quell-Schnittstelle,`** mit der die Datenquelle verbunden ist (WAN, VPN).

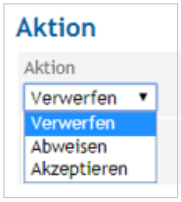
`Datenziel`

Wählen Sie den benötigten **`Dienst`** (siehe Kapitel 18) aus der Liste:

- HTTPS
- SSH

- ICMP
- SNMP
- RS 232

Aktion



Legen Sie fest, wie mit den Daten aus dieser Datenquelle verfahren werden soll: `Akzeptieren`, `Verwerfen` oder `Abweisen`.

Setzen Sie diese Einstellung auf „`Ja`“, wird jedes Mal, wenn die Bedingungen dieser Regel erfüllt sind, ein Eintrag in das Firewall-Logbuch vorgenommen. Diese Einträge können mittels Snapshot abgerufen werden (siehe Kapitel 15.6).

Um jede Aktion zu `protokollieren`, wählen Sie „`Ja`“.

Regel-Sortierebene

Bezeichnet die Sortierebene der Firewall-Regeln. Firewall-Regeln werden sequenziell verarbeitet in absteigender Reihenfolge, bis eine passende Regel gefunden ist. Die nachfolgenden Regeln finden danach keine Anwendung mehr. Die Reihenfolge der Regeln wird durch die Sortierebene beeinflusst. Die Ebene 1 wird zuerst bearbeitet, dann Ebene 2 usw.

Regeln zum Fernzugang IPv6

Anlegen von Regeln für den Fernzugang IPv6 basierender Verbindungen

Um einen neuen Fernzugang einzurichten oder die Regeln für einen bestehenden Fernzugang zu ändern, drücken Sie „**Hinzufügen**“ (hier erst den Namen für den neuen Zugang eintragen) oder „**Bearbeiten**“.

Als Beispiel wir eine Regel mit den Namen IPv6-Ferzugang-1 angelegt.

Datenquelle

Geben Sie die IPv6-Adresse und die IPv6-Netzmaske der Applikation ein, die Daten senden soll.

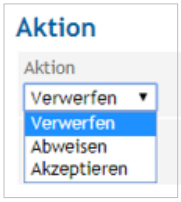
Datenziel

Wählen Sie den benötigten **Dienst** (siehe Kapitel 18) aus der Liste:

- HTTPS
- SSH

- ICMP
- SNMP
- RS 232

Aktion



Legen Sie fest, wie mit den Daten aus dieser Datenquelle verfahren werden soll: `Akzeptieren`, `Verwerfen` oder `Abweisen`.

Setzen Sie diese Einstellung auf „`Ja`“, wird jedes Mal, wenn die Bedingungen dieser Regel erfüllt sind, ein Eintrag in das Firewall-Logbuch vorgenommen. Diese Einträge können mittels Snapshot abgerufen werden (siehe Kapitel 15.6).

Um jede Aktion zu `protokollieren`, wählen Sie „`Ja`“.

Regel-Sortierebene

Bezeichnet die Sortierebene der Firewall-Regeln. Firewall-Regeln werden sequenziell verarbeitet in absteigender Reihenfolge, bis eine passende Regel gefunden ist. Die nachfolgenden Regeln finden danach keine Anwendung mehr. Die Reihenfolge der Regeln wird durch die Sortierebene beeinflusst. Die Ebene 1 wird zuerst bearbeitet, dann Ebene 2 usw.

Anwendungs-beispiele IPv6 Firewall-Regeln für den Fernzugang

Für „Alles erlauben“ reicht der Eintrag :: Datenquelle

Ganze netzte den Zugriff erlauben:

Datenquelle:

Quell-IP:

2a01:0598:990e:66bf:0000:0000:0000:0000

Quell-Netzwerkmaske:

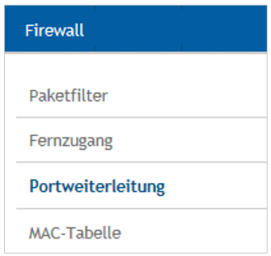
ffff:ffff:ffff:ffff:0000:0000:0000:0000

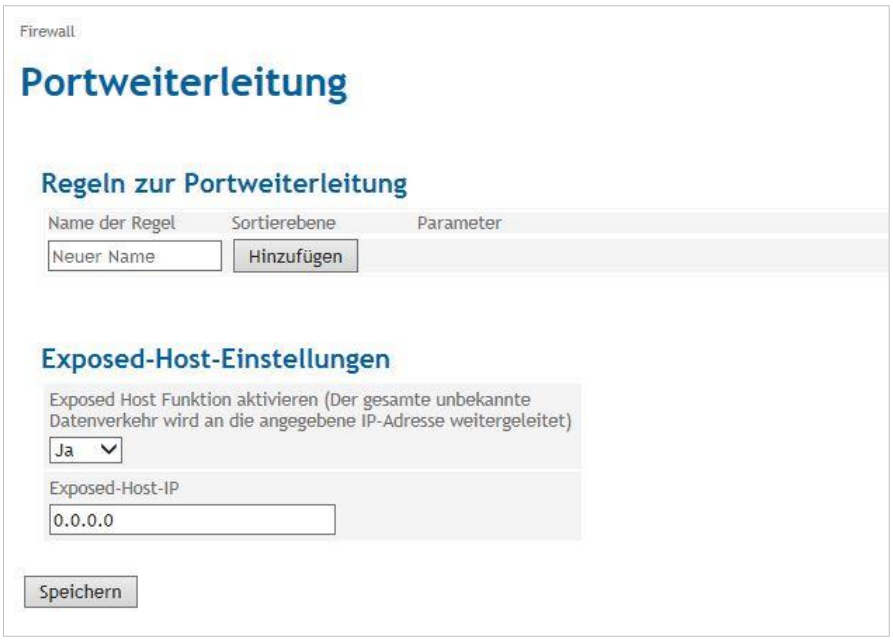
Jedem Rechner von der Datenquelle mit dem Prefix (Netz-ID) 2a01:598:990e:66bf den Fernzugang erlauben

7.3 Konfiguration der Portweiterleitung

Portweiterleitung

Öffnen Sie das Register **`Firewall`** und wählen Sie im Menü „**`Port-Weiterleitung`**“.

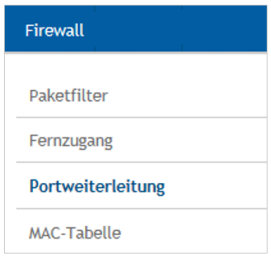


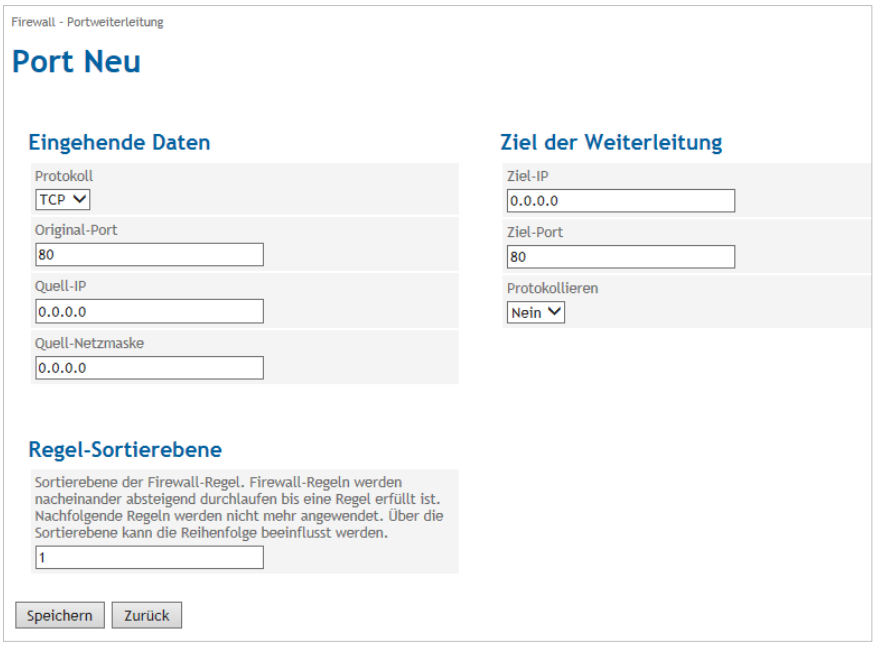


Die Portweiterleitung bestimmt, ob der beim TAINY IQ-LTE über einen bestimmten IP-Port eingegangene Datenverkehr an eine festgelegte IP-Adresse oder einen Port weitergeleitet wird.

Um eine neue Portweiterleitung einzurichten oder die Regeln für eine bestehende Weiterleitung zu ändern, drücken Sie „**`Hinzufügen`**“ (hier erst den Namen für den neuen Weiterleitung eintragen) oder „**`Bearbeiten`**“.

`Regel definieren`





Eingehender Datenverkehr

Bestimmt den Protokolltyp (TCP or UDP) der eingehenden Daten, die weitergeleitet werden sollen, sowie den IP-Port, an den die eingehenden Daten ursprünglich gesendet wurden.

Mittels Quell-IP/Netzmaske findet die Regel für die Portweiterleitung nur Anwendung auf Daten, die aus einem definierten Quell-Netzwerk kommen.

Ziel der Weiterleitung

Legt per IP-Adresse und IP-Port das Ziel fest, zu dem die Daten weitergeleitet werden.

Ist die Funktion „Protokollieren“ auf „Ja“ gesetzt, wird jedes Mal, wenn die Bedingungen dieser Regel erfüllt sind, ein Eintrag in das Firewall-Logbuch vorgenommen. Diese Einträge können mittels Snapshot abgerufen werden (siehe Kapitel 15.6).

Regel-Sortierebene

Bezeichnet die Sortierebene der Firewall-Regeln. Firewall-Regeln werden sequenziell verarbeitet in absteigender Reihenfolge, bis eine passende Regel gefunden ist. Die nachfolgenden Regeln finden danach keine Anwendung mehr. Die Reihenfolge der Regeln wird durch die Sortierebene beeinflusst. Die Ebene 1 wird zuerst bearbeitet, dann Ebene 2 usw.

Regelsortierung findet keine Anwendung für IP-Ports, die TAINY IQ-LTE selbst nutzt, wie z. B. 443, 500, 4500.

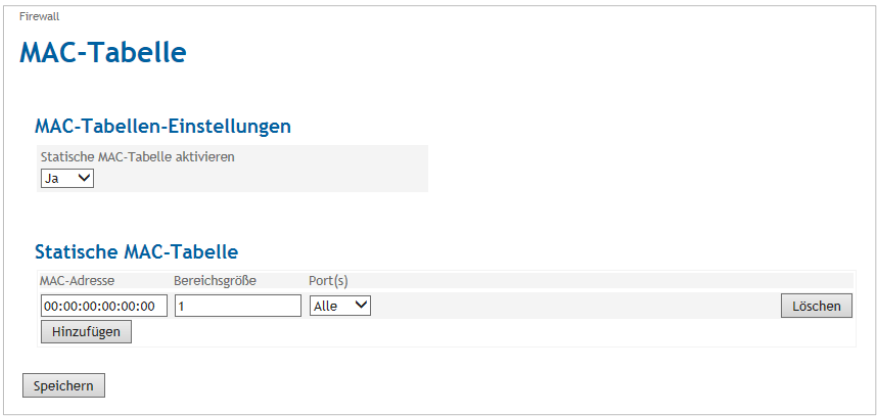
Exposed Host-Einstellungen

Soll die Exposed Host Funktion aktiviert werden, wählen Sie unter Exposed Host-Einstellungen die Option „Ja“. Tragen Sie anschließend die IP des Exposed Hosts ein.

7.4 Konfiguration MAC-Tabelle

MAC-Tabelle

Öffnen Sie das Register **`Firewall`** und wählen Sie im Menü „**`MAC-Tabelle`**“.



Ist die statische MAC-Tabellen-Funktion aktiviert, können nur Geräte über TAINY IQ-LTE kommunizieren, deren MAC-Adresse in die **`Statische MAC-Tabelle`** eingetragen wurde.

Sie können eine MAC-Adresse für alle Ports oder nur für eine bestimmte physikalische Netzschnittstelle (ETH0 bis ETH1) aktivieren.

Die `Bereichsgröße` bestimmt die Anzahl der MAC-Adressen, beginnend mit der aktuellen MAC-Adresse, die nicht blockiert wird.

8 LAN-Einstellungen TAINY IQ-LTE 6E

8.1 Konfiguration physikalische Netzwerk-Schnittstelle/VLANs erstellen

LAN-Schnittstellen

Öffnen Sie das Register **LAN** und wählen Sie im Menü „**LAN-Schnittstelle**“.

Physikalische Netzwerk-Schnittstellen

TAINY iQ bietet bis zu fünf `physikalische Netzwerk-Schnittstellen` ETH1…ETH5 zum Anschluss lokaler Applikationen. ETH0 kann als ein DSL/Kabel-WAN-Port oder als ein zusätzlicher LAN-Port (siehe Kapitel 9.3) genutzt werden.

Um jede `physikalische Netzwerk-Schnittstelle` einzeln zu konfigurieren, drücken Sie „**Bearbeiten**“ in der entsprechenden Zeile.

ETH1…ETH5

Schnittstellen-Einstellungen

Aktiviert/Deaktiviert die `physikalischen Netzwerk-Schnittstellen`. Zur Aktivierung setzen Sie die Einstellung auf „`Ja`“.

Modus

Bestimmt die Daten-Übertragungsrate (10 MBit/s oder 100 MBit/s) und das Übertragungsverfahren (Halbduplex oder Vollduplex).

Ist der Modus auf „Automatisch“ gesetzt, bestimmen TAINY iQ und das an die physikalische Netzwerk-Schnittstelle angeschlossene Gerät die Einstellungen automatisch.

VLAN-ID-Vorgabe

Diese ID ordnet die physikalische Netzwerk-Schnittstelle einem Virtual Local Area Network (VLAN = virtuelles lokales Gebiets-Netzwerk) zu. Alle physikalischen Schnittstellen, die über dieselbe VLAN-ID verfügen, sind Teil dieses VLAN.

Siehe Glossar für weitere Informationen.

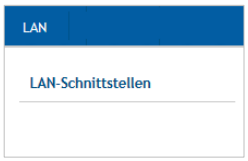
VLAN-Betrieb mit 802.1Q-getaggten Frames aktivieren

Wählen Sie „Ja“, wenn die VLAN-Tags über die physikalische Netzwerk-Schnittstelle an die angeschlossenen Anwendungen weitergeleitet werden sollen. Andernfalls werden die VLAN-Tags vor der Übertragung der Kommunikation entfernt.

8.2 Konfiguration logische Netzwerk-Schnittstelle/Adresszuordnung (DHCP)

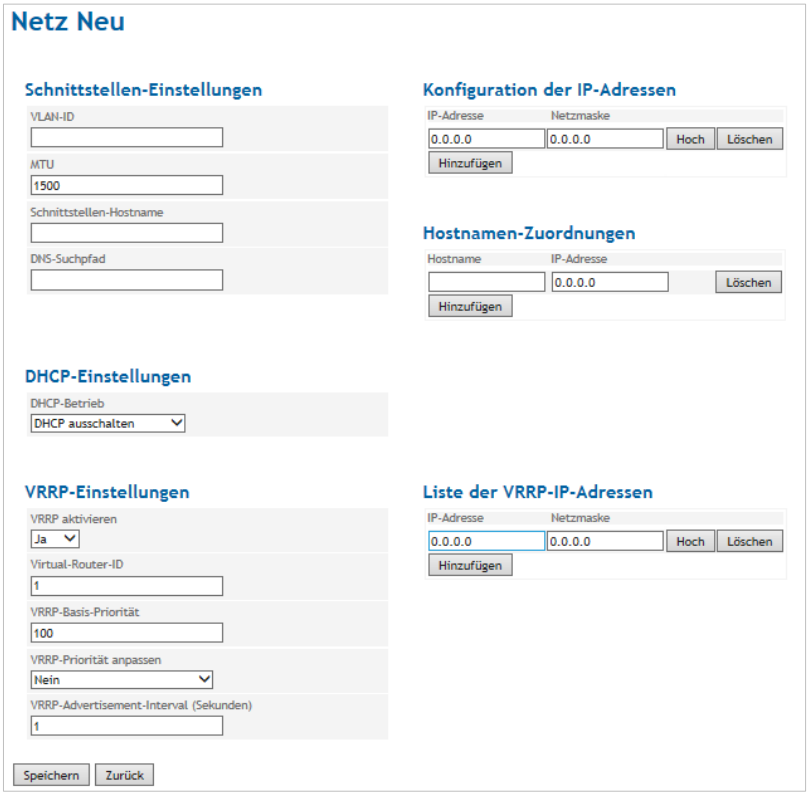
LAN-Schnittstellen

Öffnen Sie das Register **LAN** und wählen Sie im Menü „**LAN-Schnittstelle**“.



LAN 1

Um eine neue `logische Netzwerk-Schnittstelle` zu erstellen oder eine bestehende Schnittstelle zu ändern, drücken Sie „**Hinzufügen**“ (geben Sie vorab einen Namen für die neue Schnittstelle ein) oder „**Bearbeiten**“.



Schnittstellen-Einstellungen

VLAN-ID

Geben Sie die ID des VLANs ein, auf das sich die logische Netzwerk-Schnittstelle beziehen soll. Eine logische Netzwerk-Schnittstelle darf sich nur auf ein VLAN beziehen.

MTU

Geben Sie das MTU (Maximum Transmission Unit) ein, um die maximale Größe der IP-Pakete festzulegen.

Schnittstellen-Hostname

Die logische Netzwerk-Schnittstelle kann entweder mit einer IP-Adresse oder einem Hostnamen angesprochen werden. Um sie mit Hostname anzusprechen, tragen Sie den Namen in das entsprechende Feld ein.

DNS-Suchpfad

Geben Sie den Domainnamen des Suchpfades ein.

Hostnamen-Zuordnung

Hostname, IP-Adresse

TAINY iQ erlaubt es, den IP-Adressen der Gegenstelle Hostnamen zuzuordnen. Mittels dieser Funktion sprechen die an der TAINY iQ-LAN-Schnittstelle angeschlossenen Applikationen die Gegenstelle mit dem Hostnamen an. Die TAINY iQ-Funktionen (z. B. NTP) nutzen auch dieses Feature. Siehe auch Hostnamen-Zuordnung WAN-Setups Kapitel 6.12.

DHCP-Einstellungen

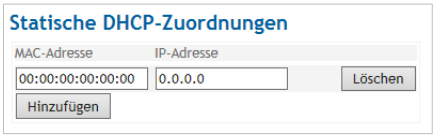
DHCP-Betriebseinstellungen

TAINY iQ bietet eine DHCP-Server- oder eine DHCP-Relais-Funktion.

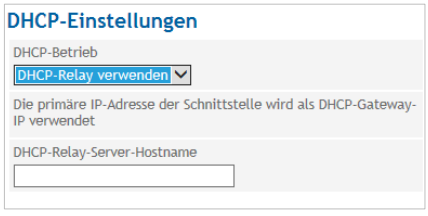
Tipp

Nur die primäre IP-Adresse der Schnittstelle (z. B. ETH0) wird als DHCP-Gateway-IP verwendet.

Ist die DHCP-Server-Funktion aktiviert, ordnet TAINY iQ selbst den an die LAN-Schnittstelle angeschlossenen Applikationen IP-Adressen zu. Definieren Sie den Bereich, aus dem die zuzuordnenden IP-Adressen und/oder die MAC-Adressen verwendet werden sollen.



Ist die DHCP-Relais-Funktion aktiviert, leitet TAINY iQ die DHCP-Anfrage der an die LAN-Schnittstelle angeschlossenen Applikationen an einen Remote-DHCP-Relais-Server weiter, der die IP-Adressen zur Verfügung stellt. Geben Sie den Hostnamen oder die IP-Adresse des DHCP-Relais-Servers ein.



8.3 Konfiguration VRRP

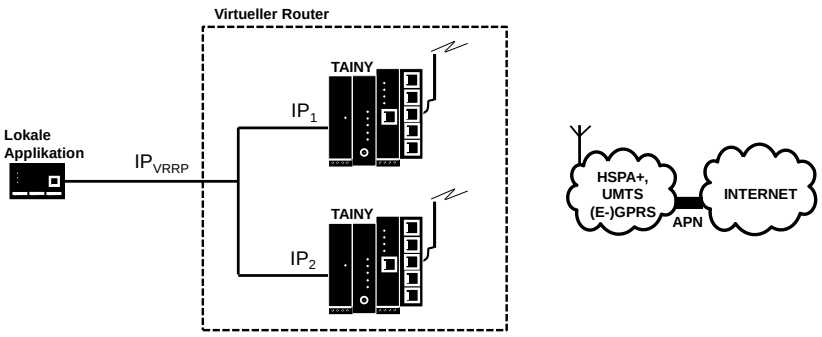
VRRP-Einstellungen

Öffnen Sie das Register **LAN** und wählen Sie im Menü „**LAN-Schnittstelle**“.

TAINY IQ unterstützt das Virtual Router Redundancy Protokoll (VRRP). Aktivieren/Deaktivieren Sie diese Funktion in den Einstellungen der logischen Netzwerk-Schnittstelle. Zwei TAINY IQ -Router fungieren als ein virtueller Router. Sollte ein TAINY IQ die WAN-Verbindung oder die VPN-Verbindung verlieren, übernimmt und unterstützt der zweite TAINY IQ die Verbindung.

Wenn Sie mehrere virtuelle Router für ein Netzwerk definieren, dann stellen Sie sicher, dass Sie diesen unterschiedliche IDs zu ordnen.

Die **VRRP-Basis-Priorität** legt fest, welcher TAINY IQ als Master und welcher als Back-up dient. Der TAINY IQ mit der höchsten Priorität ist Master.
Geben Sie Werte zwischen 1 (niedrigste Prio) und 254 (höchste Prio) ein. Die VRRP-Priorität kann im Falle einer aktiven WAN- oder VPN-Verbindung automatisch an den neuen Wert (**Angepasste VRRP-Priorität**) angepasst werden.



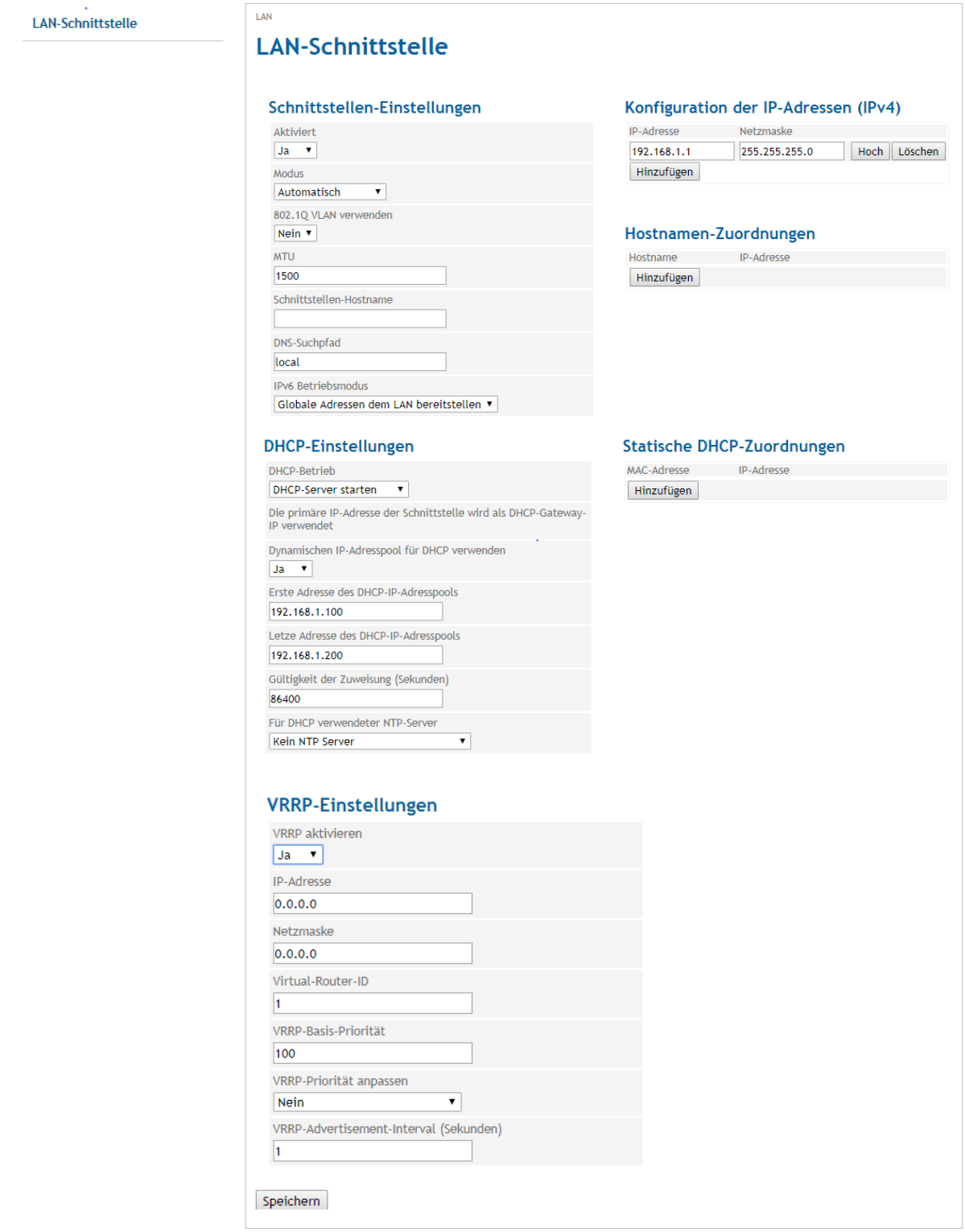
Die IP_{VRRP} ist die IP-Adresse des virtuellen Routers. Geben oder fügen Sie diese zu der **Liste der VRRP-IP-Adressen** hinzu. Nutzen Sie diese als Standard-Gateway für die lokale Applikation. IP_1 und IP_2 sind die IP-Adressen des TAINY IQ, wie in der **IP-Adressen-Konfiguration** jedes TAINY IQ eingegeben.

9 LAN-Einstellungen TAINY IQ-LTE

9.1 Konfiguration der LAN-Schnittstelle/DHCP-/VRRP-Einstellungen

LAN-Schnittstelle

Öffnen Sie das Register **LAN** und wählen Sie im Menü „**LAN-Schnittstelle**“.



Schnittstellen-Einstellungen

Aktiviert

Wählen Sie „Ja“, um die Schnittstelle zu aktivieren.

Modus

Setzen Sie den benötigten Modus, um die benötigte Datenübertragungsrate (10 MBit/s oder 100 MBit/s) und das Übertragungsverfahren (Halbduplex oder Vollduplex) zu bestimmen.

Ist der Modus auf „Automatisch“ gesetzt, bestimmen TAINY IQ-LTE und das an die LAN-Schnittstelle angeschlossene Gerät die Einstellungen automatisch.

802.1Q-VLAN verwenden

Setzen Sie die Option auf „**Ja**“ und geben Sie die VLAN-ID ein, um die Kommunikation mit den 802.1Q-getaggten Ethernet-Frames zu aktivieren.

Setzen Sie die Option auf „Nein“, um 802.1Q-Tags in dieser Schnittstelle zu deaktivieren.

MTU

Geben Sie das MTU (Maximum Transmission Unit) ein, um die maximale Größe der IP-Pakete festzulegen.

Schnittstellen-Hostname

Die logische Netzwerk-Schnittstelle kann entweder mit einer IP-Adresse oder einem Hostnamen angesprochen werden. Um sie mit Hostname anzusprechen, tragen Sie den Namen in das entsprechende Feld ein.

DNS-Suchpfad

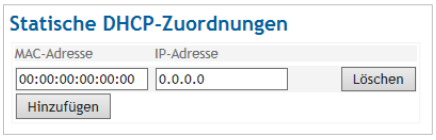
Geben Sie den Namen des Domain-Servers des Suchpfades ein.

DHCP-Einstellungen

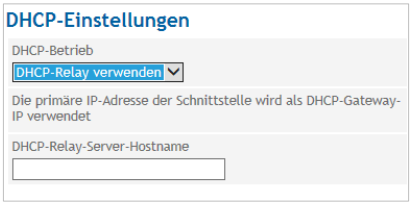
DHCP-Betriebseinstellungen

TAINY IQ-LTE bietet eine DHCP-Server- oder eine DHCP-Relais-Funktion.

Ist die DHCP-Server-Funktion aktiviert, ordnet TAINY IQ-LTE selbst den an die LAN-Schnittstelle angeschlossenen Applikationen IP-Adressen zu. Definieren Sie den Bereich, aus dem die zuzuordnenden IP-Adressen und/oder die MAC-Adressen verwendet werden sollen. Definieren Sie den Bereich, aus dem die zuzuordnenden IP-Adressen stammen und/oder definieren Sie statische Zuordnungen von Client MAC-Adresse zu IP-Adresse.



Ist die DHCP-Relais-Funktion aktiviert, leitet TAINY IQ-LTE die DHCP- Anfrage der an die LAN-Schnittstelle angeschlossenen Applikationen an einen Remote-DHCP-Relais-Server weiter, der die IP-Adressen zur Verfügung stellt. Geben Sie den Hostnamen oder die IP-Adresse des DHCP-Relais-Servers ein.



VRRP-Einstellungen

VRRP (Virtual Router Redundancy Protocol) sichert die Verfügbarkeit der wichtigen Gateways innerhalb eines Netzwerks, indem es mehrere TAINY IQ-LTEs nutzt.

Um die VRRP-Einstellungen zu konfigurieren, setzen Sie **VRRP aktivieren** auf „Ja“.

Virtual-Router-ID

ID der Gruppe der genutzten TAINY IQ-LTEs.

VRRP-Basis-Priorität

Definiert, welcher TAINY IQ-LTE Master und welcher Back-up ist. Der TAINY IQ-LTE mit der höchsten Priorität ist der Master. Geben Sie einen Wert zwischen 1 (niedrigste Prio) und 254 (höchste Prio) ein. Die VRRP-Basis-Priorität wird automatisch einem neuen Wert angepasst.

VRRP-Priorität anpassen

Im Fall einer aktiven WAN- oder VPN-Verbindung.

Liste der VRRP-IP-Adressen

IP-Adressen des VRRPs (TAINY IQ-LTEs).

IP-Adressen/ Hostnamen

Hostnamen, IP-Adresse: TAINY IQ-LTE erlaubt die Zuordnung von Hostnamen zu den IP-Adressen der Gegenstellen. Mit dieser Funktion sprechen die an die TAINY IQ-LTE-LAN-Schnittstelle angeschlossenen Anwendungen die Gegenstellen mit den hier eingetragenen Hostnamen an. TAINY IQ-LTE-Funktionen (z. B. NTP) nutzen ebenfalls dieses Feature.

9.2 Konfiguration VRRP

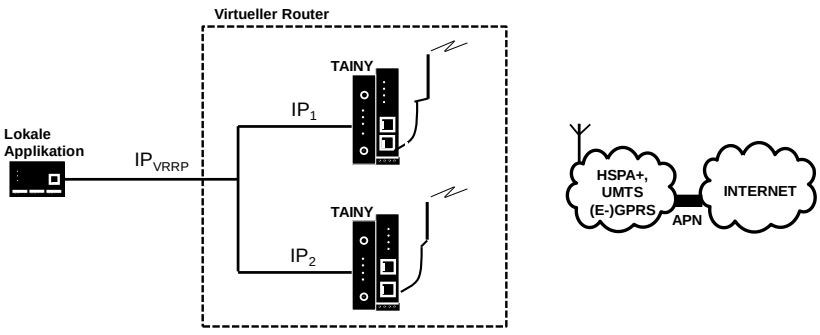
VRRP-Einstellungen

Öffnen Sie das Register **LAN** und wählen Sie im Menü „**LAN-Schnittstelle**“.

TAINY IQ-LTE unterstützt das Virtual Router Redundancy Protokoll (VRRP). Aktivieren/Deaktivieren Sie diese Funktion in den Einstellungen der logischen Netzwerk-Schnittstelle. Zwei TAINY IQ-LTE-Router fungieren als ein virtueller Router. Sollte ein TAINY IQ-LTE die WAN-Verbindung oder die VPN-Verbindung verlieren, übernimmt und unterstützt der zweite TAINY IQ-LTE die Verbindung.

Wenn Sie mehrere virtuelle Router für ein Netzwerk definieren, dann stellen Sie sicher, dass Sie diesen unterschiedliche IDs zu ordnen.

Die **VRRP-Basis-Priorität** legt fest, welcher TAINY IQ-LTE als Master und welcher als Back-up dient. Der TAINY IQ-LTE mit der höchsten Priorität ist Master.
Geben Sie Werte zwischen 1 (niedrigste Prio) und 254 (höchste Prio) ein. Die VRRP-Priorität kann im Falle einer aktiven WAN- oder VPN-Verbindung automatisch an den neuen Wert (**Angepasste VRRP-Priorität**) angepasst werden.



Die IP_{VRRP} ist die IP-Adresse des virtuellen Routers. Geben oder fügen Sie diese zu der **Liste der VRRP-IP-Adressen** hinzu. Nutzen Sie diese als Standard-Gateway für die lokale Applikation. IP_1 und IP_2 sind die IP-Adressen des TAINY IQ-LTE, wie in der IP-Adressen-Konfiguration jedes TAINY IQ-LTE eingegeben.

9.3 ETH0 als LAN-Port verwenden

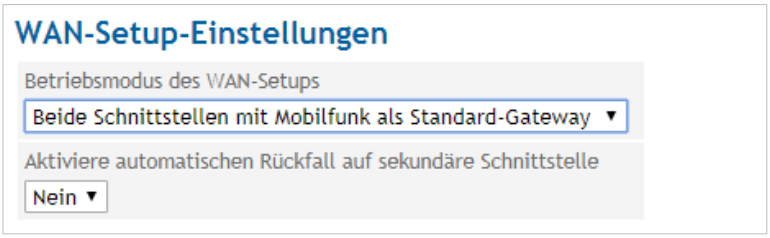
WAN-Setup-Einstellungen

Um den ETH0-Port als zusätzlichen LAN-Port für TAINY IQ-LTE nutzen zu können, nehmen Sie die im Folgenden beschriebene Konfiguration vor:

Öffnen Sie das Register **WAN** und wählen Sie im Menü „**Setup 1**“.

Setzen Sie den **Betriebsmodus des WAN-Setups** auf „Beide Schnittstellen mit Mobilfunk als Standard-Gateway“, um den ETH0-Port einzuschalten.

Da dieser priorisiert ist, wird die WAN-Kommunikation über Mobilfunk geleitet.



DSL/Kabel-Einstellungen

Wählen Sie **DSL/Kabel** im Menü. Definieren Sie eine **IP-Adresse** und **Netzmaske** für den zusätzlichen LAN-Port mit einem anderen Netzwerk als für den anderen ETH-Ports.

Nach dieser Konfiguration fungiert die ETH0-Schnittstelle als zusätzlicher LAN-Port des TAINY IQ-LTE.

Hinweis

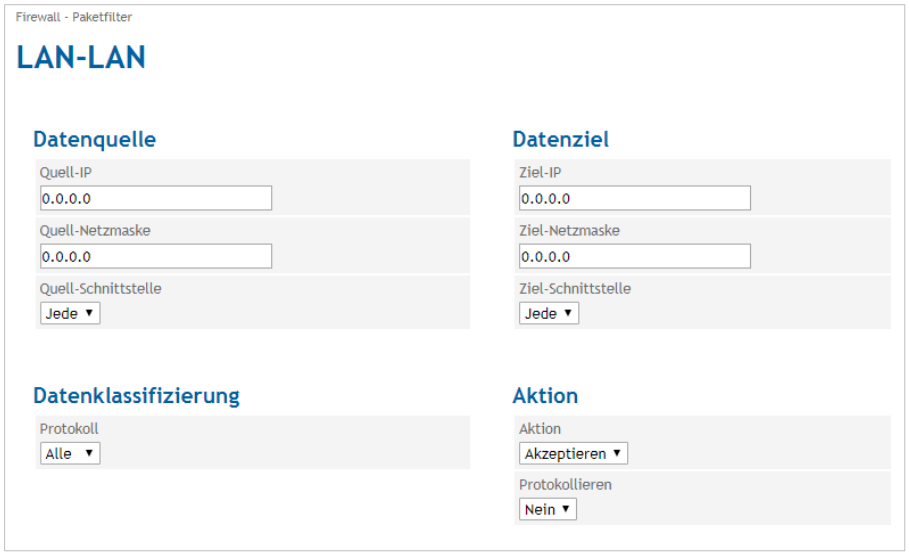
LAN Schnittstelle konfigurieren

Konfigurieren Sie 2 unterschiedliche Netzte für die ETH0-Schnittstelle und für die ETH1-Schnittstelle. Das TAINY IQ-LTE wird Datenpakete zwischen diesen beiden Netzwerken routen.

Firewall-Paketfilter

Öffnen Sie das Register **Firewall** und wählen Sie im Menü „**Paketfilter**“.

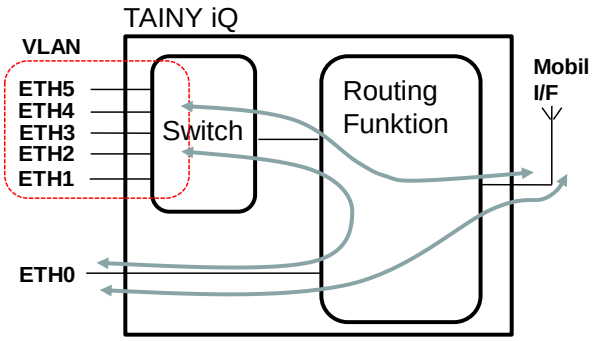
Definieren Sie eine neue Regel für den Paketfilter und erlauben Sie den Datenverkehr von LAN zu LAN.



Wählen Sie Aktion „**Akzeptieren**“ aus

Anschließend betätigen Sie „**Speichern**“

Daten können zwischen dem ETH0 und ETH15 und der Mobilfunk-Schnittstelle geroutet werden.



Die Ports ETH1 bis ETH5 können als VLANs gruppiert werde

LAN-Schnittstelle

Öffnen Sie das Register **LAN** und wählen Sie im Menü „**LAN-Schnittstelle**“.

Vergeben Sie IP eine IPv4-Adresse oder mehrere für die LAN-Schnittstelle. Mit Vergabe die IPv4-Adresse und der Subnetzmaske legen Sie gleichzeitig das Netzwerk auf der LAN-Schnittstelle (ETH1) fest.

IP-Datenpakete können zwischen der ETH0-Schnittstelle und der Mobilfunk-Schnittstelle geroutet werden.

Und:

IP-Datenpakete können zwischen der ETH0-Schnittstelle und der ETH1-Schnittstelle geroutet werden, falls die ETH0-Schnittstelle als zusätzliche LAN-Schnittstelle konfiguriert wurde mit unterschiedlichen Netzwerken.

10 UART

10.1 UART-Universal Asynchronous Receiver Transmitter

UART

Öffnen Sie das Register **UART** und wählen Sie im Menü „**RS-232-Schnittstelle**“.

Über die RS 232 Schnittstelle ist eine asynchrone, serielle Datenübertragung möglich.

Aktivierung oder Deaktivierung RS232 über IP

Aktivieren oder deaktivieren Sie RS232 und wählen `Ja` oder `Nein`.

Server TCP-Port

Geben Sie den lokal vom TAINY IQ-LTE geöffneten TCP-Port ein.

Schnittstellengeschwindigkeit

Legen Sie die benötigte Geschwindigkeit (in Baud) der Schnittstelle fest und wählen einen Wert aus der Dropdown Liste.

Datenbits

Legen Sie die Anzahl der zu verwendenden Datenbits fest und wählen einen Wert aus der Liste.

Paritätsbit

Wählen Sie ob Sie `keine`, `ungerade` oder `gerade` Parität verwenden wollen.

Anzahl der Stopp-Bits

Legen Sie die Anzahl der Stopp-Bits fest, 1 oder 2

Echo aktivieren

Wählen Sie `Ja`, wenn bei Zeicheneingabe ein Echo auf der seriellen Schnittstelle verwendet werden soll.

Flusskontrolle

Legen Sie fest, ob für den Datenfluss eine Software Flusskontrolle XON /XOFF oder keine Software Flusskontrolle verwendet werden soll.

11 Netzwerktools

11.1 Netzwerktool Ping

Ping

Öffnen Sie das Register **`Netzwerktools`** und wählen Sie im Menü „**`Ping`**“.

Mit diesem Netzwerktool wird überprüft, ob ein bestimmter Host im Netzwerk erreichbar ist und welche Zeitspanne die RTT (Round Trip Time– Paketumlaufzeit) umfasst.

`Ping-Kommando ausführen`

Um ein `Ping-Kommando auszuführen,` geben Sie die `Host-Adresse` des Hostes ein, den Sie überprüfen wollen.

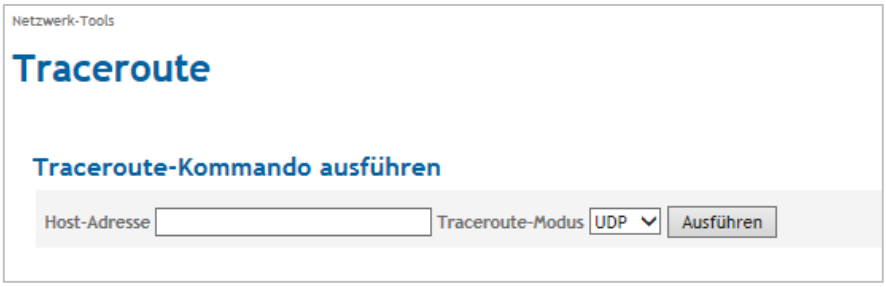
Tragen Sie die `Nutzdatengröße` (in Bytes) ein und drücken Sie `Ausführen`.

Das Ergebnis erscheint unterhalb „`Ping-Kommando-ausführen`“.

11.2 Netzwerktool Traceroute

Traceroute

Öffnen Sie das Register **`Netzwerktools`** und wählen Sie im Menü „**`Traceroute`**“.



Das Traceroute Netzwerktool zeigt auf welche Router und Knotenpunkte im Netz ein IP-Datenpaket auf dem Weg vom Sender zum Empfänger passiert.

`Traceroute-Kommando ausführen`

Um ein `Traceroute-Kommando auszuführen,` geben Sie die `Host-Adresse` des Hostes ein.

Wählen Sie den `Traceroute-Modus` aus

Drücken Sie Ausführen.

Das Ergebnis erscheint unterhalb „Traceroute-Kommando-ausführen“.

11.3 Netzwerktoll NSlookup

NSlookup

Öffnen Sie das Register **Netzwerktools** und wählen Sie im Menü „**NSlookup**“.

Das NSlookup-Netzwerktool ermittelt den Domainname einer IP-Adresse bzw. umgekehrt.

NSlookup-Kommando ausführen

Um ein NSlookup-Kommando auszuführen, geben Sie die Host-Adresse des gesuchten Hosts ein.

Drücken Sie Ausführen.

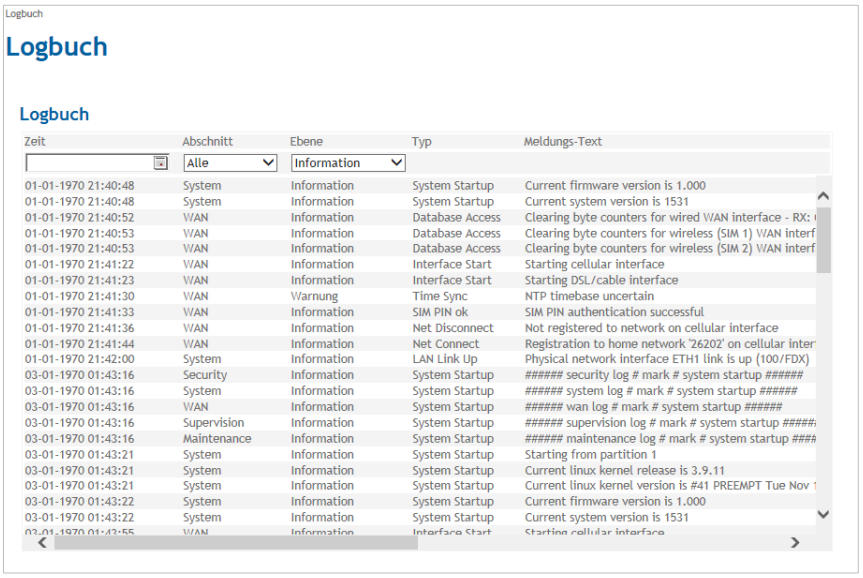
Das Ergebnis erscheint unterhalb „NSlookup-Kommando-ausführen“.

12 Logbuch

12.1 Das Logbuch lesen

Logbuch

Öffnen Sie das Register **Logbuch** und wählen Sie im Menü „**Logbuch**“.



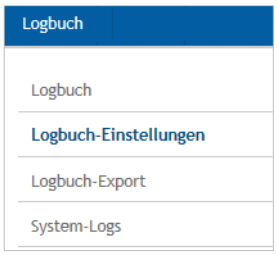
Wichtige Ereignisse von TAINY IQ-LTE werden in dieser Ansicht gesichert und angezeigt. Die Einträge werden automatisch aktualisiert.

Auch Log-Einträge, die mittels der Regeln für das Betrieb-WAN-Setup entstehen, werden ins Logbuch geschrieben (siehe Kapitel 6).

12.2 Konfiguration der Logbuch-Funktion

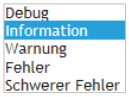
Logbuch-Einstellungen

Öffnen Sie das Register **Logbuch** und wählen Sie im Menü „**Logbuch-Einstellungen**“.



Das Logbuch ist in fünf Bereiche unterteilt: `Sicherheit`, `WAN`, `System-`, `Überwachung` und `Wartung`. Die Anzahl der gespeicherten Logeinträge kann für jeden Bereich separat festgelegt werden (**`Speichertiefe des Logbuchs`**). Ist die maximale Anzahl der Logeinträge erreicht, werden die ältesten Einträge überschrieben.

Jeder Logeintrag ist einer **`Ebene (Logmeldung)`** zugeordnet. Die niedrigste Ebene ist „`Debug`“, die höchste Ebene „`schwerer Fehler`“.



Sie können für jeden Logbuchbereich die niedrigste Ebene der zu speichernden Logmeldungen auswählen. Wählen Sie „`Debug`“, werden sämtliche Logeinträge gespeichert. Wählen Sie „`Fehler`“, werden alle Logs der Ebenen „`Fehler`“ und „`schwerer Fehler`“ gespeichert.

12.3 Logbuch-Export

Logbuch-Export

Öffnen Sie das Register **Logbuch** und wählen Sie im Menü „**Logbuch-Export**“.

Um die Daten zum **Logbuch-Export** in eine CSV-Datei zu schreiben, drücken Sie „Exportieren“.

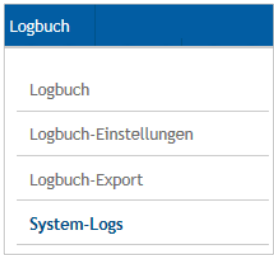
Wählen Sie die **Logbuch-Abschnitte** und die **Ebene der Logmeldungen**, die Sie exportieren möchten, aus.

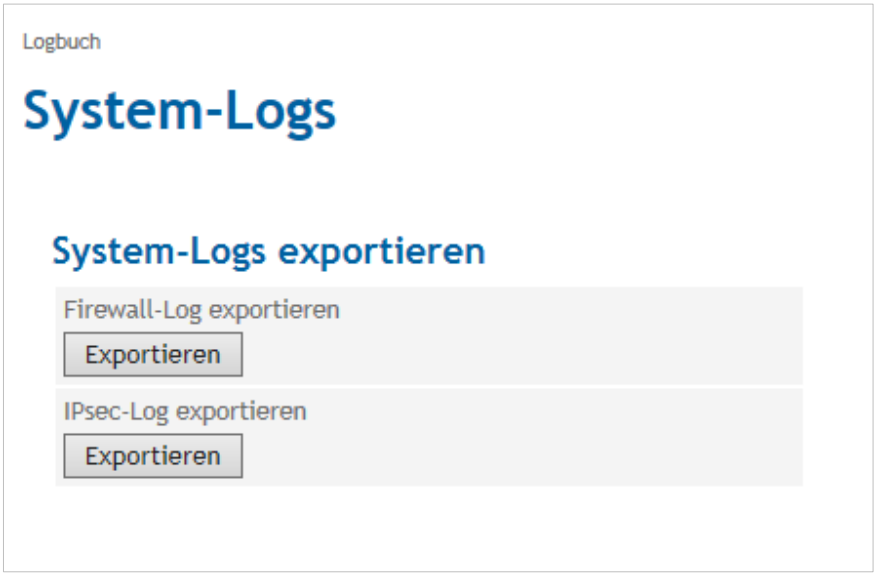
Sie können zusätzlich auch den **Zeitbereich** (**Zeitbereichsanfang** und **Zeitbereichsende**) begrenzen, aus dem Sie die Daten exportieren möchten.

12.4 System-Logs

System-Logs exportieren

Öffnen Sie das Register **Logbuch** und wählen Sie im Menü „**System-Logs**“.





Firewall-Log exportieren

Drücken Sie „Exportieren“, um die Log-Daten der Firewall in einer Zip-Datei zu einem externen Rechner zu exportieren.

Es werden die folgenden Daten gemäß der Regeln der Firewall geloggt:

accept log	Datenpakete, die von der Firewall akzeptiert wurden
drop log	Datenpakte, die von der Firewall verworfen wurden
port fw log	Datenpakte, die durch den Port forwarded (weitergeleitet) wurden
reject log	Datenpakte, die zurückgewiesen wurden

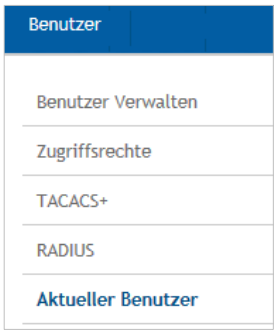
IPsec-Log exportieren

Drücken Sie „Exportieren“, um die IPsec-Log-Daten in einer Zip-Datei zu einem externen Rechner zu exportieren.

13 Benutzer verwalten, SNMP-Zugang de-/aktivieren

Aktueller Benutzer

Öffnen Sie das Register **Benutzer** und wählen Sie im Menü „**Aktueller Benutzer**“.



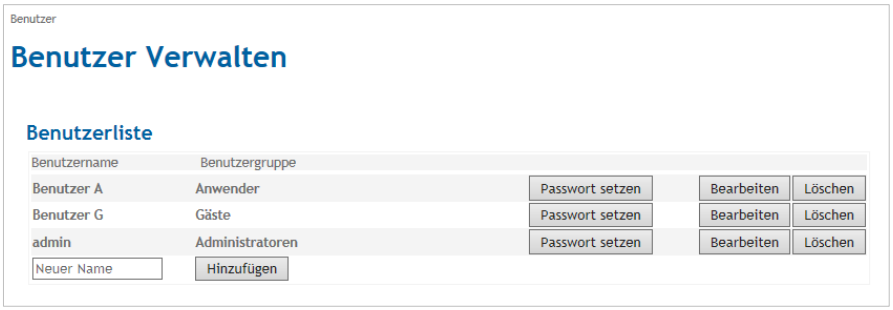
Passwort ändern

In der Ansicht **Aktueller Benutzer** werden sämtliche Informationen zu dem jeweiligen Benutzer angezeigt.

Drücken Sie „Ändern“, um das aktuelle Passwort des Benutzers zu ändern. Wurde eine Passwortlänge beim Anlegen des Benutzers festgelegt, wird diese hier angezeigt und muss beibehalten werden.

Benutzer verwalten

Öffnen Sie das Register **Benutzer** und wählen Sie im Menü „**Benutzer verwalten**“.



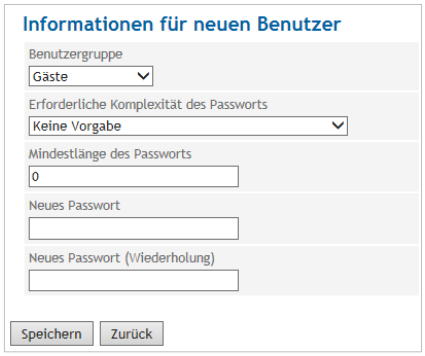
Um einen neuen Benutzer zur **Benutzerliste** hinzuzufügen oder die Einstellungen für einen bestehenden Benutzer zu ändern, drücken Sie auf „Hinzufügen“ (erst Namen eingeben) oder „Bearbeiten“.

Um einen Benutzer aus der Benutzerliste zu entfernen, drücken Sie „Löschen“ und bestätigen Sie die Sicherheitsabfrage.

Benutzer hinzufügen

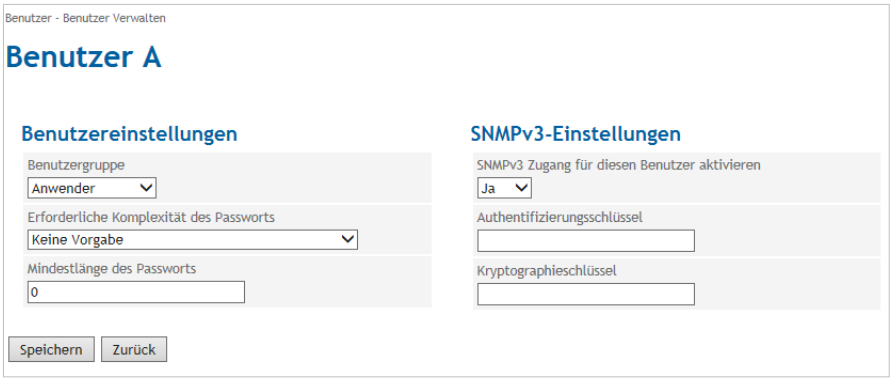
Benutzergruppe

Wählen Sie die **Benutzergruppe**, der der neue Benutzer angehören soll. Die Zugangsrechte des Benutzers werden durch die Benutzergruppe definiert. Während die Gruppe „Admin“ über unbegrenzte Zugangsrechte verfügt, sind die Zugangsrechte der Benutzergruppe „Gäste“ und „Anwender“ begrenzt (siehe unten Zugangsrechte).



Legen Sie bei Bedarf die Komplexität und Länge des Passwortes fest.

Benutzer bearbeiten



Benutzer-Einstellungen

Ändern Sie bei Bedarf die Benutzergruppe für den Benutzer.

Legen Sie in den **Benutzereinstellungen** für jeden Benutzer die „**erforderliche Komplexität des Passworts**“ (Ziffern, Buchstaben, Groß- und Kleinschreibung, Sonderzeichen) und die „**Mindestlänge des Passworts**“ fest.

SNMPv3-Einstellungen

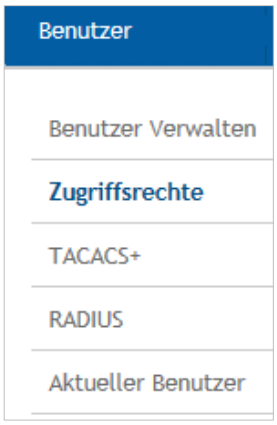
Um dem Benutzer den Zugang über **SNMPv3** zu ermöglichen, aktivieren Sie die Option mit „Ja“.

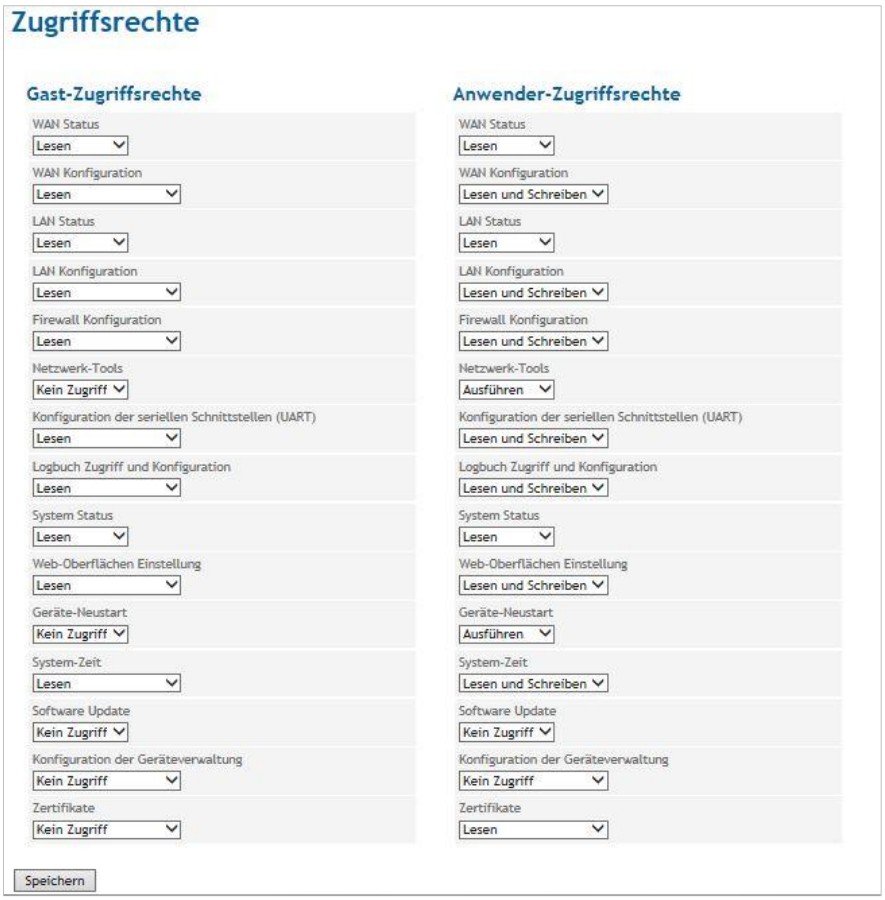
Geben Sie den **Authentifizierungschlüssel** und den **Kryptographieschlüssel** ein.

13.1 Konfiguration Anwender- und Gäste-Zugriffsrechte

Zugriffsrechte

Öffnen Sie das Register **Benutzer** und wählen Sie im Menü „**Zugriffsrechte**“.





Zugriffsrechte

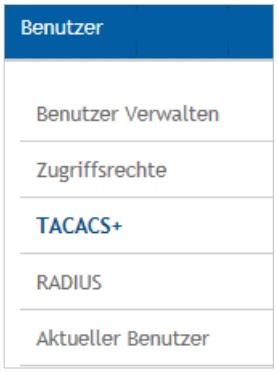
Während der Admin über vollumfängliche Zugriffsrechte verfügt, sind die Zugriffsrechte der Mitglieder der Benutzergruppen „Anwender“ und „Gäste“ begrenzt.

Definieren Sie in diesem Menü die **Zugriffsrechte** für die Benutzergruppen „**Gast-Zugriffsrechte**“ und „**Anwender-Zugriffsrechte**“ entsprechend.

13.2 Konfiguration TACACS+

TACACS+

Öffnen Sie das Register **Benutzer** und wählen Sie im Menü „**TACACS+**“.



Beim Authentifizierungsverfahren TACACS+ (Terminal Access Controller Access Control System Plus), werden die Zugangsdaten zu TAINY IQ-LTE nicht auf dem Gerät selbst gespeichert, sondern auf einem externen Server.

Geht eine Anmeldeanfrage ein, leitet TAINY IQ-LTE die Anmeldedaten an den TACACS+-Server weiter. Der Server überprüft die Gültigkeit der Daten und meldet das Ergebnis an TAINY IQ-LTE zurück, der dann die Anmeldung entsprechen ablehnt oder annimmt.

Um den Authentifizierungsprozess des TACACS+ zu aktivieren, geben Sie in diesem Abschnitt alle notwendigen Parameter ein, die TAINY IQ-LTE benötigt, um sich mit dem TACACS+-Server zu verbinden.

Sobald der TACACS+-Dienst aktiviert ist, kann die Art der Anmeldung aus der zusätzlichen Liste (`TACACS+` oder `lokal`) im Anmeldedialog ausgewählt werden.

Bei jeder Anmeldung am Router wird die Meldung „`Benutzername oder Kennwort prüfen`“ ausgegeben. Dieses Meldung erscheint selbst dann, wenn der TACAS+-Server von TAINY IQ-LTE nicht erreicht werden kann.

Dieses geschieht aus Sicherheitsgründen, um potentiellen Angreifern keine Informationen zu liefern.

Primärer/Sekundärer TACACS+-Server

Es kann ein primärer und ein sekundärer (Back-up-)TACACS+-Server verwendet werden.

Um den TACACS+-Server zu erreichen, geben Sie den `Hostnamen` (oder IP-Adresse), `Port-Nummer`, `Shared Secret` und `Authentifizierung` ein.

`Zugriffsrechte`

In den TACACS+-Protokollen sind die Zugriffsrechtsebenen der Benutzer von 1 bis 15 numerisch kodiert. TAINY IQ-LTE verfügt über drei Zugriffsrechtsebenen: Administrator, Anwender und Gast.

Um die Ebenen des TACACS+-Protokolls auf die Ebenen des TAINY IQ-LTE zu mappen, definieren Sie die minimalste TACACS+-Ebene, die auf die TAINY IQ-LTE-Adminstratorenrechte mappen sollen, und die minimalste TACACS+-Ebene, die auf die TAINY IQ-LTE-Anwenderrechte mappen soll. Alle Rechte unterhalb der Anwenderrechte sind Gastrechte.

13.3 Konfiguration RADIUS

RADIUS

Öffnen Sie das Register `Benutzer` und wählen Sie im Menü „`RADIUS`“.

Beim Authentifizierungsverfahren RADIUS (Remote Authentification Dial-In User Service, ein Client-Server Protokoll), werden die Zugangsdaten zu TAINY IQ-LTE nicht vom Gerät selbst geprüft, sondern von einem zentralen Authentifizierungs-Server.

Geht eine Anmeldeanfrage im Netzwerk ein, ein, leitet TAINY IQ-LTE die Anmeldedaten an den RADIUS-Server weiter. Der Server überprüft die Gültigkeit der Daten sowie Parameter zum Verbindungsaufbau zum Client und meldet das Ergebnis an TAINY IQ-LTE zurück, der dann die Anmeldung entsprechen ablehnt oder annimmt.

Um den Authentifizierungsprozess des RADIUS zu aktivieren, geben Sie in diesem Abschnitt alle notwendigen Parameter ein, die TAINY IQ-LTE benötigt, um sich mit dem RADIUS-Server zu verbinden.

Sobald der RADIUS-Dienst aktiviert ist, kann die Art der Anmeldung aus der zusätzlichen Liste (`RADIUS` oder `lokal`) im Anmeldedialog ausgewählt werden.

Primärer/Sekundärer RADIUS-Server

Es kann ein primärer und ein sekundärer (Back-up-) RADIUS-Server verwendet werden.

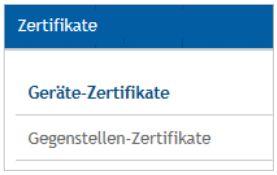
Um den RADIUS-Server zu erreichen, geben Sie den Server-`Hostnamen` (oder IP-Adresse), Server-`Port-Nummer` und `das Shared Secret` ein.

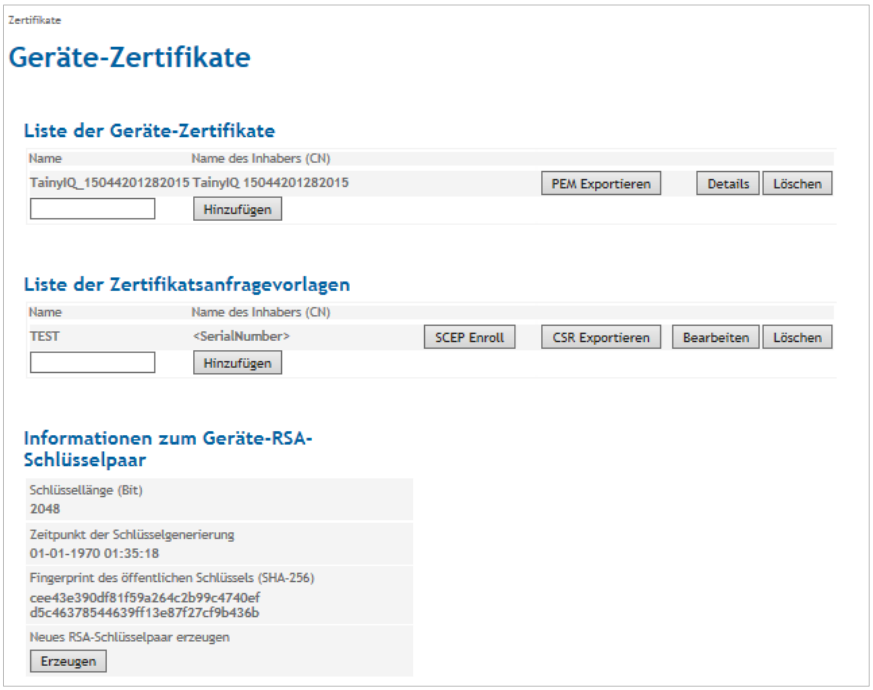
14 Zertifikate

14.1 Geräte-Zertifikate

Geräte-Zertifikate

Öffnen Sie das Register **`Zertifikate`** und wählen Sie im Menü „**`Geräte-Zertifikate`**“.





`Geräte-Zertifikate` sind sämtliche Zertifikate des TAINY IQ-LTE. Die Zertifikate der anderen Einheit sind die Gegenstellen-Zertifikate, wie im folgenden Kapitel beschrieben. Siehe auch Glossar für weitere Informationen.

Im Abschnitt Geräte-Zertifikate werden Informationen zu den **`Zertifikaten`**, den **`Zertifikatsanfragevorlagen`** und zum aktuell verwendeten **`Geräte-RSA-Schlüsselpaar`** angezeigt.

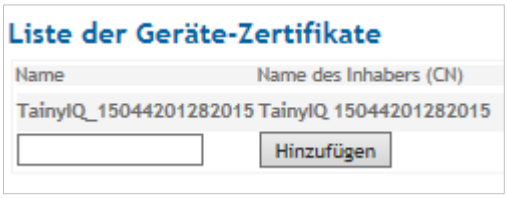
Es ist möglich, neue Zertifikate und Zertifikatsanfragevorlagen hinzuzufügen und ein neues RSA-Schlüsselpaar zu erzeugen.

`Liste der Geräte-Zertifikate`

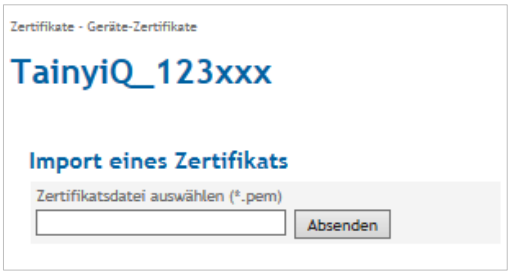
Details einsehen/Zertifikate exportieren

Drücken Sie „`Details`“, um mehr Informationen über das ausgewählte Zertifikat anzuzeigen.

Hinzufügen/Importen Geräte-Zertifikate



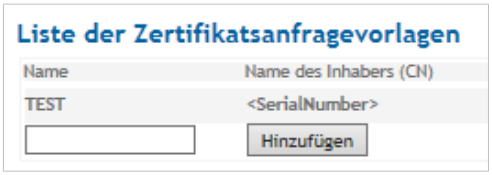
Um Zertifikate hinzuzufügen, geben Sie den Namen des Zertifikats in die **Liste der Geräte-Zertifikate** ein und drücken „Hinzufügen“.



Drücken Sie jetzt auf „Absenden“, um die Datei des neuen Zertifikats vom Administratoren-Rechner zu importieren.

Das importierte Zertifikat erscheint in der Liste der Geräte-Zertifikate.

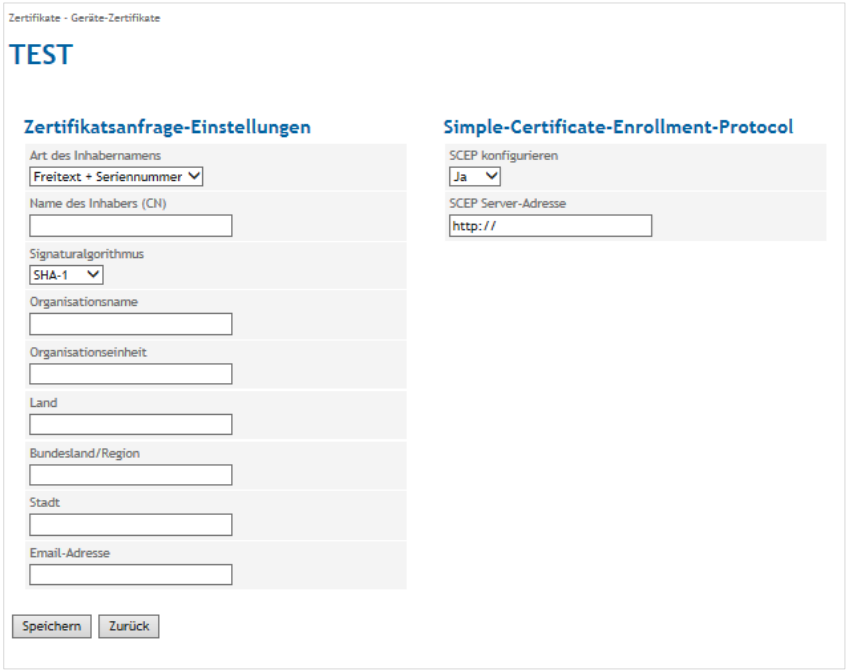
Liste der Zertifikats-anfragevorlagen



Sämtliche Anfragen erscheinen in der **Liste der Zertifikatsanfragevorlagen** mit Name und Name des Inhabers (CN).

Neue Anfragevorlage

Um eine neue `Anfragevorlage` zu erstellen, geben Sie einen Namen für die Vorlage ein und drücken dann „`Hinzufügen`“.



Zertifikatsanfrage-Einstellungen

Geben Sie die folgenden Parameter ein:

`Art des Inhabernamens/Name des Inhabers (CN)`

Wählen Sie die Option „`Freitext + Seriennummer`“ aus. Die Seriennummer wird beim Export automatisch an den Namen des Inhabers geheftet.

Geben Sie den `Namen des Zertifikatsinhabers` ein.

`Signaturalgorithmus`

Wählen Sie entweder SHA-1 oder SHA-256. Der Letztere ist aktueller und sicherer.

`Organisationsname/-einheit/-Adressdaten/E-Mail-Adresse`

Geben Sie die Namen und Kontaktdaten in die entsprechenden Felder ein.

`Land`

Geben Sie das Kürzel für das gewünschte Land ein.

Bitte verwenden Sie ausschließlich die in der folgenden Tabelle aufgeführten Kürzel für das Land. Bei der Verwendung eines anderen Kürzels können die Eingaben des gesamten Formulars nicht gespeichert werden.

Länderkennungen

Bitte das entsprechende Kürzel für das Land eintragen:

US United States of America	**CA** Canada	**AX** Åland Islands	**AD** Andorra
AE United Arab Emirates	**AF** Afghanistan	**AG** Antigua and Barbuda	**AI** Anguilla
AL Albania	**AM** Armenia	**AN** Netherlands Antilles	**AO** Angola
AQ Antarctica	**AR** Argentina	**AS** American Samoa	**AT** Austria
AU Australia	**AW** Aruba	**AZ** Azerbaijan	**BA** Bosnia and Herzegovina
BB Barbados	**BD** Bangladesh	**BE** Belgium	**BF** Burkina Faso
BG Bulgaria	**BH** Bahrain	**BI** Burundi	**BJ** Benin
BM Bermuda	**BN** Brunei Darussalam	**BO** Bolivia	**BR** Brazil
BS Bahamas	**BT** Bhutan	**BV** Bouvet Island	**BW** Botswana
BZ Belize	**CC** Cocos (Keeling) Islands	**CF** Central African Republic	**CH** Switzerland
CI Cote D'Ivoire (Ivory Coast)	**CK** Cook Islands	**CL** Chile	**CM** Cameroon
CN China	**CO** Colombia	**CR** Costa Rica	**CS** Czechoslovakia (former)
CV Cape Verde	**CX** Christmas Island	**CY** Cyprus	**CZ** Czech Republic
DE Germany	**DJ** Djibouti	**DK** Denmark	**DM** Dominica
DO Dominican Republic	**DZ** Algeria	**EC** Ecuador	**EE** Estonia
EG Egypt	**EH** Western Sahara	**ER** Eritrea	**ES** Spain
ET Ethiopia	**FI** Finland	**FJ** Fiji	**FK** Falkland Islands (Malvinas)
FM Micronesia	**FO** Faroe Islands	**FR** France	**FX** France, Metropolitan
GA Gabon	**GB** Great Britain (UK)	**GD** Grenada	**GE** Georgia
GF French Guiana	**GG** Guernsey	**GH** Ghana	**GI** Gibraltar
GL Greenland	**GM** Gambia	**GN** Guinea	**GP** Guadeloupe
GQ Equatorial Guinea	**GR** Greece	**GS** S. Georgia and S. Sandwich Isls.	**GT** Guatemala
GU Guam	**GW** Guinea-Bissau	**GY** Guyana	**HK** Hong Kong
HM Heard and McDonald Islands	**HN** Honduras	**HR** Croatia (Hrvatska)	**HT** Haiti
HU Hungary	**ID** Indonesia	**IE** Ireland	**IL** Israel
IM Isle of Man	**IN** India	**IO** British Indian Ocean Territory	**IS** Iceland
IT Italy	**JE** Jersey	**JM** Jamaica	**JO** Jordan
JP Japan	**KE** Kenya	**KG** Kyrgyzstan	**KH** Cambodia
KI Kiribati	**KM** Comoros	**KN** Saint Kitts and Nevis	**KR** Korea (South)
KW Kuwait	**KY** Cayman Islands	**KZ** Kazakhstan	**LA** Laos
LC Saint Lucia	**LI** Liechtenstein	**LK** Sri Lanka	**LS** Lesotho
LT Lithuania	**LU** Luxembourg	**LV** Latvia	**LY** Libya
MA Morocco	**MC** Monaco	**MD** Moldova	**ME** Montenegro
MG Madagascar	**MH** Marshall Islands	**MK** Macedonia	**ML** Mali
MM Myanmar	**MN** Mongolia	**MO** Macau	**MP** Northern Mariana Islands
MQ Martinique	**MR** Mauritania	**MS** Montserrat	**MT** Malta

MU Mauritius	**MV** Maldives	**MW** Malawi	**MX** Mexico
MY Malaysia	**MZ** Mozambique	**NA** Namibia	**NC** New Caledonia
NE Niger	**NF** Norfolk Island	**NG** Nigeria	**NI** Nicaragua
NL Netherlands	**NO** Norway	**NP** Nepal	**NR** Nauru
NT Neutral Zone	**NU** Niue	**NZ** New Zealand (Aotearoa)	**OM** Oman
PA Panama	**PE** Peru	**PF** French Polynesia	**PG** Papua New Guinea
PH Philippines	**PK** Pakistan	**PL** Poland	**PM** St. Pierre and Miquelon
PN Pitcairn	**PR** Puerto Rico	**PS** Palestinian Territory	**PT** Portugal
PW Palau	**PY** Paraguay	**QA** Qatar	**RE** Reunion
RO Romania	**RS** Serbia	**RU** Russian Federation	**RW** Rwanda
SA Saudi Arabia	**SB** Solomon Islands	**SC** Seychelles	**SE** Sweden
SG Singapore	**SH** St. Helena	**SI** Slovenia	**SJ** Svalbard and Jan Mayen Islands
SK Slovak Republic	**SL** Sierra Leone	**SM** San Marino	**SN** Senegal
SR Suriname	**ST** Sao Tome and Principe	**SU** USSR (former)	**SV** El Salvador
SZ Swaziland	**TC** Turks and Caicos Islands	**TD** Chad	**TF** French Southern Territories
TG Togo	**TH** Thailand	**TJ** Tajikistan	**TK** Tokelau
TM Turkmenistan	**TN** Tunisia	**TO** Tonga	**TP** East Timor
TR Turkey	**TT** Trinidad and Tobago	**TV** Tuvalu	**TW** Taiwan
TZ Tanzania	**UA** Ukraine	**UG** Uganda	**UM** US Minor Outlying Islands
UY Uruguay	**UZ** Uzbekistan	**VA** Vatican City State (Holy See)	**VC** Saint Vincent and the Grenadines
VE Venezuela	**VG** Virgin Islands (British)	**VI** Virgin Islands (U.S.)	**VN** Viet Nam
VU Vanuatu	**WF** Wallis and Futuna Islands	**WS** Samoa	**YE** Yemen
YT Mayotte	**ZA** South Africa	**ZM** Zambia	**COM** US Commercial
EDU US Educational	**GOV** US Government	**INT** International	**MIL** US Military
NET Network	**ORG** Non-Profit Organization	**ARPA** Old style Arpanet	

`Bundesland/Region`

Tragen Sie den Namen des Bundeslandes anders oder der Region ein.

`Stadt`

Tragen Sie den Namen der Stadt ein.

`Email-Adresse`

Tragen Sie hier die gültige Email- Adresse ein.

`Simple-Certificate-Enrollment-Protocol`

Setzen die Einstellung auf „`Ja`“, um ein Geräte-Zertifikat von einem konfigurierten Server zu erhalten.

Informationen zum Geräte-RSA-Schlüsselpaar

Zeigt Informationen wie `Schlüssellänge`, `Zeitpunkt der Schlüsselgenerierung` und `Fingerprint des öffentlichen Schlüssels` zu dem aktuell verwendeten RSA-Schlüsselpaar an.

Das Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel, was eine sichere Datenübertragung garantiert.

Neues RSA-Schlüsselpaar erzeugen

Um ein neues Schlüsselpaar zu erzeugen:

Wählen Sie die **`Schlüssellänge`** (in Bit) aus der Liste aus.

Drücken Sie „`Erzeugen`“, um den Erstellungsprozess zu starten.

Beachten Sie, dass der Vorgang bis zu 2 Minuten dauern kann.

Die Informationen zu dem neu erzeugten Schlüsselpaar erscheinen jetzt in den `Informationen zum Geräteschlüsselpaar`.

14.2 Gegenstellen-Zertifikate

Gegenstellen-Zertifikate

Öffnen Sie das Register **Zertifikate** und wählen Sie im Menü „**Gegenstellen-Zertifikate**“.

Gegenstellen-Zertifikate sind alle Zertifikate, die zur Authentifizierung der gegenüberstehenden Einheiten (Gegenstellen) verwendet werden.

Die Liste der CA-Zertifikate enthält die von den Certificates Authorities (Zertifizierungsstelle) ausgestellten Zertifikate die vom Tainy IQ-LTE akzeptiert werden.

Liste der Gegenstellen-Zertifikate

Gegenstellen-Zertifikate hinzufügen

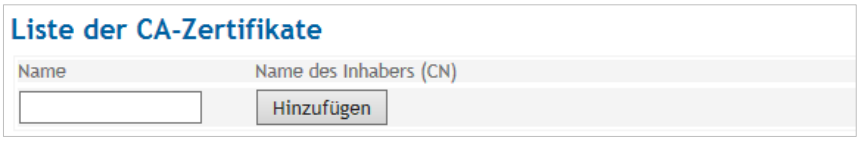
Um ein Zertifikat der Gegenstelle hochzuladen, geben Sie den Namen in das **Name**-Feld ein.

Drücken Sie auf „Hinzufügen“.

Drücken Sie „Absenden“, um die Datei des zusätzlichen Zertifikats vom Administrations-Rechner hochzuladen.

Das neue Zertifikat erscheint in der Liste der Gegenstellen-Zertifikate.

Liste der CA-Zertifikate



Ein CA-Zertifikat hinzufügen

Um ein CA-Zertifikat hochzuladen, geben Sie in der **Liste der CA-Zertifikate** den Namen in das **Name** Feld ein.

Drücken Sie auf „Hinzufügen“.

Drücken Sie „Absenden“, um die Datei des zusätzlichen CA-Zertifikats vom Administratoren-Rechner hochzuladen.

Das neue Zertifikat erscheint in der Liste der CA-Zertifikate.

15 System

15.1 Spracheinstellung

Web-Oberfläche

Öffnen Sie das Register **System** und wählen Sie im Menü „**Web-Oberfläche**“.

Sprache

Wählen Sie die **Sprache** der Web-Oberfläche in den **allgemeinen Web-Einstellungen** aus.

Web-Server-Port

Geben Sie unter **Allgemeine Web-Einstellungen** den für Verbindungen zur Web-Oberfläche zu verwendenden TCP-Port ein. Beachten Sie, dass nach der Änderung des Ports eine neue Anmeldung (Log-In) erforderlich ist.

15.2 Manuelle Einstellung Datum- und Uhrzeit

Datum und Uhrzeit

Öffnen Sie das Register **System** und wählen Sie im Menü „**Datum und Uhrzeit**“.

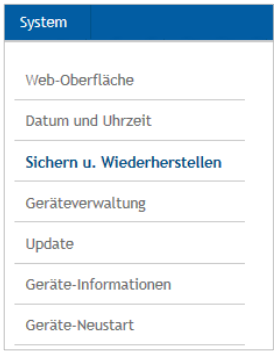
Systemzeit-Einstellungen

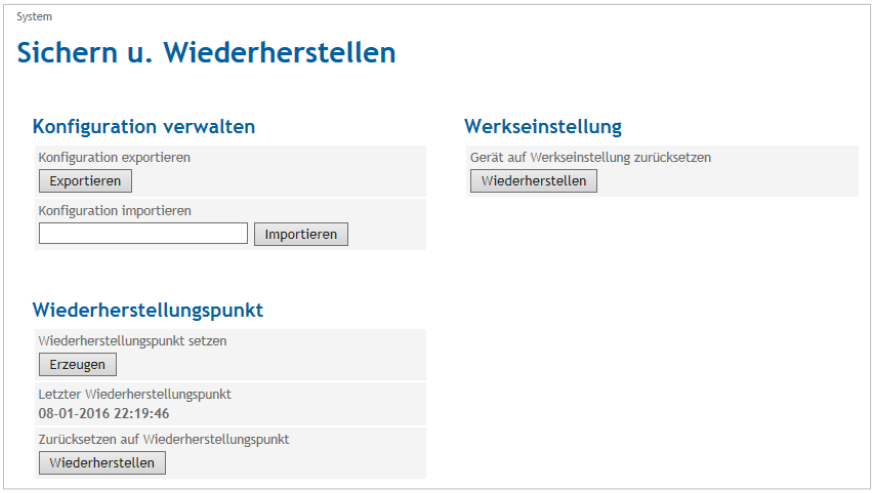
Stellen Sie die **Systemzeit** für TAINY IQ-LTE ein. Geben Sie die aktuelle Ortszeit ein. Ist die Zeitsynchronisation über NTP aktiviert, wird die eingegebene Zeit bei der nächsten Synchronisation mit NTP wieder überschrieben.

15.3 Auf Werkseinstellungen zurücksetzen/Gerätekonfigurationen verwalten

Sichern und Wiederherstellen

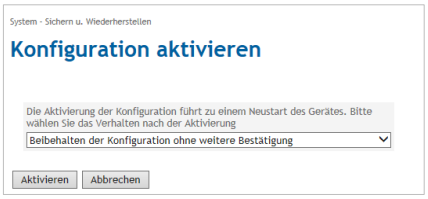
Öffnen Sie das Register **System** und wählen Sie im Menü „**Sichern und Wiederherstellen**“.





Drücken Sie unter **Konfiguration verwalten** auf „Exportieren“, um die aktuelle Konfiguration von TAINY IQ-LTE in eine Konfigurationsdatei zu schreiben.

Wählen Sie eine gültige Konfigurationsdatei aus und drücken Sie „`Importieren`“, um eine neue Konfiguration aus der Datei zu laden.



Legen Sie fest, ob die neue `Konfiguration ohne weitere Bestätigung beibehalten` werden soll oder `TAINY IQ-LTE auf die vorherige Konfiguration zurückgreifen` soll, für den Fall, dass die neue Konfiguration nicht innerhalb von 15 Minuten bestätigt wird.

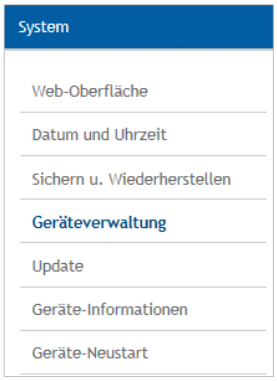
Um eine neue Konfiguration zu erstellen, exportieren Sie die aktuelle Konfiguration und editieren Sie diese in einem Text-Editor.

Beachten Sie, dass weder die lokalen Benutzer und deren Passwörter noch die Loglevel gesichert werden.

15.4 Geräteverwaltung

Geräteverwaltung

Öffnen Sie das Register **System** und wählen Sie im Menü „**Geräteverwaltung**“.



E-Mail-Einstellungen

`E-Mail-Konto einrichten`

Setzen Sie die Funktion auf „Ja“, um E-Mails von diesem Gerät senden zu können.

`SMTP-Server-Adresse/SMTP-TCP-Port`

Geben Sie die `SMTP-Server-Adresse` und den `SMTP-TCP-Port` ein.

`Benutzername/Passwort`

Geben Sie den Benutzernamen und ein Passwort für das E-Mail-Konto ein.

`Absendername`

Geben Sie den Namen ein, der im Absenderfeld der E-Mail erscheinen soll.

`STARTTLS verwenden/TLS verwenden`

Setzen Sie die Option auf „`Ja`“, um die Verschlüsselung der Konfiguration über TLS (Transport Layer Security) zu ermöglichen.

Weitere Informationen zur Konfiguration der Regeln und Bedingungen des E-Mail-Versands siehe Kapitel 6.3

SNMPv3-Einstellungen

SNMPv3-Zugriff aktivieren

Wählen Sie „Ja“, um die SNMPv3-Schnittstelle zu aktivieren.

Port

Geben Sie die Port-Nummer ein, an welcher der SNMPv3-Dienst zugänglich sein soll.

SSH-Einstellungen

SSH-Zugriff aktivieren

Wählen Sie „Ja“.

SSH-Passwort festlegen

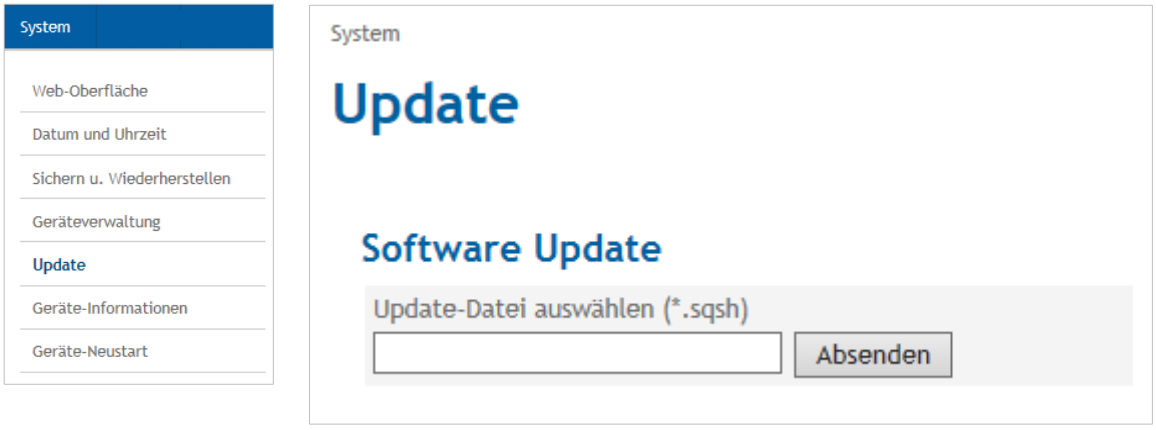
Geben Sie ein gültiges Passwort zur Authentifizierung ein.

Weitere Informationen zur Konfiguration der Regeln und Bedingungen des E-Mail-Versands siehe Kapitel 6.3

15.5 Software-Updates durchführen

Update

Öffnen Sie das Register **System** und wählen Sie im Menü „**Update**“.



Software-Update

Drücken Sie „**Absenden**“, um die benötigte Update-Datei vom Adminstrationsrechner hochzuladen.

15.6 Geräte-Informationen abfragen

Geräte-Informationen

Öffnen Sie das Register **System** und wählen Sie im Menü „**Geräte-Informationen**“.

Hardware-Informationen/ Software-Versions-Information

Die Geräte-Informationen enthalten Angaben zu den Hardware- und Software-Versionen des TAIN IQ-LTE.

Geräte-Snapshot

Der Geräte-Snapshot stellt diagnostische Informationen des TAINY IQ-LTE für die Fehlerbehebung bereit. Die Informationen werden in einer downloadbaren „tgz-Datei“ gespeichert. Sensible Daten wie Benutzernamen und Passwörter sind nicht in der Datei enthalten.

Der Snapshot enthält ebenfalls die Log-Dateien des TAINY IQ-LTE.

Drücken Sie „Erzeugen“, um einen Snapshot zu erstellen.

Setzen die Option **Snapshot-Versand konfigurieren** auf „Ja“.

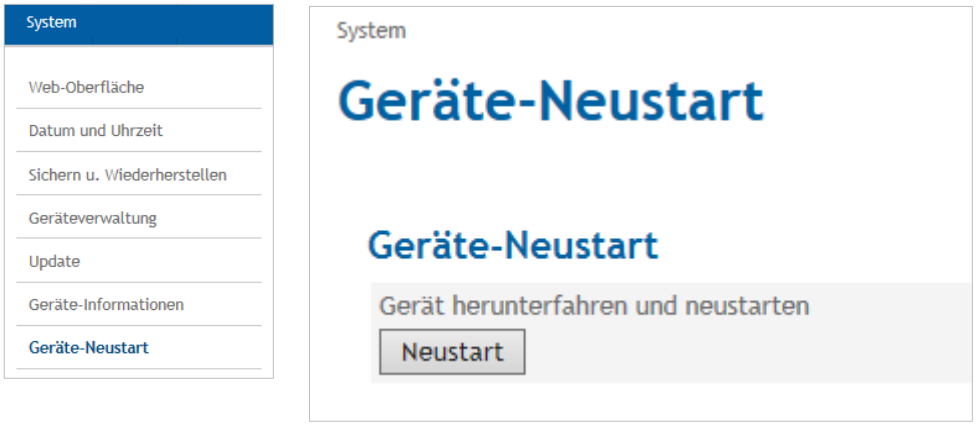
Beachten Sie, dass die Funktion E-Mail-Versand zuvor konfiguriert worden sein muss, siehe Kapitel 15.4.

Geben Sie die E-Mail-Adresse des Empfängers des Snapshots in das entsprechende Feld ein.

15.7 Neustart forcieren

Geräte-Neustart

Öffnen Sie das Register **`System`** und wählen Sie im Menü „**`Geräte-Neustart`**“.



Drücken Sie „`Neustart`“, um einen Neustart des Systems TAINY IQ-LTE herbeizuführen.

16 Wartung/Troubleshooting

16.1 Wartung

TAINY IQ-LTE ist wartungsfrei.

16.2 Troubleshooting

Sollten Sie während des Betriebs auf Probleme stoßen, suchen Sie in der folgenden Tabelle nach möglichen Lösungen:

Problem	Ursache	Lösung
Kontrollleuchten sind aus	Die Stromzufuhr ist unterbrochen	Anschlüsse zur Stromleitung und zu anderen Stromquellen prüfen
Gerät melden sich nicht an	Falsche PIN oder APN	PIN oder APN kontrollieren
	SIM-Karte ist nicht aktiviert oder im PUK-Status	Aktivierung und Status prüfen
	SIM-Karte ist nicht für den ausgewählten Dienst (UMTS, LTE) aktiviert	Aktivierung und ausgewählten Dienst prüfen
	Schlechter Empfang	Positionierung Antenne prüfen
Keine Datenverbindung vom lokalen Netzwerk zu WAN möglich	Standard-Gateway in der Anwendung falsch konfiguriert	Gateway-Einstellungen im WAN-Register prüfen
	GRE-Tunnel als Standard-Gateway gesetzt, aber noch keine Route gesetzt (trifft auch auf DNS, NTP, SNMP und Ping-Checks zu)	GRE- und Gateway-Einstellungen im WAN-Register prüfen
	Firewall ist nicht durchlässig	Firewall-Einstellungen prüfen
Kein Zugriff vom lokalen Netzwerk zu TAINY	Falsche VLAN-Parameter gesetzt	VLAN-Parameter im WAN- und LAN-Register prüfen
	Vom MAC-Filter ausgesperrt	MAC-Filter-Einstellungen prüfen
	Von der Firewall ausgesperrt	Filtereinstellungen der Firewall prüfen und ggfs. einen Reset auf Werkseinstellung durchführen
IPsec-Tunnel konfiguriert sich nicht	Fehlerhafte Zertifikate oder Schlüssel	Zertifikate und Schlüssel prüfen im Register Zertifikate
	Die Verschlüsselungs- und Hash-Verfahren stimmen nicht überein	Die ausgewählten Verfahren im WAN-Register prüfen
	Die Netzwerke sind nicht konsistent (crisscross)	Netzwerke prüfen

GRE-Tunnel konfiguriert sich nicht	Netzwerkgeräte und Router zwischen den Einheiten sind nicht korrekt konfiguriert	Konfiguration aller Geräte und Router prüfen
	Es sind nicht alle Geräte und Modems korrekt konfiguriert	U. a. die Einstellungen für die Firewall und Portweiter-leitungsregeln prüfen
	Die IPsec-Verschlüsselung ist nicht konsistent aktiviert oder deaktiviert	IPsec-Einstellungen für die GRE-Tunnelverbindung im WAN-Register prüfen
	Die Verschlüsselungs- und Hash-Verfahren des aktivierten IPsec stimmen nicht überein	IPsec-Einstellungen für die GRE-Tunnelverbindung im WAN-Register prüfen
GRE-Tunnel konfiguriert sich, aber die Kommunikation zwischen den lokalen Netzwerken ist nicht möglich	Verwenden beide Einheiten RIPv2?	Bitte prüfen
	Unterstützen beide Einheiten RIPv2?	Bitte prüfen
	Trifft beides nicht zu, sind die richtigen Routes in den Tunneln der beiden Einheiten gesetzt, sodass die Datenpakete durch die korrekten Tunnel geleitet werden	IPsec-Einstellungen für die GRE-Tunnelverbindung im WAN-Register prüfen

17 Transport, Aufbewahrung und Entsorgung

17.1 Transport

TAINY IQ-LTE wird in einem einzelnen Karton geliefert. Bewahren Sie die Verpackung für spätere Transportzwecke auf.

TAINY IQ-LTE kann mit öffentlichen Verkehrsmitteln transportiert werden (Flugzeug, Straße mit jeglicher Oberfläche, Schiff, Zug). Es sollte jedoch auf die Temperatur geachtet werden und die folgenden Werte sollten nicht über- oder unterschritten werden:

Temperaturbereich:	–40 °C …+85 °C
Relative Luftfeuchtigkeit:	max. 95 %

TAINY IQ-LTE muss entweder in einem einzelnen Karton oder in einem Gehäuse/Schrank, auf der obersten Schiene montiert, transportiert werden.

Wird TAINY IQ-LTE auf der obersten Schiene eines Gehäuses/Schranks montiert transportiert, muss sichergestellt sein, dass das Gerät nicht auf der Schiene entlangrutschen kann. Der Schrank/Das Gehäuse muss in Schichten aus stoß- und vibrationsdämpfendem Material (Styropor) verpackt sein. Die Dicke der Schichten ist abhängig von der Größe des Schrankes.

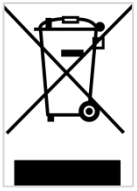
17.2 Lagerung

Trennen Sie das Gerät vor der Lagerung in jedem Fall von der Stromversorgung und entfernen Sie alle Kabel. Bewahren Sie TAINY IQ-LTE an einem wettergeschützten und nicht schwankenden Temperaturen unterworfenen Ort auf.

Temperaturbereich:	–40 °C …+85 °C
Relative Luftfeuchtigkeit:	max. 95 %

TAINY IQ-LTE muss entweder in einem einzelnen Karton oder in einem Gehäuse/Schrank, auf der obersten Schiene montiert, gelagert werden. Der Schrank/Das Gehäuse muss in Schichten aus stoß- und vibrationsdämpfendem Material (Styropor) verpackt sein. Die Dicke der Schichten ist abhängig von der Größe des Schrankes.

17.3 Entsorgung



Anwendbar in der Europäischen Union und anderen europäischen Staaten mit Systemen zur getrennten Sammlung von Wertstoffen. Altgeräte dürfen nicht in den Hausmüll! Deswegen sind Elektrogeräte mit diesem Symbol gekennzeichnet. Sollte das Gerät einmal nicht mehr benutzt werden können, so ist jeder Verbraucher gesetzlich verpflichtet, Altgeräte getrennt vom Hausmüll, z. B. bei einer Sammelstelle seiner Gemeinde/seines Stadtteils, abzugeben. Damit wird gewährleistet, dass Altgeräte fachgerecht verwertet werden, und negative Auswirkungen auf die Umwelt werden vermieden.

WEEE-Registrierungsnummer: 31323053

18 Glossar

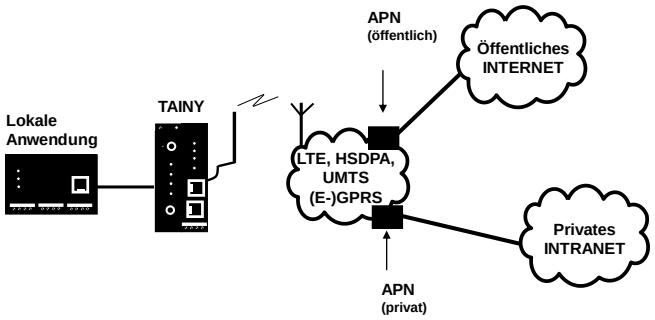
AES

Advanced Encryption Standard.

Das NIST (National Institute of Standards and Technology) entwickelt in Zusammenarbeit mit Industrieunternehmen 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 bekanntgegeben. Von den vorgeschlagenen Verschlüsselungsalgorithmen hat die NIST fünf Algorithmen in die engere Wahl gezogen: die Algorithmen MARS, RC6, Rijndael, Serpent und Twofish. Im Oktober 2000 hat man sich für Rijndael als Verschlüsselungsalgorithmus entschieden.

APN (Access Point Name)

(Übersetzt: Zugriffspunktname). Netzübergreifende Verbindungen, z. B. vom Datenfunkdienst (HSPA+, UMTS, EGPRS oder GPRS) ins Internet; werden über sogenannte APNs hergestellt.



Ein Endgerät, das eine Verbindung über den Datenfunkdienst aufbauen will, gibt durch Angabe des APNs 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 aufwendige Administrierbarkeit von symmetrischen Schlüsseln vermeiden.

Zellen-ID

Eindeutige Kennung einer Mobilfunkzelle.

CIDR

Classless InterDomain 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. Die nachfolgende Tabelle zeigt links die IP-Netzmaske, ganz rechts die entsprechende CIDR-Schreibweise.

CIDR (Tabelle)

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.

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):

	RSSI
< 6	< –101 dBm
6...10	–101 dBm… –93 dBm
11..18	–91 dBm… –77 dBm
> 18	> –75 dBm
99	Unknown/not detected

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 nächsthöheren 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. Da es sich hierbei um den ersten standardisierten Verschlüsslungs-algorithmus überhaupt handelte, setzte er sich auch schnell in der Industrie und somit außerhalb Amerikas durch.

DES arbeitet mit einer Schlüssellänge von 56 Bit, 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.

DPD

Die Dead-Peer-Detection (DPD) erkennt, ob eine IPsec-Verbindung zwischen zwei Netzen noch gültig ist oder wiederhergestellt werden muss. Diese Funktion muss von beiden Seiten unterstützt werden. Ohne DPD muss je nach Konfiguration die Verbindung entweder manuell wiederhergestellt werden oder die Lebensdauer der SA muss ablaufen.

Um zu überprüfen, ob die IPsec-Verbindung noch gültig ist, sendet DPD eine DPD-Anfrage an den anderen Teilnehmer. Wenn DPD nach einer bestimmten Anzahl von Fehlversuchen keine Antwort erhält, wird die IPsec-Verbindung unterbrochen.

DynDNS Provider

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 Dynamic-DNS-Anbieter (DNS = Domain-Name-Server).

Dann kann er bei diesem einen Host-Namen festlegen, unter dem der Rechner künftig erreichbar sein soll, z. B.: www.xyz.abc.de. Zudem stellt der Dynamic-DNS-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 Dynamic-DNS-Anbieter mit, welche IP-Adresse der Rechner zurzeit hat. Dessen Domain-Name-Server registriert die aktuelle Zuordnung Host-Name – 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 Dynamic-DNS-Anbieter registriert ist, benutzt der externe Rechner den Host-Namen des lokalen Rechners als Adresse. Dadurch wird eine Verbindung hergestellt zum zuständigen DNS (Domain-Name-Server), um dort die IP-Adresse nachzuschlagen, die diesem Host-Namen zurzeit zugeordnet ist. Die IP-Adresse wird zurückübertragen zum externen Rechner und jetzt von diesem als Zieladresse benutzt. Diese führt jetzt genau zum gewünschten lokalen Rechner.

Allen Internetadressen mittels Hostnamen liegt prinzipiell dieses Verfahren zugrunde: Zunächst wird eine Verbindung zum DNS hergestellt, um die diesem Host-Namen zugeteilte IP-Adresse zu ermitteln. Ist das geschehen, wird mit dieser „nachgeschlagenen“ IP-Adresse die Verbindung zur gewünschten Gegenstelle, bei der es sich um eine beliebige Internetpräsenz (z.B. Web-Seite) handeln kann, 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

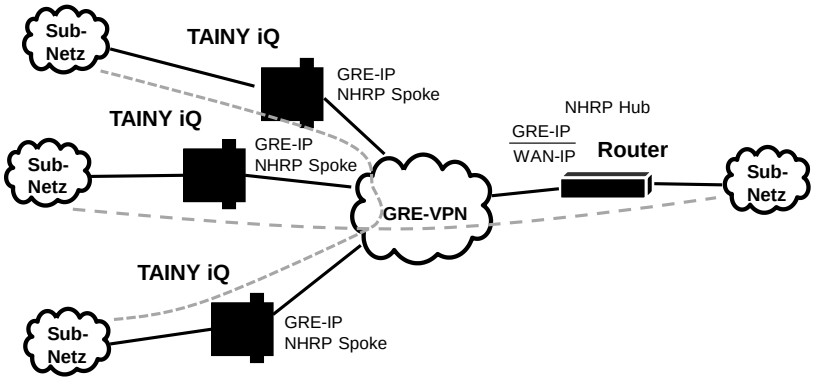
EGPRS steht für „Enhanced General Packet Radio Service“ und beschreibt einen auf GPRS beruhenden paketorientierten Datendienst, der durch EDGE-Technologie beschleunigt ist.

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 das Internet. Daten werden dabei paketorientiert vermittelt, wobei das Internet-Protokoll (IP) verwendet wird. GPRS stellt Datenraten von bis zu 115,2 KBit/s zur Verfügung.

GRE

Über TAINY IQ-LTE können unabhängige (Sub-)Netze verbunden werden. Dazu verwendet TAINY IQ-LTE das GRE(= Generic Routing Encapsulation)-Protokoll (RFC 1701; RFC 1702; RFC 2784).



Um einen DM-VPN untereinander aufbauen zu können, benötigen die (Sub-) Netze einen GRE-fähigen Router wie z. B. TAINY IQ-LTE.

Vorausgesetzt, es ist eine entsprechende Route konfiguriert, kann von einem (Sub-)Netz aus die Adresse eines anderen (Sub-)Netzes direkt angesprochen werden.

Während das GRE-Protokoll nur einen 1 : 1-Tunnel zwischen zwei Endpunkten aufbaut, ist der DM-VPN wie ein NBMA (Nonbroadcast Multiple Access) ausgerichtet. Innerhalb dieses virtuellen Netzwerks werden die Daten direkt von Endpunkt zu Endpunkt oder über ein Schaltgerät gesendet.

Bei der Verwendung des NHRP (= Next Hop Resolution Protocol) werden die Adressen der Endpunkte (NHRP-Spokes) an einem Endpunkt gesammelt, der als NHRP-Hub fungiert und auf Anfrage die Informationen mitteilt.

In einem DM-VPN muss der GRE-Endpunkt (z. B. der Router der Zentrale) im Hub-Modus laufen, während der andere Endpunkt (z. B. TAINY IQ-LTE) im Spoke-Modus läuft.

Allen Spokes im DM-VPN müssen sowohl die WAN-IP-Adresse wie auch die DM-VPN-IP-Adresse des Hubs bekannt sein.

Wenn der Hub Daten erhält, die nicht an seine mit ihm direkt verbundenen (Sub-)Netze adressiert sind, leitet er diese Daten entweder an den adressierten Endpunkt im DM-VPN weiter oder informiert den Absender darüber, wie er den adressierten Endpunkt direkt kontaktieren kann.

Das GRE-Protokoll umfasst weder Authentifizierung noch Verschlüsselung. Das kann mit einer zusätzlichen IPsec-Ebene bewirkt werden.

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.

HSPDA, HSUPA (HSPA+)

HSDPA (= High Speed Downlink Packet Access) und HSUPA (= High Speed Downlink Packet Access) sind Erweiterungen des UMTS-Netzes, die höhere Übertragungsraten bei der Datenübertragung von der Basisstation zur Mobilstation (HSDPA) bzw. von der Mobilstation zur Basisstation (HSUPA) ermöglichen.

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. Bekannt ist die Eingabe: http://www.neuhaus.de.

Bei HTTPS ist dem ursprünglichen Protokoll eine zusätzliche Komponente zum Datenschutz hinzugefügt. Während HTTP-Daten ungeschützt in Klartext übertragen werden, werden HTTPS-Daten erst nach einem Austausch von Sicherheitszertifikaten verschlüsselt übertragen.

ICCID

Der ICCID (= Integrated Circuit Card Identifier) identifiziert jeden international anerkannten SIM (Teilnehmer-Identitäts-Modul). Ein vollständiger ICCID kann 19 oder 20 Zeichen enthalten.

Er beinhaltet einen Ländercode, ein Ausstellercode, die SIM-Nummer sowie Prüfsummendaten.

IMEI

Die IMEI (= International Mobile Equipment Identity) ist die spezifische 15-stellige Serienummer des GSM- und UTMS-Endgerätes.

IMSI

Die IMSI (= International Mobile Subscriber Identity) ist eine auf der SIM-Karte gespeicherte Kennung, die den Teilnehmer identifiziert. Gewöhnlich umfasst die IMSI 15 Ziffern, kann aber auch kürzer sein.

Intranet

Ein Intranet ist ein unterschiedlich großes privates IP-Netz. Z. B. bilden das IP-Netz eines Unternehmens oder das Netzwerk mehrerer privater Rechner ein Intranet.

Das Internet dagegen ist ein öffentliches Netz. Ein Intranet sollte nur über Schutzeinrichtungen wie eine Firewall mit dem Internet verbunden werden.

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:

<table>
<tr><td></td><td>1. Byte</td><td>2. Byte</td><td>3. Byte</td><td>4. Byte</td></tr>
<tr><td>Class A</td><td>Netz-adresse</td><td colspan="3">Host-Adresse</td></tr>
<tr><td>Class B</td><td colspan="2">Netzadresse</td><td colspan="2">Host-Adresse</td></tr>
<tr><td>Class C</td><td colspan="3">Netzadresse</td><td>Host-Adresse</td></tr>
</table>

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. Bytes	Bytes für die Netzadresse	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).

IPv6

IP Version 6 (IPv6) beinhaltet eine 128-Bit-Adressierung.

Hinweis:
Die Zuteilung einer IPv6-Adresse im Mobilfunknetz ist abhängig davon, ob der verwendete Internet Mobilfunkbetreiber die Vergabe von IPv6 Adressen im Mobilen Datennetz unterstützt.
Die Erreichbarkeit mit IPv6 aus dem Internet ist abhängig vom Mobilfunkbetreiber und den abgeschlossenen Vertrag mit dem Betreiber. Mobilfunkbetreiber können private APN (access point name) für die Verwendung von ausgehenden und eingehenden IPv6 Verbindungen voraussetzen.

IP-Paket

Siehe Datagramm

IPsec

Internet Protocol Security (IPsec) ist ein Standard, der mittels IP-Datagrammen die Authentizität des Absenders, die Vertraulichkeit und die Integrität der Daten durch Verschlüsselung sicherstellt. 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 ab.

Im Transport-Mode wird in jedem IP-Datagramm zwischen IP-Header und TCP- oder UDP-Header ein IPsec-Header verwendet. 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 ist in der Payload des neuen Datagramms verschlüsselt.

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.

Location Area Code (LAC)

Ein Aufenthaltsbereich ist eine Gruppe von benachbarten GSM-Basisstationen. Sie sind alle miteinander verbunden, um die Befund- und Anrufsignalisierung für GSM-Endgeräte wie z. B. das CM-E1P01-GPRS-Modul zu ermöglichen.

Die Gruppe kann zwischen 10 und 100 GSM-Basisstationen umfassen. Jede der Gruppen verfügt über einen weltweit einzigartigen Identifikator (Location Area Code = LAC).

Long Term Evolution (LTE)

LTE ist die vierte Generation von Mobilfunknetzen, mit einer wesentlichen höheren Datenübertragungsrate als die dritte UTMS-Generation. Es ist möglich, bis 300 MBit pro Sekunde herunterzuladen. Der von den Mobilfunkanbietern genutzte Frequenzbereich liegt ausschließlich auf dem UHF-Frequenzband. Es werden mehrere Frequenzen genutzt, die regional zwischen dem mittleren und oberen Abschnitt des UHF-Bereichs von 700 bis 2600 MHz variieren können.

MCC/MNC

Der MCC (Mobile Country Code) und der MNC (Mobile Network Code) sind weltweit einzigartige Identifikatoren für ein Mobilfunknetz.

Der MCC ist dreistellig, der MNC zwei- oder dreistellig.

Im Internet befinden sich zahlreiche Webseiten mit den MCC und MNC verschiedener Länder und Netzwerkbetreiber.

MIB

Siehe SNMP

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 Ziel-Ports, dass das Datagramm eigentlich für einen internen Rechner bestimmt ist. Mithilfe 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 Bytes 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 Bytes 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 Bytes für Netzwerk-Adresse, 2 Bytes für Host-Adresse) mithilfe 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.

Paket-Filtern

Paket-Filtern ist eine zustandsorientierten Überpüfungsmethode der Firewall. Paketfilter lassen nur IP-Pakete passieren, wenn dieses vorab in den Regeln der Firewall festgelegt wurde. Das Folgende ist in den Firewall-Regeln definiert:

- Welches Protokoll (TCP, UDP, ICMP) darf passieren?
- Die zulässige Quelle des IP-Paketes (von IP/vom Port)
- Das zulässige Ziel des IP-Paketes (zur IP/zum Port)

Es ist ebenso definiert, wie mit IP-Paketen verfahren wird, die nicht passieren dürfen (verwerfen, ablehnen).

Für einen einfachen Paket-Filter ist es erforderlich, zwei Firewall-Regeln für eine Verbindung zu erstellen:

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

Bei der zustandsorientierten Firewall-Prüfung hingegen wird nur eine Regel für die Richtung der Anfrage von der Quelle zum Ziel erstellt. Die Firewall-Regel für die Richtung der Antwort vom Ziel zur Quelle richtet sich nach dem Ergebnis der Analyse der vorher gesendeten Daten. Die Firewall- Regel für die Antwort wird nach dem Erhalt der Antworten oder nach dem Ablauf einer kurzen vorgegebenen Zeitspanne wieder außer Kraft gesetzt. Daher können Antworten nur passieren, wenn vorab eine Anfrage gestellt wurde. Damit ist es unmöglich, Antwort-Regeln für einen unauthorisierten Zugang zu nutzen.

Außerdem ermöglichen Sonderverfahren den Durchlass von UDP- und ICMP-Daten, obwohl diese Daten vorab nicht angefordert wurden.

Portweiterleitung

Ist eine Firewall-Regel für die Portweiterleitung erstellt, werden die Datenpakete des externen Netzwerks, die an dem definierten IP-Port des Firewall-Gerätes eingehen, weitergeleitet. Die eingehenden Datenpakete werden an eine spezifizierte IP-Adresse und Port-Nummer im lokalen Netz weitergeleitet. Portweiterleitung kann für TCP oder UDP konfiguriert werden.

Bei der Portweiterleitung passiert das Folgende: Der Header der eingehenden Datenpakete aus dem externen Netz, die an die externe IP-Adresse des Firewall-Gerätes sowie einen spezifizierten Port adressiert sind, werden so angepasst, das sie an das interne Netz, einen bestimmten Rechner und den spezifizierten Port dieses Rechners weitergeleitet werden.
Das bedeutet, dass die IP-Adresse und die Port-Nummer im Header der eingehenden Datenpakete modifiziert werden.

Dieser Vorgang wird auch Destination-(Ziel-)NAT oder Portweiterleitung genannt.

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 öffentlichen 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 eines öffentlichen Schlüssels her, die durch die digitale Signatur einer X.509 Certification Authority (CA) beglaubigt wird. Die Signatur – eine Verschlüsselung mit dem Signaturschlüssel – kann mit dem öffentlichen Schlüssel überprüft werden, den die CA dem Zertifikatsinhaber aushändigt.

Protokoll, Übertragungs-protokoll l

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.

RADIUS

RADIUS steht für Remote Authentification Dail-In User Service. Dieses Client-Server-Protokoll steuert den sicheren Zugriff der Anwender auf das Netzwerk. Das Passwort des sich anmeldenden Anwenders wird mit einem zentralen Server abgeglichen. Der Autorisierung des Anwenders findet somit auf Nutzerebene statt. Diese Form der Autorisierung bietet Unternehmen die Möglichkeit sein Netz erfolgreich vor Angriffen zusichern und die Anwender zentral und individuell zu verwalten. Ferner können mittels des zentralen Servers auch Statistiken und Abrechnungen erstellen.

RIPv2

Das RIP (Routing Information Protocol) ist ein Routing-Protokoll, das dazu verwendet wird, automatische Routing-Tabellen der Router zu generieren. Router, deren RIPv2-Protokoll aktiviert ist, übertragen ihre Routing-Tabellen periodisch an konfigurierte Rip-Nachbarn: Ein Router kennt anfangs nur die direkt angeschlossenen Netzwerke. Daher fragt ein neuer Router sämtliche RIP-Nachbarn nach ihren kompletten Routing-Tabellen. Die Antworten werden dazu verwendet, erste Einträge für die eigene Routing-Tabelle zu generieren. Anschließend übermittelt er die generierte Routing-Tabelle an alle RIP-Nachbarn.

Service-Provider

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

SNMP

SNMP (Simple Network Management Protokoll) ist ein weit verbreiteter Mechanismus zur zentralen Kontrolle und Steuerung von Netzwerk-Komponenten wie zum Beispiel Server, Router, Switches, Drucker, Computer usw.

SNMP definiert den Kommunikationsablauf und den Aufbau der Datenpakete. Zum Transport wird UDP über IP verwendet.

SNMP definiert nicht die Werte, die gelesen oder verändert werden können.

Dies geschieht in einer MIB (Management Information Base). Die MIB ist eine Beschreibungsdatei, in denen die einzelnen Werte tabellarisch aufgeführt werden. Die MIB ist jeweils spezifisch für eine bestimmte Netzwerkkomponente oder für eine Klasse von Komponenten, zum Beispiel Switches.

SNMP-Trap

SNMP-Trap ist eine Benachrichtigung, die mittels SNMP-Agent (Simple Network Management Protokoll) von einer Netzwerk-Komponente unaufgefordert versendet wird.

Spoofing, Anti-Spoofing

In der Internet-Terminologie bedeutet Spoofing die Angabe einer falschen Adresse. Durch die falsche Internetadresse 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.

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.

TACACS+

TACACS+ (Terminal Access Controller Access Control System Plus) ist ein standardisiertes Protokoll, das der Kommunikation zwischen Clients und Servern innerhalb eines Netzwerks in den Bereichen Authentifizierung, Autorisierung und Abrechnung dient. Beispielsweise kann – wie beim TAINY IQ-LTE – ein TACACS+-Server aufgesetzt werden, der zentral die Zugangsdaten für alle Endgeräte im Netzwerk verwaltet und stellvertretend für diese bei Anmeldeanfragen die Autorisierung des jeweiligen Interessenten vornimmt. Dabei leitet das Endgerät die empfangenen Anmeldedaten an den TACACS+-Server weiter, der die für die Autorisierung notwendigen Prüfungen vornimmt und das Ergebnis der Prüfungen zurück an das Endgerät meldet.

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)

UART

UART steht für Universal Asynchron Receiver/Transmitter. Der UART ist Teil einer seriellen Schnittstelle, deren Aufgabe es ist die zu übertagenden Bytes in Bits (serielle Informationen) umzuwandeln. Während der Umwandlung wird dem Byte ein Startbit und ein Stoppbit hinzugefügt. Bei Umkehrung des Vorgangs werden die Bits wieder in Bytes umgewandelt, wobei die Übertragung asynchron stattfindet.

Es gibt verschiedene Ausführungen des UART, die sich in der Größe ihrer Byte-Puffer unterscheiden. Die vor allem zum Einsatz in Highspeed Routern verwendete Variante ist die 16550 Variante die zu einem 16 Byte großen FIFO-Puffer zusätzlich über einen Level-sensitive Interupt-triggering Mechanism verfügt, durch welchen die volle Übertragungsgeschwindigkeit erreicht wird.

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-basierten Datenübertragung und SMS-Übertragung auch die Möglichkeit zu Übertragung von Videoanwendungen.

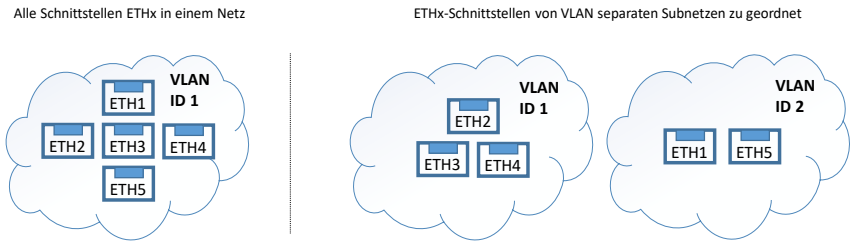
Mit Ausnahme des nordamerikanischen Raums verwendet UMTS ein Frequenzband bei 2100 MHz. In Nordamerika werden die Frequenzbänder bei 850 MHz und 1900 MHz genutzt, die auch für GSM-Netze verwendet werden.

VLAN

Die VLAN-Funktion (Virtual Local Area Network) ermöglicht die Teilung der LAN-Schnittstellen des TAINY IQ-LTE in verschiedene unabhängige virtuelle Netzwerke. Lokale Applikationen, die über identische VLAN-IDs mit LAN-Schnittstellen verbunden sind, können so über TAINY IQ-LTE miteinander kommunizieren. Besitzen sie unterschiedliche VLAN-IDs, ist die Kommunikation untereinander nicht möglich.

Die Trennung in verschiedene VLANs wird durch zusätzliche Tags (Markierungen) an den Datenpaketen möglich, die anzeigen, dass das Datenpaket zu einem bestimmten VLAN gehört.

Abhängig von der Konfiguration werden die Tags von den Datenpaketen entfernt. Entsprechend verlassen die Datenpakete das TAINY IQ-LTE mit oder ohne Tag. Werden die Tags nicht entfernt, kann eine angeschlossene externe Applikation, die das VLAN-Protokoll (802.1Q) unterstützt, in das VLAN einbezogen werden.



VPN (Virtual Private Network)

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 certificate

Eine Art „Siegel“, das 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 die 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.

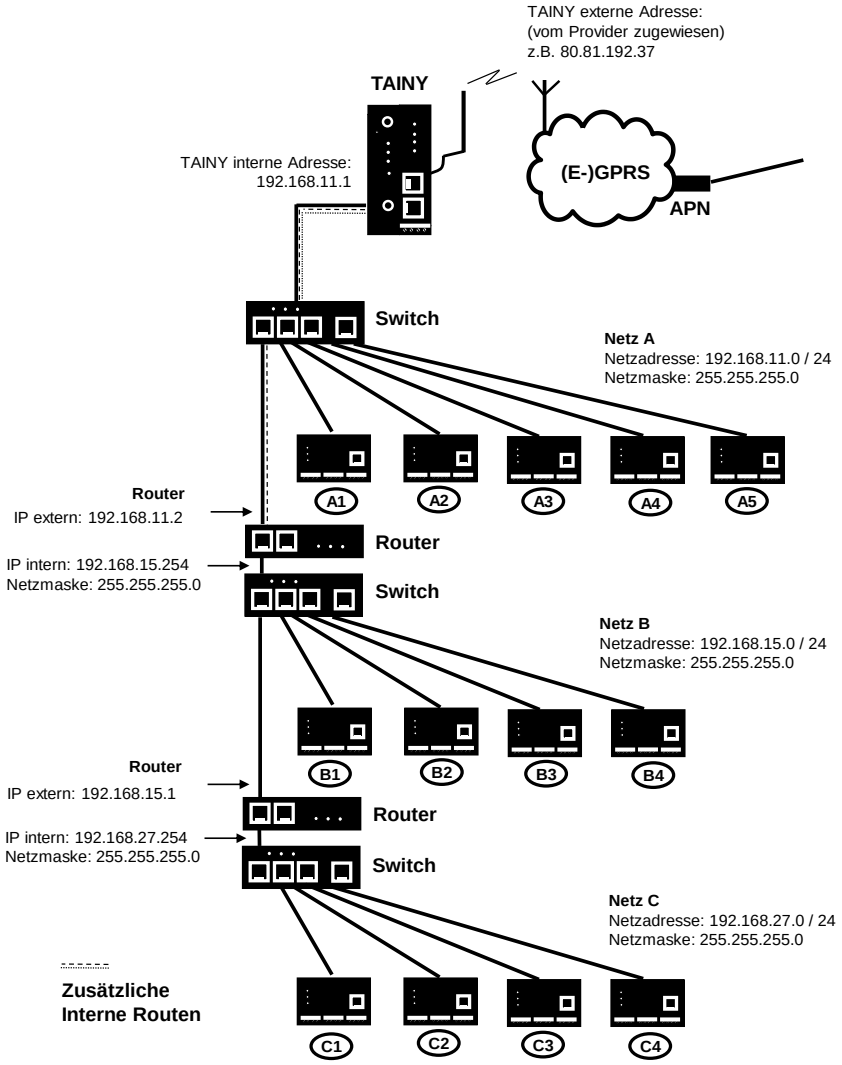
Der Hash-Wert wird auch als Fingerabdruck bezeichnet. Da er mit dem privaten Schlüssel der CA verschlüsselt ist, kann jeder, der den zugehörigen öffentlichen Schlüssel besitzt, die Bitfolge entschlüsseln und damit die Echtheit dieses Fingerabdrucks bzw. dieser Unterschrift überprüfen.

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 E-Mail-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 TAINY IQ-LTE 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 TAINY IQ-LTE 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.

19 Technische Daten

<table>
<tr><td rowspan="3">Verkabelte Schnittstellen</td><td>Ethernet (LAN)</td><td>2 x 10/100 Base-T (RJ45 plug), Ethernet IEEE802, 10/100 MBit/s, cross-over oder one-to-one, Auto-negotiation</td></tr>
<tr><td>Ethernet (LAN/WAN)</td><td>5 x 10/100 Base-T (RJ45 plug), Ethernet IEEE802, 10/100 MBit/s, cross-over oder one-to-one, Auto-negotiation</td></tr>
<tr><td>RS232</td><td>TX,RX,RTS,CTS,GND</td></tr>
<tr><td rowspan="3">Funkverbindung</td><td>Frequenzbänder</td><td>
<table>
<tr><td>GSM/GPRS/ EDGE</td><td>900 MHz, 1800 MHz</td></tr>
<tr><td>UMTS/ HSPA+</td><td>900 MHz (BdVIII), 1800 MHz (BdIII)*
2100 MHz (BdI)</td></tr>
<tr><td>LTE</td><td>800 MHz (Bd20), 900 MHz (Bd8)
1800 MHz (Bd3), 2100 MHz (Bd1)
2600 MHz (Bd7),</td></tr>
</table>
* Nicht zur Nutzung in der EU.

<table>
<tr><td>GSM/GPRS/ EDGE</td><td>850 MHz*, 900 MHz,
1800 MHz, 1900 MHz*</td></tr>
<tr><td>UMTS/ HSPA+</td><td>800 MHz (BdVI)*, 850 MHz (BdV)*,
900 MHz (BdVIII), 1900 MHz (BdII)*,
2100 MHz (BdI)</td></tr>
</table>
* Nicht zur Nutzung in der EU.
</td></tr>
<tr><td>Bänder</td><td>LTE (20,8,3,7,1)
3G (8,3,1)
2G Dual Band</td></tr>
<tr><td>Max. Sendeleistung</td><td>Class 4 (+33dBm ±2dB) für EGSM900
Class 1 (+30dBm ±2dB) für GSM1800
Class E2 (+27dBm ± 3dB) für GSM 900 8-PSK
Class E2 (+26dBm +3 /-4dB) für GSM 1800 8-PSK
Class 3 (+24dBm +1/-3dB) für UMTS 2100, FDD BdI
Class 3 (+24dBm +1/-3dB) für UMTS 1800, FDD BdIII*
Class 3 (+24dBm +1/-3dB) für UMTS 900, FDD BdVIII
Class 3 (+23dBm +-2dB) für LTE 2600, LTE FDD Bd7
Class 3 (+23dBm +-2dB) für LTE 2100, LTE FDD Bd1
Class 3 (+23dBm +-2dB) für LTE 1800, LTE FDD Bd3
Class 3 (+23dBm +-2dB) für LTE 900, LTE FDD Bd8
Class 3 (+23dBm +-2dB) für LTE 800, LTE FDD Bd20
* Nicht zur Nutzung in der EU.</td></tr>
</table>

		Class 4 (+33dBm ±2dB) for EGSM850 Class 4 (+33dBm ±2dB) for EGSM900 Class 1 (+30dBm ±2dB) for GSM1800 Class 1 (+30dBm ±2dB) for GSM1900 Class E2 (+27dBm ± 3dB) for GSM 850 8-PSK Class E2 (+27dBm ± 3dB) for GSM 900 8-PSK Class E2 (+26dBm +3 /-4dB) for GSM 1800 8-PSK Class E2 (+26dBm +3 /-4dB) for GSM 1900 8-PSK Class 3 (+24dBm +1/-3dB) for UMTS 2100, FDD BdI Class 3 (+24dBm +1/-3dB) for UMTS 1900, FDD BdII* Class 3 (+24dBm +1/-3dB) for UMTS 900, FDD BdVIII Class 3 (+24dBm +1/-3dB) for UMTS 850, FDD BdV* Class 3 (+24dBm +1/-3dB) for UMTS 800, FDD BdVI* * Nicht zur Nutzung in der EU.
	HSPA+	HSDPA Cat. 10/HSUPA Cat. 6 Datenraten: DL: max. 14,4 Mbps, UL: max. 5,76 Mbps
	EDGE (EGPRS)	EDGE-Klasse 12 Datenraten: DL: max. 237 kbps, UL: max. 237 kbps
	GPRS	GPRS-Klasse 12 Datenraten: DL: max. 85,6 kbps, UL: max. 85,6 kbps
	Antennen-anschlüsse	SMA-Buchse nominale Impedanz: 50 Ohm
Sicherheits-funktionen	VPN	Dynamic-Multipoint-VPN IPsec
	Firewall	Stateful inspection firewall Anti-spoofing Portweiterleitung MAC-Tabelle
Zusätzliche Funktionen		VLAN, PPPoE, DNS Cache, DHCP Server, NTP, Verbindungsprüfung, TACACS+, E-Mail und Snapshot-Versand
Management		Webbasierte Administrations-Benutzeroberfläche SNMPv3, Logbuch, Snapshot, Zertifikate
Umweltbe-dingungen	Temperaturbereich	Betrieb: –20 °C bis +70 °C* Lagerung: –40 °C bis +85 °C * Automatische Abschaltung des Funkmoduls, sobald eine kritische Temperatur erreicht wird.
	Luftfeuchtigkeit	0–95 %, nicht kondensierend
Stromversorgung	I (nominal) Irms: 570-165 mA; Imax:650 mA U (nominal) 12–60 V_{DC}	

Gehäuse	Ausführung	Hutschienengehäuse
	Material	Kunststoff
	Schutzklasse	IP20
	Abmessungen	114,5 mm x 45 mm x 99 mm (D x W x H)
	Gewicht	ca. 250g
Konformität	CE-Kennzeichen	Die Geräte entsprechen bei bestimmungsgemäßer Verwendung der Richtlinie 2014/53/EU (RED). Die Geräte entsprechen der Richtlinie 2011/65/EU (ROHS). Die CE-Konformitätserklärungen finden Sie unter www.neuhaus.de www.sagemcom.com, oder wenden Sie sich an unseren Kundendienst.
	Funk	EN 301 511 [v.12.5.1] EN 301 908-1 [v.11.1.1] EN 301 908-2 [v.11.1.1] EN 301 908-13 [v.11.1.2]
	EMV	Draft EN 301 489-1 [v.2.2.0] Draft EN 301 489-52 [v.2.2.0] EN 55032 [2015] EN 61000-6-2 / AC [2005 / 2005]
	Sicherheit & Gesundheit	EN 62368-1 / AC / [2014 / 2015] EN 62479 [2010] Schutzklasse 2, Verschmutzungsgrad 2, Überspannungskategorie 2
	Umwelt	ROHS (EN 50581 [2012]) WEEE
	Funkmodul	GCF und PTCRB zertifiziert

20 Vereinfachte EU-Konformitätserklärung

CE Vereinfachte EU-Konformitätserklärung

Hiermit erklärt Sagemcom Dr. Neuhaus GmbH, dass die Funkanlagen Typ TAINY IQ-LTE und TAINY IQ-LTE 6E der Richtlinie 2014/53 / EU entsprechen. Der vollständige Text der EU-Konformitätserklärungen ist unter folgenden Internetadressen verfügbar:

www.neuhaus.de oder www.sagemcom.com

Frequenzbänder

GSM/GPRS/EDGE: 900/1800MHz

UMTS/HSPA+: 900/1800/2100MHz

LTE: 800/900/1800/2100/2600MHz

Max. Sendeleistung

Class 4 (2W) for EGSM900

Class 1 (1W) for GSM1800

Class E2 (0,5W) for GSM900 8-PSK

Class E2 (0,4W) for GSM1800 8-PSK

Class 3 (0,25W) for UMTS/HSPA+

Class 3 (0,20W) for LTE

GPRS/EGPRS

Multi-slot Class 12