DSR-211-Serie

Industrieller LTE/HSPA+/UMTS/GSM-Router

Handbuch

AddSecure GmbH
Breite Straße 10
D-40670 Meerbusch
Telefon: +49 (0)2159/ 693 75-0
Fax: +49 (0)2159/ 922 430 0
E-Mail: info.digicomm@addsecure.com

Dokument Revision: 21-01

Software-Version: 3.0.17 (26)

Weitere Informationen zu unseren Produkten finden Sie unter www.addsecure.de.

Über dieses Dokument

Dieses Dokument enthält Hardware- und Softwareinformationen zur Router- Serie DSR-211, einschließlich Einführung, Installation, Konfiguration und Betrieb.

Rechtliche Informationen

Der Inhalt dieses Dokuments wird „wie besehen“ zur Verfügung gestellt. Sofern nicht durch geltendes Recht vorgeschrieben, werden keine Garantien jeglicher Art, weder ausdrücklich noch stillschweigend, einschließlich, aber nicht beschränkt auf die stillschweigende Gewährleistung der Marktgängigkeit und Eignung für einen bestimmten Zweck, in Bezug auf die Genauigkeit und Zuverlässigkeit oder den Inhalt dieses Dokuments gegeben.
AddSecure behält sich das Recht vor, dieses Dokument jederzeit und ohne vorherige Ankündigung zu überarbeiten oder zurückzuziehen.
AddSecure ist unter keinen Umständen verantwortlich für Daten- oder Einkommensverluste oder für besondere, zufällige, Folge- oder indirekte Schäden, wie auch immer verursacht.

Weitere Informationen über AddSecure finden Sie unter folgender Internetadresse: https://www.addsecure.de.

Wichtiger Hinweis

Aufgrund der Natur der drahtlosen Kommunikation können die Übertragung und der Empfang von Daten niemals garantiert werden. Daten können verzögert werden, beschädigt werden (d. h. Fehler aufweisen) oder ganz verloren gehen. Obwohl erhebliche Verzögerungen oder Datenverluste selten sind, wenn drahtlose Geräte wie der Router in einem gut aufgebauten Netzwerk auf normale Weise verwendet werden, sollte der Router nicht in Situationen verwendet werden, in denen ein Versagen beim Senden oder Empfangen von Daten zu Schäden jeglicher Art für den Benutzer oder eine andere Partei führen könnte, einschließlich, aber nicht beschränkt auf Personenschäden, Tod oder Verlust von Eigentum. AddSecure übernimmt keine Verantwortung für Schäden jeglicher Art, die durch Verzögerungen oder Fehler in den mit dem Router übertragenen oder empfangenen Daten entstehen, oder für das Versagen des Routers, solche Daten zu übertragen oder zu empfangen.

Sicherheitsvorkehrungen

Allgemein

Der Router erzeugt Hochfrequenzenergie (HF). Bei der Verwendung des Routers muss auf Sicherheitsfragen im Zusammenhang mit HF-Störungen sowie auf die Vorschriften für HF-Geräte geachtet werden.
Verwenden Sie Ihren Router nicht in Flugzeugen, Krankenhäusern, an Tankstellen oder an Orten, an denen die Verwendung von Mobilfunkprodukten verboten ist.
Vergewissern Sie sich, dass der Router die Geräte in der Nähe nicht stört. Zum Beispiel: Herzschrittmacher oder medizinische Geräte. Die Antenne des Routers sollte von Computern, Bürogeräten, Haushaltsgeräten usw. entfernt sein.
Für den ordnungsgemäßen Betrieb muss eine externe Antenne an den Router angeschlossen werden. Verwenden Sie nur zugelassene Antennen mit dem Router. Bitte wenden Sie sich an einen autorisierten Händler, um eine zugelassene Antenne zu finden.
Halten Sie die Antenne immer mit einem Mindestsicherheitsabstand von 20 cm oder mehr vom menschlichen Körper entfernt. Stellen Sie die Antenne nicht in metallische Kisten, Behälter usw.

HF-Expositionserklärungen

Für mobile Geräte ohne Kollokation gilt: die Sendeantenne ist mehr als 20 cm vom Körper des Benutzers entfernt installiert oder aufgestellt.

FCC-Erklärung zur HF-Strahlenexposition

Dieser Sender darf nicht zusammen mit einer anderen Antenne oder einem anderen Sender aufgestellt werden oder in Verbindung mit diesen betrieben werden.
Dieses Gerät entspricht den FCC-Grenzwerten für HF-Strahlenbelastung, die für eine unkontrollierte Umgebung festgelegt wurden. Dieses Gerät sollte mit einem Mindestabstand von 20 Zentimetern zwischen der Strahlenquelle und dem menschlichen Körper installiert und betrieben werden.

Hinweis: Einige Fluggesellschaften erlauben möglicherweise die Benutzung von Mobiltelefonen, während das Flugzeug am Boden steht und die Tür offen ist. Zu diesem Zeitpunkt kann ein Router verwendet werden.

Verwendung des Routers im Fahrzeug

Prüfen Sie vor der Installation des Routers, ob in Ihrem Land Vorschriften oder Gesetze bestehen, die die Verwendung von Mobilfunkgeräten in Fahrzeugen zulassen.
Der Fahrer oder Bediener eines Fahrzeugs sollte den Router nicht während der Fahrt bedienen.
Lassen Sie den Router durch qualifiziertes Personal installieren. Informieren Sie sich bei Ihrem Fahrzeughändler über mögliche Störungen elektronischer Teile durch den Router.
Der Router sollte über einen abgesicherten Anschluss im Sicherungskasten des Fahrzeugs an das Versorgungsnetz des Fahrzeugs angeschlossen werden.
Seien Sie vorsichtig, wenn der Router von der Hauptbatterie des Fahrzeugs gespeist wird. Die Batterie kann nach längerer Zeit entladen werden.

Um eine fehlerfreie Nutzung zu gewährleisten, installieren und betreiben Sie Ihren Router bitte mit Sorgfalt.
Beachten Sie stets Folgendes:
Setzen Sie den Router keinen extremen Bedingungen wie hoher Luftfeuchtigkeit / Regen, hohen Temperaturen, direktem Sonnenlicht, ätzenden / aggressiven Chemikalien, Staub oder Wasser aus.
Versuchen Sie nicht, den Router zu zerlegen oder zu modifizieren. Es befindet sich kein vom Benutzer zu wartendes Teil im Inneren und die Garantie würde erlöschen.
Lassen Sie den Router nicht fallen, schlagen oder schütteln Sie ihn nicht. Verwenden Sie den Router nicht unter extremen Vibrationsbedingungen.
Ziehen Sie nicht an der Antenne oder dem Stromversorgungskabel. Anbringen/ Lösen durch Halten des Steckers.
Schließen Sie den Router nur gemäß Handbucha an. Bei Nichtbeachtung erlischt die Garantie.
Im Falle von Störungen oder Fragen, wenden Sie sich bitte an unseren Support unter (02159) 693 75-50.

Informationen zu Vorschriften und Typgenehmigung

Tabelle 1: Richtlinien

2011/65/EU	Die europäische Richtlinie RoHS 2.0 2011/65/EU wurde am 1. Juli 2011 vom Europäischen Parlament und dem Europäischen Rat zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten erlassen.
2012/19/EU	Die europäische Richtlinie WEEE 2012/19/EU wurde am 24. Juli 2012 vom Europäischen Parlament und dem Europäischen Rat über Elektro- und Elektronik-Altgeräte erlassen.
2013/56/EU	Die europäische Richtlinie 2013/56/EU ist eine Batterierichtlinie, die am 10. Dezember 2013 im EU-Amtsblatt veröffentlicht wurde. Die in diesem Produkt verwendete Knopfbatterie entspricht der Norm der Richtlinie 2013/56/EU.

Tabelle 2: Giftige oder gefährliche Substanzen oder Elemente mit definierten Konzentrationsgrenzen

Name des Teils	Gefährliche Substanzen										
	(Pb)	(Hg)	(Cd)	(Cr (VI))	(PBB)	(PBDE)	(PBDE)	(DEHP)	(BBP)	(DBP)	(DIBP)
Metallteile	o	o	o	o	o	o					
Schaltungsmodule	x	o	o	o	o	o					
Kabel und Kabelbaugruppen	o	o	o	o	o	o					
Kunststoff- und Polymerteile	o	o	o	o	o	o					

o:
Weist darauf hin, dass dieser giftige oder gefährliche Stoff, der in allen homogenen Materialien für dieses Teil enthalten ist, unter den in SJ/T11363-2006 geforderten Grenzwerten liegt.
x:
Weist darauf hin, dass dieser giftige oder gefährliche Stoff, der in mindestens einem der homogenen Materialien für dieses Teil enthalten ist, die in SJ/T11363-2006 geforderten Grenzwerte überschreiten könnte.

Inhalt

Inhaltsverzeichnis

Bitte beachten Sie: Dies ist ein Handbuch für die DSR-211-Serie.
Bitte prüfen Sie, welches Modell Sie verwenden.

1. Produktübersicht

1.1 Hauptmerkmale

Der DSR-211 ist ein robuster industrieller Mobilfunk-Router, mit dem unzugängliche oder mobile Außenstationen, die keinen Zugang zum Telefonnetz oder ADSL haben, in zentrale Netze integriert werden können.

Schnittstellen

- GSM/GPRS/EDGE/ UMTS/ HSPA+/FDD LTE
  Alternativ: CDMA, LTE-450
- WLAN, GPS & GLONASS
  Alternativ: LoraWAN
- USB-Port zur Übernahme der Konfiguration
- SD-Karte zur Speichererweiterung
- 2 x 10/100Mbps Ethernet 2 x LAN oder 1 x LAN & 1 WAN Anschluss, Digitale IOs
  Alternativ: 4 x 10/100Mbps Ethernet
- Serielle Schnittstellen 1x RS-232, 1x RS-485 (Schraubklemme)
- TCP client/server
- Modbus RTU auf Modbus TCP
- Virtueller COM
- Modbus Abfrage DIOs

Management

- WEB-GUI
- CLI
- SNMP v3 (alle Parameter im GUI können per SNMP abgefragt oder verändert werden)
- SMS

Sicherheit

- HTTP, HTTPs
- Telnet, SSH2
- VPN: IPSec/OpenVPN Client/Server
- RADIUS / TACACS
- Firewall: SPI, Anti-DoS, Filter, Access Control
- Port Control

Bridge/Router

- VLAN
- Layer 2 über VPN (VPN-Bridging)
- NAT, DMZ, RIP v1/v2, OSPF, DDNS, VRRP, GRE
- WAN-Link Backup

Mobilfunk

- Dual SIM
- Bevorzugte Provider
- Auswahl bestes Netz mit Health-Check mit einer (National Roaming) oder zwei SIM-Karten

Hardware

- Hutschienen- oder Wandmontage
- Spannung 9-60VDC
- Temperaturbereich -40 bis +75°C

1.2 Inhalt der Verpackung

Bevor Sie Ihre DSR-211 Router installieren, überprüfen Sie, ob dem Kit die folgenden Inhalte beiliegen:
Hinweis: Die folgenden Bilder dienen nur zur Veranschaulichung und zeigen nicht die tatsächliche Größe.

Überprüfen Sie Ihr Paket, um sicherzustellen, dass es die folgenden Elemente enthält:

1x DSR-211- (Modell optional)
Weitere Einzelheiten über die Antennenschnittstelle finden Sie in Abschnitt 1.3 Spezifikationen.

1 x 3-poliger 5-mm-Klemmenblock (Male) für die Stromversorgung

1 x 7-poliger steckbarer Klemmenblock mit für den seriellen Anschluss, I/O- und Konsolenanschluss

Hinweis: Sollte einer der oben genannten Artikel fehlen oder beschädigt sein, wenden Sie sich bitte an Ihren AddSecure-Vertriebspartner.

Optionales Zubehör (kann separat erworben werden):

3G/4G SMA-Mobilfunkantenne (Stummelantenne oder Magnetantenne optional)

Stummelantenne

Magnetantenne

RP-SMA-WiFi-Antenne (Stummelantenne oder Magnetantenne optional)

Stummelantenne

Magnetantenne

Wandmontage-Kit

Montagesatz für 35-mm-Tragschiene

Ethernet-Kabel x 1

AC/DC- Netzadapter (12 V DC, 1,5A; EU-, US-, UK-, AU-Stecker optional)

1.3 Spezifikationen

Mobilfunkschnittstelle

- Anzahl der Antennen: 2 (AUX + MAIN)
- Anschluss: SMA, weiblich
- SIM: 2 (3,0 V & 1,8 V)
- Mobilfunkstandards: GSM/GPRS/EDGE/WCDMA/HSDPA/HSUPA/HSPA+/DC HSPA+/TD SCDMA/CDMA (CDMA 1X/EVDO)/FDD LTE/TDD LTE
- GSM: max. DL/UL = 9,6/2,7 kbit/s
- GPRS: max. DL/ UL = 86 kbit/s
- EDGE: max. DL/ UL = 236,8 kbit/s
- WCDMA/TD-SCDMA: max. DL/UL = 2,8 Mbit/s/384 kbit/s
- EVDO: max. DL/UL = 5,4 Mbit/s/14,7 kbit/s
- HSPA+: max. DL/UL = 21/5,76 Mbit/s, Fallback auf 2G
- DC HSPA+: max. DL/UL = 42/5,76 Mbit/s, Fallback auf 2G
- FDD LTE: max. DL/UL = 100/50 Mbit/s, Fallback auf 2G/ 3G
- TDD LTE: max. DL/UL = 100/50 Mbit/s, Fallback auf 2G/ 3G

Ethernet-Schnittstelle

- Anzahl der Ports: 2 x 10/100 Mbit/s, 2 x LAN oder 1 x LAN + 1 x WAN
- Magnetisolationsschutz: 1,5 KV

WiFi-Schnittstelle (optional)

- Anzahl der Antennen: 1
- Anschluss: RP-SMA, männlich
- Mobilfunkstandards: 802.11a/b/g/n, unterstützt AP- und Client-Modus
- Frequenzbänder: 2,4 GHz, 5 GHz
- Sicherheit: Open (offen),WPA, WPA2, WEP
- Verschlüsselung: AES, TKIP, WEP64
- Datengeschwindigkeit: Bis zu 150 Mbit/s
- Empfangsempfindlichkeit:
  1 M -97 dBm (< 8 % PER)
  54 Mbit/s -76,5 dBm (< 10 % PER)
  MCS7 (20 MHz) -72 dBm (< 10 % PER)
  MCS7 (40 MHz) -69 dBm (< 10 % PER)
  (+/ - 1 dBm)

GPS- & GLONASS-Schnittstelle (optional)

- Anzahl der Antennen: 1
- Anschluss: SMA, weiblich mit 50 Ohm Impedanz
- Tracking-Empfindlichkeit:
  GPS: größer als -148 dBm
  GLONASS: größer als -140 dBm
  Horizontale Positionsgenauigkeit: GPS: 2,5 m
  GLONASS: 4,0 m
  Protokoll: NMEA-0183 V2.3

Serielle Schnittstelle

- Anzahl der Ports: 1 x RS-232 + 1 x RS-485 oder 2 x RS-232 oder 2 x RS-485
- Anschluss: 3,5-mm-Klemmenblock
- ESD-Schutz: ±15 KV
- Parameter: 8E1, 8O1, 8N1, 8N2, 7E2, 7O2, 7N2, 7E1
- Baudrate: 300 Baud/s bis 230.400 Baud/s
- RS-232: TxD, RxD, RTS, CTS, GND
- RS-485: Daten+ (A), Daten- (B)

Digitaleingang / Digitalausgang

- Typ: 2 x DI (potentialfreier Kontakt) + 2 x DO (spannungsführender Kontakt) 4 x DI, 4 x DO, 3 x DI + 1 x DO oder 3 x DO + 1 x DI
- Anschluss: 3,5-mm-Klemmenblock
- Isolation: 3 KV DC oder 2 KV rms
- Absolutes Maximum V DC: „V+“ +5 V DC (DI), 30 V DC (DO)
- Absolutes Maximum A DC: 300 mA
- Digitales Filterzeitintervall: per Software wählbar

Sonstiges

- 1 x RST-Taste
- 1 x MicroSD-Schnittstelle
- 1 x USB 2.0-Host mit bis zu 480 Mbit/s
- 1 x CLI-Schnittstelle
- LED-Anzeigen: 1 x RUN, 1 x PPP, 1 x USR, 1 x RSSI, 1 x NET, 1 x SIM

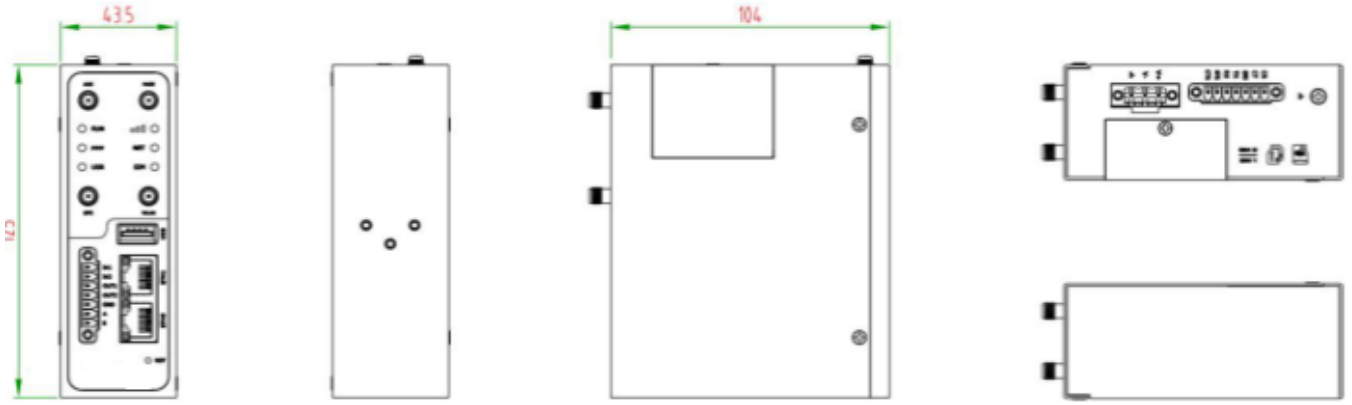
Stromversorgung und –verbrauch

- Anschluss: 3-polige 5-mm-Buchse mit Verriegelung
- Eingangsspannung: 9 bis 60 V DC
- Leistungsaufnahme: Leerlauf: 100 mA bei 12 V; Datenverbindung: 400 mA (Spitze) bei 12 V

Physikalische Merkmale

- Gehäuse und Gewicht: Metall, 570 g
- Schutzart: IP30
- Abmessungen: 125 mm x 104 mm x 43,5 mm
- Installation: Tisch- oder Wandmontage oder Montage auf 35-mm-Tragschiene

1.4 Abmessungen



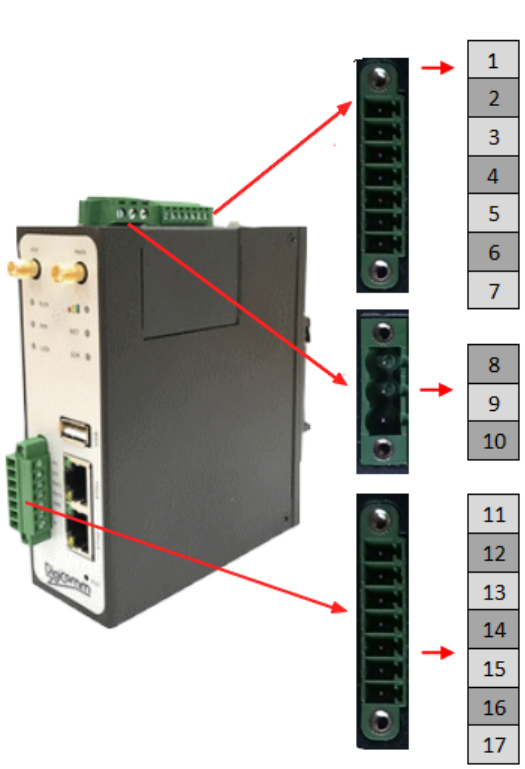
1.5 Warnung

WARNUNG

EXPLOSIONSGEFAHR. NICHT ENTFERNEN ODER ERSETZEN, SOLANGE DER STROMKREIS UNTER SPANNUNG STEHT, ES SEI DENN, DER BEREICH IST FREI VON ENTZÜNDBAREN KONZENTRATIONEN.

2. Hardware-Installation

2.1 Pin-Belegung



PIN	Debug	RS232	Direction
1	RXD		Device → DSR-211
2	TXD		DSR-211 → Device
3	GND	GND	
4		TXD	DSR-211 → Device
5		RXD	Device → DSR-211
6		RTS	DSR-211 → Device
7		CTS	Device → DSR-211

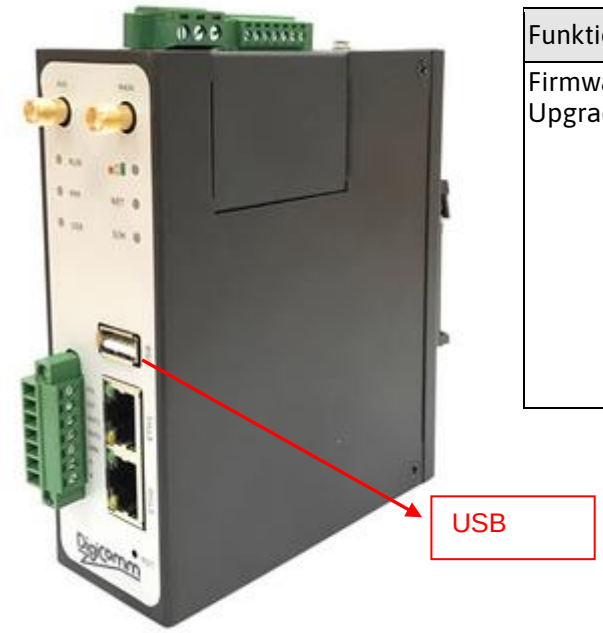
PIN	Power	Digital I/O	RS485	Direction
8	Positive			
9	Negative			
10	GND			
11		Input 1		DSR-211 – Device
12		Input 2		DSR-211 ← Device
13		Output 1		DSR-211 ▸ Device
14		Output 2		DSR-211 → Device
15		GND		
16			Data+(A)	DSR-211 → Device
17			Data- (B)	DSR-211 → Device

2.2 LED-Anzeigen

Name	Farbe	Status	Beschreibung
RUN	Grün	Ein, schnell blinkend (250 ms Blinkzeit)	Der Router ist eingeschaltet (das System initialisiert sich gerade)
		Ein, blinkend (500 ms Blinkzeit)	Der Router nimmt den Betrieb auf
		Aus	Der Router ist ausgeschaltet
PPP	Grün	Ein, dauerhaft leuchtend	Link-Verbindung funktioniert
		Aus	Link-Verbindung funktioniert nicht
USR-OpenVPN	Grün	Ein, dauerhaft leuchtend	OpeVPN-Verbindung ist hergestellt
		Aus	OpenVPN-Verbindung ist nicht hergestellt
USR-IPsec	Grün	Ein, dauerhaft leuchtend	IPsec-Verbindung ist hergestellt
		Aus	IPsec-Verbindung ist nicht hergestellt
USR-WiFi	Grün	Ein, dauerhaft leuchtend	Wi-Fi ist aktiviert und funktioniert einwandfrei
		Aus	Wi-Fi ist deaktiviert oder funktioniert nicht richtig
	Grün	Ein, dauerhaft leuchtend	Hohe Signalstärke (21–31) ist verfügbar
	Gelb	Ein, dauerhaft leuchtend	Mittlere Signalstärke (11–20) ist verfügbar
	Rot	Ein, dauerhaft leuchtend	Niedrige Signalstärke (1–10) ist verfügbar
	--	Aus	Kein Signal
NET	Grün	Ein, dauerhaft leuchtend	Verbindung zum 4G-Netz ist hergestellt
	Gelb	Ein, dauerhaft leuchtend	Verbindung zum 3G-Netz ist hergestellt
	Rot	Ein, dauerhaft leuchtend	Verbindung zum 2G-Netz ist hergestellt
	--	Aus	Verbindung zum Netzwerk ist nicht hergestellt oder wird nicht aufgebaut
SIM	Grün	Ein, blinkend	Der Router verwendet die Backup-Karte
		Aus	Der Router verwendet die Hauptkarte

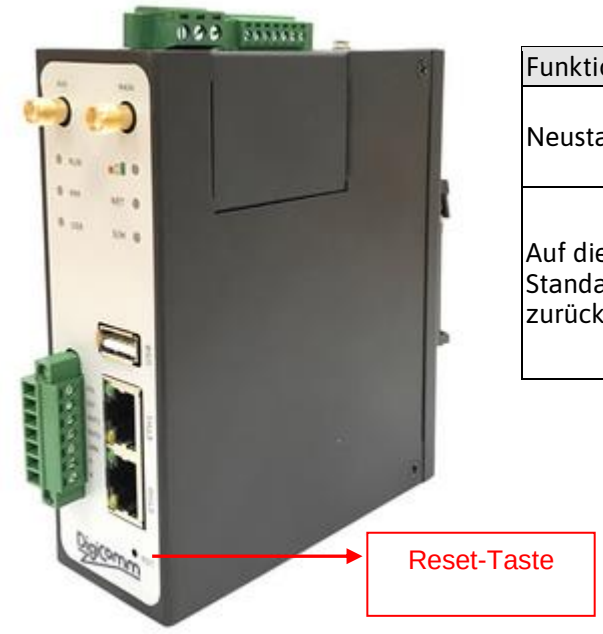
Hinweis: Sie können den Anzeigetyp der USR-LED wählen. Weitere Einzelheiten finden Sie unter 3.30 Service > Erweitert

2.3 USB-Schnittstelle



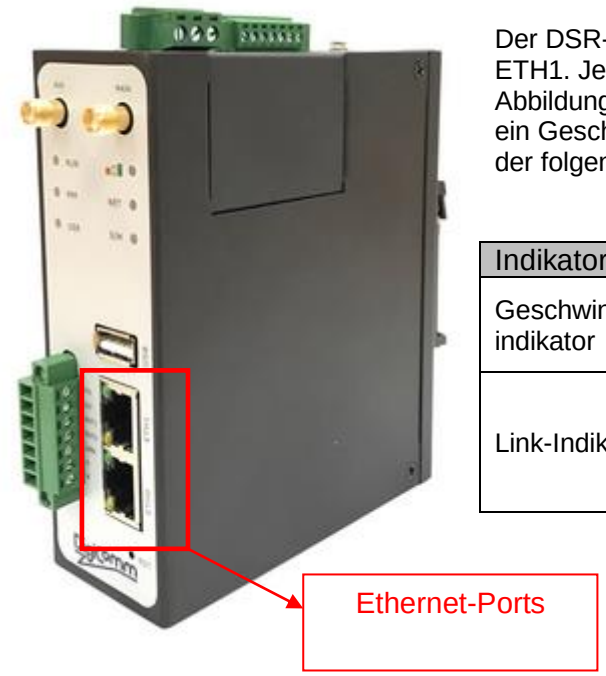
Funktion	Verwendung
Firmware-Upgrade	Die USB-Schnittstelle wird für Batch-Firmware-Upgrades verwendet, kann aber nicht zum Senden oder Empfangen von Daten von verwendet werden. Sie können ein USB-Speichergerät an die USB-Schnittstelle des Routers anschließen, z. B. eine U-Disk oder Festplatte. Wenn sich in diesem USB-Speichergerät eine unterstützte Konfigurationsdatei oder eine Router-Firmware befindet, aktualisiert der Router die Konfigurationsdatei oder die Firmware automatisch. Für weitere Einzelheiten siehe 3.11 Schnittstelle > USB

2.4 Reset-Taste



Funktion	Verwendung
Neustart	Drücken und halten Sie die RST-Taste mindestens 5 und höchstens 7 Sekunden lang. Der Router wird dann neu gestartet.
Auf die werkseitige Standardeinstellung zurücksetzen	Warten Sie nach dem Einschalten des Routers 5 Sekunden lang, drücken und halten Sie die RST-Taste, bis alle sechs LEDs nacheinander zu blinken beginnen, und lassen Sie die Taste dann los, um den Router auf die Werkseinstellungen zurückzusetzen.

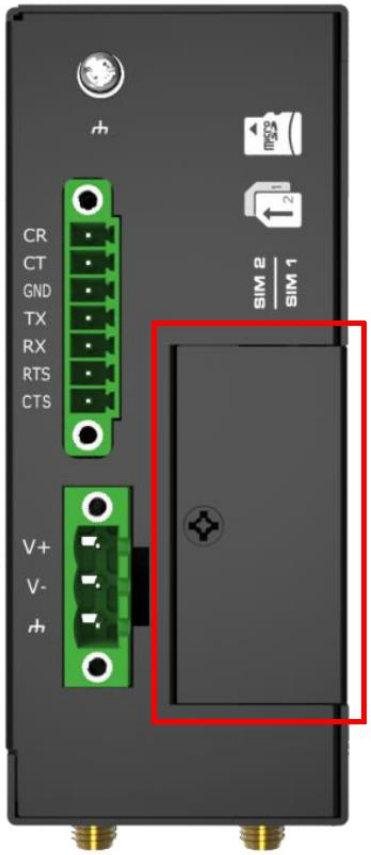
2.5 Ethernet-Ports

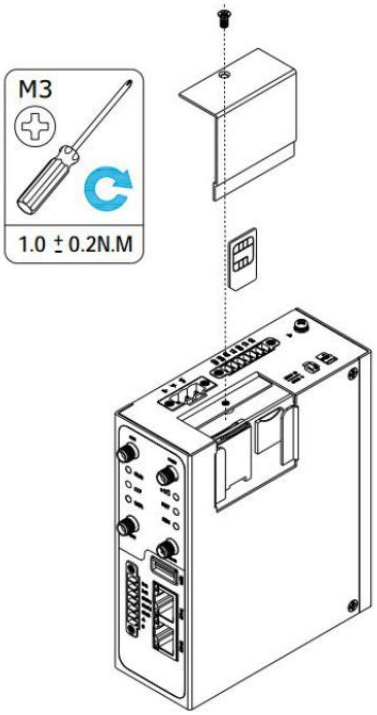


Der DSR-211 Router verfügt über zwei Ethernet-Ports ETH0 und ETH1. Jeder Ethernet-Port verfügt über zwei LED-Anzeigen (siehe Abbildung links). Die gelbe Anzeige ist ein Link-Indikator, die grüne ein Geschwindigkeitsindikator. Einzelheiten zum Status finden Sie in der folgenden Tabelle.

Indikator	Status	Beschreibung
Geschwindigkeits indikator	Ein, dauerhaft leuchtend	100 Mbit/s-Modus
	Aus	10 Mbit/s-Modus
Link-Indikator	Ein, dauerhaft leuchtend	Verbindung ist hergestellt
	Ein, blinkend	Daten werden übertragen
	Aus	Verbindung ist nicht hergestellt

2.6 SIM-Karte/ MicroSD-Karte einlegen oder entfernen





Legen Sie die SIM/MicroSD-Karte ein oder entfernen Sie sie wie in den folgenden Schritten beschrieben:

SIM-Karte/ MicroSD-Karte einlegen

1. Stellen Sie sicher, dass der Router ausgeschaltet ist.
2. Um die Steckplatzabdeckung zu entfernen, lösen Sie die Schrauben der Abdeckung mit einem Schraubendreher und suchen Sie dann den SIM-Kartensteckplatz/ SD-Kartensteckplatz.
3. Zum Einlegen der SIM-Karte/ MicroSD-Karte drücken Sie die Karte mit Ihrem Finger, bis Sie ein Klicken hören, und ziehen Sie dann die mit der Abdeckung verbundenen Schrauben mit einem Schraubendreher fest.
4. Setzen Sie die Abdeckung wieder auf und ziehen Sie die mit der Abdeckung verbundenen Schrauben mit einem Schraubendreher fest.

SIM-Karte / MicroSD-Karte entfernen

1. Stellen Sie sicher, dass der Router ausgeschaltet ist.
2. Um die Steckplatzabdeckung zu entfernen, lösen Sie die Schrauben der Abdeckung mit einem Schraubendreher und suchen Sie dann den SIM-Kartensteckplatz/ SD-Kartensteckplatz.
3. Um die SIM-Karte/ MicroSD-Karte zu entnehmen, drücken Sie die Karte mit Ihrem Finger, bis sie herausspringt, und nehmen Sie sie dann heraus.
4. Setzen Sie die Abdeckung wieder auf und ziehen Sie die mit der Abdeckung verbundenen Schrauben mit einem Schraubendreher fest.

Hinweis:

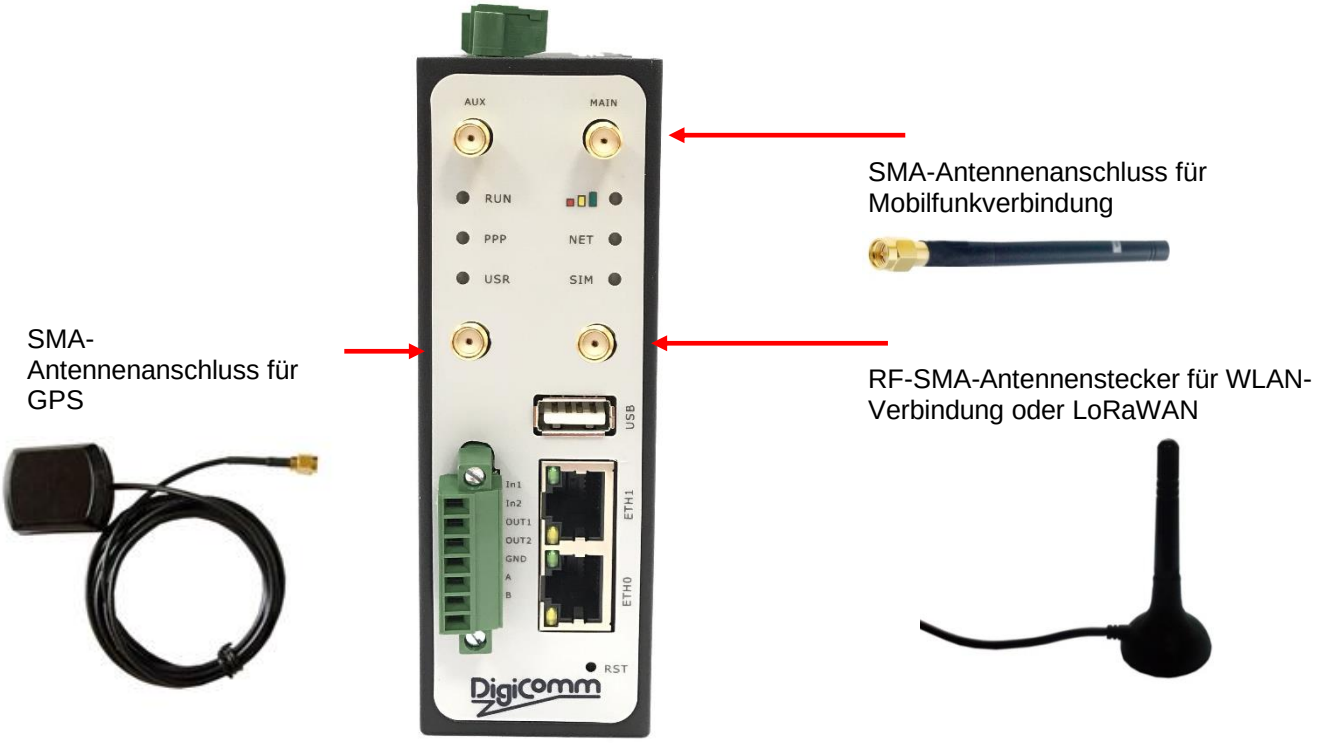
1. Das empfohlene Drehmoment für das Einsetzen beträgt 0,5 Nm, das maximal zulässige Drehmoment beträgt 0,7 Nm.

2. Verwenden Sie eine spezielle Karte, wenn das Gerät bei extremen Temperaturen eingesetzt wird (Temperatur über 40 °C), da es mit der regulären Karte bei Langzeitbetrieb in rauer Umgebung häufig zu Verbindungsabbrüchen kommen wird.
3. Vergessen Sie nicht, den Deckel fest zuzudrehen, damit er nicht gestohlen wird.
4. Berühren Sie nicht das Metall der Kartenoberfläche, da sonst Informationen auf der Karte verloren gehen oder zerstört werden können.
5. Verbiegen oder zerkratzen Sie die Karte nicht.
6. Halten Sie die Karte von Elektrizität und Magnetismus fern.
7. Vergewissern Sie sich, dass der Router ausgeschaltet ist, bevor Sie die Karte einsetzen oder entfernen.

2.7 Externe Antenne anbringen (SMA-Typ)

Bringen Sie die externe SMA-Antenne am Anschluss des Routers an und drehen Sie sie fest. Stellen Sie sicher, dass sich die Antenne im richtigen Frequenzbereich des ISP befindet und eine Impedanz von 50 Ohm aufweist.

Hinweis: Das empfohlene Anzugsdrehmoment beträgt 0,35 Nm.



2.8 Router montieren

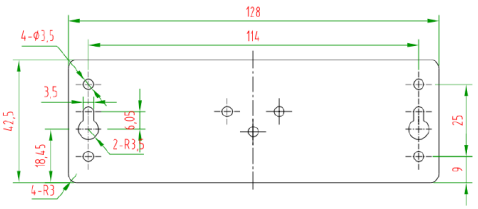
Der Router kann auf einen Schreibtisch gestellt oder an einer Wand mit einer 35-mm-Tragschiene montiert werden.

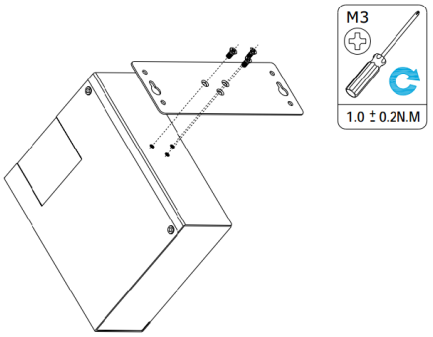
Hinweis:
Bei Verwendung benötigt das Gerät eine geeignete Umgebung.

1. Wenn der Router sich in Innenräumen befindet, muss er mit einem Gehäuse für Innenräume versehen werden.
2. Wenn der Router sich im Freien befindet, muss es mit einem wettergeeigneten Gehäuse versehen werden.

Es gibt zwei Methoden zur Montage des Routers:

1. Wandmontage (Maße in mm)

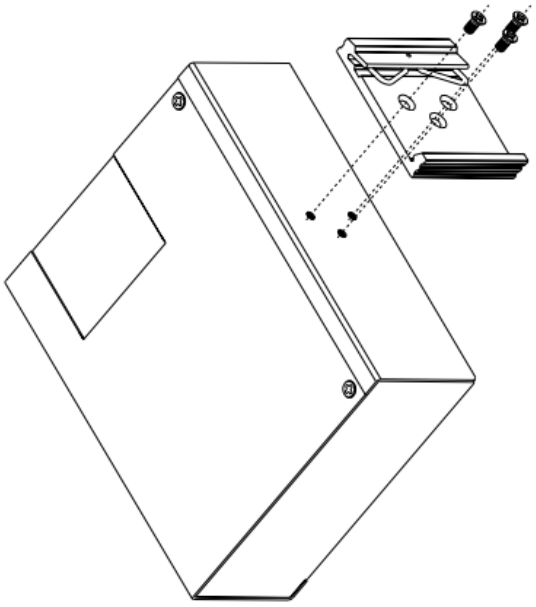


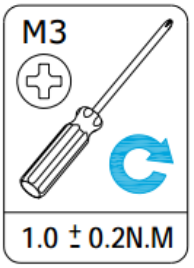


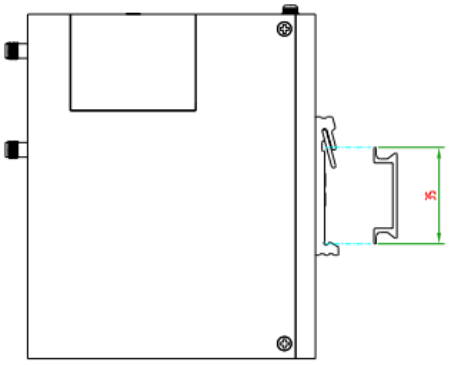
Verwenden Sie M3*4-Flachkopfschrauben (3 St.), um den Wandmontagesatz am Router zu befestigen, und verwenden Sie dann M3-Trockenbauschrauben (2 St.), um den Router samt Wandmontagesatz an der Wand zu befestigen.

Hinweis: Das empfohlene Drehmoment für die Montage beträgt 1,0 Nm, der maximal zulässige Drehmoment beträgt 1,2 Nm.

2. Hutschienenmontage (Maße in mm)







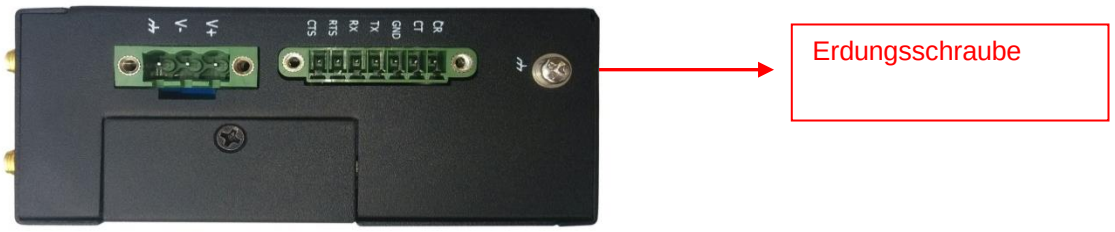
Verwenden Sie M3*6-Flachkopfschrauben (3 St.), um die Tragschiene am Router zu befestigen, und hängen Sie die Tragschiene dann an die Montagehalterung. Es ist notwendig, einen Standardbügel zu wählen.

Hinweis: Das empfohlene Drehmoment für die Montage beträgt 1,0 Nm, der maximal zulässige Drehmoment beträgt 1,2 Nm.

2.9 Router erden

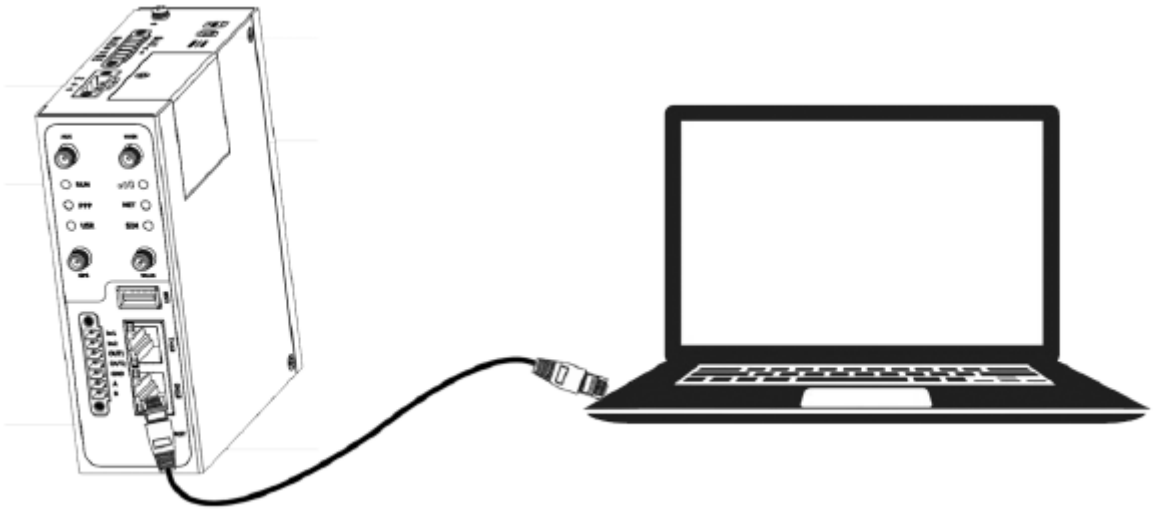
Das Erden des Routers hilft, den Rauscheffekt durch elektromagnetische Interferenz (EMI) zu verhindern. Verbinden Sie den Router vor dem Einschalten über die Erdungsschraube mit dem Erdungsleiter am Standort.

Hinweis: Dieses Produkt eignet sich für die Montage auf einer sicher geerdeten Geräteoberfläche, wie z.B. einer Metallplatte.

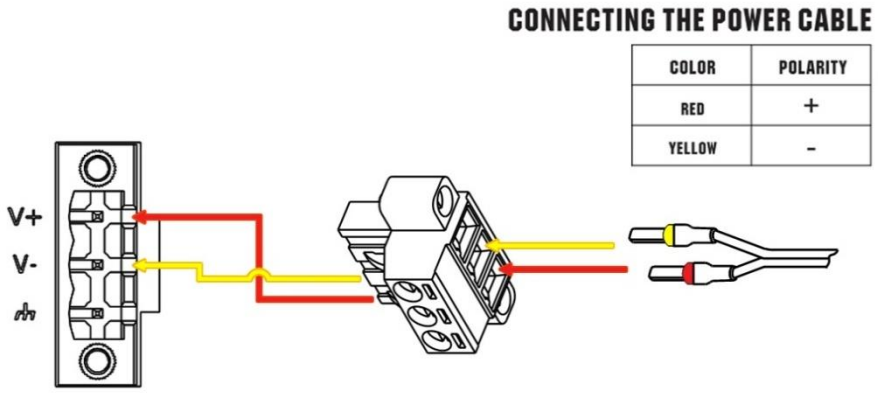


2.10 Router mit einem Computer verbinden

Schließen Sie ein Ethernet-Kabel an den mit ETH0 oder ETH1 gekennzeichneten Port an der Vorderseite des DSR-211-L Routers an und verbinden Sie das andere Ende des Kabels mit Ihrem Computer.



2.11 Stromversorgung



Der DSR-211 Router bietet einen Verpolungsschutz. Zum korrekten Anschluss des Netzteils ist aber stets die Abbildung oben zu beachten. Zum Netzteil gehören zwei Kabel. In Anlehnung an die Farbe des Kopfes schließen Sie das rot markierte Kabel über einen Klemmenblock an den Pluspol an und verbinden das gelbe Kabel auf die gleiche Weise mit dem Minuspol. Der letzte Schritt ist das Einstecken des Netzadapters in Ihre Steckdose.

Hinweis: Der Bereich der Versorgungsspannung beträgt 9 bis 60 V DC.

3. Erstkonfiguration

Der Router kann über Ihren Webbrowser konfiguriert werden, möglich sind IE 8.0 oder höher, Chrome und Firefox usw. Für die Konfiguration wird eine einfache und benutzerfreundliche Schnittstelle angeboten. Es gibt verschiedene Möglichkeiten, den Router anzuschließen, entweder über einen externen Repeater/ Hub oder direkt an Ihren PC. Stellen Sie jedoch sicher, dass auf Ihrem PC eine Ethernet-Schnittstelle ordnungsgemäß installiert ist, bevor Sie den Router anschließen. Sie müssen Ihren PC so konfigurieren, dass er eine IP-Adresse über einen DHCP-Server oder eine feste IP-Adresse erhält, die sich im gleichen Subnetz wie der Router befinden muss. Wenn Sie Probleme beim Zugriff auf die Webschnittstelle des Routers haben, ist es ratsam, Ihr Firewall-Programm auf Ihrem PC zu deaktivieren, da dies tendenziell zu Problemen beim Zugriff auf die IP-Adresse des Routers führt.

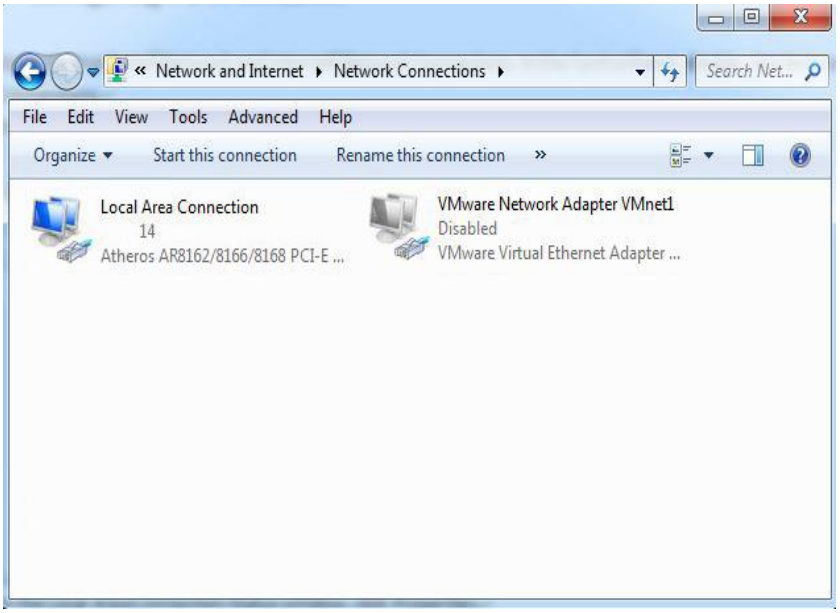
Hinweis: Vergessen Sie bitte nicht die Firewall nach Abschluss der Konfiguration wieder zu aktivieren.

3.1 Den PC konfigurieren

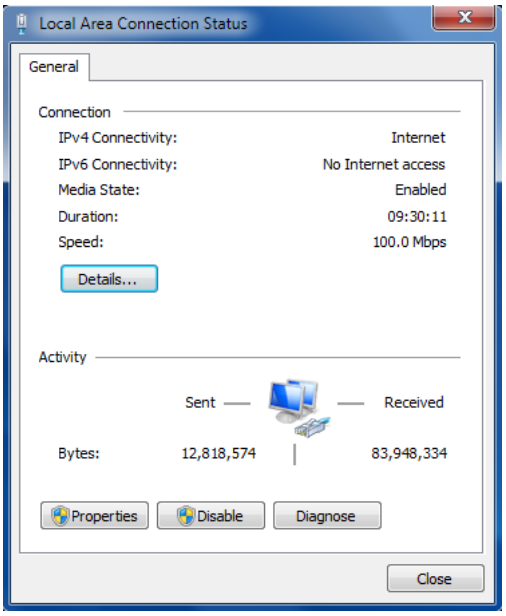
Es gibt zwei Methoden, um eine IP-Adresse für den PC zu erhalten. Eine besteht darin, eine IP-Adresse automatisch über die „Local Area Connection“ zu beziehen, und eine andere darin, eine statische IP-Adresse innerhalb desselben Subnetzes des Routers manuell zu konfigurieren. Bitte beachten Sie die folgenden Schritte.

Hier nehmen wir Windows 7 als Beispiel, die Konfiguration für andere Windows-Systeme ist ähnlich.

1. Klicken Sie auf Start > Systemsteuerung, Doppelklick auf Netzwerk- und Freigabecenter und dann auf LAN-Verbindung.

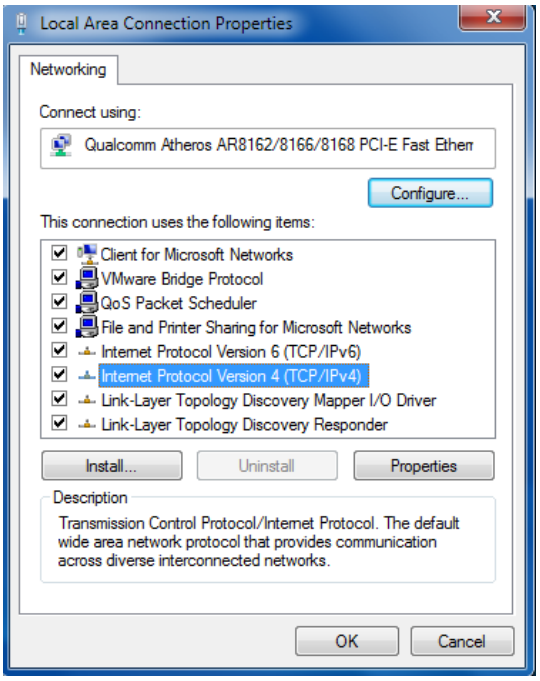


2. Klicken Sie im Fenster der LAN-Verbindung auf Eigenschaften.



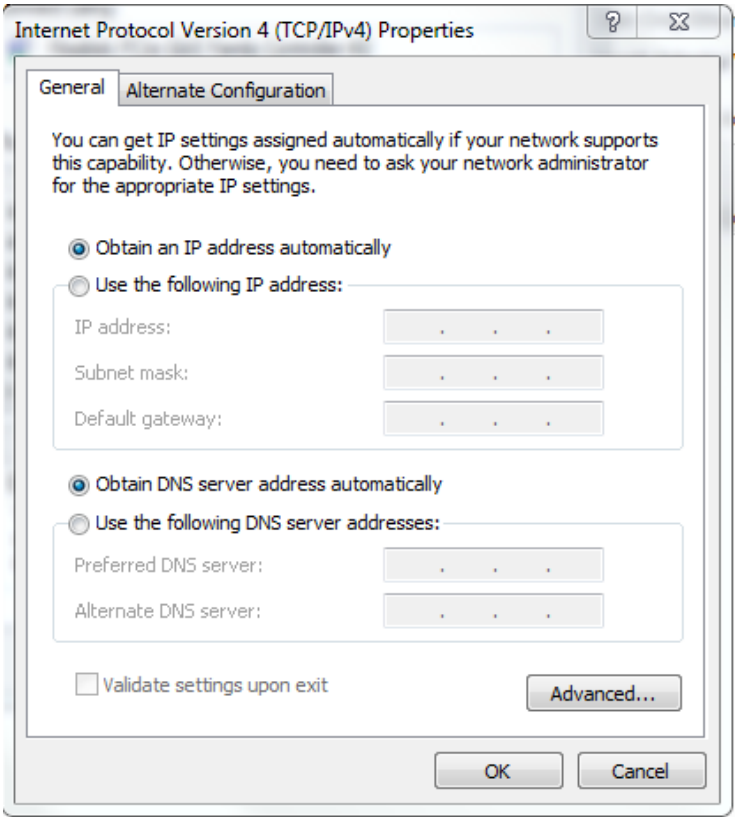
Nun haben Sie die Möglichkeit TCP/IPv4 oder TCP/IPv6 auszuwählen.

3. Wählen Sie Internet Protocol Version 4 (TCP/IPv4) und klicken Sie auf Eigenschaften.

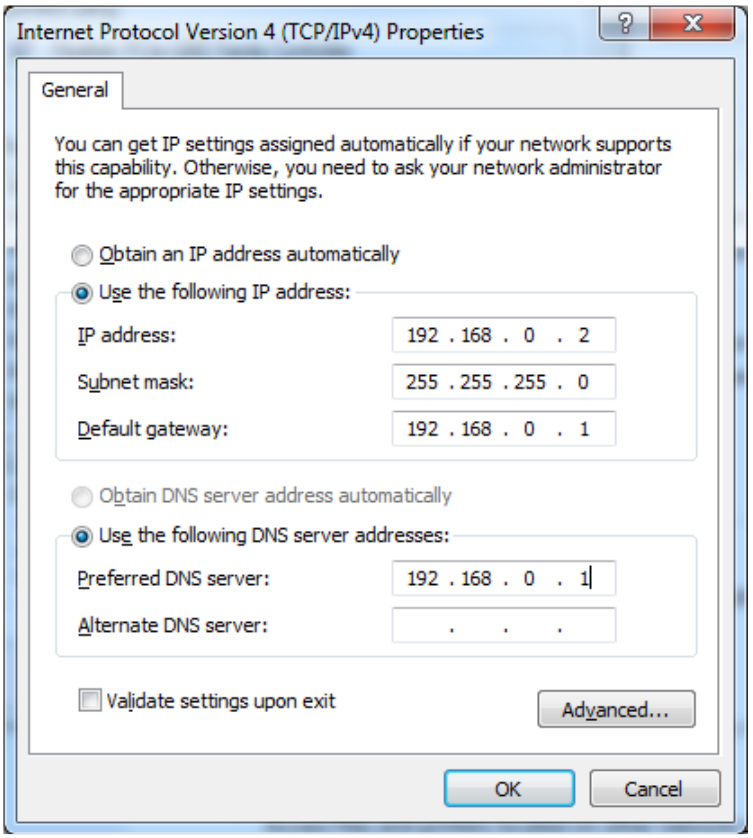


Es gibt zwei Möglichkeiten zur Konfiguration der IP-Adresse des PCs

Sie erhalten automatisch eine IP-Adresse:



Sie verwenden die folgende IP-Adresse:
(Manuelle Konfiguration einer statischen IP-Adresse innerhalb desselben Subnetzes des Routers)

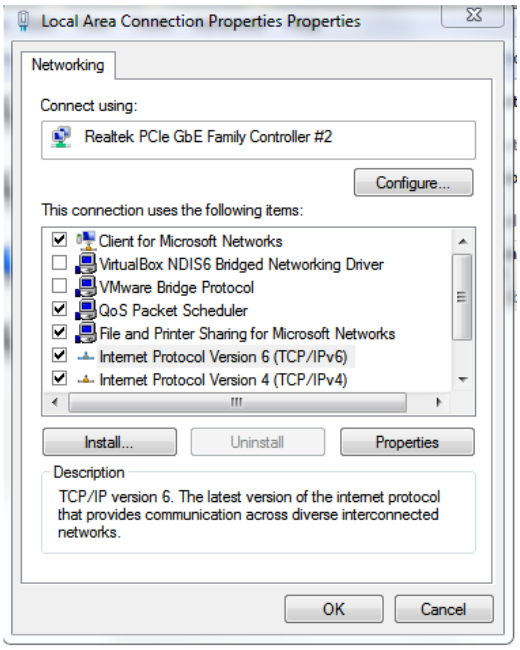


5. Klicken Sie auf OK, um die Konfiguration abzuschließen.

Wählen Sie TCP/IPv6 aus, gehen Sie bitte wie folgt vor:

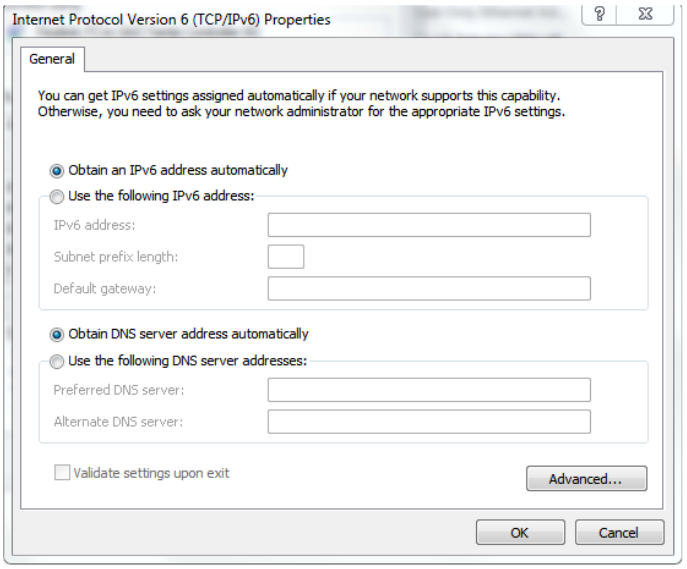
Hinweis: Für die Nutzung von IPv6 wird eine spezielle Firmware benötigt. Einige APP's funktionieren unter dieser Firmware nicht. Bitte sprechen Sie uns an, sollten Sie Hilfe benötigen.

1. Wählen Sie Internet Protocol Version 6 (TCP/IPv6) und klicken Sie auf Eigenschaften.

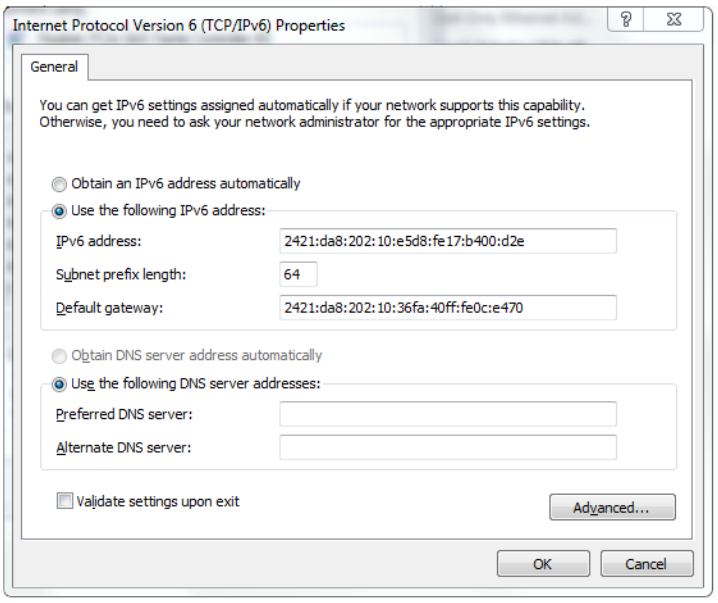


2. Es gibt zwei Möglichkeiten zur Konfiguration der IP-Adresse des PCs

Sie erhalten automatisch eine IP-Adresse:



3.Sie verwenden die folgende IP-Adresse:
(Manuelle Konfiguration einer statischen IP-Adresse innerhalb desselben Subnetzes des Routers)



4. Klicken Sie auf OK, um die Konfiguration abzuschließen.

3.2 Werkseitige Standardeinstellungen

Bevor Sie Ihren Router konfigurieren, müssen Sie die folgenden Standardeinstellungen kennen.

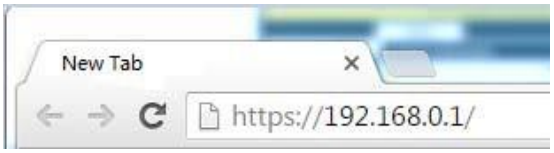
Punkt	Beschreibung
Username (Benutzername)	admin
Password (Passwort)	admin
Eth0	192.168.0.1/255.255.255.0, LAN-Modus
Eth1	
DHCP Server (DHCP-Server)	Aktiviert

3.3 Router Login

Um sich auf der Verwaltungsseite anzumelden und den Konfigurationsstatus Ihres Routers einzusehen, befolgen Sie bitte die folgenden Schritte.

1. Öffnen Sie auf Ihrem PC einen Webbrowser wie Internet Explorer, Chrome oder Firefox usw.
2. Geben Sie in Ihrem Webbrowser die IP-Adresse des Routers in die Adressleiste ein und drücken Sie die Eingabetaste.

Die Standard-IP-Adresse des DSR-211 Routers ist 192.168.0.1, die tatsächliche Adresse kann davon abweichen.

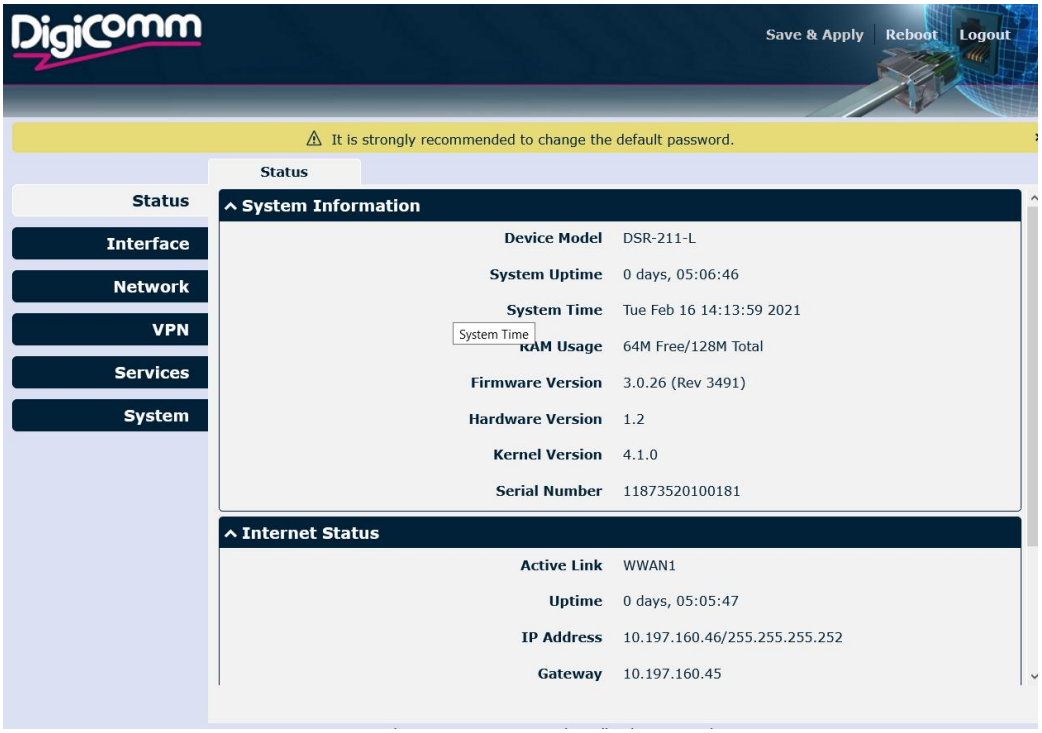


3. Geben Sie auf der Anmeldeseite den Benutzernamen und das Passwort ein, und klicken dann auf LOGIN (ANMELDUNG). Der Standardbenutzername und das Passwort lauten: „admin“.

Hinweis: Wenn Sie mehr als sechs Mal den falschen Benutzernamen oder das falsche Passwort eingeben, wird die Anmeldung für 5 Minuten gesperrt.

3.4 Konfiguration

Nach dem Anmelden wird z. B. die Startseite der Webschnittstelle des DSR-211 Routers angezeigt.



Von der Startseite aus können Sie Vorgänge wie das Speichern der Konfiguration, den Neustart des Routers und das Abmelden durchführen. Wenn Sie sich mit dem Original Passwort am Router anmelden, wird auf der Seite das folgende Popup angezeigt:

Klicken Sie auf  , um das Popup zu schließen. Es wird aus Sicherheitsgründen dringend empfohlen, den Standardbenutzernamen und/ oder das Standardpasswort zu ändern. Um Ihren Benutzernamen und/oder Ihr Passwort zu ändern, siehe 3.36 System > Benutzerverwaltung.

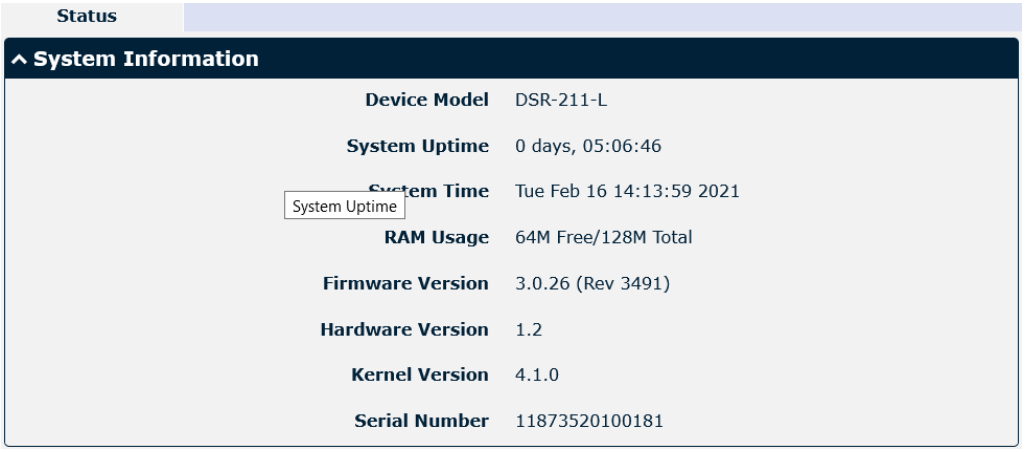
Konfiguration		
Punkt	Beschreibung	Schaltfläche
Save & Apply (Speichern & Übernehmen)	Klicken Sie darauf, um die aktuelle Konfiguration im Flashspeicher des Routers zu speichern und die Änderung auf jeder Konfigurationsseite anzuwenden, damit die Änderung wirksam wird.	
Reboot (Neustart)	Klicken Sie darauf, um den Router neu zu starten. Wenn die Schaltfläche Reboot gelb ist, bedeutet dies, dass einige abgeschlossene Konfigurationen erst nach einem Neustart wirksam werden.	
Logout (Abmeldung)	Klicken Sie darauf, um den aktuellen Benutzer sicher abzumelden. Nach dem Abmelden wechselt die Ansicht zur Login-Seite. Wird die Webseite direkt ohne Abmeldung geschlossen, kann der nächste Benutzer sich vor dem Timeout ohne Passwort mit diesem Browser einloggen.	
Submit (Übernehmen)	Klicken Sie darauf, um die Änderung auf der aktuellen Konfigurationsseite zu speichern.	
Cancel (Abbrechen)	Klicken Sie darauf, um die Änderung auf der aktuellen Konfigurationsseite zu verwerfen.	

Hinweis: Die Schritte zur Änderung der Konfiguration sind nachstehend aufgeführt:

1. Sie nehmen Änderungen auf der Seite vor;
2. Sie klicken unten auf dieser Seite auf Submit (Übermitteln);
3. Sie nehmen Änderungen auf einer anderen Seite vor;
4. Sie klicken unten auf dieser Seite auf Submit (Übermitteln);
5. Sie schließen alle Änderungen ab;
6. Sie klicken auf Save & Apply (Speichern & Übernehmen).

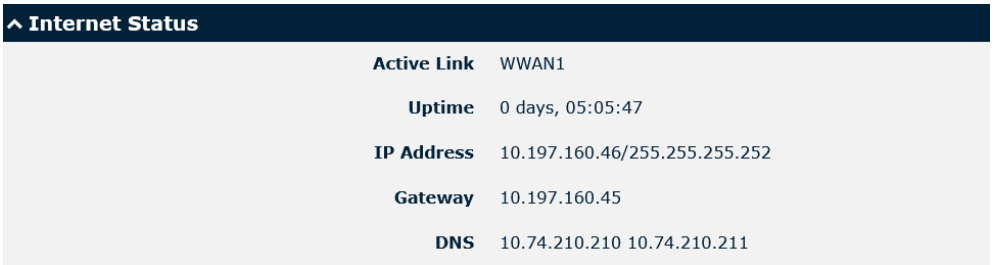
3.5 Status

Auf dieser Seite können Sie die Systeminformationen, den Internet-Status und den LAN-Status Ihres Routers einsehen.



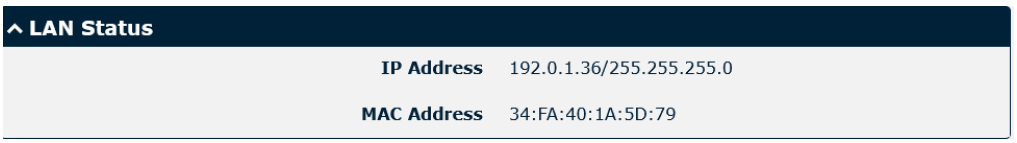
System Information	
Punkt	Beschreibung
Device Model (Gerätemodell)	Zeigt den Modellnamen Ihres Gerätes an
System Uptime (Systemverfügbarkeit)	Zeigt die aktuelle Verbindungsdauer des Routers an
System Time (Systemzeit)	Zeigt die aktuelle Systemzeit an
RAM Usage (RAM-Nutzung)	Zeigt die aktuelle RAM-Nutzung und den Gesamtspeicher an
Firmware Version	Zeigt die auf dem Router laufende Firmware-Version an
Hardware Version	Zeigt die aktuelle Hardware-Version an
Kernel Version	Zeigt die aktuelle Kernel-Version an
Serial Number (Seriennummer)	Zeigt die Seriennummer Ihres Gerätes an

Internet Status



Internet Status	
Punkt	Beschreibung
Uptime (Verfügbarkeit)	Zeigt die aktuelle Zeit an, in der der Link verbunden war.
IPv4 Link Description (IPv4-Link-Beschreibung)	Zeigt den aktuellen Online-Link an: WWAN1, WWAN2, WAN oder WLAN.
IPv4 Address (IPv4-Adresse)	Zeigt die IPv4-Adresse des aktuellen Links an.
IPv4 Gateway (IPv4-Gateway)	Zeigt das IPv4-Gateway des aktuellen Links an.
IPv4 DNS (IPv4-DNS)	Zeigt den aktuellen IPv4-DNS-Server an.
IPv6 Link Description (IPv6-Link-Beschreibung)	Zeigt den aktuellen Online-Link an: WWAN1, WWAN2, WAN oder WLAN.
IPv6 Address (IPv6-Adresse)	Zeigt die IPv6-Adresse des aktuellen Links an.
IPv6 Gateway	Zeigt das IPv6-Gateway des aktuellen Links an.
IPv6 DNS (IPv6-DNS)	Zeigt den aktuellen IPv6-DNS-Server an.

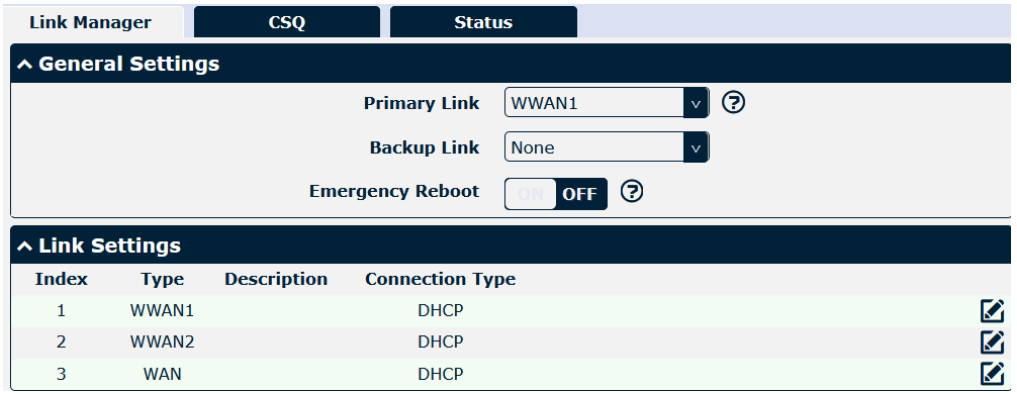
LAN Status



LAN Status	
Punkt	Beschreibung
IP Address (IP-Adresse)	Zeigt die IPv4-Adresse und die Netzmaske des Routers an.
IPv6 Address (IPv6-Adresse)	Zeigt die vom Router erhaltene IPv6-Adresse und Präfixlänge zusammen mit dem aktuellen Backup-Link an.
Inactive IPv6 Address (Inaktive IPv6-Adresse)	Zeigt die vom Router erhaltene IPv6-Adresse und Präfixlänge zusammen mit dem aktuellen Online-Link an.
MAC Address (MAC-Adresse)	Zeigt die MAC-Adresse des Routers an.

3.6 Schnittstelle > Link-Manager

In diesem Abschnitt können Sie die Link-Verbindung einrichten.

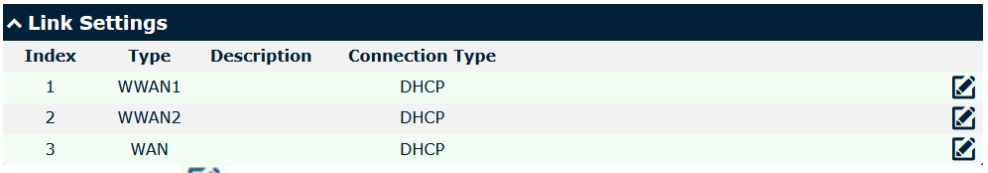


General Settings @ Link Manager (Allgemeine Einstellungen @ Link Manager)		
Punkt	Beschreibung	Standard
Primary Link (Primärer Link)	Wählen Sie aus „WWAN1“, „WWAN2“, „WAN“ oder „WLAN“. WWAN1: Wählen Sie diese Option, um SIM1 als primären drahtlosen Link festzulegen. WWAN2: Wählen Sie diese Option, um SIM2 als primären drahtlosen Link festzulegen. WAN: Wählen Sie diese Option, um den WAN-Ethernet-Port als primären verkabelten Link festzulegen Hinweis: WAN-Link ist nur verfügbar, wenn eth0 als WAN-Port unter Interface (Schnittstelle) > Ethernet (Ethernet) > Ports (Anschlüsse) > Port Settings (Anschlusseinstellungen) aktiviert ist. WLAN: Wählen Sie diese Option, um WLAN als primären drahtlosen Link festzulegen. Hinweis: Der WLAN-Link ist nur verfügbar, wenn Wi-Fi als Client-Modus aktiviert ist, siehe 3.10 Schnittstelle > Wi-Fi.	WWAN1
Backup Link (Backup-Link)	Wählen Sie aus „None (Kein)“, „WWAN1“, „WWAN2“, „WAN“ oder „WLAN“. None: Kein Backup-Link ist ausgewählt WWAN1: Wählen Sie diese Option, um SIM1 als drahtlosen Backup-Link festzulegen. WWAN2: Wählen Sie diese Option, um SIM2 als drahtlosen Backup-Link festzulegen. WAN: Wählen Sie diese Option, um einen WAN-Ethernet-Port als kabelgebundenen Backup-Link einzurichten Hinweis: Der WAN-Link ist nur verfügbar, wenn eth0 als WAN-Schnittstelle unter Interface (Schnittstelle) > Ethernet (Ethernet) > Ports (Anschlüsse) > Port Settings (Anschlusseinstellungen) aktiviert ist. WLAN: Wählen Sie diese Option, um WLAN als drahtlosen Backup-Link festzulegen. Hinweis: Der WLAN-Link ist nur verfügbar, wenn Wi-Fi als Client-Modus aktiviert ist, siehe 3.10 Schnittstelle > Wi-Fi.	WWAN2

Backup Mode (Backup-Modus)	Wählen Sie aus „Cold Backup“, „Warm Backup“ oder „Load Balancing“. Cold Backup: Der inaktive Link ist im Standby-Modus offline. Warm Backup: Der inaktive Link ist im Standby-Modus online. Load Balancing: Zwei Links werden gleichzeitig verwendet. Hinweis: Der Warm-Backup-Modus ist für doppeltes SIM-Backup nicht verfügbar.	Cold Backup
Revert Interval (Rückkehrintervall)	Geben Sie die Anzahl der Minuten an, die vergehen, bis der primäre Link geprüft wird, wenn ein Backup-Link im Cold-Backup-Modus verwendet wird. 0 bedeutet Prüfung deaktivieren. Hinweis: Das Rückkehrintervall ist nur im Cold-Backup-Modus verfügbar.	0
Emergency Reboot (Notfall-Neustart)	Aktiveren Sie diese Option, um den Neustart des gesamten Systems zu ermöglichen, wenn keine Links verfügbar sind.	OFF (AUS)

Hinweis: Klicken Sie auf das Fragezeichen und Sie erhalten Hilfe.

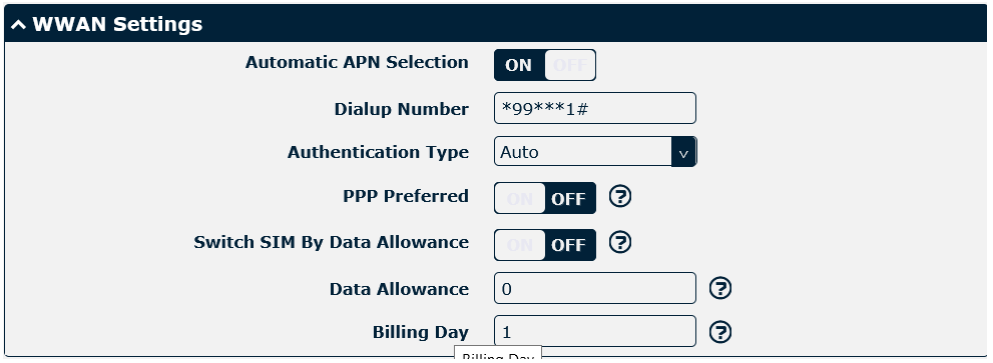
Mit Link Settings (Link-Einstellungen) können Sie die Parameter der Link-Verbindung konfigurieren, einschließlich WWAN1/ WWAN2, WAN und WLAN. Es wird empfohlen, die Ping-Erkennung zu aktivieren, um den Router immer online zu halten. Die Ping-Erkennung erhöht die Zuverlässigkeit, verbraucht jedoch auch Datenverkehr.



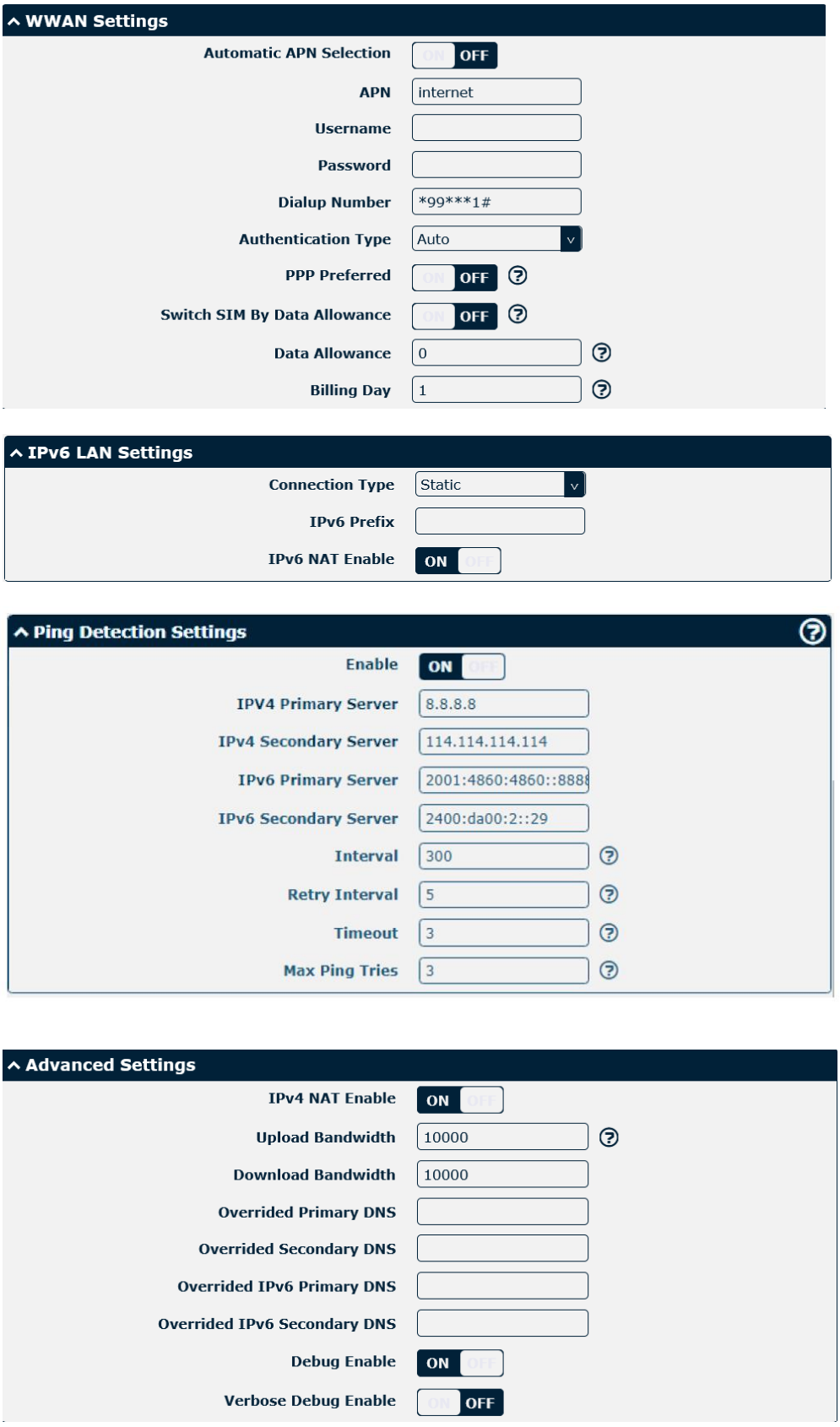
Klicken Sie auf auf der rechten Seite, um in das Konfigurationsfenster zu gelangen.

WWAN1/ WWAN2

Bei Aktivierung der Option „Automatic APN Selection“(Automatische APN-Auswahl) wird das Fenster wie unten dargestellt.



Das Fenster wird wie unten dargestellt, wenn die Option „Automatic APN Selection“ (Automatische APN-Auswahl) deaktiviert wird.


WWAN Settings
Automatic APN Selection
OFF
APN
internet
Username
Password
Dialup Number
*99***1#
Authentication Type
Auto
PPP Preferred
OFF
Switch SIM By Data Allowance
OFF
Data Allowance
0
Billing Day
1
IPv6 LAN Settings
Connection Type
Static
IPv6 Prefix
IPv6 NAT Enable
ON
Ping Detection Settings
Enable
ON
IPV4 Primary Server
8.8.8.8
IPv4 Secondary Server
114.114.114.114
IPv6 Primary Server
2001:4860:4860::8888
IPv6 Secondary Server
2400:da00:2::29
Interval
300
Retry Interval
5
Timeout
3
Max Ping Tries
3
Advanced Settings
IPv4 NAT Enable
ON
Upload Bandwidth
10000
Download Bandwidth
10000
Overrided Primary DNS
Overrided Secondary DNS
Overrided IPv6 Primary DNS
Overrided IPv6 Secondary DNS
Debug Enable
ON
Verbose Debug Enable
OFF

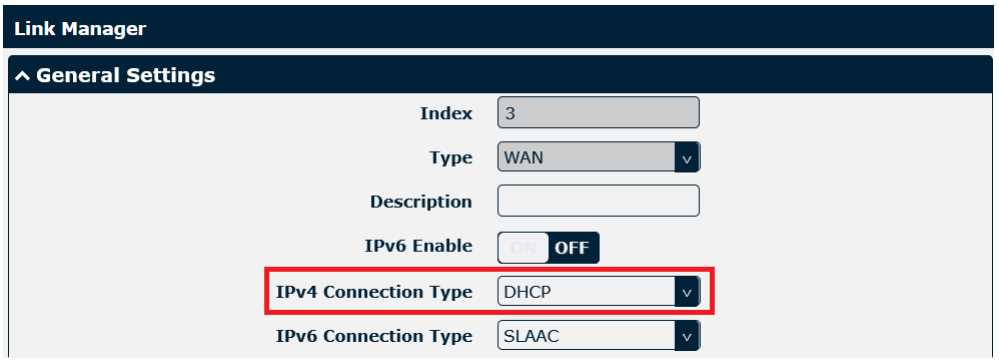
Link Settings (WWAN) (Link-Einstellungen (WWAN)		
Punkt	Beschreibung	Standard
General Settings (Allgemeine Einstellungen)		
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Type (Typ)	Zeigt den Typ des Links an.	WWAN1
Description (Beschreibung)	Sie können eine Beschreibung für diesen Link eingeben.	Null
IPv6	Klicken Sie auf den Schalter, um IPv6 zu aktivieren/deaktivieren.	OFF (AUS)
WWAN Settings (WWAN-Einstellungen)		
Automatic APN Selection (Automatische APN-Auswahl)	Klicken Sie auf den Schalter, um die Option „Automatic APN Selection“(Automatische APN-Auswahl) zu aktivieren/ deaktivieren. Nach der Aktivierung erkennt das Gerät den Namen des Zugangspunktes automatisch. Alternativ können Sie diese Option deaktivieren und den Namen des Zugangspunktes manuell hinzufügen.	ON (EIN)
APN	Geben Sie den Zugangspunktnamen für die Mobilfunk-Einwahlverbindung ein, der vom lokalen ISP bereitgestellt wird.	internet
Username (Benutzername)	Geben Sie den Benutzernamen für die Mobilfunk-Einwahlverbindung ein, der vom lokalen ISP bereitgestellt wird.	Null
Password (Passwort)	Geben Sie das Passwort für die Mobilfunk-Einwahlverbindung ein, das vom lokalen ISP bereitgestellt wird.	Null
Einwahlnummer	Geben Sie die Einwahlnummer für die Mobilfunkverbindung ein, die vom lokalen ISP bereitgestellt wird.	Telefonnummer
Authentication Type (Authentifizierungs-Typ)	Wählen Sie aus „Auto“, „PAP“ oder „CHAP“ entsprechend den Anforderungen des lokalen ISP.	Auto
PPP Preferred (PPP bevorzugt)	Die PPP-Einwahlmethode wird bevorzugt.	OFF (AUS)
Switch SIM By Data Allowance (SIM Karte Wechsel wenn Datenvolumen verbraucht)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Nach der Aktivierung wird auf eine andere SIM-Karte gewechselt, wenn das Datenlimit erreicht ist. Hinweis: Wird nur für Dual-SIM-Backup verwendet.	OFF (AUS)
Data Allowance (Datenvolumen)	Legt die monatliche Begrenzung des Datenvolumens fest. Das System prüft wie viel Datenvolumen verbraucht wurde, wenn Sie einen Wert eingeben. Unter Interface (Schnittstelle) > Link Manager > Status > WWAN Data Usage Statistic) können Sie den Wert eintragen. 0 bedeutet, dass die Aufzeichnung des Datenvolumens deaktiviert ist.	0
Billing Day (Abrechnungstag)	Geben Sie den monatlichen Abrechnungstag an. Die Datenverkehrsstatistik wird ab diesem Tag neu berechnet.	1

IPv6 LAN Settings (IPv6-LAN-Einstellungen)		
Link Settings (WWAN) (Link-Einstellungen (WWAN)		
Connection Type (Verbindungstyp)	Wählen Sie den Link, um dem lokalen Netzwerk ein IPv6-Präfix zuzuweisen.	Delegated (delegiert)
IPv6 prefix (IPv6-Präfix)	Legen Sie das statische IPv6-Präfix fest, das durch den Link zum LAN zugewiesen wird.	null
Enable IPv6 NAT (IPv6-NAT aktivieren)	Stellen Sie den Link ein, um IPv6-NAT zu aktivieren.	OFF (AUS)
Ping Detection Settings (Ping-Erkennungs-Einstellungen)		
Enable (Aktivieren)	Klicken Sie auf den Schalter, um den Ping-Erkennungsmechanismus, eine Keep-Alive-Richtlinie des DSR-200 Routers, zu aktivieren/deaktivieren.	ON (EIN)
IPv4 Primary Server (Primärer IPv4-Server)	Der Router sendet einen Ping an diese primäre Adresse / diesen Domänennamen, um zu prüfen, ob die aktuelle IPv4-Konnektivität aktiv ist.	8.8.8.8
IPv4 Secondary Server (Sekundärer IPv4-Server)	Der Router sendet einen Ping an diese sekundäre Adresse / diesen Domänennamen, um zu prüfen, ob die aktuelle Konnektivität aktiv ist.	114.114.114.114
IPv6 Primary Server (Primärer IPv6-Server)	Der Router sendet einen Ping an diese primäre Adresse / diesen Domänennamen, um zu prüfen, ob die aktuelle IPv6-Konnektivität aktiv ist.	2001:4860:4860::8888
IPv6 Secondary Server (Sekundärer IPv6-Server)	Der Router sendet einen Ping an diese sekundäre Adresse / diesen Domänennamen, um zu prüfen, ob die aktuelle IPv6-Konnektivität aktiv ist.	2400:da00:2::29
Interval (Intervall)	Legen Sie das Ping-Intervall fest.	300
Retry Interval (Wiederholungs-Intervall)	Legen Sie das Ping-Wiederholungsintervall fest. Wenn der Ping fehlgeschlagen ist, pingt der Router in jedem Wiederholungsintervall erneut.	5
Timeout (Zeitüberschreitung)	Legen Sie die Ping-Zeitüberschreitung fest.	3
Max Ping Tries (Max. Ping-Versuche)	Legen Sie die maximalen Ping-Versuche fest. Wenn die maximale kontinuierliche Anzahl der Ping-Versuche erreicht ist, wird zu einem anderen Link gewechselt oder Notfallmaßnahmen werden ergriffen.	3
Advanced Settings (Erweiterte Einstellungen)		
NAT Enable (NAT aktivieren)	Klicken Sie auf den Schalter, um die Option Network Address Translation zu aktivieren/ deaktivieren.	ON (EIN)
Upload Bandwidth (Upload-Bandbreite)	Legen Sie die für QoS verwendete Upload-Bandbreite, gemessen in kbit/s, fest.	10000
Download Bandwidth (Download-Bandbreite)	Legen Sie die für QoS verwendete Download-Bandbreite, gemessen in kbit/s, fest.	10000
Specify the Primary DNS server (Primären DNS-Server spezifizieren)	Definiert den primären IPv4-DNS-Server, der von dem Link verwendet wird.	Null

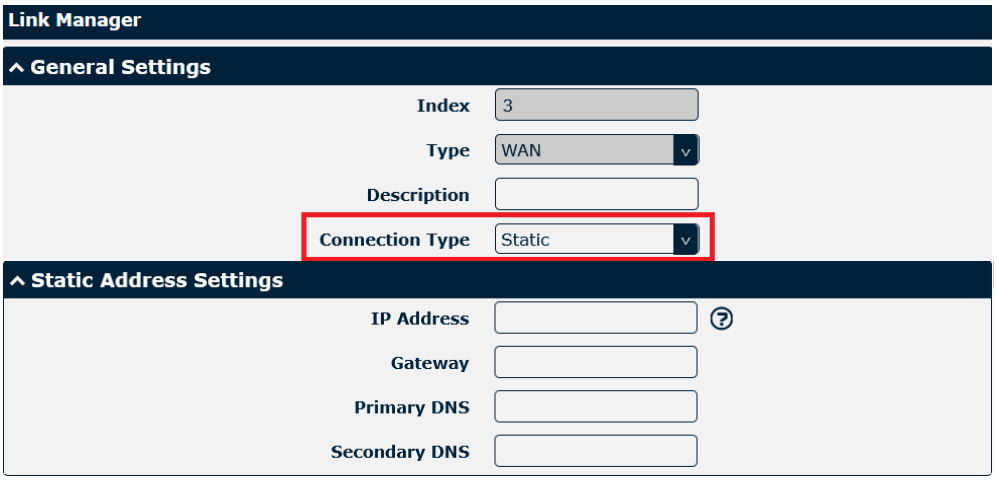
Specify the Secondary DNS server (Sekundären DNS-Server spezifizieren)	Definiert den sekundären IPv4-DNS-Server, der von Link verwendet wird.	Null
Specify the IPv6 Primary DNS server (Primären IPv6-DNS-Server spezifizieren)	Definiert den primären IPv6-DNS-Server, der von dem Link verwendet wird.	Null
Specify the IPv6 Secondary DNS server (Sekundären IPv6-DNS-Server spezifizieren	Definiert den sekundären IPv6-DNS-Server, der von Link verwendet wird.	Null
Debug Enable (Debugging aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option für die Ausgabe von Debugging-Informationen.	ON (EIN)
Verbose Debug Enable (Ausführliches Debugging aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option für die Ausgabe von ausführlichen Debugging-Informationen.	OFF (AUS)

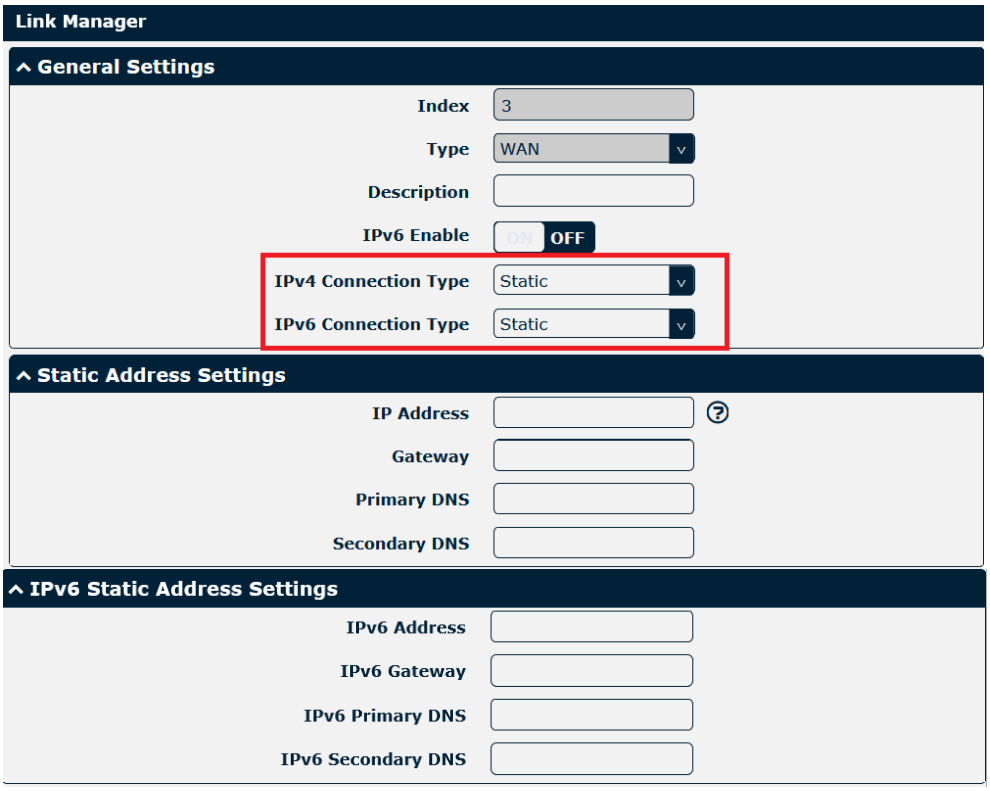
WAN

Der Router erhält die IP automatisch vom DHCP-Server, wenn „DHCP“ als IPv4-Verbindungstyp gewählt wird. Der Router erhält das IPv6-Präfix automatisch vom DHCP-Server, wenn als IPv6-Verbindungstyp „SLAAC“ gewählt wird. Das Fenster wird wie unten dargestellt angezeigt.

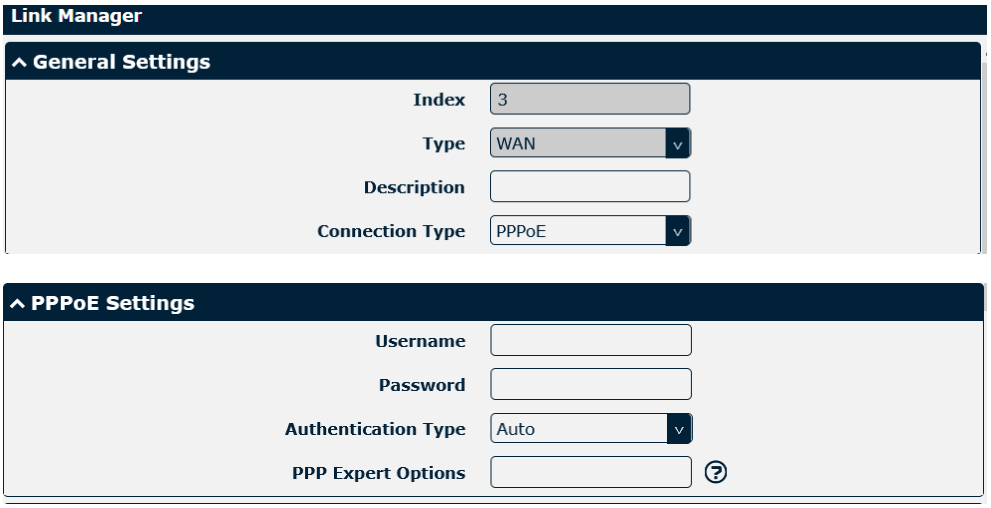


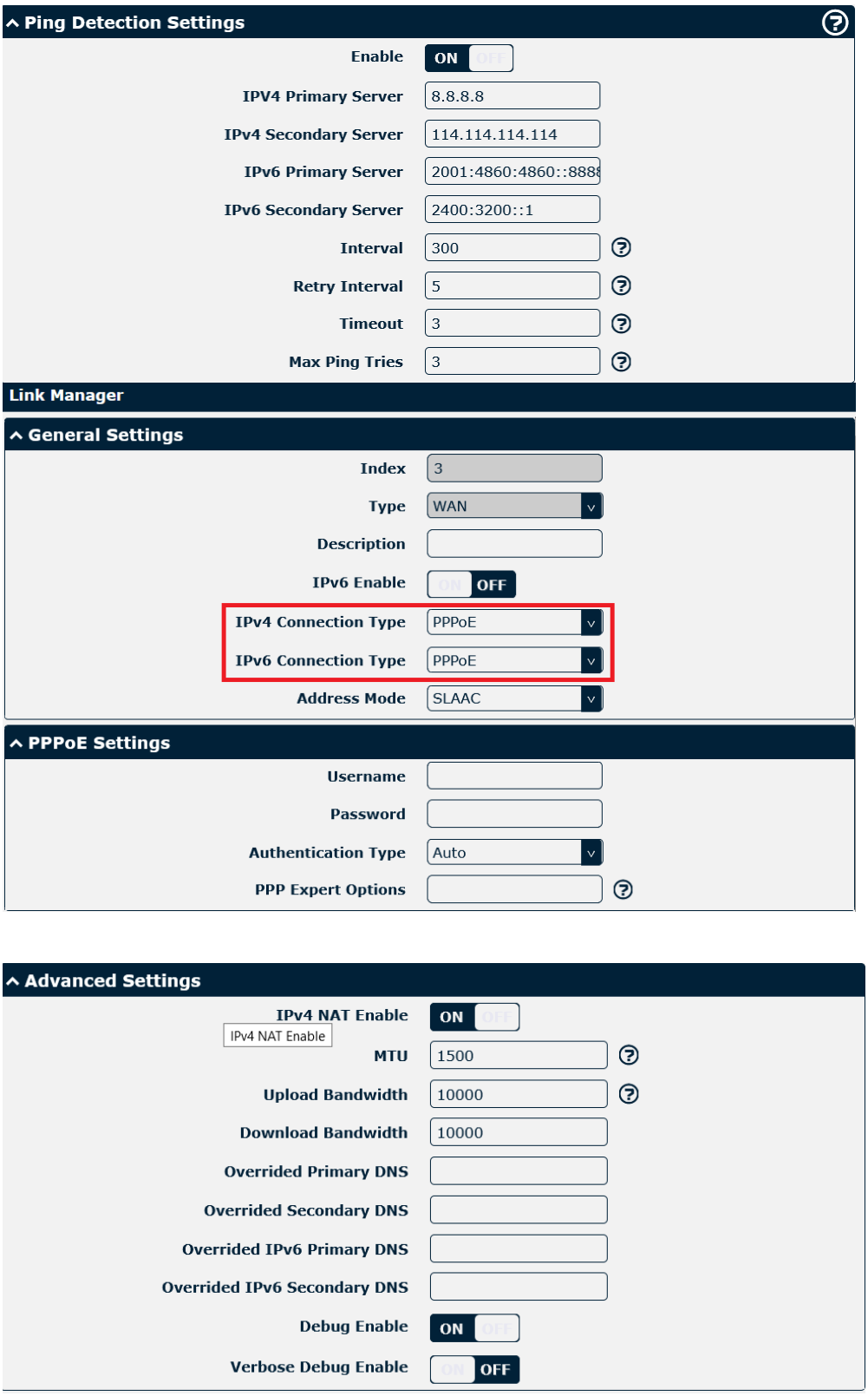
Wenn Sie „Static“ („Statisch“) als IPv4- und IPv6-Verbindungstyp wählen, wird das Fenster wie unten dargestellt.





Wenn Sie „PPPoE“ als IPv4- und IPv6-Verbindungstyp wählen, wird das Fenster wie unten dargestellt.




Ping Detection Settings
Enable
ON
OFF
IPV4 Primary Server
8.8.8.8
IPv4 Secondary Server
114.114.114.114
IPv6 Primary Server
2001:4860:4860::8888
IPv6 Secondary Server
2400:3200::1
Interval
300
Retry Interval
5
Timeout
3
Max Ping Tries
3
Link Manager
General Settings
Index
3
Type
WAN
Description
IPv6 Enable
ON
OFF
IPv4 Connection Type
PPPoE
IPv6 Connection Type
PPPoE
Address Mode
SLAAC
PPPoE Settings
Username
Password
Authentication Type
Auto
PPP Expert Options

Advanced Settings
IPv4 NAT Enable
ON
OFF
IPv4 NAT Enable
MTU
1500
Upload Bandwidth
10000
Download Bandwidth
10000
Overrided Primary DNS
Overrided Secondary DNS
Overrided IPv6 Primary DNS
Overrided IPv6 Secondary DNS
Debug Enable
ON
OFF
Verbose Debug Enable
ON
OFF

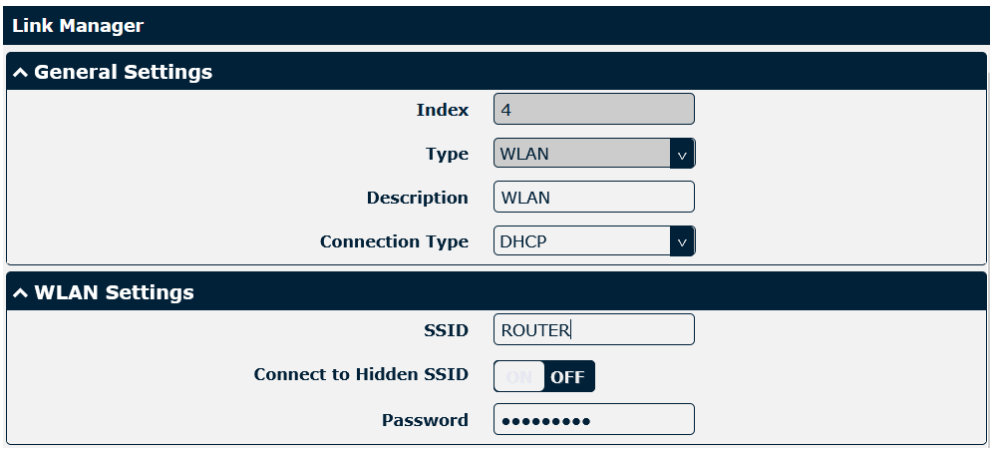
Link Settings (WAN) (Link-Einstellungen (WAN)		
Punkt	Beschreibung	Standard
General Settings (Allgemeine Einstellungen)		
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Type (Typ)	Zeigt den Typ des Links an.	WAN
Description (Beschreibung)	Sie können eine Beschreibung für diesen Link eingeben.	Null
Enable IPv6 (IPv6 aktivieren)	Klicken Sie auf den Schalter, um IPv6 zu aktivieren/ deaktivieren.	OFF (AUS)
IPv4 connection type (IPv4-Verbindungstyp)	Wählen Sie aus „DHCP“, „Static IP“ („Statische IP“) oder „PPPoE“.	DHCP
IPv6 connection type (IPv6-Verbindungstyp)	Wählen Sie aus „SLAAC“, „DHCPv6“, „Static IP“ („Statische IP“) oder „PPPoE“.	SLAAC
Address type (Adresstyp)	Wählen Sie aus „SLAAC“ oder „DHCPv6“.	SLAAC
IPv4 Static Address Settings (Einstellungen für statische IPv4-Adressen)		
IP Address (IP-Adresse)	Stellen Sie die IP-Adresse mit Netzmaske ein, die auf das Internet zugreifen kann. IP-Adresse mit Netzmaske, z. B. 192.168.1.1/ 24	Null
Gateway (Gateway)	Stellen Sie das Gateway der IPv4-Adresse im WAN-Port ein.	Null
Primary DNS (Primäres DNS)	Legen Sie das primäre DNS fest.	Null
Secondary DNS (Sekundäres DNS)	Legen Sie das sekundäre DNS fest.	Null
IPv6 Static Address Settings (Einstellungen für statische IPv6-Adressen)		
IPv6 Address (IPv6-Adresse)	Stellen Sie die IPv6-Adresse mit Netzmaske ein, die auf das Internet zugreifen kann. IP-Adresse mit Netzmaske, z. B. 2521:da8:202:10::20/64	Null
Gateway (Gateway)	Stellen Sie das Gateway der IPv6-Adresse im WAN-Port ein.	Null
IPv6 Primary DNS (Primäres IPv6-DNS)	Legen Sie den primären IPv6-DNS-Server fest, der von dem Link verwendet wird.	Null
IPv6 Secondary DNS (Sekundäres IPv6-DNS)	Legen Sie den sekundären IPv6-DNS-Server fest, der von dem Link verwendet wird.	Null
PPPoE Settings (PPPoE-Einstellungen)		
Username (Benutzername)	Geben Sie den von Ihrem Internet Service Provider bereitgestellten Benutzernamen ein.	Null
Password (Passwort)	Geben Sie das von Ihrem Internet Service Provider bereitgestellte Passwort ein.	Null
Authentication Type (Authentifizierungs-	Wählen Sie aus „Auto“, „PAP“ oder „CHAP“ entsprechend den Anforderungen des lokalen ISP.	Auto
PPP Expert Options (PPP-Expertenoptionen)	Geben Sie die PPP-Expertenoptionen ein, die für die PPPoE-Einwahl verwendet werden. Sie können einige andere PPP-Wählzeichenfolgen in dieses Feld eingeben. Jede Zeichenfolge kann durch ein Semikolon getrennt werden.	Null

IPv6 LAN Settings (IPv6-LAN-Einstellungen)		
Connection type (Verbindungstyp)	Wählen Sie den Link, um dem LAN IPv6-Präfixe zuzuweisen.	Delegated (delegiert)
IPv6 Prefix (IPv6-Präfix)	Setzt das statische IPv6-Präfix, das durch den Link zum LAN zugewiesen wird.	Null
Enabled IPv6 NAT (Aktiviertes IPv6-NAT)	Richten Sie Links ein, um IPv6-NAT zu aktivieren.	OFF (AUS)
Ping Detection Settings (Ping-Erkennungs-Einstellungen)		
Enable (Aktivieren)	Klicken Sie auf den Schalter, um den Ping-Erkennungsmechanismus, eine Keep-Alive-Richtlinie des DSR-211 Routers, zu aktivieren/ deaktivieren.	ON (EIN)
Primary Server (Primärer Server)	Der Router sendet einen Ping an diese primäre Adresse / diesen Domänennamen, um zu prüfen, ob die aktuelle IPv4-Konnektivität aktiv ist.	8.8.8.8
Secondary Server (Sekundärer Server)	Der Router sendet einen Ping an diese sekundäre Adresse / diesen Domänennamen, um zu prüfen, ob die aktuelle IPv4-Konnektivität aktiv ist.	114.114.114.114
IPv6 Primary Server (Primärer IPv6-Server)	Der Router sendet einen Ping an diese primäre Adresse / diesen Domänennamen, um zu prüfen, ob die aktuelle IPv6-Konnektivität aktiv ist.	2001:4860:4860::8888
IPv6 Secondary Server (Sekundärer IPv6-Server)	Der Router sendet einen Ping an diese sekundäre Adresse / diesen Domänennamen, um zu prüfen, ob die aktuelle IPv6-Konnektivität aktiv ist.	2400:da00:2::29
Interval (Intervall)	Legen Sie das Ping-Intervall fest.	300
Retry Interval (Wiederholungs-Intervall)	Legen Sie das Ping-Wiederholungsintervall fest. Wenn der Ping fehlgeschlagen ist, pingt der Router in jedem Wiederholungsintervall erneut.	5
Timeout (Zeitüberschreitung)	Legen Sie die Ping-Zeitüberschreitung fest.	3
Max Ping Tries (Max. Ping-Versuche)	Legen Sie die maximalen Ping-Versuche fest. Wenn die maximale kontinuierliche Anzahl der Ping-Versuche erreicht ist, wird zu einem anderen Link gewechselt oder Notfallmaßnahmen werden ergriffen.	3
Advanced Settings (Erweiterte Einstellungen)		
NAT Enable (NAT aktivieren)	Klicken Sie auf den Schalter, um die Option Network Address Translation zu aktivieren/deaktivieren.	ON (EIN)
MTU (MÜE)	Geben Sie die maximale Übertragungseinheit ein.	1500
Upload Bandwidth (Upload-Bandbreite)	Geben Sie die für QoS verwendete Upload-Bandbreite, gemessen in kbit/s, ein.	10000
Download Bandwidth (Download-Bandbreite)	Geben Sie die für QoS verwendete Download-Bandbreite, gemessen in kbit/s, ein.	10000
Specify the Primary DNS server (Primären DNS-Server spezifizieren)	Definiert den primären IPv4-DNS-Server für den Link.	Null

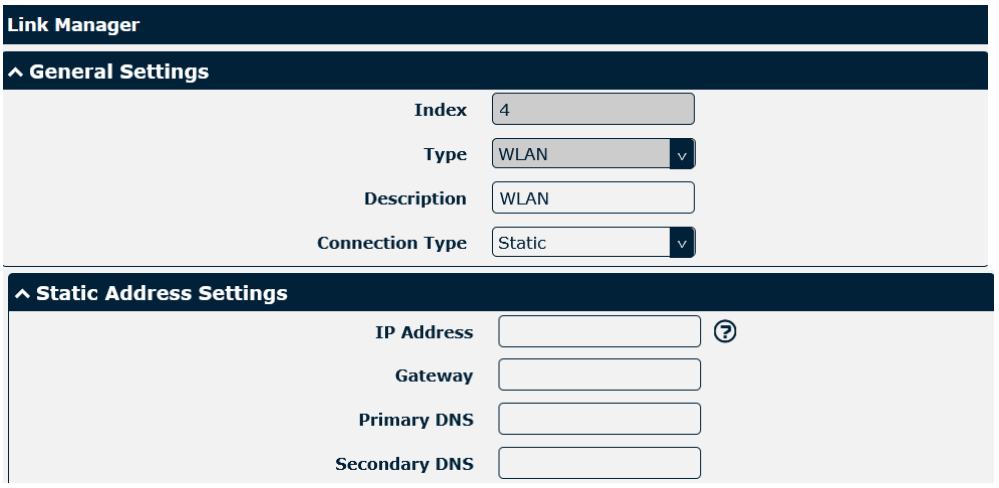
Specify the SecondaryDNS server (Sekundären DNS-Server spezifizieren)	Definiert den sekundären IPv4-DNS-Server für den Link.	Null
Specify the IPv6 Primary DNS server (Primären IPv6-DNS-Server spezifizieren)	Definiert den primären IPv6-DNS-Server für den Link.	Null
Specify the IPv6 Secondary DNS server (Sekundären IPv6-DNS-Server spezifizieren	Definiert den sekundären IPv6-DNS-Server für den Link.	Null
Debug Enable (Debugging aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/deaktivieren. Aktivieren Sie diese Option für die Ausgabe von Debugging-Informationen.	ON (EIN)
Verbose Debug Enable (Ausführliches Debugging aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option für die Ausgabe von ausführlichen Debugging-Informationen.	OFF (AUS)

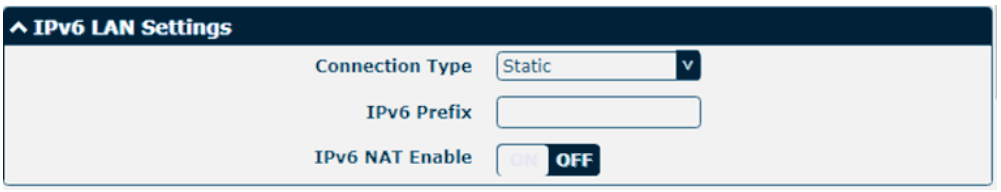
WLAN

Der Router erhält automatisch die IP vom WLAN-AP (Access Point), wenn als Verbindungstyp „DHCP“ gewählt wird. Die spezifische Parameterkonfiguration von SSID ist wie unten dargestellt.

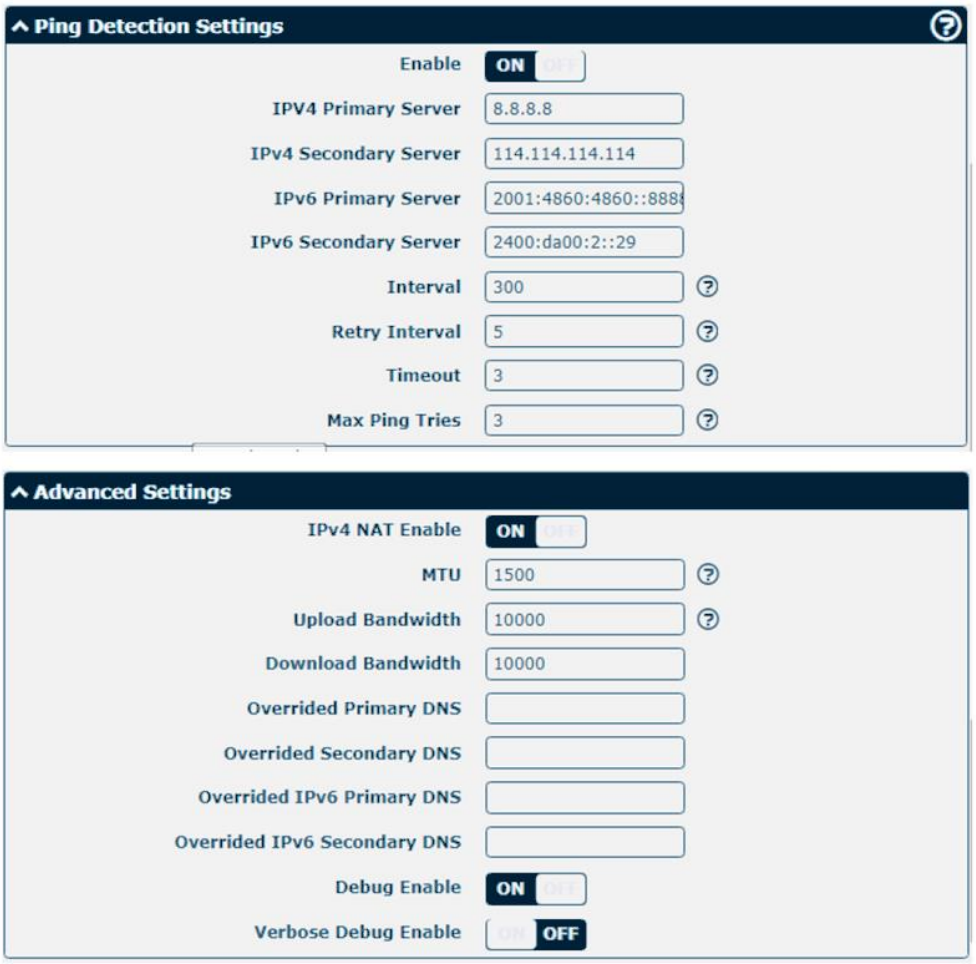


Wenn Sie als IPv4-Verbindungstyp „Static“ („Statisch“) wählen, wird das Fenster wie unten dargestellt.





Hinweis: Der DSR-211 unterstützt PPPoE bei gewähltem WLAN-Verbindungstyp nicht.



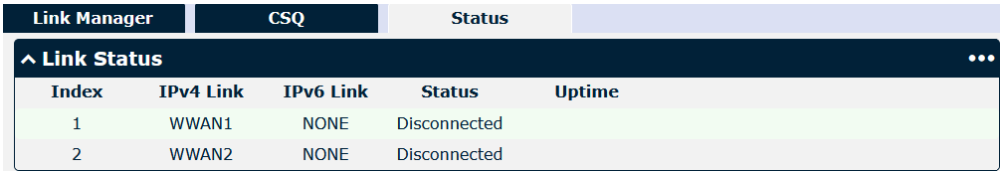
Link Settings (WLAN) (Link-Einstellungen (WLAN)		
Punkt	Beschreibung	Standard
General Settings (Allgemeine Einstellungen)		
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Type (Typ)	Zeigt den Typ des Links an.	WLAN
Description (Beschreibung)	Sie können eine Beschreibung für diesen Link eingeben.	Null
Enable IPv6 (IPv6 aktivieren)	Klicken Sie auf den Schalter, um IPv6 zu aktivieren/ deaktivieren.	OFF (AUS)
IPv4 Connection Type (IPv4-Verbindungstyp)	Wählen Sie aus „DHCP“ oder „Static“(„Statisch“).	DHCP
WLAN Settings (WLAN-Einstellungen)		
SSID	Geben Sie eine 1–32 Zeichen lange SSID ein, mit der sich Ihr Router verbinden möchte. SSID (Service Set Identifier) ist der Name Ihres drahtlosen Netzwerks.	router
Connect to Hidden SSID (Mit verborgener SSID verbinden)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn der Router im Client-Modus arbeitet und eine Verbindung zu einem Zugangspunkt mit verborgener SSID herstellen muss, müssen Sie diese Option aktivieren.	OFF (AUS)
Password (Passwort)	Geben Sie ein 8–63 Zeichen langes Passwort des Zugangspunkts ein, mit dem sich Ihr Router verbinden möchte.	Null
Static Address Settings (Einstellungen für statische Adressen)		
IP Address (IP-Adresse)	Geben Sie die IP-Adresse mit Netzmaske ein, die auf das Internet zugreifen kann, z. B. 192.168.1.1/24	Null
Gateway	Geben Sie die IP-Adresse des Wi-Fi-AP ein.	Null
Primary DNS (Primäres DNS)	Legen Sie das primäre DNS fest.	Null
Secondary DNS (Sekundäres DNS)	Legen Sie das sekundäre DNS fest.	Null
IPv6 LAN Settings (IPv6-LAN-Einstellungen)		
Connection type (Verbindungstyp)	Wählen Sie den Link, um dem LAN IPv6-Präfixe zuzuweisen.	Delegated (delegiert)
IPv6 Prefix (IPv6-Präfix)	Setzt das statische IPv6-Präfix, das durch den Link zum LAN zugewiesen wird.	Null
Enabled IPv6 NAT (Aktiviertes IPv6-NAT)	Richten Sie Links ein, um IPv6-NAT zu aktivieren.	OFF (AUS)
Ping Detection Settings (Ping-Erkennungs-Einstellungen)		
Enable (Aktivieren)	Klicken Sie auf den Schalter, um den Ping-Erkennungsmechanismus, eine Keep-Alive-Richtlinie des DSR-211 Routers, zu aktivieren/ deaktivieren.	ON (EIN)

Primary Server (Primärer Server)	Der Router sendet einen Ping an diese sekundäre Adresse / diesen Domänennamen, um zu prüfen, ob die aktuelle Konnektivität aktiv ist.	8.8.8.8
Secondary Server (Sekundärer Server)	Der Router sendet einen Ping an diese sekundäre Adresse / diesen Domänennamen, um zu prüfen, ob die aktuelle Konnektivität aktiv ist.	114.114.114.114
IPv6 Primary Server (Primärer IPv6-Server)	Der Router sendet einen Ping an diese primäre Adresse / diesen Domänennamen, um zu prüfen, ob die aktuelle IPv6-Konnektivität aktiv ist.	2001:4860:4860::8888 8
IPv6 Secondary Server (Sekundärer IPv6-Server)	Der Router sendet einen Ping an diese sekundäre Adresse / diesen Domänennamen, um zu prüfen, ob die aktuelle IPv6-Konnektivität aktiv ist.	2400:da00:2::29
Interval (Intervall)	Legen Sie das Ping-Intervall fest.	300
Retry Interval (Wiederholungs-Intervall)	Legen Sie das Ping-Wiederholungsintervall fest. Wenn der Ping fehlgeschlagen ist, pingt der Router in jedem Wiederholungsintervall erneut.	5
Timeout (Zeitüberschreitung)	Legen Sie die Ping-Zeitüberschreitung fest.	3
Max Ping Tries (Max. Ping-Versuche)	Legen Sie die maximalen Ping-Versuche fest. Wenn die maximale kontinuierliche Anzahl der Ping-Versuche erreicht ist, wird zu einem anderen Link gewechselt oder Notfallmaßnahmen werden ergriffen.	3
Advanced Settings (Erweiterte Einstellungen)		
NAT Enable (NAT aktivieren)	Klicken Sie auf den Schalter, um die Option Network Address Translation zu aktivieren/ deaktivieren.	ON (EIN)
MTU (MÜE)	Geben Sie die maximale Übertragungseinheit ein.	1500
Upload Bandwidth (Upload-Bandbreite)	Geben Sie die für QoS verwendete Upload-Bandbreite, gemessen in kbit/s, ein.	10000
Download Bandwidth (Download-Bandbreite)	Geben Sie die für QoS verwendete Download-Bandbreite, gemessen in kbit/s, ein.	10000
Specify the Primary DNS server (Primären DNS-Server spezifizieren)	Definiert den primären IPv4-DNS-Server für den Link.	Null
Specify the Secondary DNS server (Sekundären DNS-Server spezifizieren)	Definiert den sekundären IPv4-DNS-Server für den Link.	Null
Specify the IPv6 Primary DNS server (Primären IPv6-DNS-Server spezifizieren)	Definiert den primären IPv6-DNS-Server für den Link.	Null
Specify the IPv6 Secondary DNS server (Sekundären IPv6-DNS-Server spezifizieren	Definiert den sekundären IPv6-DNS-Server für den Link.	Null
Debug Enable (Debugging aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option für die Ausgabe von Debugging-Informationen.	ON (EIN)

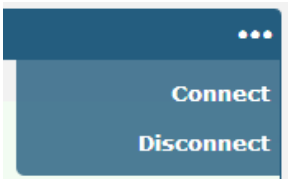
Verbose Debug Enable (Ausführliches Debugging aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option für die Ausgabe von ausführlichen Debugging-Informationen.	OFF (AUS)

Status

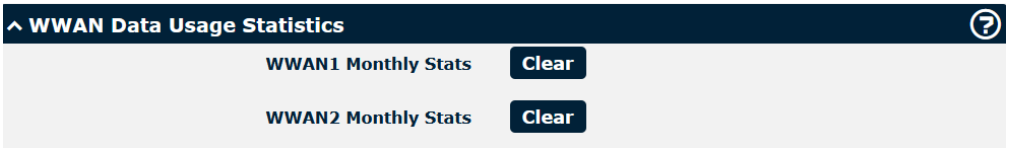
Auf dieser Seite können Sie den Status der Linkverbindung anzeigen und die monatlichen Statistiken zur Datennutzung löschen.



Klicken Sie auf die Schaltfläche g echts, um den Verbindungsstatus der aktuellen Linkverbindung auszuwählen.



Klicken Sie auf die Zeile des Links, und es werden die Detailinformationen der aktuellen Linkverbindung angezeigt.



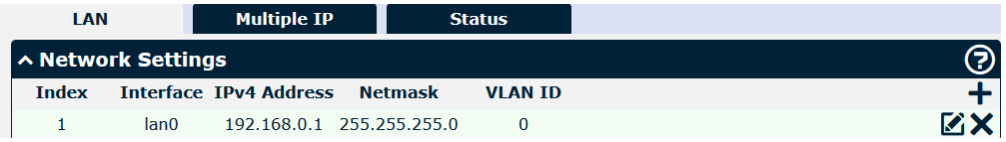
Klicken Sie auf die Schaltfläche Clear (Löschen), um die monatlichen Nutzungsstatistiken für den Datenverkehr von SIM1 oder SIM2 zu löschen. Datenstatistiken werden nur angezeigt, wenn die Funktion Data Allowance (Datenkontingent) unter Interface (Schnittstelle) > Link Manager > Link Settings (Link-Einstellungen) > WWAN Settings (WWAN-Einstellungen) > Data Allowance (Datenkontingent) aktiviert ist.

3.7 Schnittstelle > LAN

In diesem Abschnitt können Sie die entsprechenden Parameter für den LAN-Port einstellen. Der DSR-211 Router verfügt über zwei LAN-Ports, ETH0 und ETH1. ETH0 und ETH1 können frei zwischen lan0 und lan1 wählen, aber mindestens ein LAN-Port muss als lan0 zugewiesen werden. Die Standardeinstellungen von ETH0 und ETH1 sind lan0 und ihre Standard-IP ist 192.168.0.1 / 255.255.255.0.

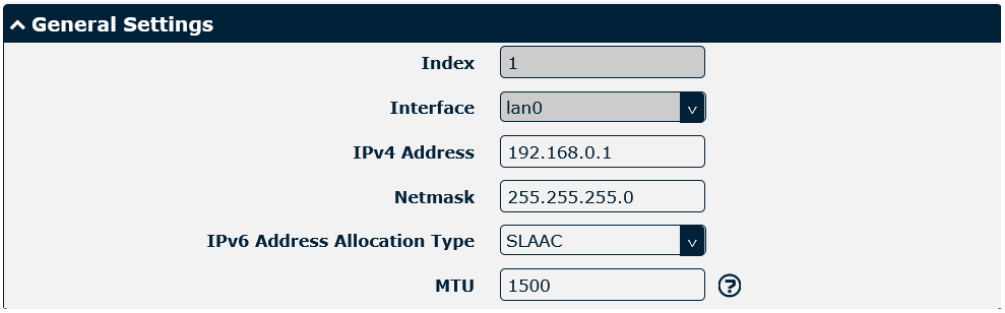
LAN

Standardmäßig gibt es einen LAN-Port (lan0) in der Liste. Um mit dem Hinzufügen eines neuen LAN-Ports (lan1) zu beginnen, konfigurieren Sie bitte zuerst ETH0 oder ETH1 als lan1 unter Ethernet > Ports > Port Settings (Port-Einstellungen). Andernfalls wird für den Vorgang „List is full“ („Liste ist voll“) gemeldet.



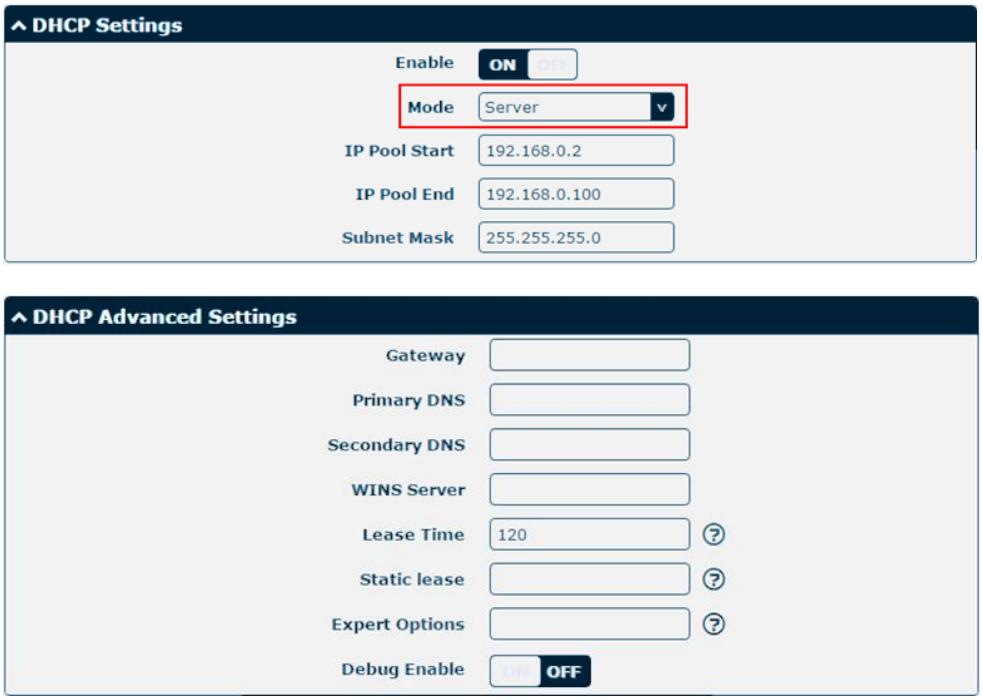
Hinweis: Lan0 kann nicht gelöscht werden.

Klicken Sie auf , um einen neuen LAN-Port hinzuzufügen, oder Sie klicken auf , um den aktuellen LAN-Port zu löschen. Klicken Sie jetzt auf um die Konfiguration des LAN-Ports zu bearbeiten.

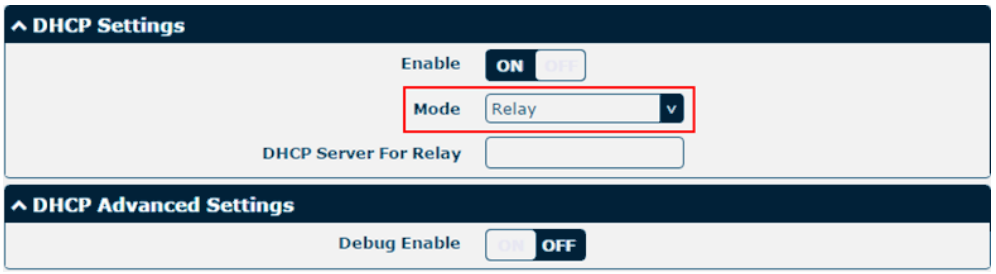


General Settings (Allgemeine Einstellungen)		
Punkt	Beschreibung	Standard
Index	Gibt die Ordinalzahl der Liste an.	--
Interface (Schnittstelle)	Zeigt den bearbeiteten Port an. Lan1 ist nur verfügbar, wenn es von einem der ETH0 oder ETH1 unter Ethernet > Ports > Port Settings (Port-Einstellungen) ausgewählt wurde	--
IP Address (IP-Adresse)	Stellen Sie die IP-Adresse des LAN-Ports ein.	192.168.0.1
Netmask (Netzmaske)	Legen Sie die Netzmaske des LAN-Ports fest.	255.255.255.0
IPv6 Address AllocationType (Zuweisungstyp IPv6-IP-Adresse)	Legen Sie die Methode der Zuweisung von IPv6-Adressen auf der LAN-Seite fest.	SLAAC
MTU (MÜE)	Geben Sie die maximale Übertragungseinheit ein.	1500

Wenn Sie als Modus „Server“ wählen, wird das Fenster wie unten dargestellt:



Wenn Sie als Modus „Relay“ („Relais“) wählen, wird das Fenster wie unten dargestellt.

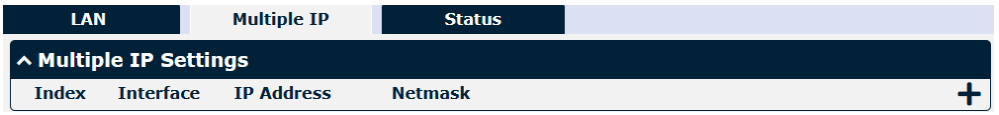


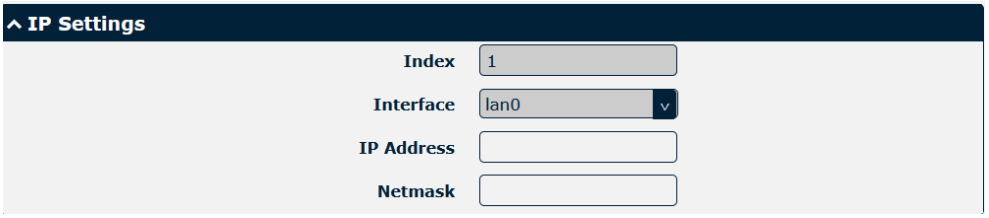
LAN		
Punkt	Beschreibung	Standard
DHCP Settings (DHCP-Einstellungen)		
Enable (Aktivieren)	Klicken Sie auf den Schalter, um die DHCP-Funktion zu aktivieren/ deaktivieren.	ON (EIN)
Mode (Modus)	Wählen Sie aus „Server“ oder „Relay“ („Relais“). Server: IP-Adresse an DHCP-Clients leasen, die an den LAN-Port angeschlossen wurden Relay: Ein Router kann ein DHCP-Relay sein, das einen Relay-Tunnel bereitstellt, um das Problem zu lösen, dass DHCP-Client und DHCP-Server sich nicht in demselben Subnetz befinden.	Server
IP Pool Start (IP-Pool-Beginn)	Definieren Sie den Beginn des Pools von IP-Adressen, die an DHCP-Clients geleast werden.	192.168.0.2

IP Pool End (IP-Pool-Ende)	Definieren Sie das Ende des Pools von IP-Adressen, die an DHCP-Clients geleast werden sollen.	192.168.0.100
Subnet Mask (Subnetzmaske)	Definieren Sie die Subnetzmaske der IP-Adresse, die durch DHCP-Clients vom DHCP-Server bezogen wird.	255.255.255.0
DHCP Server for Relay (DHCP-Server für Relay)	Geben Sie die IP-Adresse des DHCP-Relay-Servers ein.	Null
DHCP Advanced Settings (Erweiterte DHCP-Einstellungen)		
Gateway (Gateway)	Definieren Sie das vom DHCP-Server den Clients zugewiesene Gateway, das sich im selben Netzwerksegment wie der DHCP-Adresspool befinden. muss.	Null
Primary DNS (Primäres DNS)	Definieren Sie den primären DNS-Server, den der DHCP-Server den Clients zuweist.	Null
Secondary DNS (Sekundäres DNS)	Definieren Sie den sekundären DNS-Server, den der DHCP-Server den Clients zuweist.	Null
WINS Server (WINS-Server)	Definieren Sie den Windows Internet Naming Service, der durch DHCP-Clients von einem DHCP-Server bezogen wird.	Null
Lease Time (Lease-Zeit)	Legen Sie die Lease-Zeit fest, die der Client die vom DHCP-Server erhaltene IP-Adresse verwenden kann, gemessen in Sekunden.	120
Static lease (Statischer Lease)	Binden Sie einen Lease, um einer IP-Adresse eine entsprechende MAC-Adresse zuzuweisen. Format: mac,ip;mac,ip;..., z. B. FF:ED:CB:A0:98:01,192.168.0.200	Null
Expert Options (Expertenoptionen)	Geben Sie in diesem Feld einige andere Optionen des DHCP-Servers ein. Format: config-desc;config-desc, z. B. log dhcp;quiet-dhcp	Null
Debug Enable (Debugging aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/deaktivieren. Aktivieren Sie diese Option für die Ausgabe von DHCP-Informationen.	OFF (AUS)

Multi-IP

Klicken Sie auf +, um eine Multi-IP zum LAN-Port hinzuzufügen, oder klicken Sie auf ✕, um die Multi-IP des LAN-Ports zu löschen. Klicken Sie nun auf , um die Multi-IP des LAN-Ports zu bearbeiten.

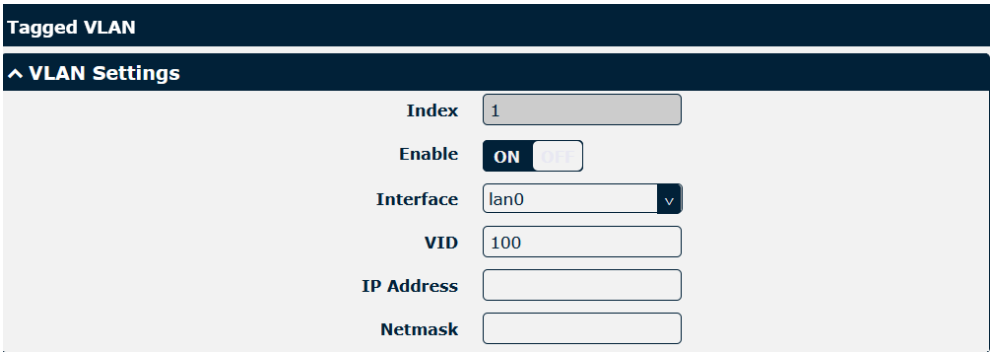




IP Settings (IP-Einstellungen)		
Punkt	Beschreibung	Standard
Index	Gibt die Ordinalzahl der Liste an.	--
Interface (Schnittstelle)	Zeigt den bearbeiteten Port an, schreibgeschützt.	lan0
IP Address (IP-Adresse)	Stellen Sie die Multi-IP-Adresse des LAN-Ports ein.	Null
Netmask (Netzmaske)	Legen Sie die Multi-Netzmaske des LAN-Ports fest.	Null

VLAN Trunk (VLAN-Trunk)

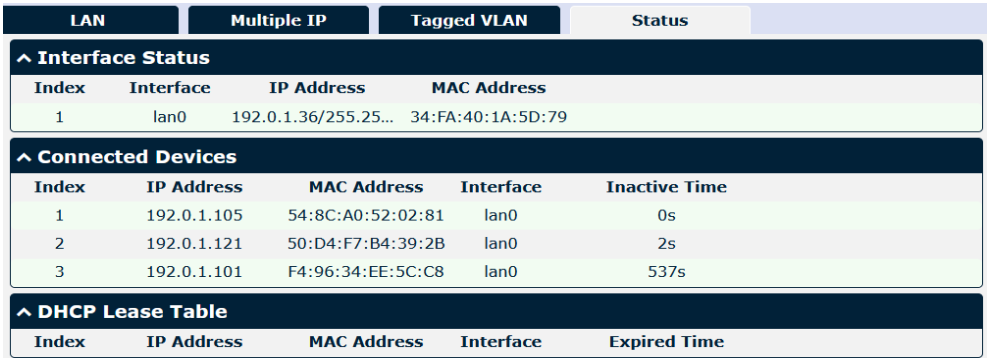
Klicken Sie auf + um ein VLAN hinzuzufügen. Die maximale Anzahl beträgt 8.



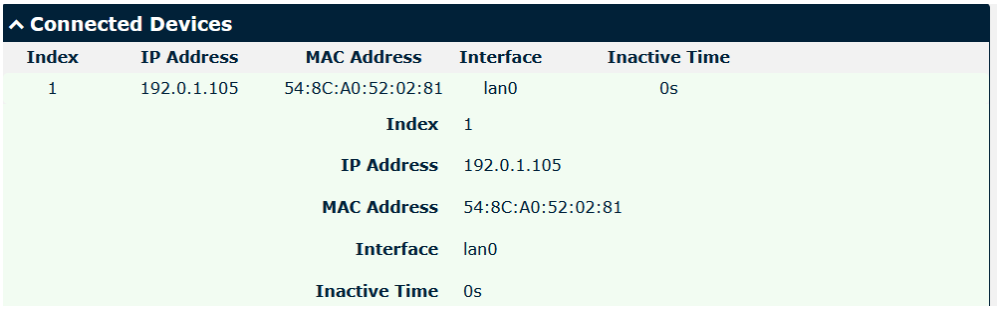
VLAN Trunk		
Punkt	Beschreibung	Standard
Index	Gibt die Ordinalzahl der Liste an.	--
Enable (Aktivieren)	Klicken Sie auf den Schalter, um dieses VLAN zu aktivieren/ deaktivieren. Aktivieren Sie diese Option, damit der Router das VLAN-Tag kapseln und entkapseln kann.	ON (EIN)
Interface (Schnittstelle)	Wählen Sie die Schnittstelle, die die VLAN-Trunk-Funktion aktivieren möchte. Die Auswahl von „lan0“ oder „lan1“ hängt von dem entsprechenden LAN-Port von EHT0 und ETH1 ab.	lan0
VID	Legen Sie die Tag-ID des VLAN und die Ziffern von 1 bis 4094 fest.	100
IP Address (IP-Adresse)	Legen Sie die IP-Adresse des VLAN-Ports fest.	Null
Netmask (Netzmaske)	Legen Sie die Netzmaske des VLAN-Ports fest.	Null

Status

In diesem Abschnitt können Sie den Status der LAN-Verbindung einsehen.



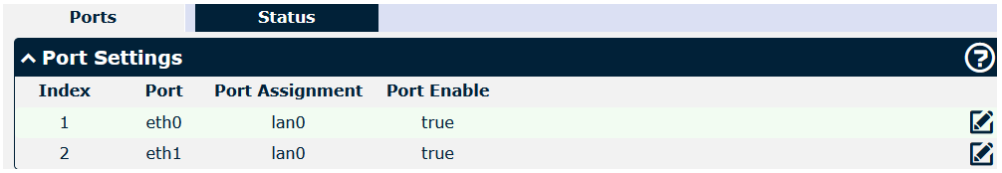
Klicken Sie auf Status und die detaillierten Statusinformationen werden unter der Zeile angezeigt. Bitte beachten Sie den Screenshot unten.



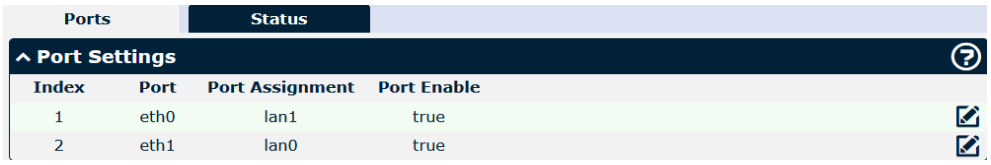
3.8 Schnittstelle > Ethernet

In diesem Abschnitt können Sie die entsprechenden Parameter für Ethernet einstellen. Der DSR-211 Router verfügt über zwei Ethernet-Ports, darunter ETH0 und ETH1. ETH0 auf dem Router kann entweder als WAN- oder als LAN-Port konfiguriert werden, während ETH1 nur als LAN-Port konfiguriert werden kann. Standardmäßig sind ETH0 und ETH1 lan0, und ihre IP lautet 192.168.0.1 / 255.255.255.0. Da lan0 einem Port und der WAN-Port dem ETH0 zugeordnet werden müssen, gibt es vier Konfigurationen.
Sie können die geeignete Konfiguration wählen, die Ihren aktuellen Bedürfnissen entspricht.
Die spezifischen Port-Konfigurationen sind unten dargestellt.

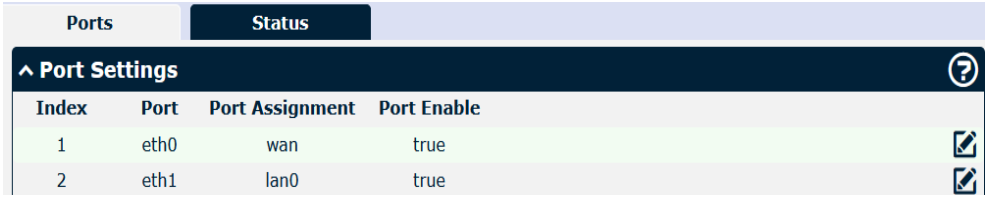
Beispiel 1: Beide Ethernet-Pots (ETH) sind als Bridge mit der gleichen IP konfiguriert.



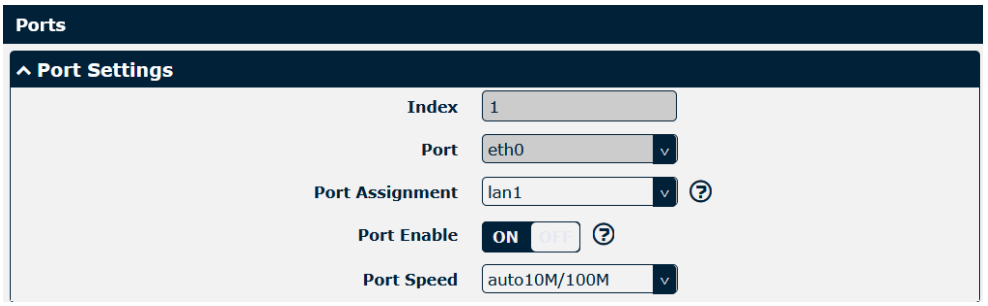
Beispiel 2: Beide Ethernet-Ports sind getrennt und haben unterschiedliche IP-Adressen.



Beispiel 3: Ethernet-Port ETH0 ist als WAN-Port und ETH1 als LAN-Port konfiguriert. (Wenn das DSR-211 als Net-Net-Router genutzt wird)

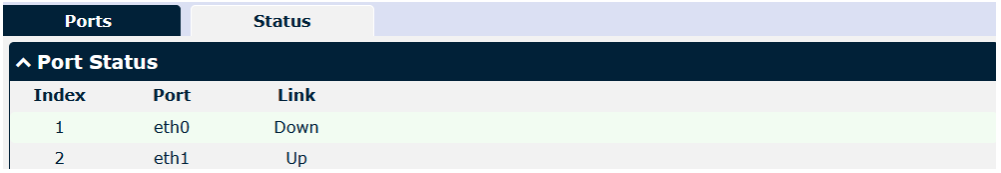


Klicken Sie auf die Schaltfläche von eth0, um seine Parameter zu konfigurieren. Die Port-Zuweisung kann durch Auswahl aus der Dropdown-Liste geändert werden.

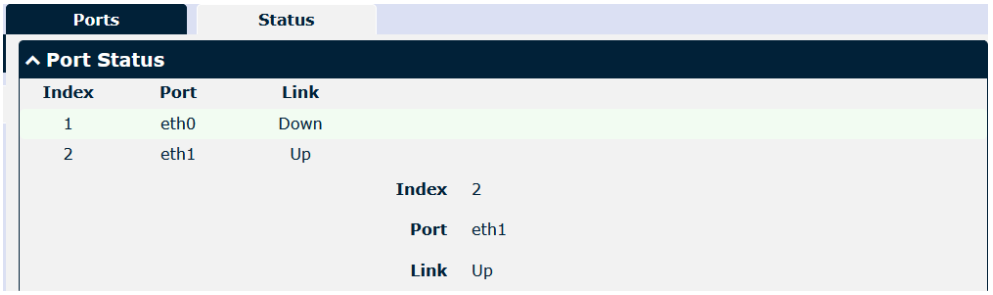


Port Settings (Port-Einstellungen)		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Port	Zeigt den bearbeiteten Port an, schreibgeschützt.	--
Port Assignment (Port-Zuweisung)	Wählen Sie den Typ des Ethernet-Ports als WAN-Port oder als LAN-Port. Wenn Sie den Port als LAN-Port unter Interface (Schnittstelle) > LAN > Network Settings (Netzwerk-Einstellungen) > General Settings (Allgemeine Einstellungen) festlegen, können Sie auf die Dropdown-Liste klicken, um zwischen „lan0“ oder „lan1“ zu wählen.	lan0

In dieser Spalte können Sie den Status des Ethernet-Ports einsehen.

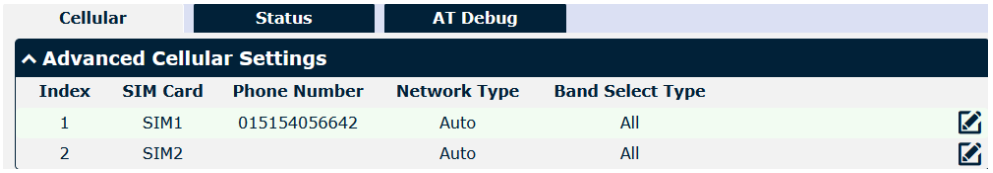


Klicken Sie auf die Zeile mit dem Status und die detaillierten Statusinformationen werden unter der Zeile angezeigt. Bitte beachten Sie den Screenshot unten.

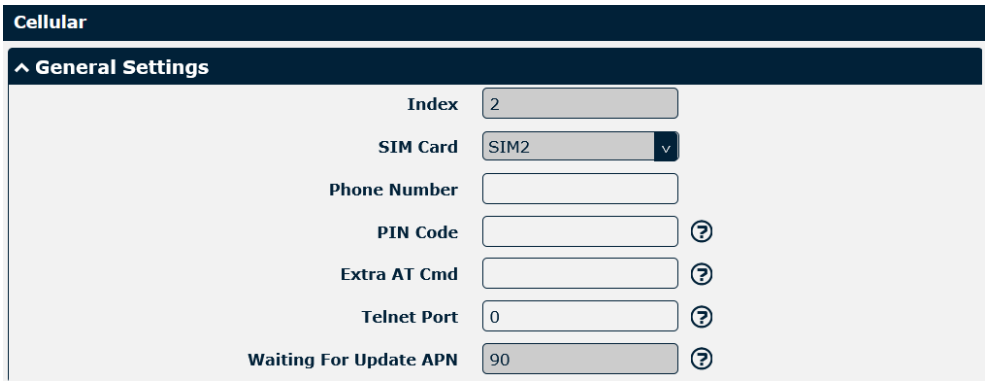


3.9 Schnittstelle > Mobilfunk

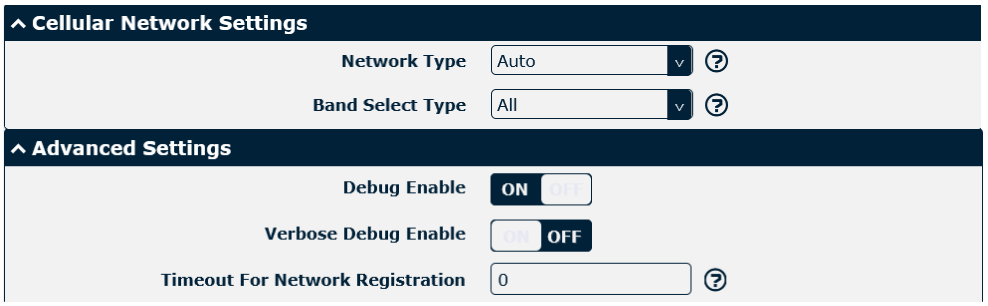
In diesem Abschnitt können Sie die entsprechenden Parameter von Cellular (Mobilfunk) einstellen. Der DSR-211 Router verfügt über zwei SIM-Kartensteckplätze, unterstützt jedoch aufgrund seiner Einzelmodulbauweise nicht zwei SIM-Karten gleichzeitig online. Wenn eine einzelne SIM-Karte zum ersten Mal eingesetzt wird, sind die Steckplätze SIM1 und SIM2 verfügbar.



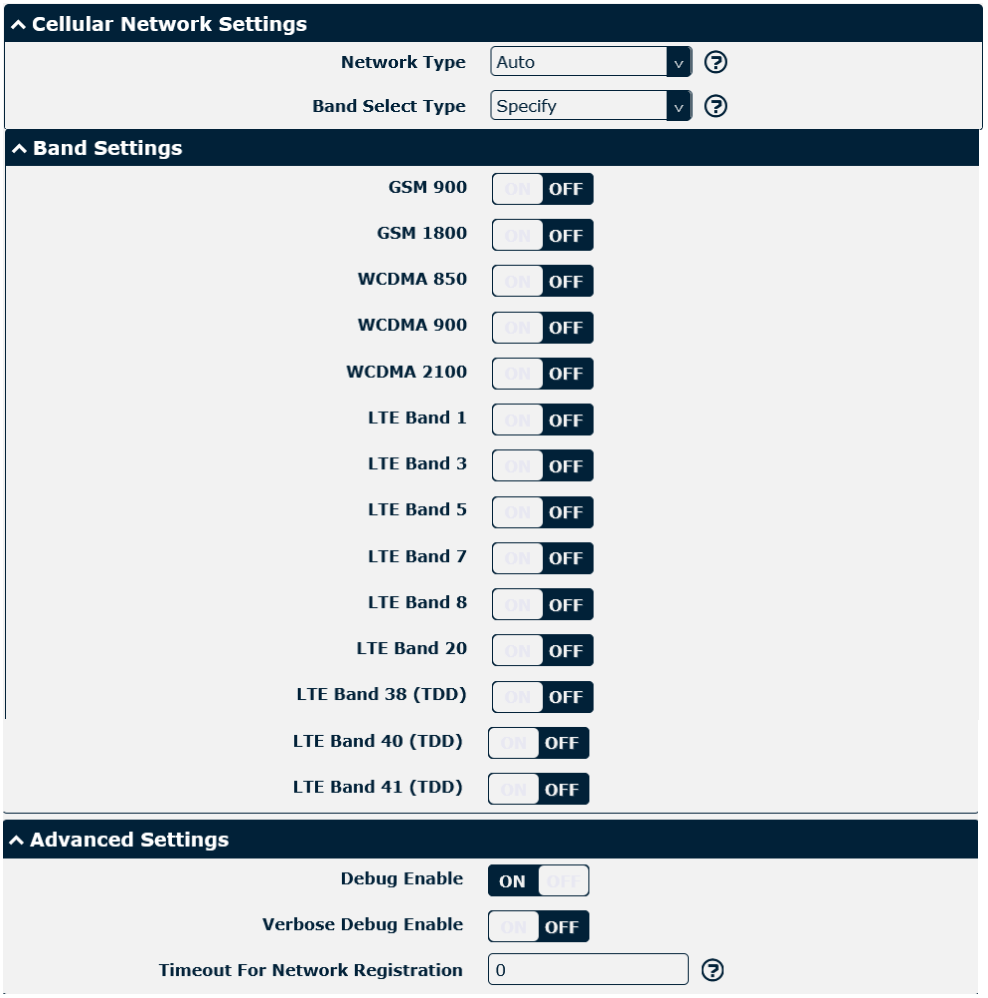
Klicken Sie auf  von SIM1, um die Parameter zu bearbeiten.



Das Fenster wird wie unten dargestellt, wenn Sie als Netzwerktyp „Auto“ wählen.



Das Fenster wird wie unten dargestellt, wenn Sie als Bandauswahl-Typ „Specify“ („Spezifizieren“) wählen.



Cellular (Mobilfunk)		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
SIM Card (SIM-Karte)	Legen Sie die aktuell bearbeitete SIM-Karte fest.	SIM1
Phone Number (Telefonnummer)	Geben Sie die Telefonnummer der SIM-Karte ein.	Null
PIN Code (PIN-Code)	Geben Sie einen 4–8-stelligen PIN-Code ein, der zum Entsperren der SIM-Karte verwendet wird.	Null
Extra AT Cmd (Zusätzliche AT-Befehle)	Geben Sie die für die Mobilfunk-Initialisierung verwendeten AT-Befehle ein.	Null
Telnet Port (Telnet-Anschluss)	Geben Sie den Port an, der den Telnet-Dienst überwacht, der für AT über Telnet verwendet wird.	0
Cellular Network Settings (Einstellungen für Mobilfunknetze)		
Network Type (Netzwerktyp)	Wählen Sie aus „Auto“, „2G Only“ („Nur 2G“), „2G First“ („2G bevorzugt“), „3G Only“ („Nur 3G“), „3G First“ („3G bevorzugt“), „4G Only“ („Nur 4G“), „4G First“ („4G bevorzugt“). Auto: Automatische Verbindung zum Netzwerk mit dem besten Signal 2G Only (Nur 2G): Nur das 2G-Netz wird verbunden 2G First: Das 2G-Netz wird bevorzugt verbunden 3G Only (Nur 3G): Nur das 3G-Netz wird verbunden 3G First: Das 3G-Netz wird bevorzugt verbunden 4G Only (Nur 4G): Nur das 4G-Netz wird verbunden 4G First: Das 4G-Netz wird bevorzugt verbunden	Auto
Band Select Type (Bandauswahl-Typ)	Wählen Sie aus „All“ („Alle“) oder „Specify“ („Spezifizieren“). Sie können bestimmte Bänder wählen, wenn Sie „Specify“ („Spezifizieren“) wählen.	All (Alle)
Advanced Settings (Erweiterte Einstellungen)		
Debug Enable (Debugging aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option für die Ausgabe von Debugging-Informationen.	ON (EIN)
Verbose Debug (Ausführliches Debugging) Enable (Aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option für die Ausgabe von ausführlichen Debugging-Informationen.	OFF (AUS)

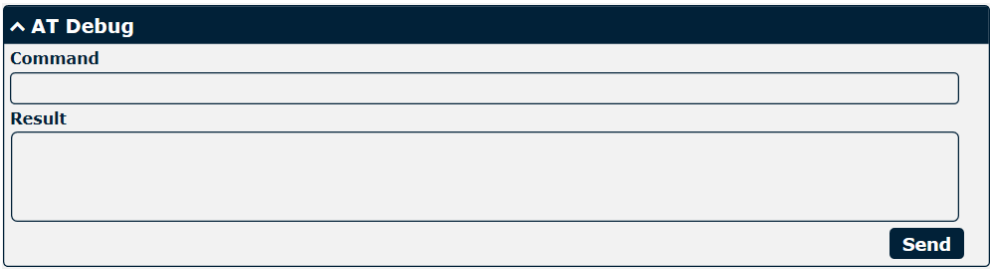
In diesem Abschnitt können Sie den Status der Mobilfunkverbindung einsehen.

Klicken Sie auf die Zeile mit dem Status und die detaillierten Statusinformationen werden unter der Zeile angezeigt.

Status	
Punkt	Beschreibung
Index (Index)	Gibt die Ordinalzahl der Liste an.
Modem Status	Zeigt den Status des Funkmoduls an.
Modem Model	Zeigt das Modell des Funkmoduls an.
Current SIM (Aktuelle SIM)	Zeigt die SIM-Karte an, die Ihr Router verwendet.
Phone Number (Telefonnummer)	Zeigt die Telefonnummer der aktuellen SIM-Karte an. Hinweis: Diese Option wird angezeigt, wenn Sie manuell unter Cellular (Mobilfunk) > Advanced Cellular Settings (Erweiterte Mobilfunkeinstellungen) > SIM1/ SIM2 > General Settings (Allgemeine Einstellungen) > Phone Number (Telefonnummer) eingegeben wird.
IMSI	Zeigt die IMSI-Nummer der aktuellen SIM-Karte an.
ICCID	Zeigt die ICCID-Nummer der aktuellen SIM-Karte an.
Registration (Anmeldung)	Zeigt den aktuellen Netzwerkstatus an.
Network Provider (Netzanbieter)	Zeigt den Namen des Netzanbieters an.
Network Type (Netzwerktyp)	Zeigt den aktuellen Netzwerkdiensttyp an, z. B. GPRS.

Signal Strength (Signalstärke)	Zeigt die vom Funkmodul erkannte Signalstärke an.
Registered band (Registriertes Band)	Zeigt das aktuelle Frequenzband an.
RSRP	Zeigt die empfangene Leistung des Referenzsignals an.
RSRQ	Zeigt die Empfangsqualität des Referenzsignals an.
Bit Error Rate	Zeigt die aktuelle Bitfehlerrate an.
PLMN ID (PLMN-ID)	Zeigt die aktuelle PLMN-ID an.
Local Area Code (Ortsnetzkennzahl)	Zeigt die aktuelle Ortsnetzkennzahl an, die zur Identifizierung verschiedener Gebiete verwendet wird.
Cell ID (Zellen-ID)	Zeigt die aktuelle Zellen-ID an, die zum Lokalisieren des Routers verwendet
IMEI	Zeigt die IMEI-Nummer (International Mobile Equipment Identity) des Funkmoduls an.
Firmware Version (Firmware-Version)	Zeigt die aktuelle Firmware-Version des Funkmoduls an.

Diese Seite ermöglicht es Ihnen, das AT-Debugging zu überprüfen.



AT Debug (AT-Debugging)		
Punkt	Beschreibung	Standard
Command (Befehl)	Geben Sie den AT-Befehl, den Sie an das Funkmodul senden möchten, in dieses Textfeld ein.	Null
Result (Ergebnis)	In diesem Textfeld wird der vom Funkmodul zurückgesendete AT-Befehl angezeigt.	Null
Send	Klicken Sie auf die Schaltfläche, um den AT-Befehl zu senden.	--

3.10 Schnittstelle > Wi-Fi

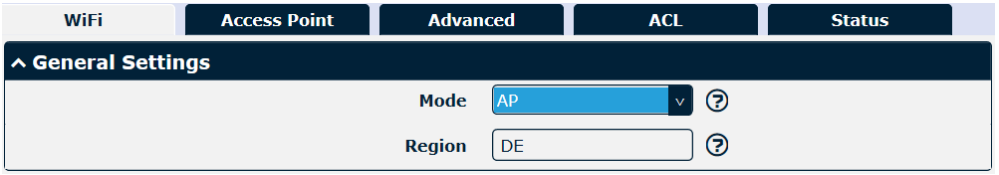
In diesem Abschnitt können Sie die Parameter von zwei Wi-Fi-Modi konfigurieren. Der DSR-211 Router unterstützt den Wi-Fi-Accesspoint-Modus oder den Client-Modus, wobei standardmäßig der Accesspoint-Modus genutzt wird.

Hinweis: Beim Wechsel zwischen Accesspoint- und Client-Modus muss ein Neustart durchgeführt werden, damit die Konfiguration wirksam wird.

Wi-Fi-Accesspoint

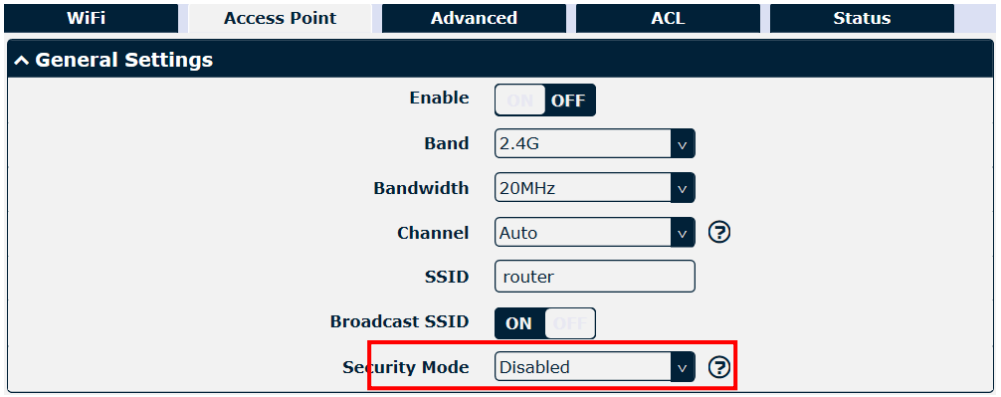
Konfigurieren des DSR-211 Routers als Wi-Fi-AP

Klicken Sie auf Interface (Schnittstelle) > Wi-Fi > Wi-Fi, wählen Sie „AP“ (Accesspoint) als Modus und klicken Sie auf „Submit“ („Übermitteln“).

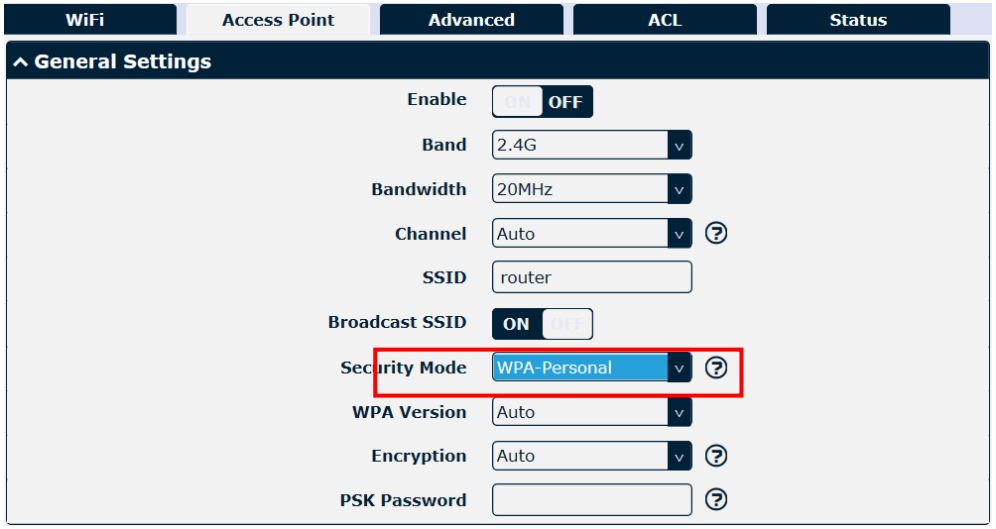


Hinweis: Bitte denken Sie daran, nach Abschluss der Konfiguration auf Save & Apply (Speichern & Übernehmen) > Reboot (Neustart) zu klicken, damit die Konfiguration wirksam wird.

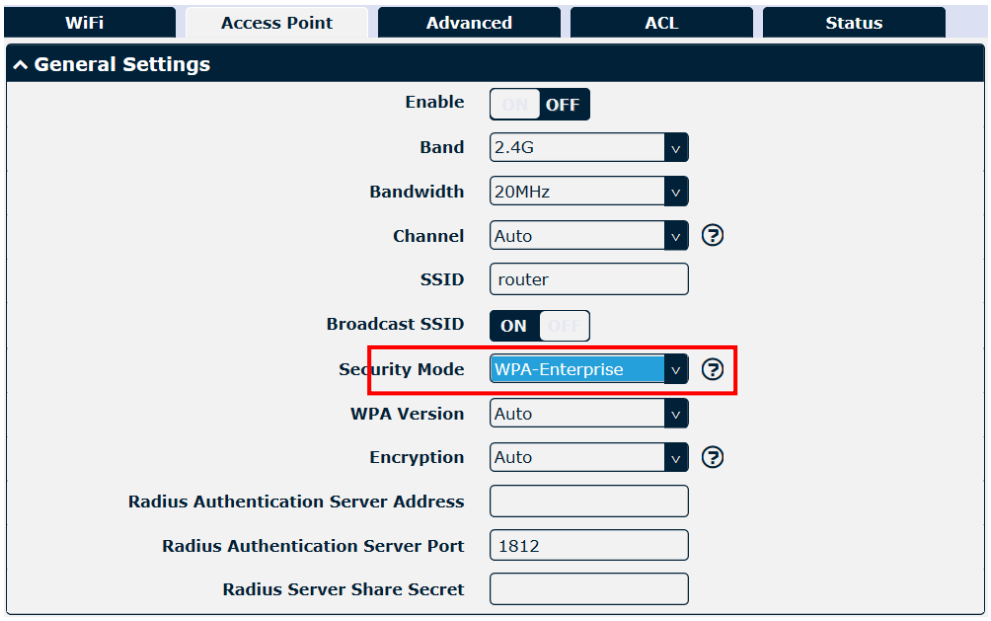
Klicken Sie auf die Spalte Access Point (Zugangspunkt), um die Parameter von Wi-Fi-AP zu konfigurieren. Standardmäßig ist der Sicherheitsmodus auf „Disabled“ („Deaktiviert“) eingestellt.



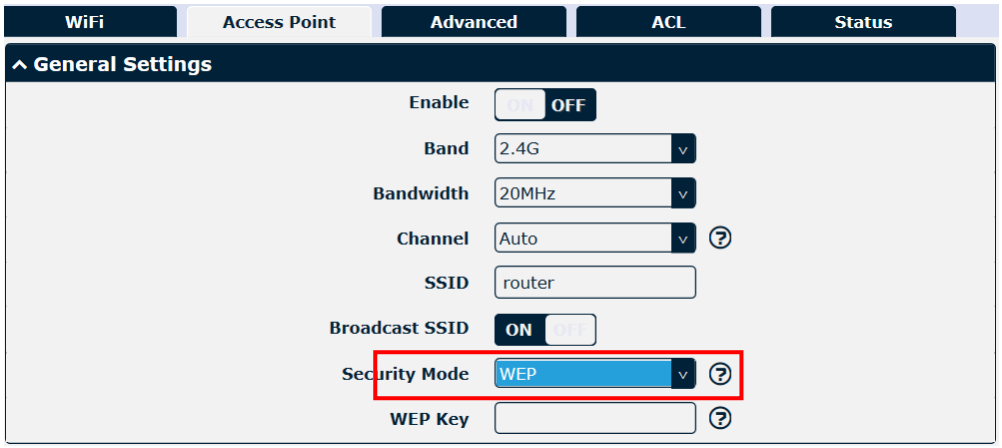
Das Fenster wird wie unten dargestellt, wenn „WPA-Personal“ als Sicherheitsmodus eingestellt wird.



Wenn „WEP-Enterprise“ als Sicherheitsmodus eingestellt ist, wird das Fenster wie unten dargestellt angezeigt:

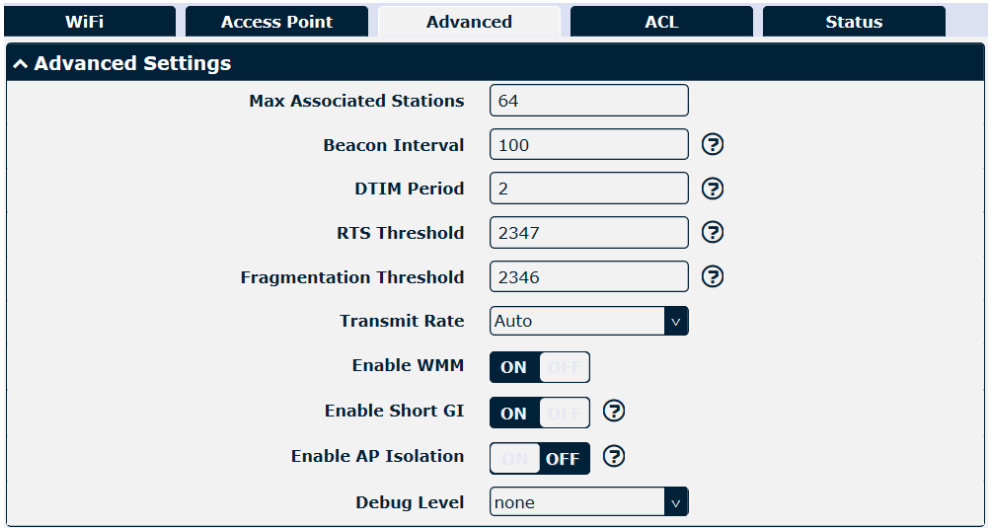


Wenn „WEP“ als Sicherheitsmodus ausgewählt ist, wird das Fenster wie folgt angezeigt:

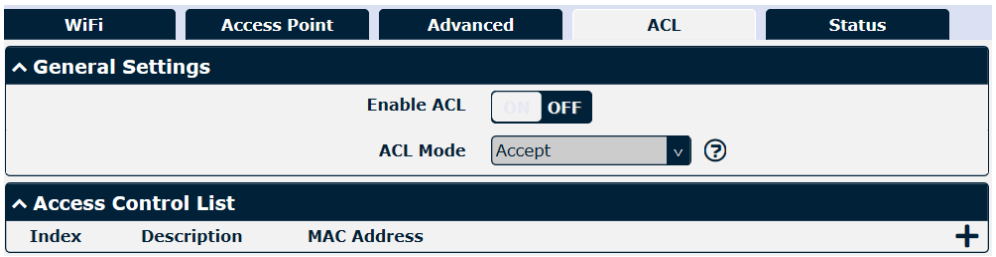


General Settings @ Access Point (Allgemeine Einstellungen unter Zugangspunkt)		
Punkt	Beschreibung	Standard
Enable (Aktivieren)	Klicken Sie auf den Schalter, um die Option Wi-Fi-Zugangspunkt zu aktivieren/ deaktivieren.	OFF (AUS)
Band	Wählen Sie aus „2.4G“ oder „5G“.	2.4G
Bandwidth (Bandbreite)	Wählen Sie aus „20MHz“ und „40MHz“. Die Kanalbreite von 40 MHz bietet die doppelte Datenrate im Vergleich zu einem einzelnen 20-MHz-Kanal.	20MHz
Channel (Kanal)	Wählen Sie den Frequenzkanal, einschließlich „Auto“, „1“, „2“ ...„13“. Auto: Der Router scannt alle Frequenzkanäle, bis der beste gefunden wurde. 1~13: Router wird für die Arbeit auf diesem Kanal festgelegt Es folgen die Frequenzen der Kanäle 1~13. 1: 2412 MHz 2: 2417 MHz 3: 2422 MHz 4: 2427 MHz 5: 2432 MHz 6: 2437 MHz 7: 2442 MHz 8: 2447 MHz 9: 2452 MHz 10: 2457 MHz 11: 2462 MHz 12: 2467 MHz 13: 2472 MHz	Auto
SSID	Geben Sie den Service Set Identifier, den Namen Ihres drahtlosen Netzwerks, ein. Die SSID eines Clients und die SSID des AP müssen identisch sein, damit der Client und der AP miteinander kommunizieren können. Geben Sie 1 bis 32 Zeichen ein.	router
Broadcast SSID (SSID senden)	Klicken Sie auf den Schalter, um das Senden der SSID zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, kann der Client Ihre SSID scannen. Wenn diese Option deaktiviert ist, kann der Client Ihre SSID nicht scannen. Wenn Sie eine Verbindung mit dem Router-AP herstellen möchten, müssen Sie die SSID des Router-AP auf Seiten des Wi-Fi-Client manuell eingeben.	ON (EIN)
Security Mode (Sicherheitsmodus)	Wählen Sie aus „Disabled“ („Deaktiviert“), „WPA-Personal“ oder „WEP-Enterprise“. Disabled (Deaktiviert): Benutzer können ohne Passwort auf das Wi-Fi zugreifen, wenn die Sicherheit deaktiviert ist. Hinweis: Es wird aus Sicherheitsgründen dringend empfohlen, diese Art von Modus nicht zu wählen. WPA-Personal: WiFi-Zugangsschutz, es kann nur ein Passwort für die Identitätsauthentifizierung vergeben werden. WEP-Enterprise: Sicherer Wi-Fi-Netzwerkschutz mit RADIUS-Dienst.WEP: Wired Equivalent Privacy bietet Verschlüsselung für die Datenübertragung drahtloser Geräte.	Disabled (Deaktiviert)
WPA Version (WPA-Version)	Wählen Sie aus „Auto“, „WPA“ oder „WPA2“. Auto: Der Router wählt automatisch die am besten geeignete WPA-Version. WPA2 ist ein stärkeres Sicherheitsmerkmal als WPA.	Auto

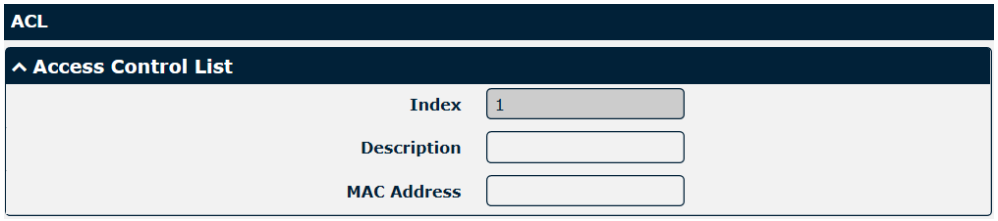
Encryption (Verschlüsselung)	Wählen Sie aus „Auto“, „TKIP“ oder „AES“. Auto: Der Router wählt automatisch die am besten geeignete Verschlüsselung. TKIP: Die TKIP-Verschlüsselung (Temporal Key Integrity Protocol) verwendet eine drahtlose Verbindung. TKIP-Verschlüsselung kann für WPA-PSK und WPA mit 802.1x-Authentifizierung verwendet werden. Hinweis: Es wird nicht empfohlen, TKIP-Verschlüsselung im 802.11n-Modus zu verwenden. AES: Die AES-Verschlüsselung verwendet eine drahtlose Verbindung. AES kann für WPA-PSK und WPA mit 802.1x-Authentifizierung verwendet werden. AES ist ein stärkerer Verschlüsselungsalgorithmus als TKIP.	Auto
PSK Password (PSK-Passwort)	Geben Sie das Passwort für den Pre-shared Key (PSK) ein. Geben Sie 8 bis 63 Zeichen ein.	Null
Radius Authentication server address (Adresse des RADIUS-Authentifizierungsservers)	Vom RADIUS-Server verwendete Adresse.	Null
Radius Authentication server port (Port des RADIUS-Authentifizierungsservers)	Vom RADIUS-Server verwendeter Port.	1812
Radius Authentication server shared key (Gemeinsamer Schlüssel des RADIUS-Authentifizierungsservers)	Zwischen dem RADIUS-Client und dem RADIUS-Server wird eine vertrauenswürdige Verbindung hergestellt, und der Austausch von Authentifizierungsnachrichten wird durch den gemeinsamen Schlüssel gewährleistet.	Null



Advanced Settings (Erweiterte Einstellungen)		
Punkt	Beschreibung	Standard
Maximum number of access points (Maximale Anzahl von Zugangspunkten)	Legt die maximale Anzahl von Clients fest, die auf den Geräte-AP zugreifen dürfen. (Der Wert 0 bedeutet keine Begrenzung.)	64
Signal interval (Signalintervall)	Legt den Signalintervall fest, in dem der Geräte-AP Beacon-Nachrichten sendet, die zur Anzeige des Vorhandenseins eines drahtlosen Netzwerks verwendet werden.	100
DTIM cycle (DTIM-Zyklus)	Legen Sie den Zeitraum für die Delivery Traffic Indication Message fest, d. h. Übermittlung von Übertragungsanweisungs-informationen. DTIM wird im Energiesparmodus verwendet. Geräte-APs senden basierend auf diesem Intervall Multicast-Verkehr.	2
RTS / CTS threshold (RTS/CTS-Schwelle)	Legen Sie die Request to Send-Schwelle fest, also die Schwelle für Sendeanfragen. Wenn der Schwellenwert auf 2347 eingestellt ist, sendet der Geräte-AP vor dem Senden von Daten keine Erkennungssignale; wenn der Schwellenwert auf 0 eingestellt ist, muss der Geräte-AP vor dem Senden von Daten Erkennungssignale senden.	2347
Fragmentation threshold (Fragmentierungsschwelle)	Legen Sie den Paketschwellenwert für WiFi-AP-Pakete fest. Die empfohlene Standardeinstellung ist 2346.	2346
Transmission rate (Übertragungsrate)	Datenübertragungsraten können automatisiert oder standardmäßig festgelegt werden. Wählen Sie aus „Auto“, „1Mbps“, „2Mbps“, „5.5Mbps“, „6Mbps“, „11Mbps“, „12Mbps“, „18Mbps“, „24Mbps“, „36Mbps“, „48Mbps“ oder „54Mbps“.	Auto
Enable WMM (WMM aktivieren)	Klicken Sie auf den Schalter, um die WMM-Option zu aktivieren/ deaktivieren.	ON (EIN)
Enable Short GI (Kurzes Schutzintervall aktivieren)	Klicken Sie auf den Schalter, um das kurze Schutzintervall zu aktivieren/ deaktivieren. Es ist die Leerperiode zwischen zwei Symbolen und bietet Pufferzeit für die Signalverzögerung. Die Verwendung eines kurzen Schutzintervalls kann die Datenrate um 11 % erhöhen, kann aber auch zu höheren Paketfehlerraten führen.	ON (EIN)
Enable AP isolation (AP-Isolation aktiveren)	Klicken Sie auf den Schalter, um die Option AP-Isolation zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, werden alle angeschlossenen drahtlosen Geräte, auf die nicht direkt über das WLAN zugegriffen werden kann, isoliert.	OFF (AUS)
Commissioning level (Inbetriebnahme-Level)	Wählen Sie das Debugging-Level aus. Wählen Sie aus „verbose“ („ausführlich“), „debug“ („Debugging“), „info“ („Information“), „notice“ („Hinweis“), „warning“ („Warnung“) oder „none“ („kein“).	none (kein)

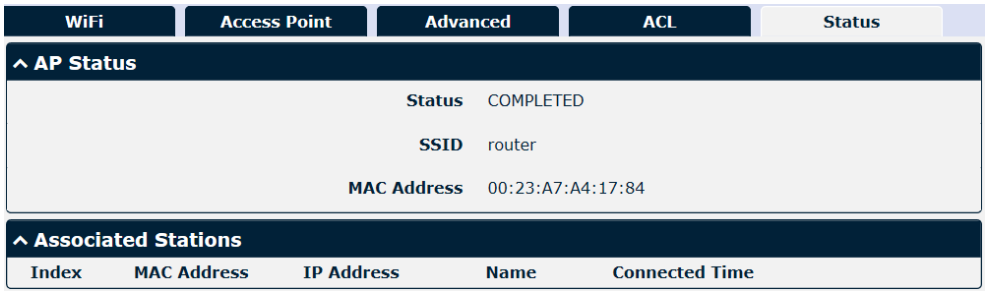


Klicken Sie auf +, um der Access Control List eine MAC-Adresse hinzuzufügen. Die maximale Anzahl an MAC-Adressen beträgt 64.



ACL		
Punkt	Beschreibung	Standard
General Settings (Allgemeine Einstellungen)		
Enable ACL (ACL aktivieren)	Klicken Sie auf den Schalter, um die Option ACL (Access Control List) zu aktivieren.	OFF (AUS)
ACL Mode (ACL-Modus)	Wählen Sie aus „Accept“ („Zulassen“) oder „Deny“ („Ablehnen“). Accept (Zulassen): Nur die Pakete, die zu den Entitäten der „Access Control List“ passen, werden zugelassen. Deny (Ablehnen): Alle Pakete, die zu den Entitäten der „Access Control List“ passen, werden abgelehnt. Hinweis: Router können nur Geräte zulassen oder ablehnen, die zu einem bestimmten Zeitpunkt in der „Access Control List“ enthalten sind.	Accept (Zulassen)
Access Control List		
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Beschreibung	Geben Sie eine Beschreibung für diese Access Control List ein.	Null
MAC Address (MAC-Adresse)	Fügen Sie hier eine MAC-Adresse hinzu.	Null

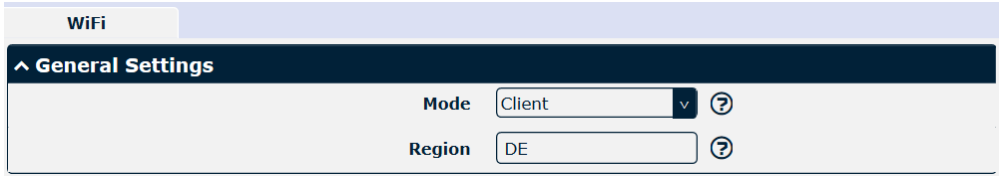
In diesem Abschnitt können Sie den Status des AP einsehen.



Hinweis: Die WiFi-Funktion ist am Router standardmäßig deaktiviert. Wenn Sie die Funktion verwenden müssen, schalten Sie bitte WiFi gemäß den folgenden Schritten ein und konfigurieren Sie den Router als WiFi-Client.

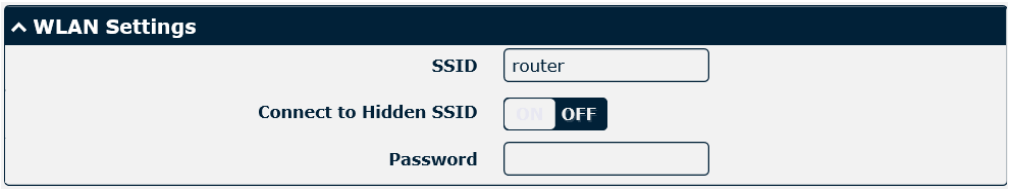
Wi-Fi-Client

Konfigurieren Sie den DSR-211 als Wi-Fi-Client. Klicken Sie auf Interface (Schnittstelle) > Wi-Fi > Wi-Fi, wählen Sie „Client“ als Modus und klicken Sie auf Submit („Übermitteln“) > Save & Apply (Speichern & Übernehmen).



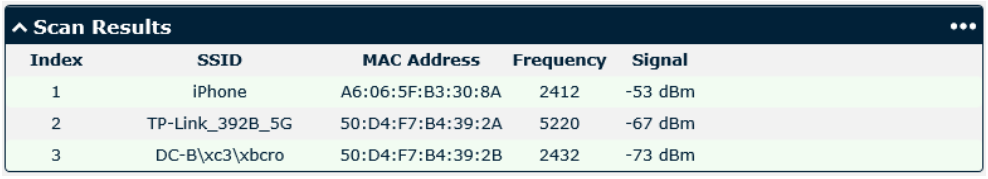
In der Schnittstellenliste erscheint dann eine Spalte „WLAN“.

Klicken Sie auf Interface (Schnittstelle) > Link Manager > Link Settings (Link-Einstellungen), klicken Sie auf die Bearbeiten-Schaltfläche von WLAN, und konfigurieren Sie dann die entsprechenden Parameter des WLANs.



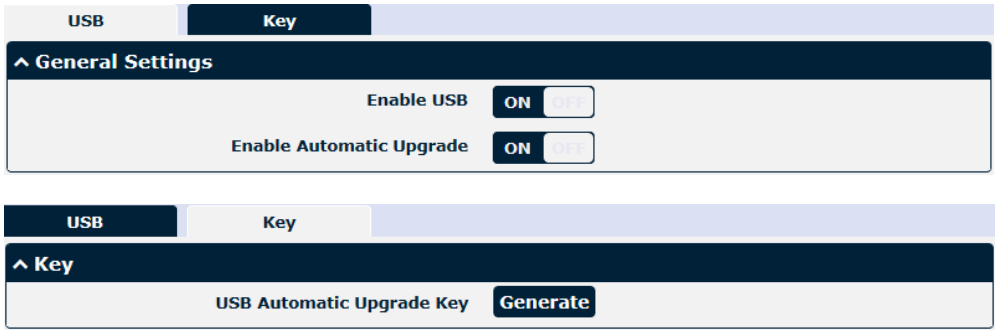
Klicken Sie auf Interface (Schnittstelle) > WLAN, um die Parameter des WiFi-Clients zu konfigurieren, nachdem Sie den Modus als Client eingestellt haben. Bitte denken Sie daran, nach Abschluss der Konfiguration auf Save & Apply (Speichern & Übernehmen) > Reboot (Neustart) zu klicken, damit die Konfiguration wirksam wird.

In diesem Fenster können Sie nach allen verfügbaren SSIDs in Ihrem Gebiet scannen und auf eine der in der Liste „Scan Results“ („Scanergebnisse“) angezeigten SSIDs klicken.



3.11 Schnittstelle > USB

In diesem Abschnitt können Sie die USB-Parameter einstellen. Die USB-Schnittstelle des DSR-211 Routers kann für Firmware- und Konfigurations-Upgrades verwendet werden.

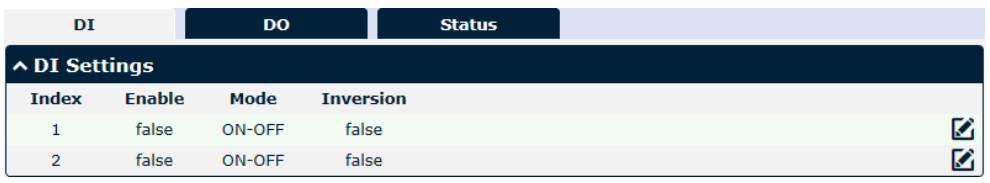


General Settings @ USB (Allgemeine Einstellungen unter USB)		
Punkt	Beschreibung	Standard
Enable USB (USB aktivieren)	Klicken Sie auf den Schalter, um die USB-Option zu aktivieren/ deaktivieren.	ON (EIN)
Enable Automatic Firmware Updating (Automatische Firmware-Aktualisierung aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option, um die Firmware des DSR-211 automatisch zu aktualisieren, wenn ein USB-Speichergerät mit DSR-211-Firmware eingesteckt wird.	ON (EIN)
Key (Schlüssel)		
USB Automatic Update Key (USB-Schlüssel für automatische Aktualisierung)	Klicken Sie auf Generate (Generieren), um einen Schlüssel zu generieren. Dieser wird verwendet, um die Schlüsseldatei auf der U-Disk zu verifizieren. Wenn sie konsistent ist, kann das Upgrade erfolgen.	--

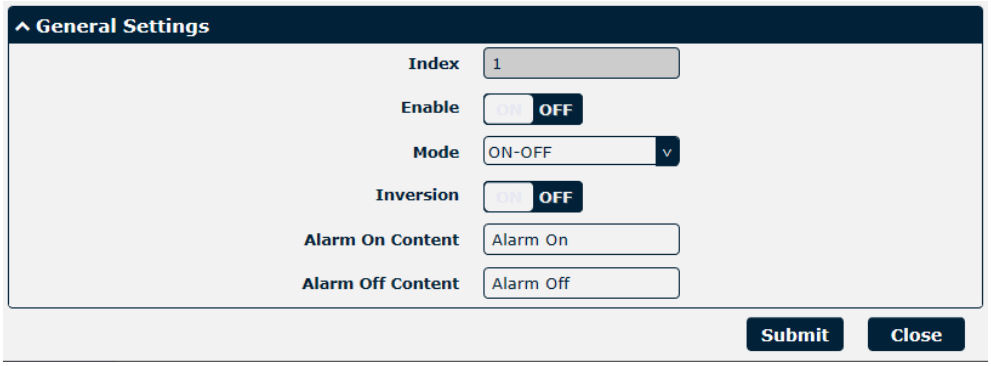
3.12 Schnittstelle > DI / DO

In diesem Abschnitt können Sie die DI/ DO-Parameter einstellen. Digital Input und Digital Output sind die spezifischen Schnittstellen für den DSR-211. Die DI-Schnittstelle kann zur Alarmauslösung verwendet werden, während die DO-Schnittstelle zur Steuerung des Slave-Gerätes verwendet werden kann, um eine Echtzeitüberwachung zu realisieren.

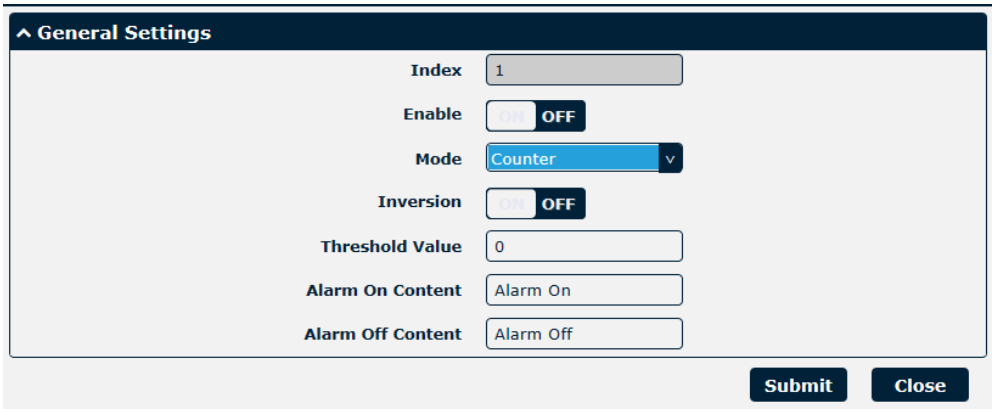
DI



Klicken Sie die Schaltfläche ganz rechts . in der Zeile Index 1.
Der Standardmodus (Mode) ist „ON-OFF“ („EIN-AUS“).



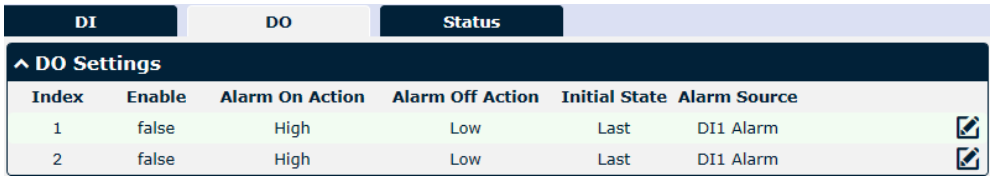
Wenn Sie als Modus „Counter“ („Zähler“) wählen, wird das Fenster wie unten dargestellt.



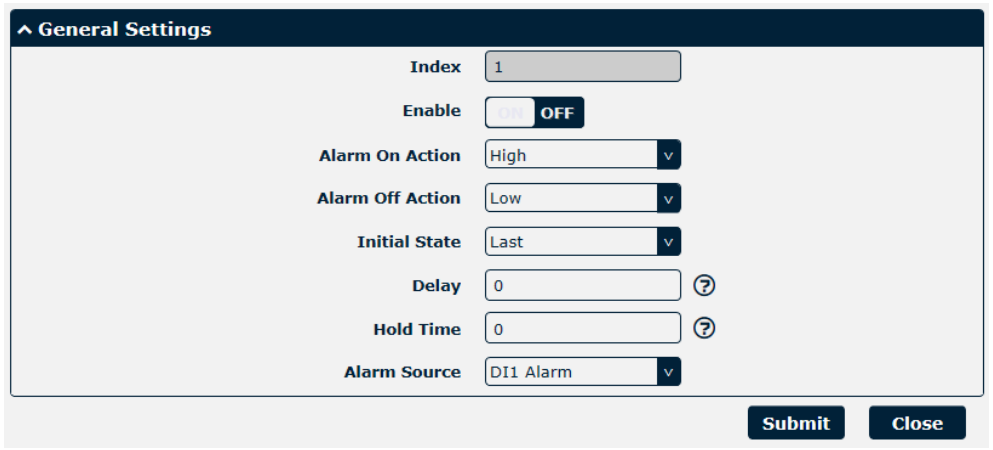
General Settings @ DI (Allgemeine Einstellungen unter DI)		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Enable (Aktivieren)	Klicken Sie auf den Schalter, um dieses DI zu aktivieren/ deaktivieren.	OFF (AUS)
Mode (Modus)	Wählen Sie aus „ON-OFF“ („EIN-AUS“) oder „Counter“ („Zähler“). ON-OFF (EIN-AUS): Die DI-Schnittstelle unterstützt ON- und OFF-Modus (EIN und AUS) (hoher oder niedriger elektrischer Pegel) zum Auslösen eines DI-Alarms. Der Modus ist standardmäßig auf ON (EIN) eingestellt und der Modus OFF (AUS) ist nur verfügbar, wenn die Invertierungsfunktion aktiviert ist. ON (EIN) – In diesem Modus wird der DI-Alarmstatus auf ON (EIN) gesetzt, wenn die DI-Schnittstelle von GND geöffnet wird oder ein hoher elektrischer Pegel eingegeben wird (Logik 1). Im Gegensatz dazu wird der DI-Alarmstatus auf OFF (AUS) gesetzt, wenn die DI-Schnittstelle mit GND verbunden wird oder ein niedriger elektrischer Pegel (Logik 0) eingegeben wird. OFF (AUS) – In diesem Modus wird der DI-Alarmstatus auf ON (EIN) gesetzt, wenn die DI-Schnittstelle mit GND verbunden wird oder ein niedriger elektrischer Pegel eingegeben wird (Logik 0). Im Gegensatz dazu wird der DI-Alarmstatus auf OFF (AUS) gesetzt, wenn die DI-Schnittstelle von GND geöffnet wird oder ein hoher elektrischer Pegel (Logik 1) eingegeben wird. Counter (Zähler): Ereigniszähler-Modus	ON-OFF (EIN-AUS)
Inversion (Umkehrung)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Ermöglicht die Einstellung des DI-Modus als OFF-Modus (AUS).	OFF (AUS)
Threshold Value (Schwellenwert)	Legen Sie den Schwellenwert fest. Alarm wird ausgelöst, wenn der Ereigniszähler diesen Wert erreicht. Nach Auslösen des Alarms zählt DI weiter, löst aber keinen Alarm mehr aus. Geben Sie 0 bis 65535 Ziffern ein. (0 = wird keinen Alarm auslösen) Hinweis: Diese Option ist nur verfügbar, wenn DI im Modus „Counter“ („Zähler“) betrieben wird.	Null
Alarm On Content (Alarm-Ein-Inhalt)	Wenn der Alarm ausgelöst wird, wird der Inhalt angezeigt.	Alarm On (Alarm
Alarm Off (Alarm-Aus-Inhalt)	Wenn der Alarm ausgeschaltet wird, wird der Inhalt angezeigt.	Alarm Off (Alarm Aus)

Hinweis: Die Einstellung ist standardmäßig „High“-Alarm, nach Aktivierung der Schaltfläche „Inversion“ („Umkehr“) wechselt die Einstellung auf „Low“-Alarm.

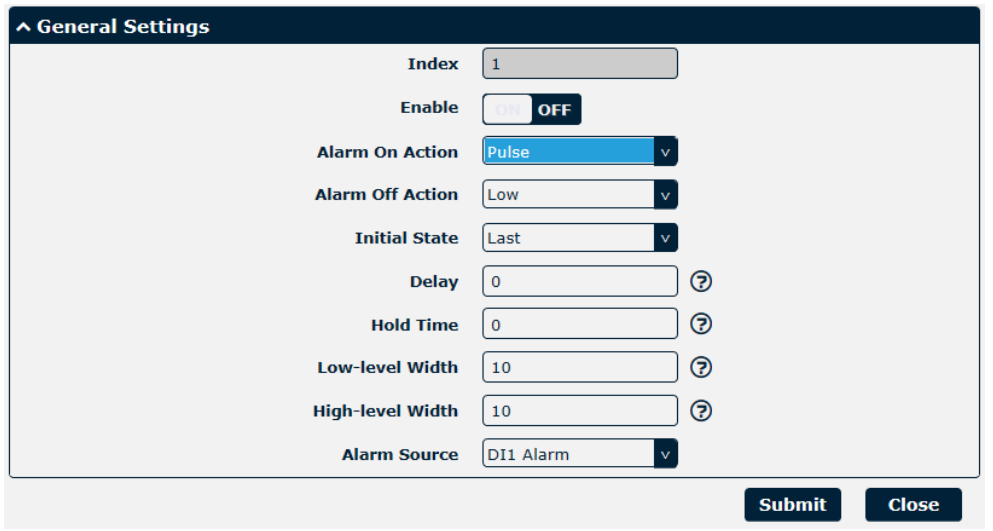
DO



Klicken Sie auf , um das DO-Konfigurationsfenster zu öffnen.



Das Fenster wird wie unten dargestellt, wenn Sie „Pulse“ („Impuls“) als Alarm-Ein-Aktion wählen.



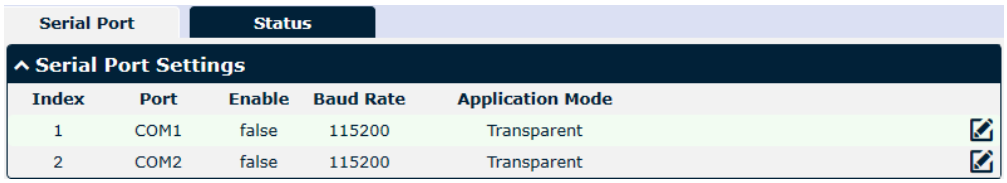
DO		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Enable (Aktivieren)	Klicken Sie auf den Schalter, um dieses DO zu aktivieren/ deaktivieren.	OFF (AUS)
Alarm On Action (Alarm-ein-Aktion)	Der Digitalausgang wird bei einem Alarm ausgelöst. Die Auswahl erfolgt aus „High“ („Hoch“), „Low“ („Niedrig“) oder „Pulse“ („Impuls“). High (Hoch): ein hoher elektrischer Ausgangspegel Low (Niedrig): ein niedriger elektrischer Ausgangspegel Pulse (Impuls): Erzeugt beim Auslösen eine Rechteckwelle, wie in den Impulsmodus-Parametern angegeben	High (Hoch)
Alarm Off Action (Alarm-aus-Aktion)	Der Digitalausgang wird ausgelöst, wenn der Alarm aufgehoben wird. Die Auswahl erfolgt aus „High“ („Hoch“), „Low“ („Niedrig“) oder „Pulse“ („Impuls“). High (Hoch): ein hoher elektrischer Ausgangspegel Low (Niedrig): ein niedriger elektrischer Ausgangspegel Pulse (Impuls): Erzeugt beim Auslösen eine Rechteckwelle, wie in den Impulsmodus-Parametern angegeben	Low (Niedrig)
Initial State (Anfangszustand)	Geben Sie den Status des Digitalausgangs beim Einschalten an. Die Auswahl erfolgt aus „Last“ („Zuletzt“), „High“ („Hoch“) oder „Low“ („Niedrig“). Last (Zuletzt): Der Status der DO entspricht dem Status beim letzten Ausschalten. High (Hoch): DO-Schnittstelle ist auf hohem elektrischem Pegel. Low (Niedrig): DO-Schnittstelle ist auf niedrigem elektrischem Pegel.	Low (Niedrig)
Delay (Verzögerung)	Stellen Sie die Verzögerungszeit für den DO-Alarmstart ein. Der erste Impuls wird nach einer „Delay“ („Verzögerung“) erzeugt. Geben Sie einen Wert zwischen 0 und 30000 ms ein. (0 = Impuls ohne Verzögerung erzeugen)	0
Hold Time (Haltezeit)	Legen Sie die Haltezeit des DO-Status (Alarm On Action / Alarm Off Action) fest. Wenn die Aktionszeit diese festgelegte Zeit erreicht, stoppt DO die Aktion. Geben Sie einen Wert zwischen 0 und 255 Sekunden ein. (0 = weitermachen bis zur nächsten Aktion)	0
Low-level Width (Niedrige Pulsbreite)	Stellen Sie die niedrige Pulsbreite ein. Diese Option ist verfügbar, wenn Pulse (Impuls) als „Alarm On Action“ („Alarm-Ein-Aktion“) / „Alarm Off Action“ („Alarm-Aus-Aktion“) aktiviert wird. Im Impuls-Ausgabemodus erzeugt der ausgewählte digitale Ausgangskanal eine Rechteckwelle entsprechend den Festlegungen in den Impulsmodus-Parametern. Die niedrigen Pulsbreiten werden hier angegeben. Geben Sie einen Wert zwischen 1 und 30000 ms ein.	10
High-level Width (Hohe Pulsbreite)	Legen Sie die hohe Pulsbreite fest. Diese Option ist verfügbar, wenn Pulse (Impuls) als „Alarm On Action“ („Alarm-Ein-Aktion“) / „Alarm Off Action“ („Alarm-Aus-Aktion“) aktiviert wird. Im Impuls-Ausgabemodus erzeugt der ausgewählte digitale Ausgangskanal eine Rechteckwelle entsprechend den Festlegungen in den Impulsmodus-Parametern. Die hohen Pulsbreiten werden hier angegeben. Geben Sie einen Wert zwischen 1 und 30000 ms ein.	10
Alarm Source (Alarmquelle)	Der Digitalausgang wird entsprechend der verschiedenen Alarmquellen initiiert. Wählen Sie aus „DI1 Alarm“ und „DI2 Alarm“. DI1/ DI2 Alarm: Digitalausgang löst die entsprechende Aktion aus, wenn ein Alarm vom Digitaleingang vorliegt.	DI1 Alarm

Status

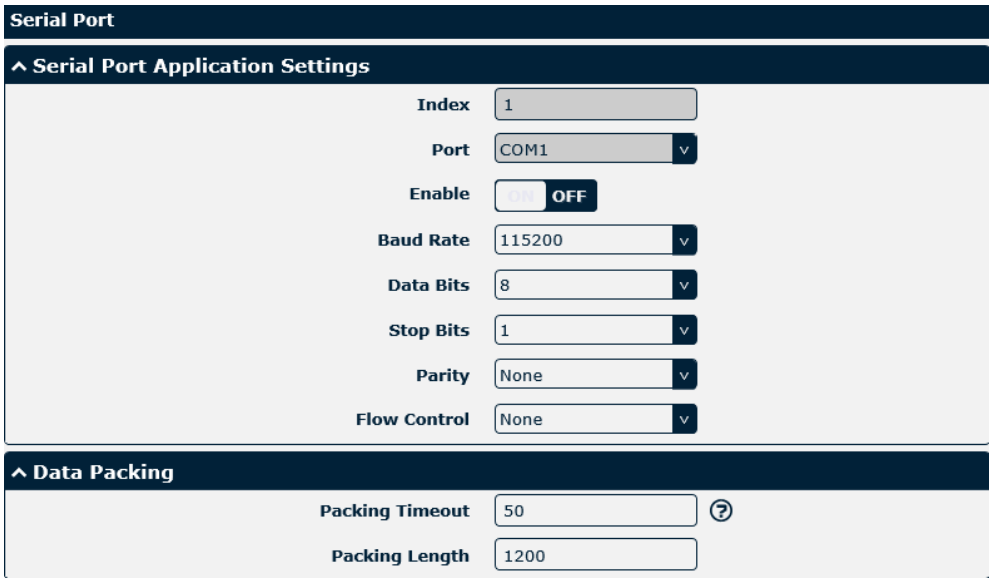
In diesem Fenster können Sie den Status der DO- und DI-Schnittstelle anzeigen. Hier kann auch der Zähleralarm von DI gelöscht werden. Klicken Sie auf die Schaltfläche Clear, um die monatlichen DI1- oder DI2-Nutzungsstatistiken für Zähleralarm zu löschen.

3.13 Schnittstelle > Serielle Schnittstelle

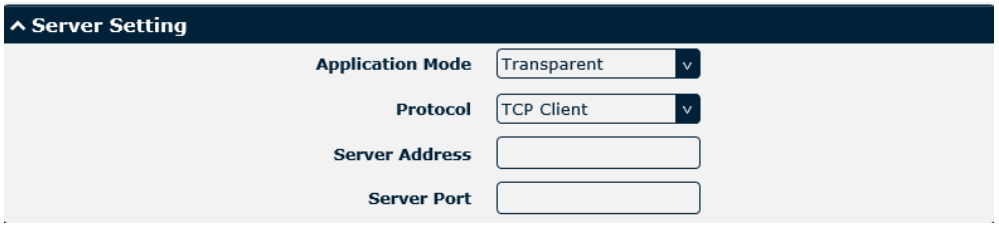
In diesem Abschnitt können Sie die Parameter der seriellen Schnittstelle einstellen. Der DSR-211 Router unterstützt eine COM1 und eine COM2, kann aber auch als zwei COM1 oder zwei COM2 konfiguriert werden.



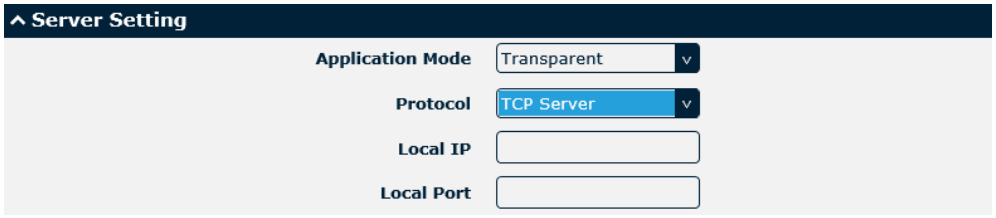
Klicken Sie auf die Schaltfläche auf der rechten Seite von COM1 und das Popup-Fenster wird wie folgt dargestellt:



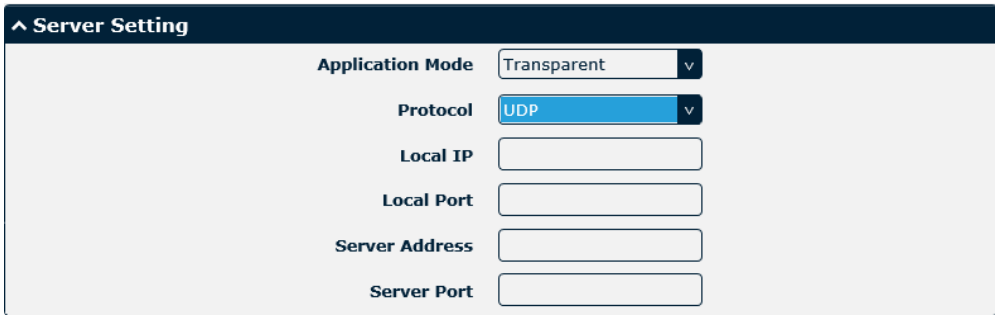
Das Fenster wird wie folgt dargestellt, wenn Sie „Transparent“ als Anwendungsmodus und TCP Client als Protokoll wählen.



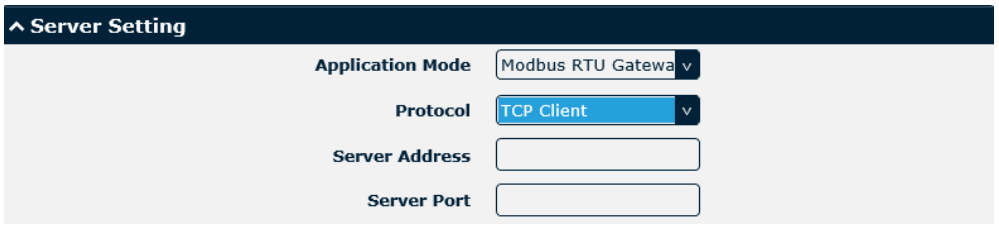
Das Fenster wird wie folgt dargestellt, wenn Sie „Transparent“ als Anwendungsmodus und TCP Server als Protokoll wählen.



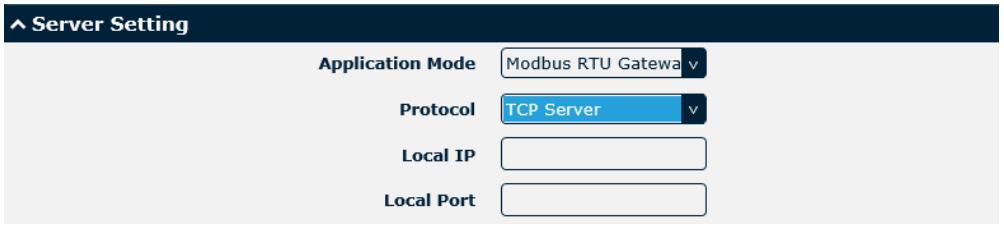
Das Fenster wird wie folgt dargestellt, wenn Sie „Transparent“ als Anwendungsmodus und UDP als Protokoll wählen.



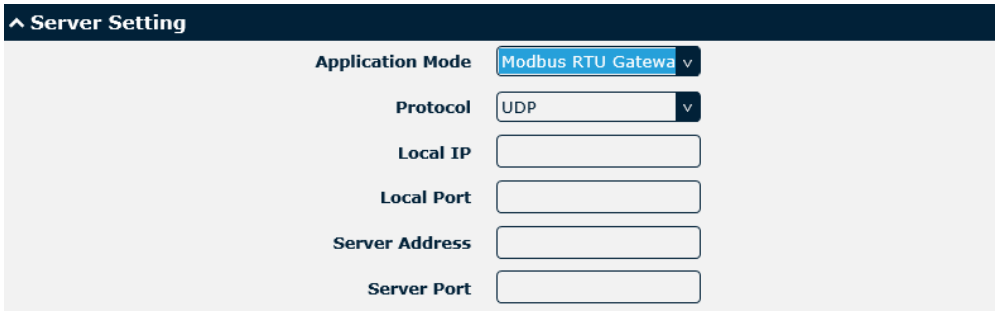
Das Fenster wird wie folgt dargestellt, wenn Sie „Modbus RTU Gateway“ als Anwendungsmodus und TCP Client als Protokoll wählen.



Das Fenster wird wie folgt dargestellt, wenn Sie „Modbus RTU Gateway“ als Anwendungsmodus und TCP Server als Protokoll wählen.



Das Fenster wird wie folgt dargestellt, wenn Sie „Modbus RTU Gateway“ als Anwendungsmodus und UDP als Protokoll wählen.



Serial Port (Serielle Schnittstelle)		
Punkt	Beschreibung	Standard
Serial Port Application Settings (Anwendungseinstellungen für die serielle Schnittstelle)		
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Port	Zeigt den Namen der aktuellen seriellen Schnittstelle an, schreibgeschützt.	--
Enable (Aktivieren)	Klicken Sie auf den Schalter, um diesen seriellen Port zu aktivieren/deaktivieren. Wenn der Status OFF (AUS) ist, ist der serielle Port nicht verfügbar.	OFF (AUS)
Baud Rate (Baudrate)	Wählen Sie aus „300“, „600“, „1200“, „2400“, „4800“, „9600“, „19200“, „38400“, „57600“, „115200“ oder „230400“.	115200
Data Bits (Daten-Bits)	Wählen Sie aus „7“ oder „8“.	8
Stop Bits (Stopp-Bits)	Wählen Sie aus „1“ oder „2“.	1
Parity (Parität)	Wählen Sie aus „None“ („Keine“), „Odd“ („Ungerade“) oder „Even“ („Gerade“).	None (Keine)

Flow control (Fluss-Steuerung)	Wählen Sie aus „None“ („Keine“), „Software“ oder „Hardware“.	None (Keine)
Data Packing (Datenpaketierung)		
Packing Timeout (Zeitüberschreitung beim Packen)	Legen Sie die Zeitüberschreitung beim Packen fest. Der serielle Port stellt die Daten in eine Warteschlange im Puffer und sendet die Daten an das Mobilfunk-WAN/ Ethernet-WAN, wenn die Intervall-Zeitüberschreitung im Feld erreicht ist. Hinweis: Daten werden auch dann entsprechend der Paketlänge gesendet, wenn die Daten die Intervall-Zeitüberschreitung im Feld nicht erreichen.	50
Packing Length (Paketlänge)	Legen Sie die Paketlänge fest. Die Einstellung der Paketlänge bezieht sich auf die maximale Datenmenge, die sich vor dem Senden im Puffer des seriellen Ports ansammeln darf. Wenn eine Paketlänge zwischen 1 und 3000 Bytes angegeben ist, werden die Daten im Puffer gesendet, sobald sie die angegebene Länge erreichen.	1200
Server Settings (Server-Einstellungen)		
Application Mode (Anwendungsmodus)	Wählen Sie aus Transparent oder Modbus RTU Gateway. Transparent: Der Router überträgt die seriellen Daten transparent. Modbus RTU Gateway: Der Router wandelt die Modbus-RTU-Daten in Modbus-TCP-Daten um und sendet diese (und umgekehrt).	Transparent
Protocol (Protokoll)	Wählen Sie aus TCP Client, TCP Server und UDP. TCP Client: Der Router arbeitet als TCP-Client, initiiert eine TCP-Verbindung zum TCP-Server. Die Serveradresse unterstützt sowohl IP als auch Domänennamen. TCP Server: Der Router arbeitet als TCP-Server und wartet auf Verbindungsanfragen von TCP-Clients. UDP: Der Router arbeitet als UDP-Client.	TCP Client
Serial Port Application Settings (Anwendungseinstellungen für die serielle Schnittstelle)		
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Server Address (Server-Adresse)	Geben Sie die Adresse des Servers ein, der die vom seriellen Port des Routers gesendeten Daten empfängt. Möglich sind IP-Adresse oder Domänenname.	Null
Server Port	Geben Sie den spezifizierten Port des Servers ein, der für den Empfang der seriellen Daten verwendet wird.	Null
Local IP @ Transparent	Geben Sie die LAN-IP des Routers ein, die an den Internet-Port des Routers weitergeleitet wird.	Null
Local Port @ Transparent	Geben Sie den Port der LAN-IP des Routers ein.	Null
Local IP @ Modbus	Geben Sie die lokale IP unter Modbus-Modus ein.	Null
Local Port @ Modbus	Geben Sie den lokalen Port unter Modbus-Modus ein.	Null

Klicken Sie auf die Spalte „Status“, um den aktuellen seriellen Anschlusstyp anzuzeigen.

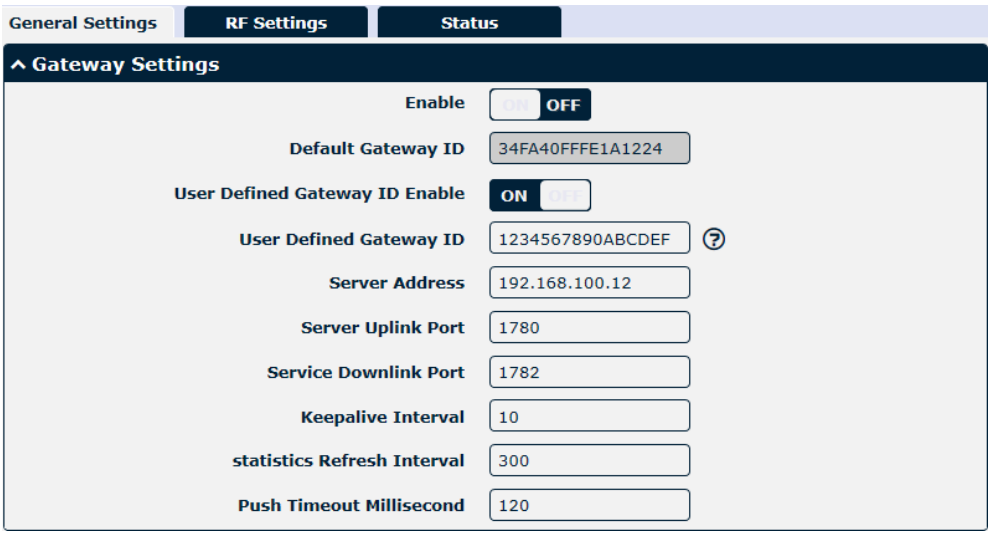
3.14 Schnittstelle > LoRa

In diesem Abschnitt können Sie die LoRaWAN-Parameter einstellen.

Hinweis: Für die Nutzung von LoRA wird eine spezielle Firmware benötigt. Einige APP's funktionieren unter dieser Firmware nicht. Bitte sprechen Sie uns an, sollten Sie Hilfe benötigen.

General Settings (Allgemeine Einstellungen)

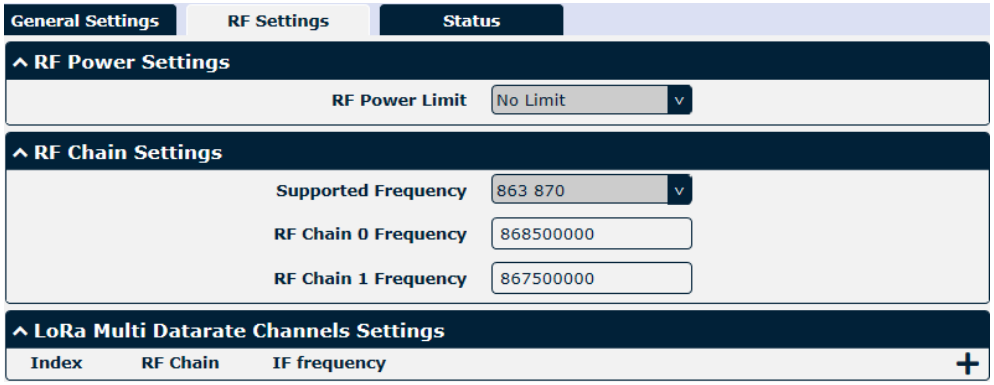
Klicken Sie auf „General Settings" („Allgemeine Einstellungen") > „Gateway Settings" („Gateway-Einstellungen"), um Ihre Knotenparameter zu konfigurieren. Im Folgenden sehen Sie ein Beispiel:



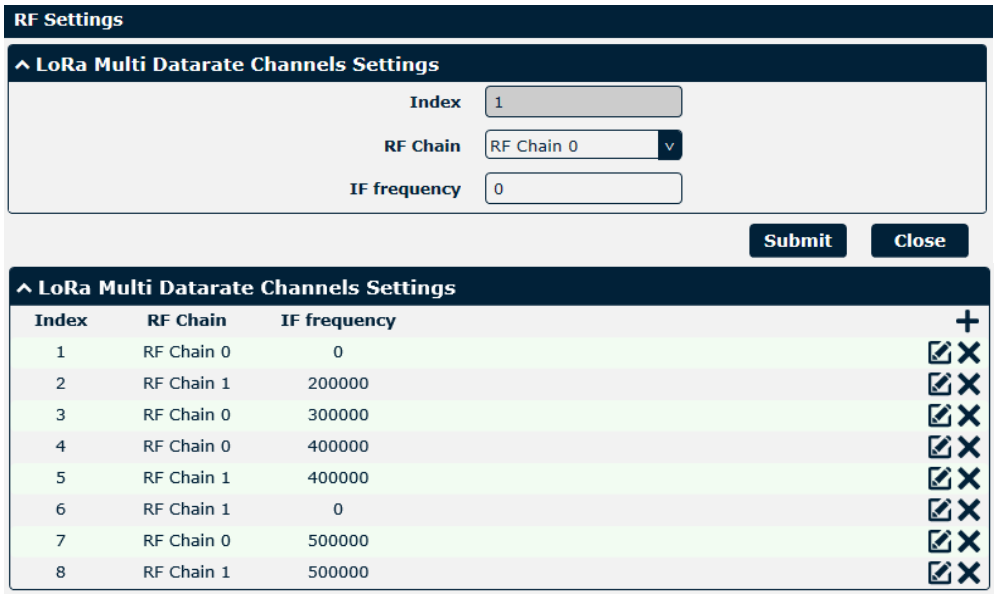
Gateway Settings (Gateway-Einstellungen)		
Punkt	Beschreibung	Standard
Enable (Aktivieren)	Klicken Sie auf den Schalter, um die LoRaWAN-Weiterleitung des Gateways zu aktivieren/deaktivieren.	OFF (AUS)
Default Gateway ID (Standard-Gateway-ID)	Legen Sie die Standard-Gateway-ID fest. Sie können die Gateway-ID auch mit einer eindeutigen 64-Bit-Sequenz selbst definieren.	Null
User Defined Gateway ID Enable (Benutzerdefinierte	Klicken Sie auf den Schalter, um diese Option zu aktivieren/deaktivieren.	OFF (AUS)
User Defined Gateway ID (Benutzerdefinierte	Geben Sie Ihre definierte Gateway-ID ein.	Null
Server Address (Server-Adresse)	Geben Sie die Remote-IP des LoRaWAN-Servers ein.	Null
Server Uplink Port (Server-Uplink-Port)	Geben Sie den Port des LoRaWAN-Servers zum Hochladen von Daten ein.	Null
Server Downlink Port (Server-Downlink-Port)	Geben Sie den Port des LoRaWAN-Servers an, um Daten an Ihr Gateway zu senden.	Null

Keepalive Interval (Keepalive-Intervall)	Geben Sie das Intervall des Keepalive-Pakets ein, das vom Gateway zum LoRaWAN-Server gesendet wird, um die Verbindung stabil und aufrecht zu halten.	Null
Statistics Refresh Interval (Statistik-Aktualisierungsintervall)	Geben Sie das Intervall zum Aktualisieren des Statistikstatus Ihres Gateways ein.	Null
Push Timeout Millisecond (Push-Zeitüberschreitung Millisekunden)	Geben Sie die Zeitüberschreitung für das Warten auf die Antwort vom Server ein, nachdem das Gateway Modusdaten gesendet hat, gemessen in ms.	Null

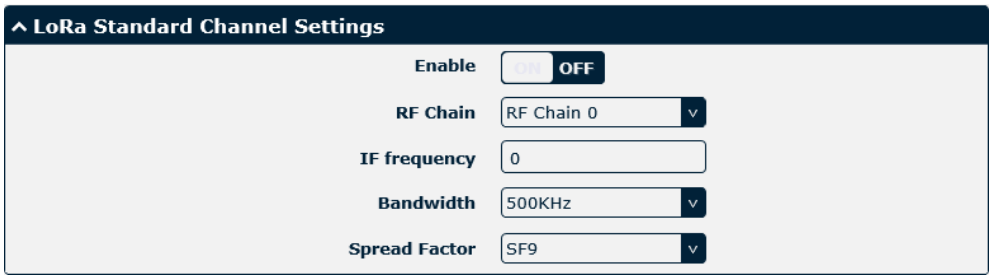
RF Settings (HF-Einstellungen)



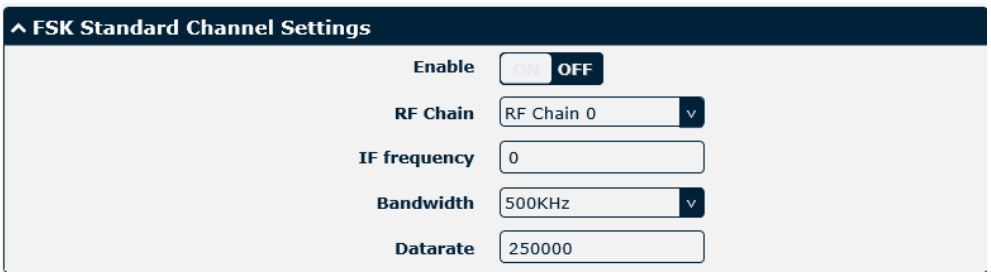
Klicken Sie auf +, um einen Kanal hinzuzufügen. Die maximale Anzahl beträgt 8.



Verwenden Sie den LoRa-Standardkanal, um die Kommunikation zwischen Knoten und Gateway herzustellen.



Verwenden Sie die FSK-Modulation anstelle von LoRa.

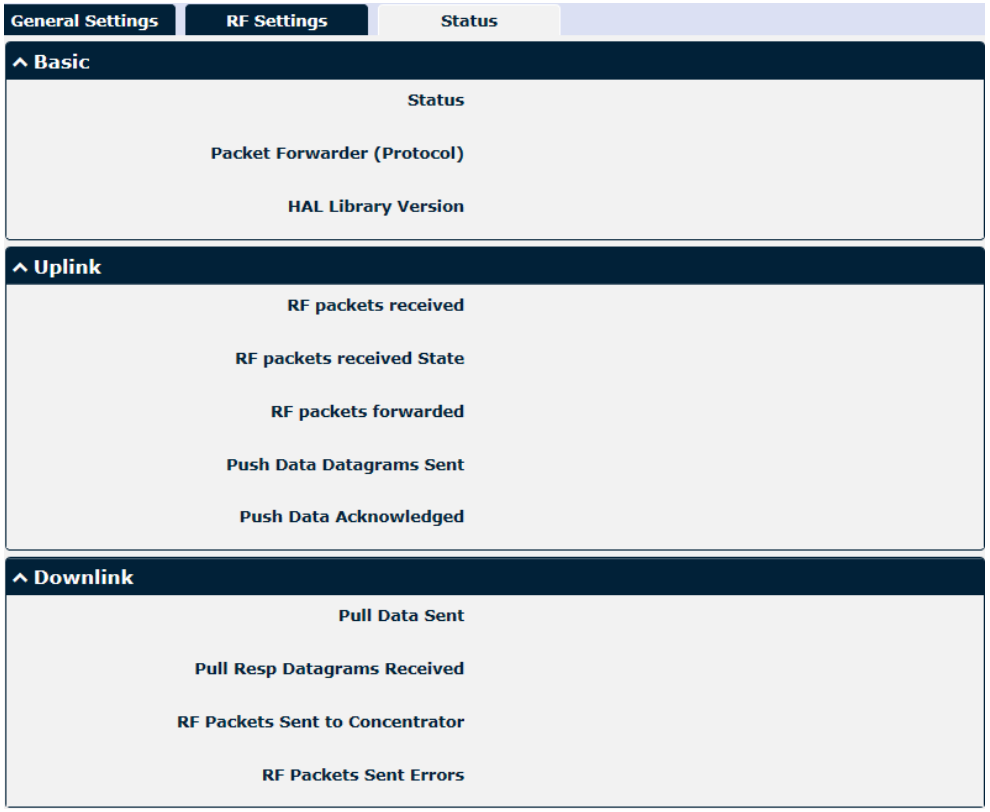


RF Settings (HF-Einstellungen)		
Punkt	Beschreibung	Standard
RF Power Settings (HF-Leistungseinstellungen)		
RF Power Limit (HF-Leistungsbegrenzung)	Wird zur Angabe der maximalen Sendeleistung für das aktuelle Gateway verwendet. No_Limit (Keine Begrenzung): Die Sendeleistung ist nicht begrenzt, abhängig von dem vom LoRaWAN-Server gesendeten Sendeleistungswert. EU_433: Die maximale Sendeleistung ist auf 10 dBm oder weniger begrenzt. EU_868_870: Die maximale Sendeleistung ist auf 14 dBm oder weniger begrenzt. CN_470_510: Die maximale Sendeleistung ist auf 17 dBm oder weniger begrenzt. US_902_928: Die maximale Sendeleistung ist auf 26 dBm oder weniger begrenzt. AU_915_928: Maximale Sendeleistungsgrenze liegt unter 26 dBm. AS_923: Die maximale Sendeleistung ist auf 14 dBm oder weniger begrenzt. KR_920_923: Die maximale Sendeleistung ist auf 23 dBm oder weniger begrenzt. Max_Power (Max. Leistung): Nutzt die maximale Sendeleistung, die etwa 24,5 dBm beträgt. Hinweis: Die oben genannten Optionen sind nicht konfigurierbar und müssen vor der Auslieferung eingestellt werden.	No Limit (Keine Beschränkung)
RF Chain Settings (HF-Ketten-Einstellungen)		
Supported Frequency (Unterstützte Frequenz)	Wählen Sie die unterstützte Frequenz in Abhängigkeit vom LoRaWAN-Modul.	863870
RF Chain 0 Frequency (Frequenz HF-Kette 0)	Geben Sie die Mittenfrequenz des Funk-Transceivers 0 ein, der das Senden und Empfangen unterstützt.	Null
RF Chain 1 Frequency (Frequenz HF-Kette 1)	Geben Sie die Mittenfrequenz des Funktransceivers 1 ein, der nur das Empfangen von Daten von Knoten unterstützt.	Null
LoRa Multi Datarate Channels Settings (Einstellungen für LoRa-Kanäle mit mehreren Datenraten)		
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
RF Chain (HF-Kette)	Wählen Sie Chain 0 oder Chain 1 als HF-Kette.	RF Chain 0

IF frequency (IF-Frequenz)	Geben Sie die IF-Frequenz ein, gemessen in Hz. Der Versatz zwischen der Mittenfrequenz eines bestimmten Kanals und der Mittenfrequenz der Kette beträgt 0/1. Beispiel: HF-Kette 0, IF-Frequenz: -20000. Das bedeutet, dass die Mittenfrequenz dieses Kanals 868300000 = 868500000 - 200000 sein sollte.	0
LoRa Standard Channel Settings (LoRa Standard-Kanal-Einstellungen)		
Enable (Aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren.	OFF (AUS)
RF Chain (HF-Kette)	Wählen Sie Chain 0 oder Chain 1 als HF-Kette.	Chain 0
RF Settings (HF-Einstellungen)		
IF frequency (IF-Frequenz)	Geben Sie die IF-Frequenz mit einem Wert von -500000 bis 500000 ein, gemessen in Hz. Der Versatz zwischen der Mittenfrequenz eines bestimmten Kanals und der Mittenfrequenz der Kette beträgt 0/1.	0
Bandwith (Bandbreite)	Wählen Sie die wählbare Bandbreite, gemessen in kHz.	500KHz
Spread Factor (Spreizfaktor)	Geben Sie den wählbaren Spreizfaktor ein. Der Kanal mit großem Spreizfaktor entspricht einer niedrigen Rate, während der Kanal mit kleinem Spreizfaktor einer hohen Rate entspricht.	250000
FSK Standard Channel Settings (FSK-Standard-Kanal-Einstellungen)		
Enable (Aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren.	OFF (AUS)
RF Chain (HF-Kette)	Wählen Sie Chain 0 oder Chain 1 als HF-Kette.	Chain 0
IF frequency (IF-Frequenz)	Geben Sie die IF-Frequenz mit einem Wert von -500000 bis 500000 ein, gemessen in Hz. Der Versatz zwischen der Mittenfrequenz eines bestimmten Kanals und der Mittenfrequenz der Kette beträgt 0/1.	0
Bandwith (Bandbreite)	Wählen Sie die wählbare Bandbreite, gemessen in kHz.	500KHz
Datarate	Geben Sie die Datenrate im Wert von 500 bis 250000 ein, gemessen in Bit.	250000

Status

Klicken Sie auf „Status“, um Ihren Knotenstatus anzuzeigen.



Status	
Punkt	Beschreibung
Basic (Grundlegend)	
Status	Zeigt den LoRaWAN-Status Ihres Gateways an.
Packet Forwarder (Protokoll)	Zeigt die Version des Packet Forwarder an.
HAL Library Version (Version HAL-Bibliothek)	Zeigt die Treiberversion des LoRaWAN-Chipsatzes im Gateway an.
Uplink	
RF packets received (Empfangene HF-Pakete)	Zeigt die Anzahl der Datenpakete vom Knoten bis zum Gateway an.
RF packets received State (Zustand der empfangenen HF-Pakete)	Zeigt den Empfangsstatus der HF-Pakete an. CRC_OK: Prozentualer Anteil der CRC-Verifizierung CRC_Fail: Prozentualer Anteil des CRC-Versagens NO_CRC: Prozentualer Anteil an anormalen Paketen ohne CRC
RF packets forwarded (Weitergeleitete HF-Pakete)	CRC-geprüfte Pakete werden vom Gateway zum Server gesendet.
Push Data Datagrams Set (Push-Daten-Datagramm-Satz)	Die Gesamtmenge der vom Gateway zum Server gesendeten Pakete, einschließlich der weitergeleiteten HF-Pakete und Statistikpakete.

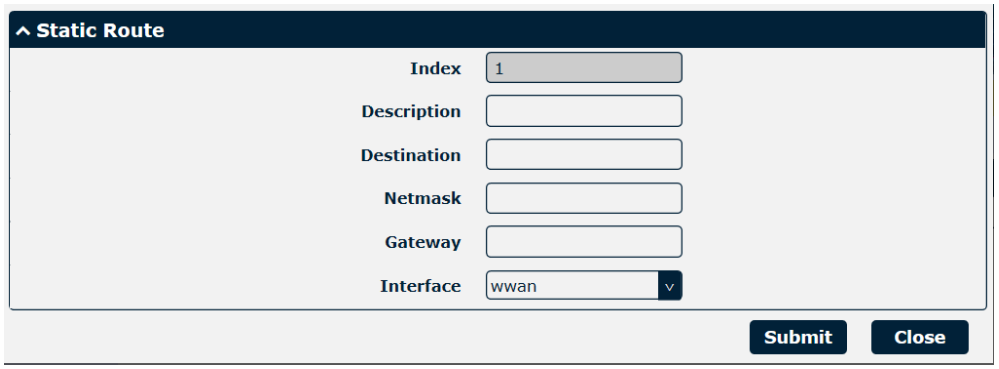
Push Data Acknowledged (Bestätigte Push-Daten)	Prozentualer Anteil der bestätigten Pakete unter den gesendeten Push-Daten.
Downlink	
Pull Data Sent (Gesendete Pull-Daten)	Zeigt die Anzahl der an den Server gesendeten Keepalive-Pakete und den Prozentsatz der Bestätigungspakete bezüglich der Keepalive-Pakete vom Server an.
Pull Resp Datagrams Received (Empfangene Pull-Resp-Datagramme)	Zeigt die Anzahl und Größe der Pakete an, die vom Server zum Gateway gesendet werden.
RF Packets Sent to Concentrator (An den Konzentrator gesendete RF-Pakete)	Zeigt die Anzahl und Größe der RF-Pakete an, die vom Gateway zum Knoten gesendet werden.
RF Packets Sent Errors (Fehler bei gesendeten HF-Paketen)	Zeigt die Anzahl der HF-Pakete an, die nicht vom Server zum Knoten gesendet werden können.

3.15 Netzwerk > Route

In diesem Abschnitt können Sie die statische Route festlegen. Statische Route ist eine Form des Routings, die auftritt, wenn ein Router einen manuell konfigurierten Routing-Eintrag verwendet und nicht Informationen aus einem dynamischen Routing-Verkehr entnimmt. Das Route Information Protocol (RIP) ist in kleinen Netzwerken mit stabiler Nutzungsrate weit verbreitet. Open Shortest Path First (OSPF) ist für Router innerhalb eines einzelnen autonomen Systems und wird in großen Netzwerken eingesetzt.

Static Route (Statische Route)

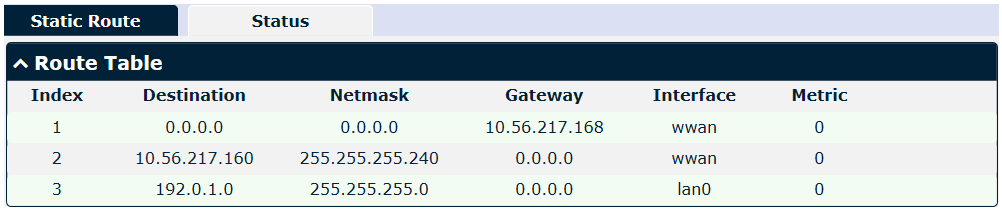
Klicken Sie auf + um eine statische Route hinzuzufügen. Die maximale Anzahl beträgt 20.



Static Route (Statische Route)		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Description (Beschreibung)	Geben Sie eine Beschreibung für diese Route ein.	Null
Destination (Ziel)	Geben Sie die IP-Adresse des Ziel-Hosts oder des Zielnetzes ein.	Null
Netmask/ IPv6 address Prefix Length (Präfix-Länge Netzmaske/IPv6-Adresse)	Geben Sie die Netzmaske des Ziel-Hosts oder des Zielnetzes ein.	Null
Gateway	Definieren Sie das Gateway des Ziels.	Null
Interface (Schnittstelle)	Wählen Sie den entsprechenden Port des Links, den Sie konfigurieren möchten.	wwan1

Status

In diesem Fenster können Sie den Status der Route einsehen.



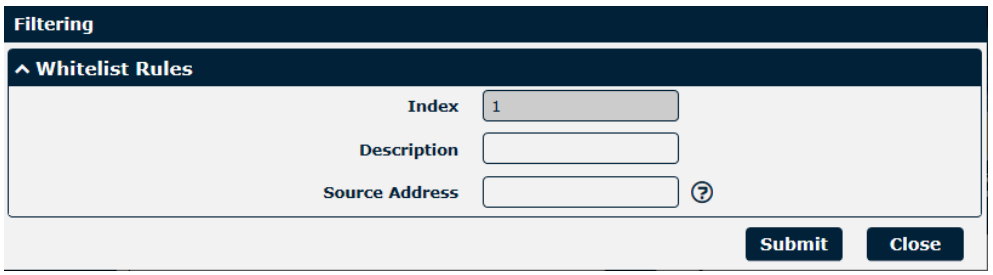
3.16 Netzwerk > Firewall

In diesem Abschnitt können Sie die Firewall und die zugehörigen Parameter einstellen, einschließlich Filterung, Port-Mapping und DMZ.

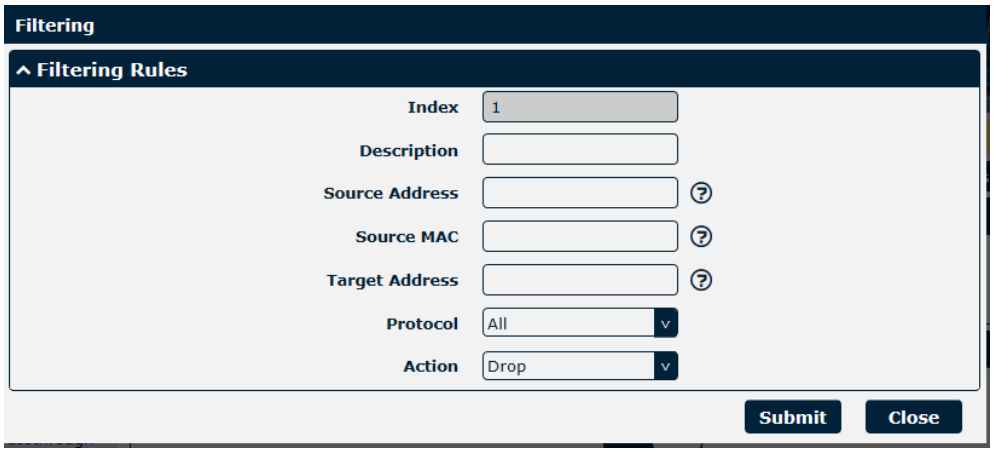
Filterung

Die Filterregeln können verwendet werden, um bestimmte Benutzer oder Ports für den Zugriff auf Ihren Router zuzulassen oder zu sperren.

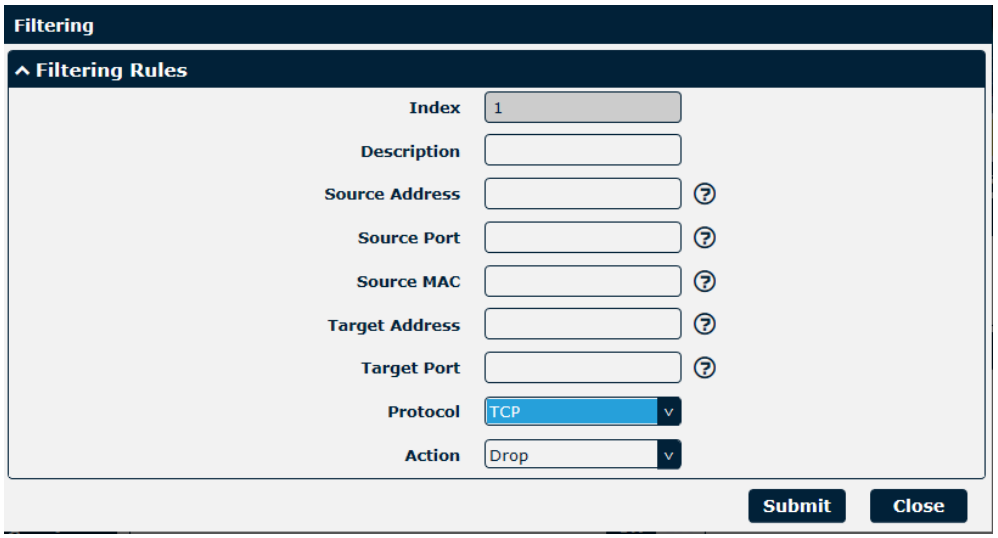
Klicken Sie auf +, um die Whitelist hinzuzufügen:



Klicken Sie auf +, um eine Filterregel hinzuzufügen, die maximale Anzahl beträgt 50. Das Fenster wird wie unten dargestellt, wenn Sie „All“ („Alle“) als Standardeinstellung oder „ICMP v6“ oder „ICMPv6“ als Protokoll wählen. Wir nehmen hier „All“ („Alle“) als Beispiel.



Wenn Sie als Protokoll „TCP“, „UDP“ oder „TCP-UDP“ wählen, wird das Fenster wie unten dargestellt. Nehmen Sie hier „TCP“ als Beispiel.



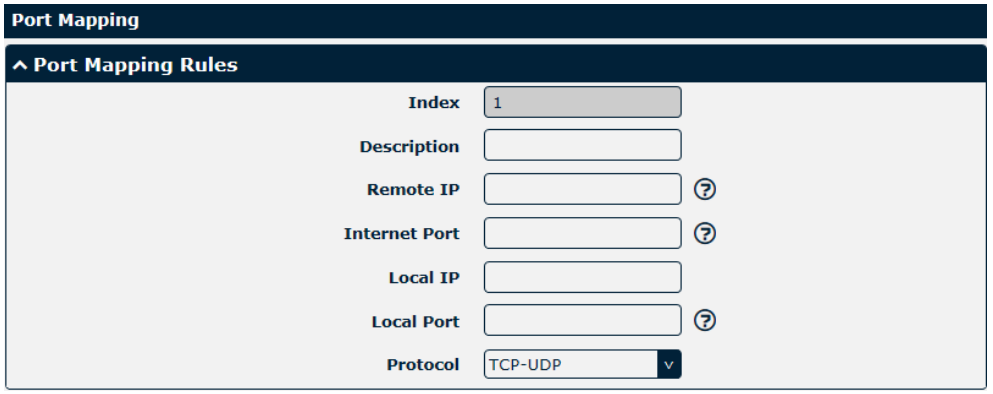
Filtering (Filterung)		
Punkt	Beschreibung	Standard
General Settings (Allgemeine Einstellungen)		
Enable Filtering (Filterung aktivieren)	Klicken Sie auf den Schalter, um die Filteroption zu aktivieren/ deaktivieren.	ON (EIN)
Default Filtering Policy (Standard-Filterrichtlinie)	Wählen Sie aus „Accept“ („Zulassen“) oder „Drop“ („Verwerfen“). Kann nicht geändert werden, wenn die Tabelle mit den Filterregeln nicht leer ist. Accept (Zulassen): Der Router lässt alle Verbindungsanfragen mit Ausnahme der Hosts zu, die der Filterliste Drop (Verwerfen) entsprechen. Drop (Verwerfen): Der Router verwirft alle Verbindungsanfragen mit Ausnahme der Hosts, die der Filterliste Accept (Zulassen) entsprechen.	Accept (Zulassen)
Access Control Settings (Zugangskontroll-Einstellungen)		
Enable Remote SSH Access (Remote-SSH-Zugang aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, kann der Internetbenutzer über SSH aus der Ferne auf den Router zugreifen.	OFF (AUS)
Enable Local SSH Access (Lokalen SSH-Zugang aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, kann der LAN-Benutzer über SSH lokal auf den Router zugreifen.	ON (EIN)
Enable Remote Telnet Access (Remote-Telnet-Zugang aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, kann der Internetbenutzer über Telnet aus der Ferne auf den Router zugreifen.	OFF (AUS)

Enable Local Telnet Access (Lokalen Telnet-Zugang aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, kann der LAN-Benutzer über Telnet lokal auf den Router zugreifen.	ON (EIN)
Enable Remote HTTP Access (Remote-HTTP-Zugang aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, kann der Internetbenutzer über HTTP aus der Ferne auf den Router zugreifen.	OFF (AUS)
Enable Local HTTP Access (Lokalen HTTP-Zugang aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, kann der LAN-Benutzer über HTPP lokal auf den Router zugreifen.	ON (EIN)
Enable Remote HTTPS Access (Remote-HTTPS-Zugang aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, kann der Internetbenutzer über HTTPS aus der Ferne auf den Router zugreifen.	ON (EIN)
Enable Remote Ping Respond (Remote-Ping-Antwort aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, antwortet der Router auf Ping-Anfragen anderer Hosts aus dem Internet.	ON (EIN)
Enable DOS Defending (DOS-Verteidigung aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, wehrt sich der Router gegen einen DOS-Angriff. Ein DOS-Angriff ist ein Versuch, einen Rechner oder eine Netzwerkressource für die vorgesehenen Benutzer unzugänglich zu machen.	ON (EIN)
Enable Console (Konsole aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren.	ON (EIN)
Enable vpn nat traversal (VPN-NAT-Transversal aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, wird NAT-Traversal für GRE / L2TP / PPTP VPN-Pakete aktiviert.	OFF (AUS)
whitelist (Whitelist)		
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Beschreibung	Geben Sie eine Beschreibung für diese Whitelist ein.	Null
Source Address (Quell-Adresse)	Legt fest, ob der Zugriff von einer oder einem Bereich von IP-Adressen, die durch die Quell-IP-Adresse definiert sind, oder von allen IP-Adressen erlaubt ist.	Null
Filtering Rules (Filterregeln)		
Punkt	Gibt die Ordinalzahl der Liste an.	-
Description (Beschreibung)	Geben Sie eine Beschreibung für diese Filterregel ein.	Null
Source Address (Quell-Adresse)	Legt fest, ob der Zugriff von einer oder einem Bereich von IP-Adressen, die durch die Quell-IP-Adresse definiert sind, oder von allen IP-Adressen erlaubt ist.	Null
Source Port (Quell-Port)	Spezifizieren Sie den Ursprung eines Zugriffs und geben Sie seinen Quell-Port ein.	Null
Source MAC (Quell-MAC-Adresse)	Geben Sie die MAC-Adresse der definierten Quell-IP-Adresse ein.	Null
Target Address (Zieladresse)	Legt fest, ob der Zugriff auf eine oder einen Bereich von IP-Adressen, die durch die Ziel-IP-Adresse definiert sind, oder auf alle IP-Adressen erlaubt ist.	Null

Target Port (Ziel-Port)	Geben Sie den Ziel-Port ein, auf den der Ursprung des Zugriffs zugreifen möchte.	Null
Protocol (Protokoll)	Wählen Sie aus „All“ („Alle“), „TCP“, „UDP“, „ICMP“ oder „TCP-UDP“. Hinweis: Es wird empfohlen, „All“ („Alle“) zu wählen, wenn Sie nicht wissen, welches Protokoll Ihrer Anwendung Sie verwenden sollen.	All (Alle)
Filtering (Filterung)		
Action (Aktion)	Wählen Sie aus „Accept“ („Zulassen“) oder „Drop“ („Verwerfen“). Accept (Zulassen): Wenn die Standardfilterrichtlinie Drop (Verwerfen) ist, löscht der Router alle Verbindungsanfragen mit Ausnahme der Hosts, die der Filterliste Accept (Zulassen) entsprechen. Drop (Verwerfen): Wenn die Standardfilterrichtlinie Accept (Zulassen) ist, lässt der Router alle Verbindungsanfragen mit Ausnahme der Hosts zu, die dieser Dropdown-Filterliste entsprechen.	Drop (Verwerfen)

Port Mapping (Port-Mapping)

Klicken Sie auf +, um Port-Mapping-Regeln hinzuzufügen. Die maximale Anzahl der Regeln beträgt 40.



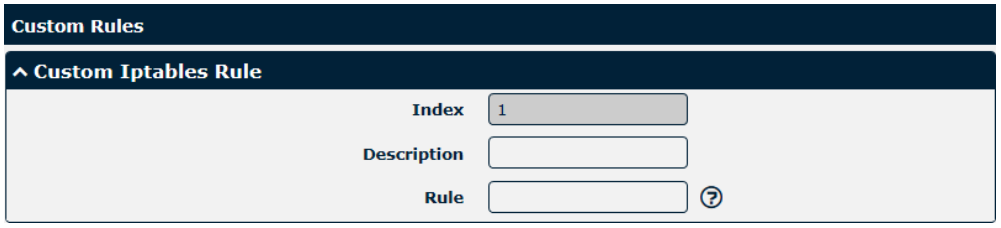
Port Mapping Rules (Port-Mapping-Regeln)		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Description (Beschreibung)	Geben Sie eine Beschreibung für diese Portzuordnung ein.	Null
Remote IP (Remote-IP)	Geben Sie den Host oder das Netzwerk an, der bzw. das auf die lokale IP-Adresse zugreifen kann. Leer bedeutet unbegrenzt. Beispiel: 10.10.10.10/ 255.255.255.255 oder 192.168.1.0/24.	Null
Internet Port (Internet-Port)	Legen Sie den Internet-Port des Routers fest, auf den andere Hosts vom Internet aus zugreifen können.	Null
Local IP (Lokale IP)	Geben Sie die LAN-IP des Routers ein, die an den Internet-Port des Routers weitergeleitet wird.	Null
Local Port (Lokaler Port)	Geben Sie den Port der LAN-IP des Routers ein.	Null

Protocol (Protokoll)	Wählen Sie aus „TCP“, „UDP“ oder „TCP-UDP“, abhängig von den Anforderungen Ihrer Anwendung.	TCP-UDP

Custom Rules (Benutzerdefinierte Regeln)

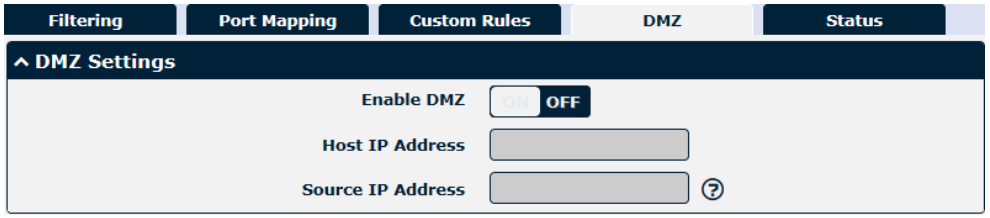
Benutzerdefinierte Regeln sind Regeln, die Sie selbst definieren. Klicken Sie auf Network (Netzwerk) > Firewall> Custom Rule (Benutzerdefinierte Regel) und es erscheint folgende Darstellung:

Klicken Sie auf +, um eine benutzerdefinierte IPv4- oder IPv6-Regel hinzuzufügen. Das Fenster wird wie folgt angezeigt (wir nehmen „IPv4“ als Beispiel):



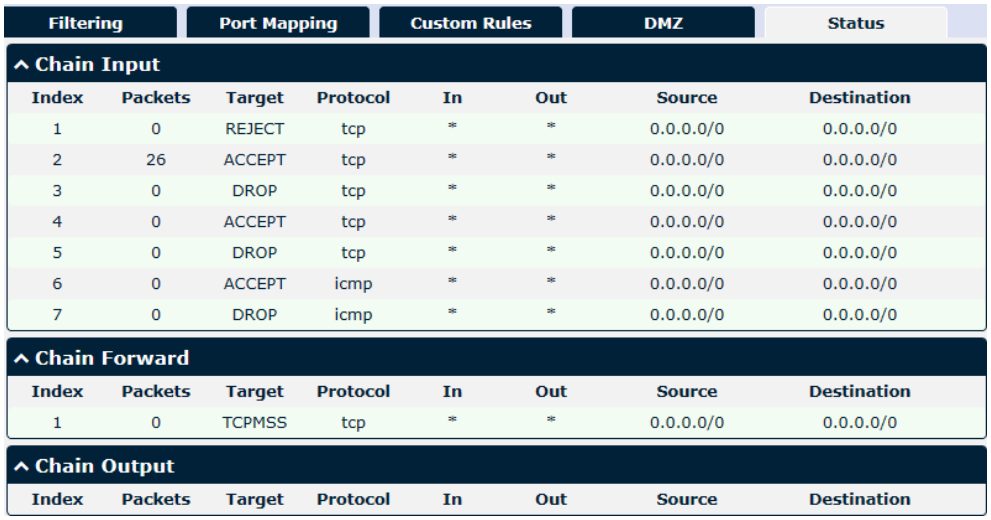
Custom Ip tables Rule (Benutzerdefinierte Iptables-Regel)		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Beschreibung	Geben Sie die Beschreibung der Regel ein.	Null
Rule (Regel)	Geben Sie eine „iptables“-Regel an.	Null

DMZ



DMZ Settings (DMZ-Einstellungen)		
Punkt	Beschreibung	Standard
Enable DMZ (DMZ aktivieren)	Klicken Sie auf den Schalter, um die DMZ zu aktivieren/deaktivieren. Ein DMZ-Host ist ein Host im internen Netzwerk, bei dem alle Ports exponiert sind, mit Ausnahme der Ports, die anderweitig weitergeleitet werden.	OFF (AUS)
Host IP Address (Host-IP-Adresse)	Geben Sie die IP-Adresse des DMZ-Hosts in Ihrem internen Netzwerk ein.	Null
Source IP Address (Quell-IP-Adresse)	Legen Sie die Adresse fest, die mit dem DMZ-Host kommunizieren kann. 0.0.0.0 bedeutet für beliebige Adressen.	Null

Status



3.17 Netzwerk > IP-Passthrough

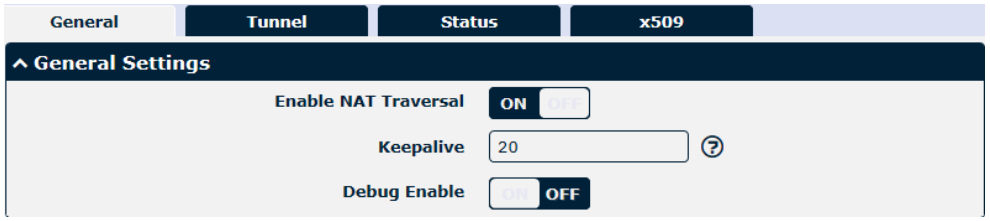
Klicken Sie auf Network (Netzwerk) > IP Passthrough > IP Passthrough, um die Option IP Passthrough zu aktivieren oder deaktivieren.

Wenn der Router den IP-Passthrough aktiviert, aktiviert das Endgerät (z. B. der PC) den DHCP-Client-Modus und stellt die Verbindung zum LAN-Port des Routers her; nach der erfolgreichen Einwahl des Routers erhält der PC automatisch die vom ISP zugewiesene IP-Adresse und DNS-Serveradresse.

3.18 VPN > IPsec

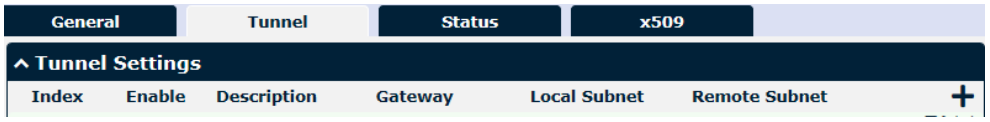
IPsec (Internet Protocol Security) ist ein auf der Internet-Protokollschicht aufgebautes Protokoll, das es zwei Hosts ermöglicht, auf sichere Weise kommunizieren.
IPsec ist die Richtung der sicheren Vernetzung. Sie bietet einen aktiven Schutz von Ende-zu-Ende-Sicherheit, um Angriffe aus privaten Netzwerken und dem Internet zu verhindern.

Klicken Sie auf Virtual Private Network (Virtuelles privates Netzwerk) > IPsec > General (Allgemein), um die IPsec-Parameter festzulegen.

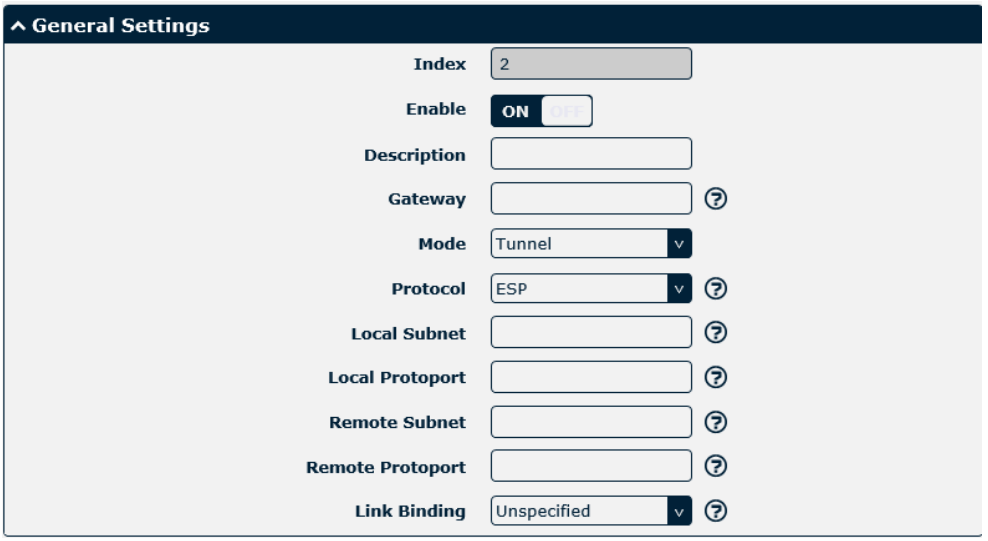


General Settings @ General (Allgemeine Einstellungen @ Allgemein)		
Punkt	Beschreibung	Standard
Survival time (Survival-Zeit)	Stellen Sie die Survival-Zeit in Sekunden ein. Der Router sendet in regelmäßigen Abständen Keepalive-Pakete an einen NAT-Server (Network Address Translation), um zu verhindern, dass die Datensätze in der NAT-Tabelle verschwinden.	20
Optimize DH index size (DH-Index-Größe optimieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn sie bei Verwendung von dhgroup17 oder dhgroup18 aktiviert ist, hilft sie, die Zeit zur Erzeugung von dh-Schlüsseln zu verkürzen. (DH = Diffie-Hellman-Schlüsselaustausch)	OFF (AUS)
Debug Enable (Debugging aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option für die Ausgabe von IPsec-VPN-Informationen an den Debugging-Port.	OFF (AUS)

Tunnel

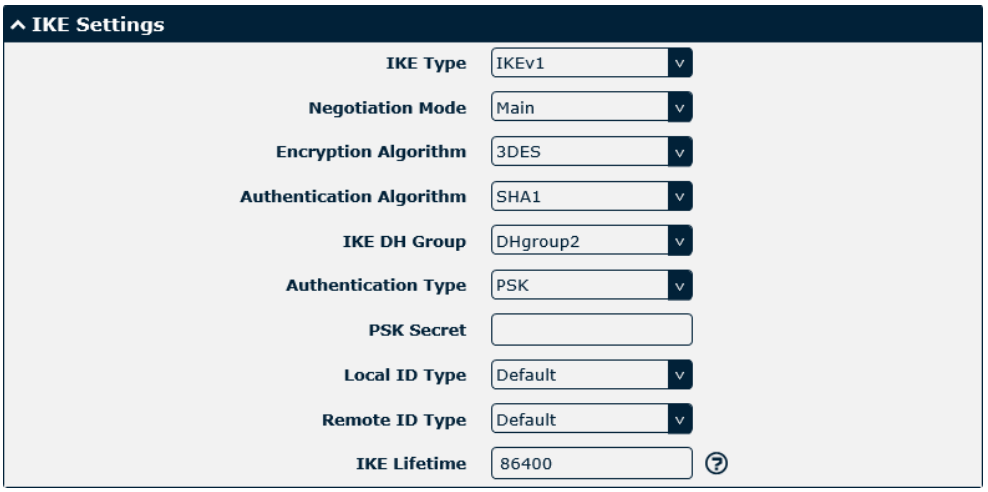


Klicken Sie auf n Tunneleinstellungen hinzuzufügen. Die maximale Anzahl beträgt 3.

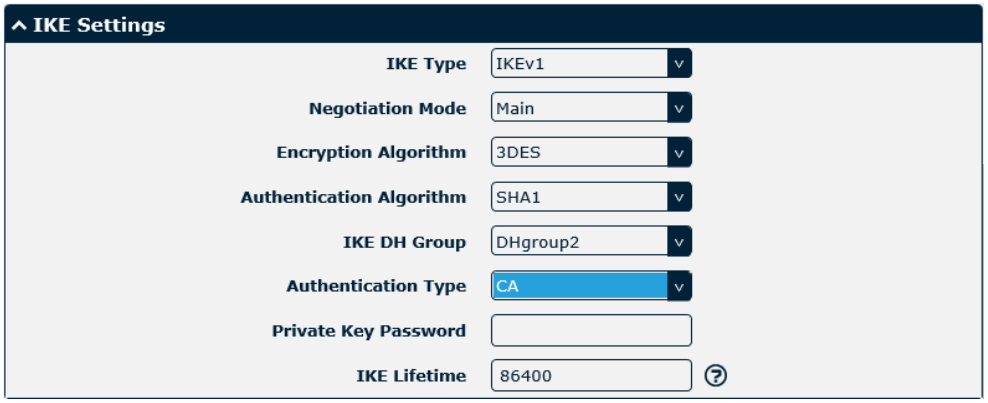


General Settings @ Tunnel (Allgemeine Einstellungen @ Tunnel)		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Enable (Aktivieren)	Klicken Sie auf den Schalter, um diesen IPsec-Tunnel zu aktivieren/ deaktivieren.	ON (EIN)
Beschreibung	Geben Sie eine Beschreibung für diesen IPsec-Tunnel ein.	Null
Gateway (Gateway)	Geben Sie die Adresse des IPsec-VPN-Servers der entfernten Seite ein. 0.0.0.0 steht für eine beliebige Adresse.	Null
Mode (Modus)	Wählen Sie aus „Tunnel“ und „Transport“. Tunnel: Häufig zwischen Gateways oder an einer Endstation zu einem Gateway verwendet, wobei das Gateway als Proxy für die dahinter liegenden Hosts fungiert. Transport: Wird zwischen Endstationen oder zwischen einer Endstation und einem Gateway verwendet, wenn das Gateway als Host behandelt wird, z. B. eine verschlüsselte Telnet-Sitzung von einer Workstation zu einem Router, bei der der Router das eigentliche Ziel ist.	Tunnel
Protocol (Protokoll)	Wählen Sie das Sicherheitsprotokolle „ESP“ oder „AH“ aus. ESP: Verwendung des ESP-Protokolls AH: Verwendung des AH-Protokolls	ESP
Local Subnet (Lokales Subnetz)	Geben Sie die Adresse des lokalen Subnetzes mit einer durch IPsec geschützten Maske ein, z. B. 192.168.1.0/ 24.	Null
Remote Subnet (Entferntes Subnetz)	Geben Sie die Adresse des entfernten Subnetzes mit einer durch IPsec geschützten Maske ein, z. B. 10.8.0.0/ 24.	Null
Link binding (Link-Bindung)	Wählen Sie aus WWAN1, WWAN2, WAN oder WLAN.	Not bound

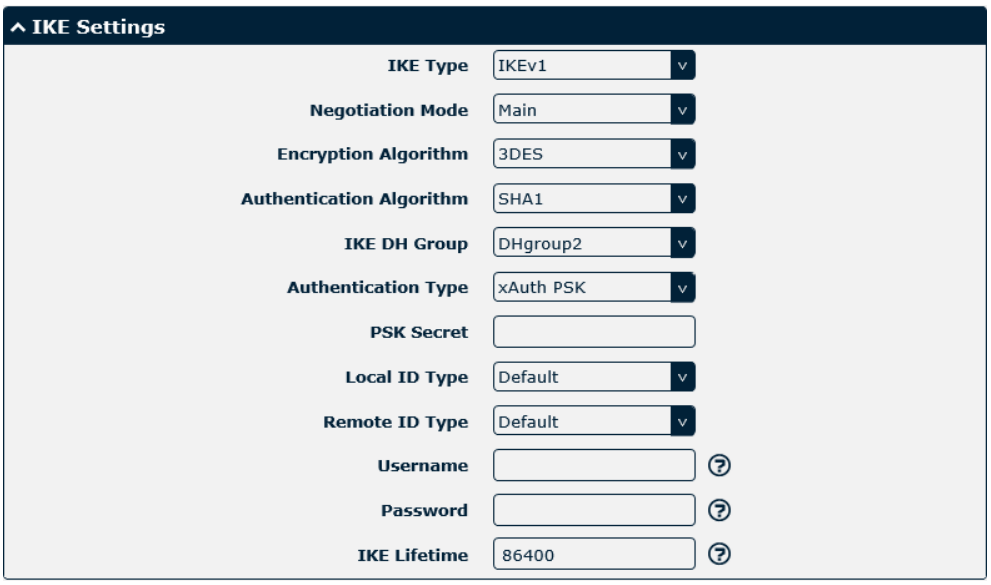
Wenn Sie als Authentifizierungstyp „PSK“ wählen, wird das Fenster wie unten dargestellt.



Wenn Sie als Authentifizierungstyp „CA“ wählen, wird das Fenster wie unten dargestellt.



Wenn Sie als Authentifizierungstyp „xAuth PSK“ wählen, wird das Fenster wie unten dargestellt.

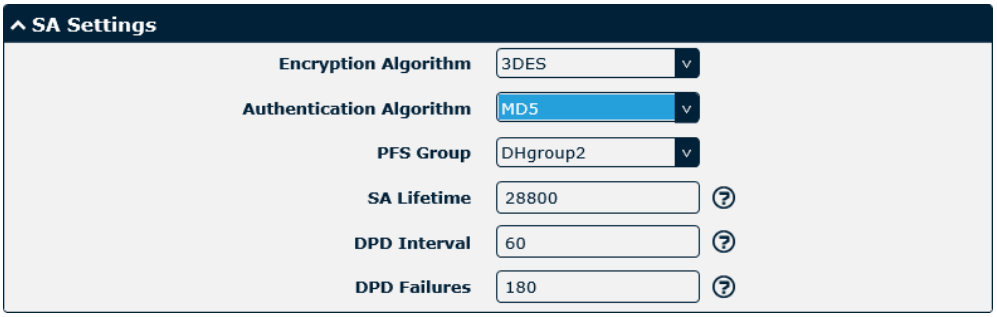


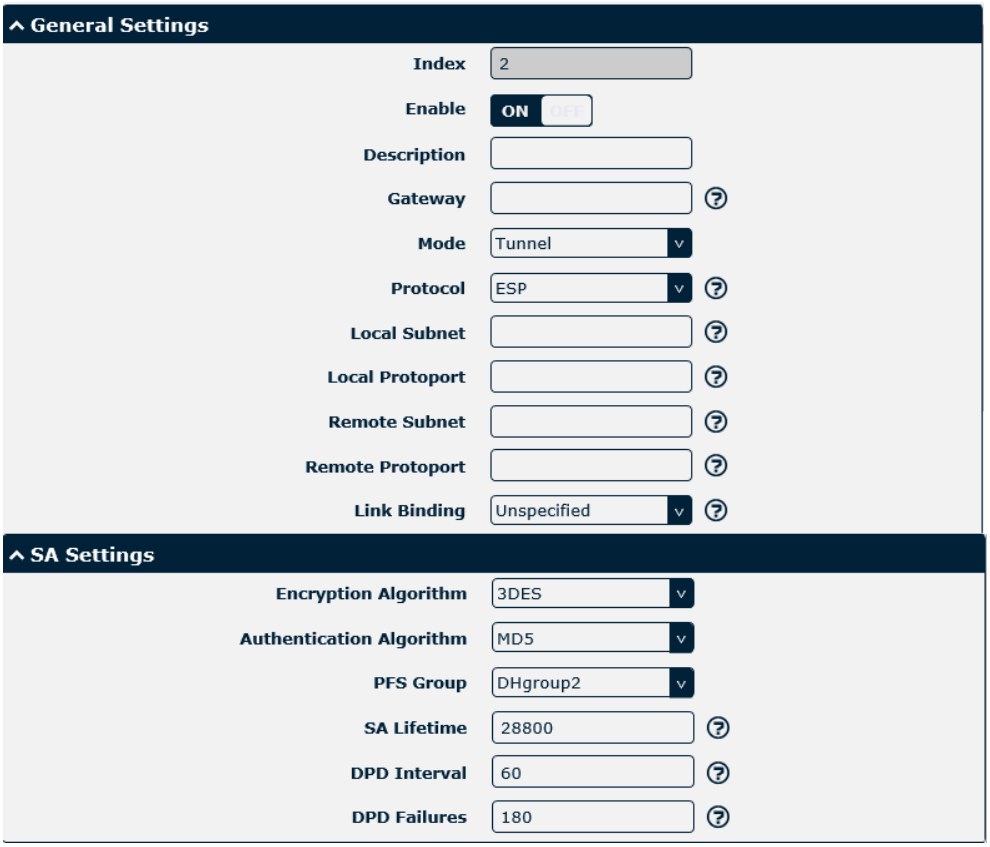
Wenn Sie als Authentifizierungstyp „xAuth CA“ wählen, wird das Fenster wie unten dargestellt:

IKE Settings (IKE-Einstellungen)		
Punkt	Beschreibung	Standard
IKE Type (IKE-Typ)	Wählen Sie aus IKE v1 und IKE v2.	IKE v1
Negotiation Mode (Verhandlungsmodus)	Wählen Sie für den IKE-Verhandlungsmodus in Phase 1 aus „Main“ („Haupt“) und „Aggressive“ („Aggressiv“). Wenn die IP-Adresse eines Endes eines IPsec-Tunnels dynamisch ermittelt wird, muss der IKE-Verhandlungsmodus „Aggressive“ sein. In diesem Fall können SAs eingerichtet werden, solange der Benutzername und das Passwort korrekt sind.	Main (Haupt)
Authentication Algorithm (Authentifizierungsalgori	Wählen Sie aus „MD5“, „SHA1“, „SHA2 256“ oder „SHA2 512“, die bei IKE-Verhandlungen verwendet werden sollen.	SHA1
Encryption Algorithm (Verschlüsselungsalgorithmus)	Wählen Sie aus „3DES“, „AES128“, „AES192“ und „AES256“ aus, die bei IKE-Verhandlungen verwendet werden sollen. 3DES: 168-Bit-3DES-Verschlüsselungsalgorithmus im CBC-Modus verwenden AES128: 128-Bit-AES-Verschlüsselungsalgorithmus im CBC-Modus verwenden AES256: 256-Bit-AES-Verschlüsselungsalgorithmus im CBC-Modus verwenden	3DES
IKE DH Group (IKE-DH-Gruppe)	Wählen Sie DH-Pakete für IKE-Verhandlungen (Network Key Exchange) aus. Wählen Sie aus „DHgroup1“, „DHgroup2“, „DHgroup5“, „DHgroup14“, „DHgroup15“, „DHgroup16“, „DHgroup17“ oder „DHgroup18“, die in der Schlüsselverhandlungsphase 1 verwendet werden sollen.	PSK
Authentication Type (Authentifizierungs-Typ)	Wählen Sie aus „PSK“, „CA“, „PKCS#12“, „xAuth PSK“ und „xAuth CA“ aus, die bei IKE-Verhandlungen verwendet werden sollen. PSK: Pre-shared Key (Vorab vereinbarter Schlüssel) CA: Certification Authority (Zertifizierungsstelle) xAuth: Extended Authentication to AAA server (Erweiterte Authentifizierung zum AAA-Server)	PSK

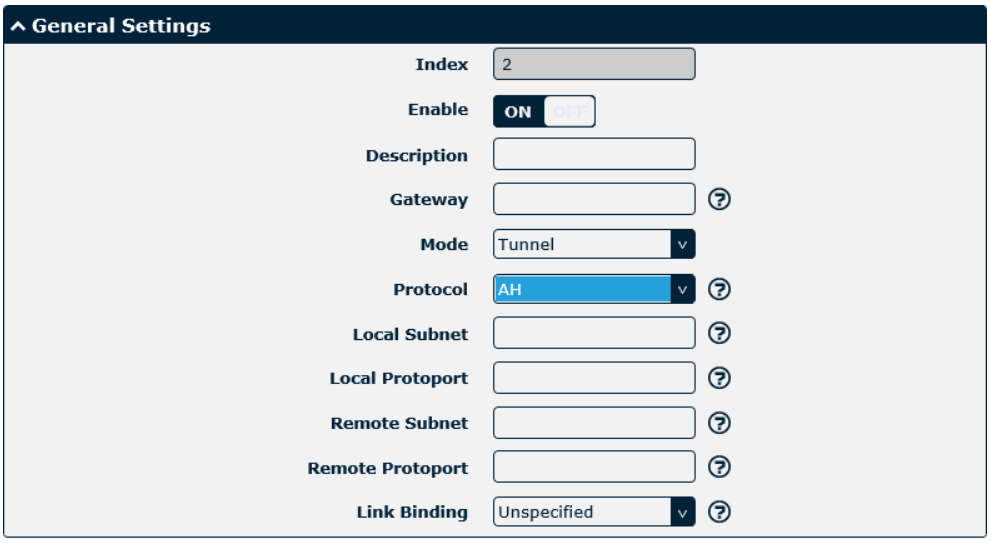
PSK Secret (PSK-Geheimnis)	Geben Sie den Pre-shared Key ein.	Null
Local ID Type (Lokaler ID-Typ)	Wählen Sie für die IKE-Verhandlung aus „Standard“, „FQDN“ und „User FQDN“ („Benutzer-FQDN“). Voreinstellung: Verwendet eine IP-Adresse als ID in IKE-Verhandlungen. FQDN: Verwendet einen FQDN-Typ als ID in IKE-Verhandlungen. Wenn diese Option ausgewählt ist, geben Sie für das lokale Sicherheits-Gateway einen Namen ohne At-Zeichen (@) ein, z. B. test.AddSecure.com. User FQDN (Benutzer-FQDN): Verwendet einen Benutzer-FQDN-Typ als ID in IKE-Verhandlungen. Wenn diese Option ausgewählt ist, geben Sie eine Namenszeichenfolge mit einem At-Zeichen „@“ für das lokale Sicherheits-Gateway ein, z. B. test@AddSecure.com.	Standard
Remote ID Type (Remote-IP-Typ)	Wählen Sie für die IKE-Verhandlung aus „Standard“, „FQDN“ und „User FQDN“ („Benutzer-FQDN“). Voreinstellung: Verwendet eine IP-Adresse als ID in IKE-Verhandlungen. FQDN: Verwendet einen FQDN-Typ als ID in IKE-Verhandlungen. Wenn diese Option ausgewählt ist, geben Sie für das lokale Sicherheits-Gateway einen Namen ohne At-Zeichen (@) ein, z. B. test.AddSecure.com. User FQDN (Benutzer-FQDN): Verwendet einen Benutzer-FQDN-Typ als ID in IKE-Verhandlungen. Wenn diese Option ausgewählt ist, geben Sie eine Namenszeichenfolge mit einem At-Zeichen „@“ für das lokale Sicherheits-Gateway ein, z. B. test@AddSecure.de.	Standard
Private Key Password (Passwort für privaten Schlüssel)	Geben Sie den privaten Schlüssel unter den Authentifizierungstypen „CA“ und „xAuth CA“ ein.	Null
Username (Benutzername)	Geben Sie den Benutzernamen ein, der für die Authentifizierungstypen „xAuth PSK“ und „xAuth CA“ verwendet wird.	Null
Password (Passwort)	Geben Sie das Passwort ein, das für die Authentifizierungstypen „xAuth PSK“ und „xAuth CA“ verwendet wird.	Null
IKE Lifetime (IKE-Lebensdauer)	Legen Sie die Lebensdauer in der IKE-Verhandlung fest. Bevor ein SA ausläuft, verhandelt die IKE über ein neues SA. Sobald das neue SA eingerichtet ist, tritt es sofort in Kraft, und das alte SA wird automatisch gelöscht, wenn es ausläuft.	86400

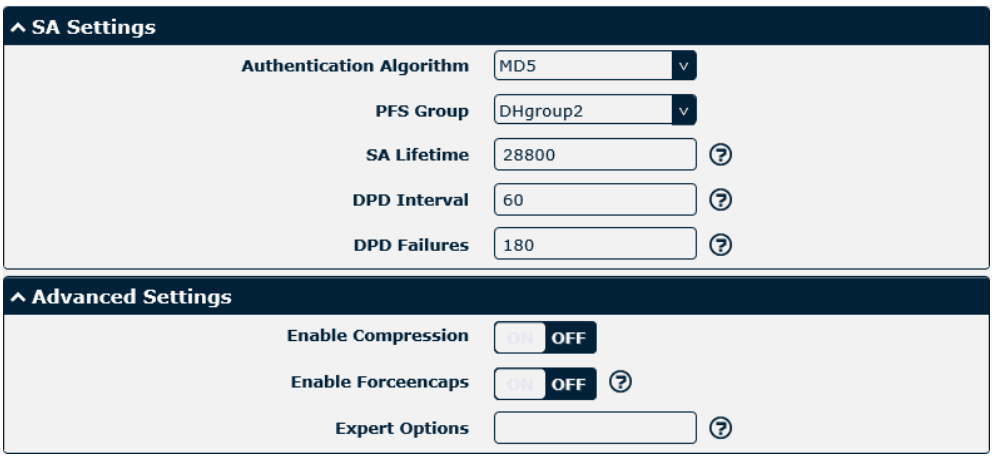
Klicken Sie auf VPN > IPsec > Tunnel > General Settings (Allgemeine Einstellungen) und wählen Sie ESP als Protokoll. Die spezifische Parameterkonfiguration ist wie unten dargestellt.





Wenn Sie AH als Protokoll wählen, wird das Fenster der SA-Einstellungen wie unten dargestellt angezeigt.



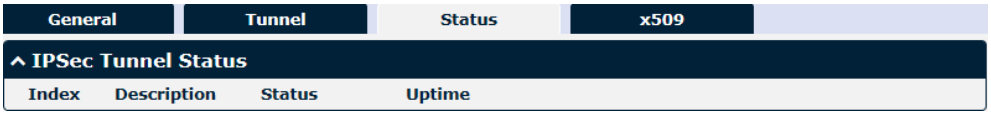


SA Settings (SA-Einstellungen)		
Punkt	Beschreibung	Standard
Encrypt Algorithm (Verschlüsselungs-Algorithmus)	Wählen Sie aus „3DES“ , „AES128“ oder „AES256“, wenn Sie unter „Protocol“ („Protokoll“) „ESP“ auswählen. Höhere Sicherheit bedeutet komplexere Umsetzung und geringere Geschwindigkeit. DES reicht aus, um die allgemeinen Anforderungen zu erfüllen. Verwenden Sie 3DES, wenn hohe Vertraulichkeit und Sicherheit erforderlich sind.	3DES
Authentication Algorithm (Authentifizierungsalgorithmus)	Wählen Sie aus „MD5“, „SHA1“, „SHA2 256“ oder „SHA2 512“, die bei SA-Verhandlungen verwendet werden sollen.	MD5
PFS Group (PFS-Gruppe)	Wählen Sie aus „PFS（N/A）“, „DHgroup1“, „DHgroup2“, „DHgroup5“, „DHgroup14“, „DHgroup15“, „DHgroup16“, „DHgroup17“ oder „DHgroup18“ zur Verwendung in SA-Verhandlungen.	DHgroup2
SA Lifetime (SA-Lebensdauer)	Legen Sie die IPsec-SA-Lebensdauer fest. Bei Verhandlungen über die Einrichtung von IPsec-SAs verwendet IKE den kleineren Wert der lokal festgelegten und der vom Peer vorgeschlagenen Lebensdauer.	28800
DPD Interval (DPD-Intervall)	Stellen Sie das Intervall ein, nach dem DPD ausgelöst wird, wenn keine IPsec-geschützten Pakete von der Gegenstelle empfangen werden. DPD ist eine Dead-Peer-Erkennung. DPD stellt unregelmäßig tote IKE-Peers fest. Wenn die lokale Seite ein IPsec-Paket sendet, überprüft DPD den Zeitpunkt, zu dem das letzte IPsec-Paket von der Gegenstelle empfangen wurde. Wenn die Zeit das DPD-Intervall überschreitet, wird ein DPD-Hallo an den Peer gesendet. Wenn die lokale Seite innerhalb des DPD-Paket-Wiederholungsintervalls keine DPD-Bestätigung erhält, sendet sie das DPD-Hallo erneut. Wenn die lokale Seite nach der maximalen Anzahl von Neuübertragungsversuchen immer noch keine DPD-Bestätigung erhält, betrachtet sie den Peer als bereits tot und löscht die IKESA und die IPsec-SAs auf der Grundlage der IKE SA.	60
DPD Failures (DPD-Versagen)	Stellen Sie die Zeitüberschreitung von DPD-Paketen (Dead Peer Detection) ein.	180

Advanced Settings (Erweiterte Einstellungen)		
Enable Compression (Kompression aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option, um die inneren Header von IP-Paketen zu komprimieren.	OFF (AUS)
Enable Forced Encapsulation (Erzwungene Einkapselung aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Nach der Aktivierung wird die UDP-Einkapselung von esp-Paketen erzwungen, auch wenn keine NAT-Bedingung erkannt wird. Dies kann helfen, restriktive Firewalls zu überwinden.	OFF (AUS)
Expert Options (Expertenoptionen)	Fügen Sie hier weitere PPP-Konfigurationsoptionen hinzu, Format: config-desc;config-desc, z. B. protostack=netkey;plutodebug=none	Null

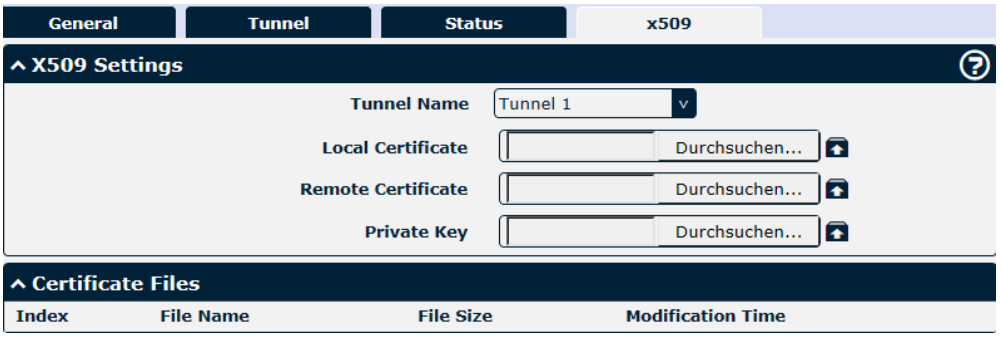
Status

In diesem Abschnitt können Sie den Status des IPsec-Tunnels einsehen.



x509

In diesem Abschnitt können Benutzer die X509-Zertifikate für den IPsec-Tunnel hochladen.

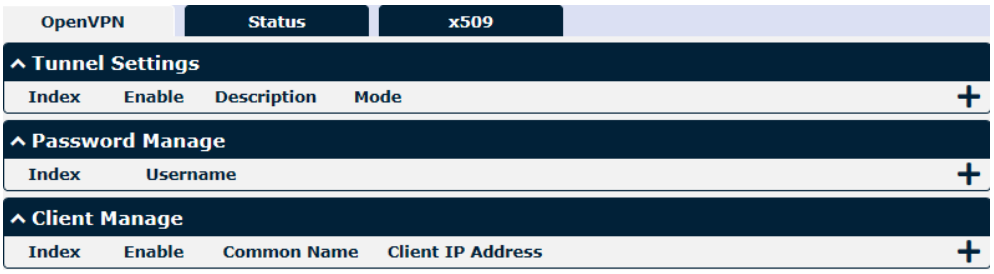


x509		
Punkt	Beschreibung	Standard
X509 Settings (X509-Einstellungen)		
Tunnel Name (Tunnelname)	Wählen Sie einen gültigen Tunnel.	Tunnel 1
Local Certificate (Lokales Zertifikat)	Klicken Sie auf „Choose File“ („Datei auswählen“), um eine lokale Zertifikatsdatei von Ihrem Computer hochzuladen, und importieren Sie diese Datei dann in Ihren Router. Das richtige Dateiformat wird wie folgt angezeigt: @ca.crt @remote.crt @local.crt @private.key @crl.pem	Null
Remote Certificate (Remote-Zertifikat)	Klicken Sie auf „Choose File“ („Datei auswählen“), um eine Remote-Zertifikatsdatei von Ihrem Computer hochzuladen, und importieren Sie diese Datei dann in Ihren Router.	Null
Private Key (Privater Schlüssel)	Wählen Sie die richtige private Schlüsseldatei zum Importieren in den Router.	Null
Certificate Files (Zertifikat-Dateien)		
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
File Name (Dateiname)	Zeigt den Namen des importierten Zertifikats an.	Null
File Size (Dateigröße)	Zeigt die Größe der Zertifikatsdatei an.	Null
Modification Time (Änderungszeit)	Zeigt den Zeitstempel an, wann die Zertifikatsdatei zuletzt geändert wurde.	Null

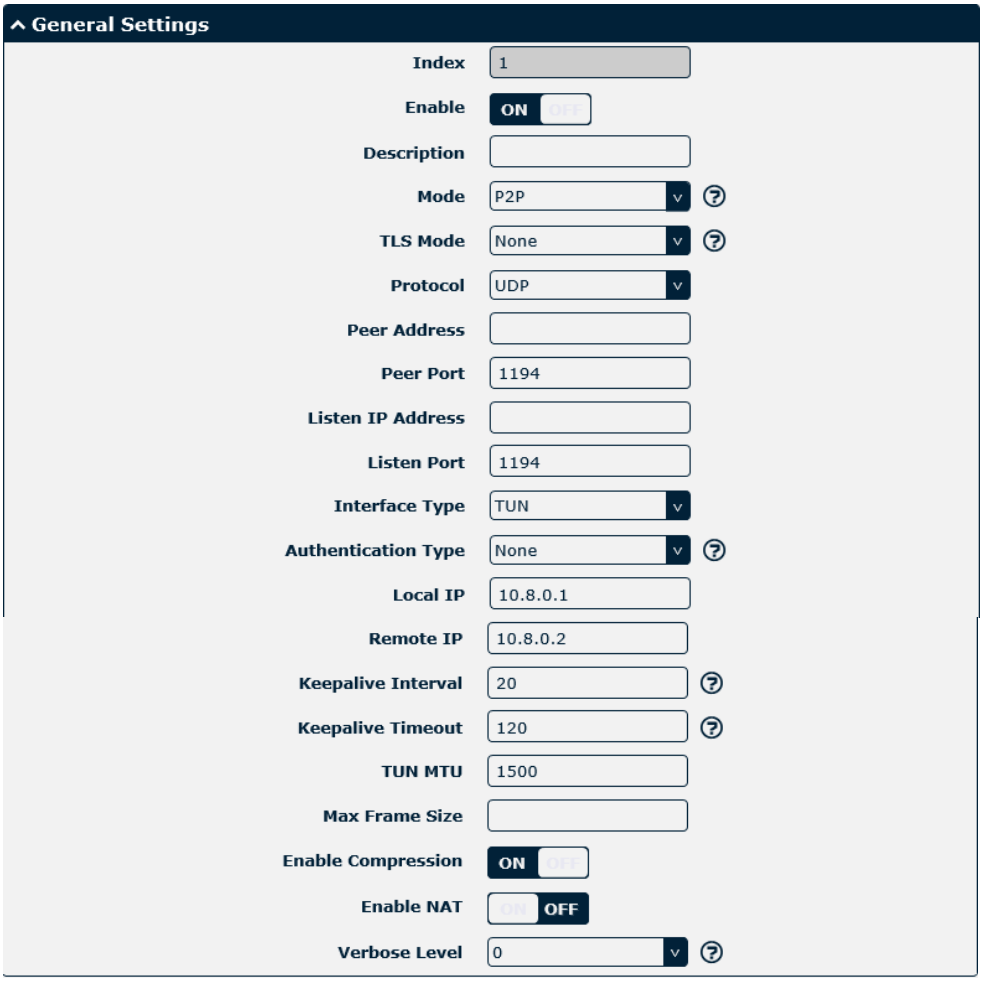
3.19 VPN > OpenVPN

In diesem Abschnitt können Sie OpenVPN und die zugehörigen Parameter einstellen. OpenVPN ist eine Open-Source-Softwareanwendung, die Virtual Private Network (VPN)-Techniken zur Schaffung sicherer Punkt-zu-Punkt- oder Standort-zu-Standort-Verbindungen in gerouteten oder gebrückten Konfigurationen und Fernzugriffseinrichtungen implementiert. Der Router unterstützt Punkt-zu-Punkt- und Punkt-zu-Mehrpunkt-Verbindungen.

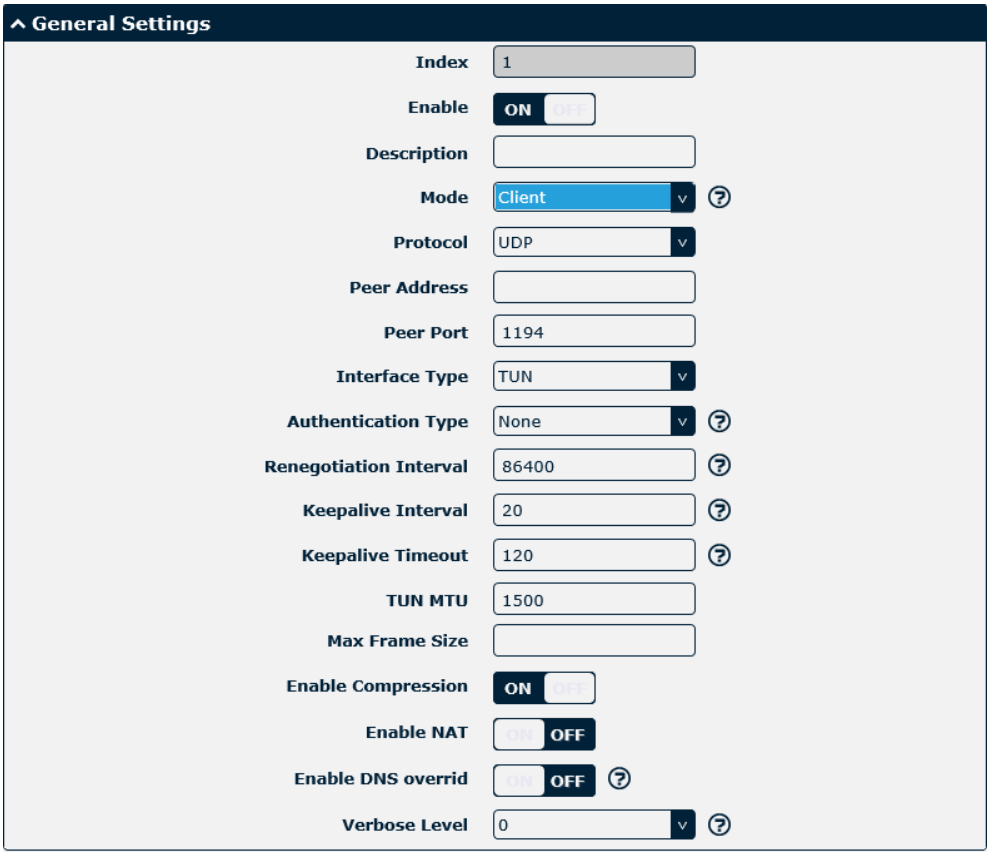
OpenVPN



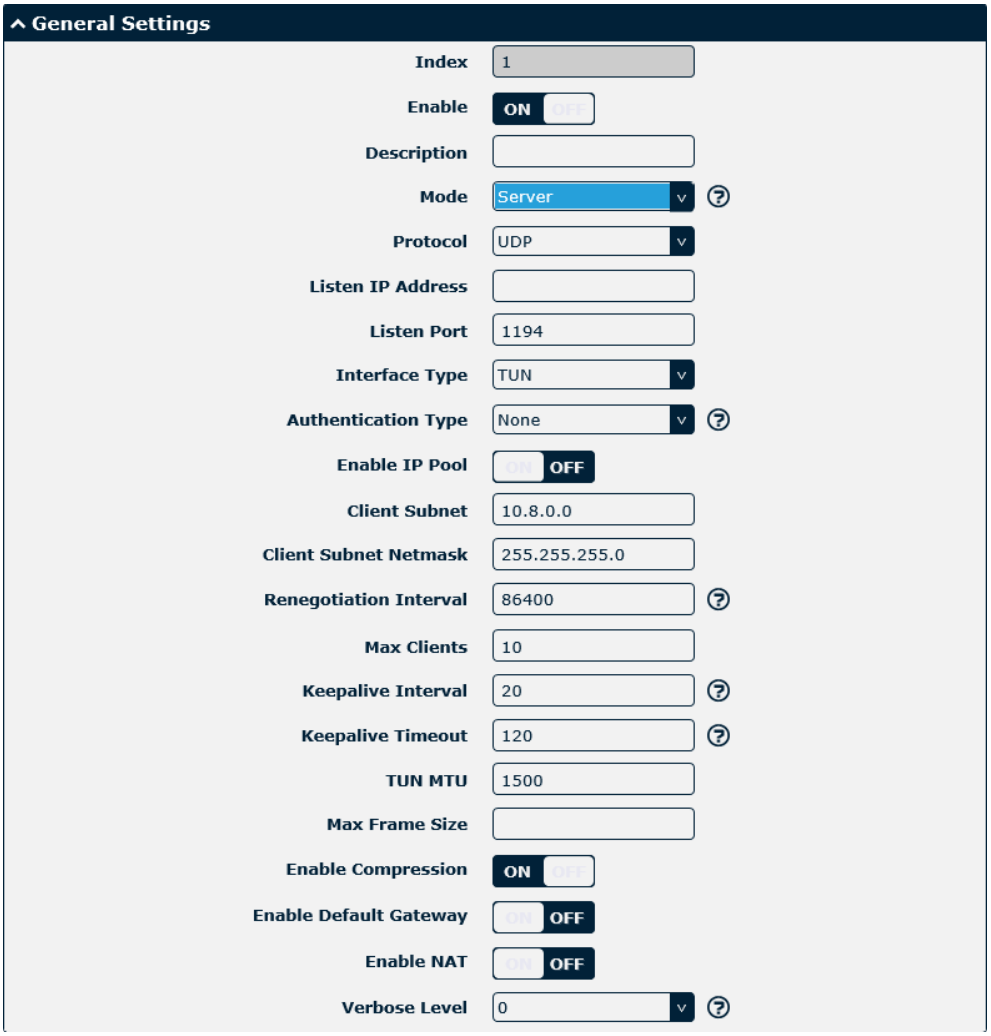
Klicken Sie auf +, um Tunneleinstellungen hinzuzufügen. Die maximale Anzahl beträgt 3. Wenn Sie als Authentifizierungstyp „None“ („Keine“) wählen, wird das Fenster wie unten dargestellt. Standardmäßig ist der Modus „P2P“ eingestellt.


General Settings
Index
1
Enable
ON
OFF
Description
Mode
P2P
TLS Mode
None
Protocol
UDP
Peer Address
Peer Port
1194
Listen IP Address
Listen Port
1194
Interface Type
TUN
Authentication Type
None
Local IP
10.8.0.1
Remote IP
10.8.0.2
Keepalive Interval
20
Keepalive Timeout
120
TUN MTU
1500
Max Frame Size
Enable Compression
ON
OFF
Enable NAT
ON
OFF
Verbose Level
0

Wenn Sie als Modus „Client“ wählen, wird das Fenster wie unten dargestellt:

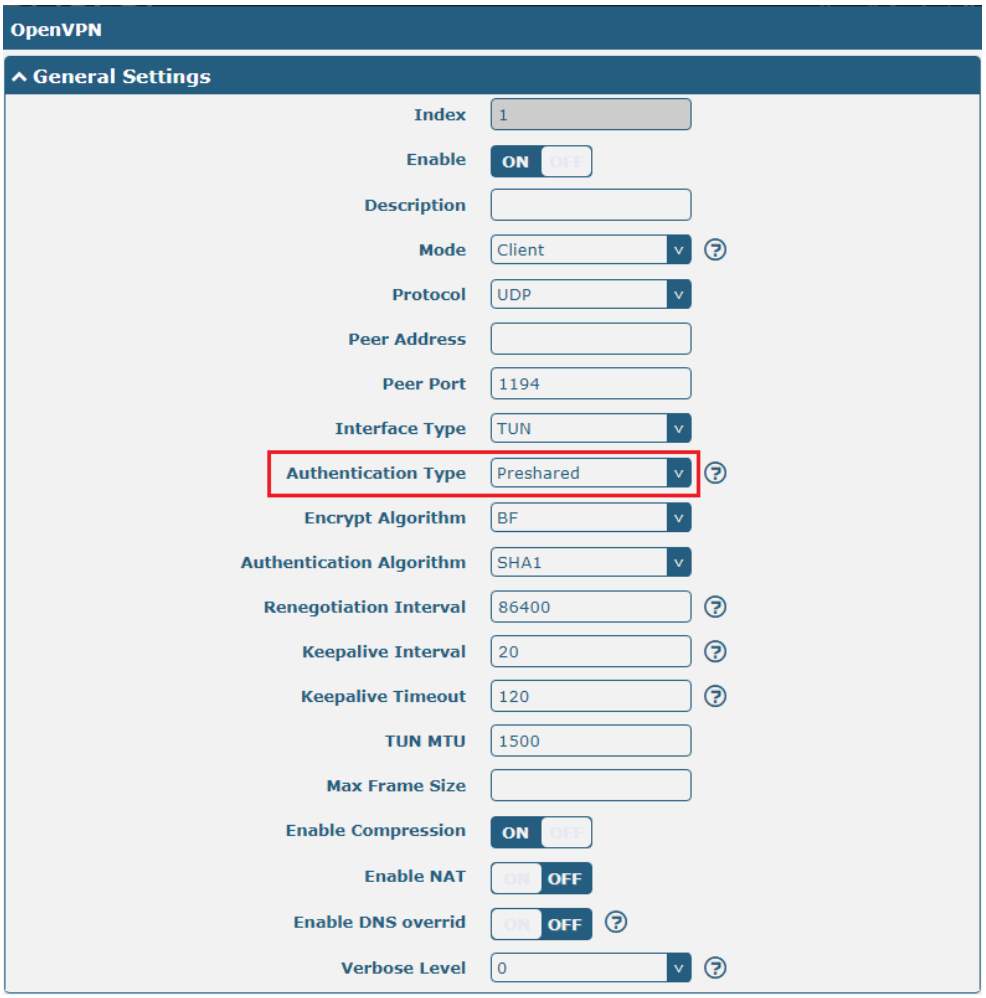


Wenn Sie als Modus „Server“ wählen, wird das Fenster wie unten dargestellt:

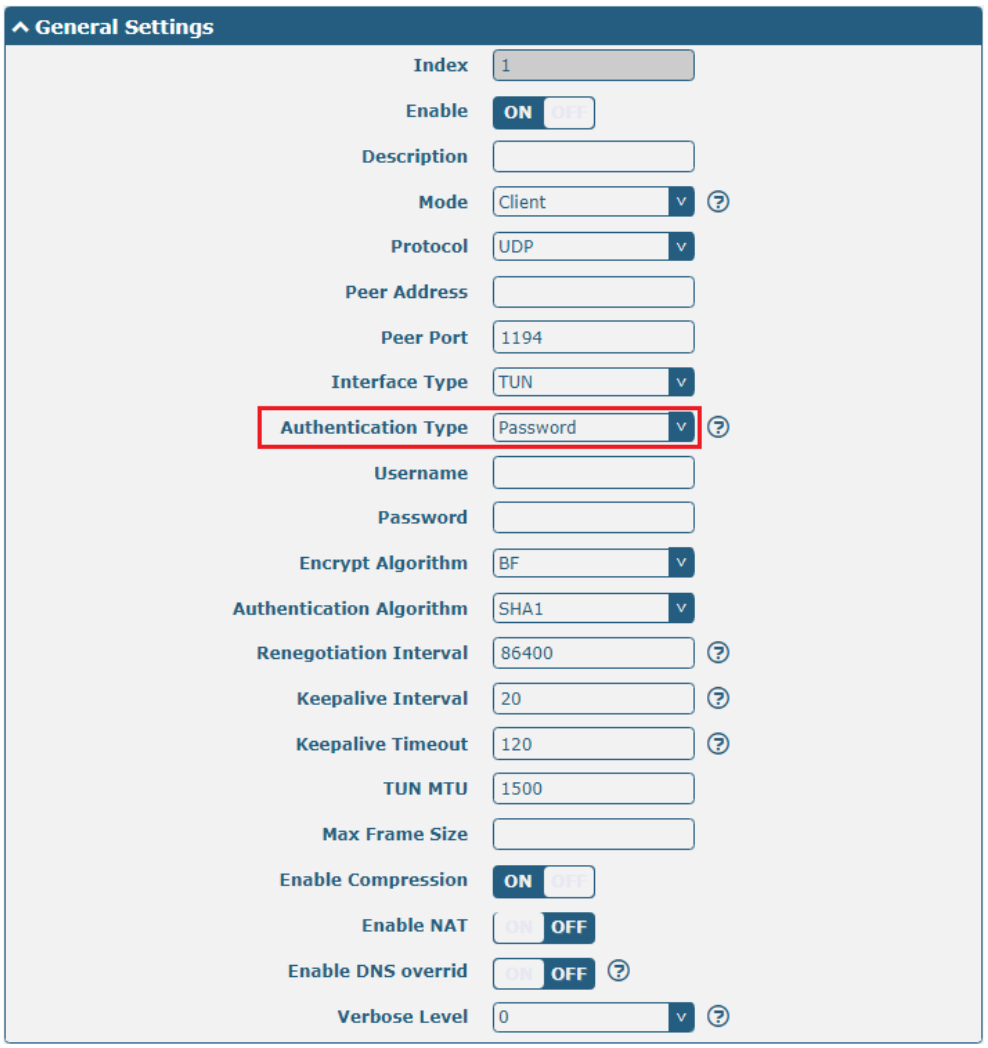


Wenn Sie als Authentifizierungstyp „None“ („Keine“) wählen, wird das Fenster wie unten dargestellt.

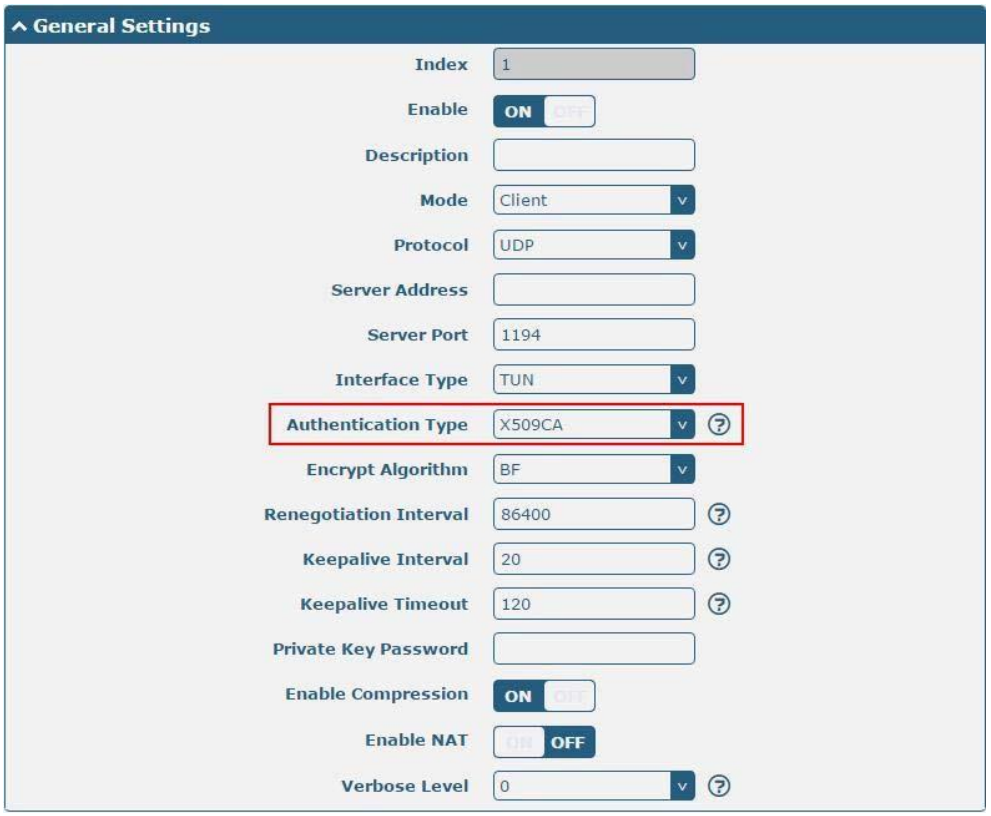
Wenn Sie als Authentifizierungstyp „Preshared“ wählen, wird das Fenster wie unten dargestellt:



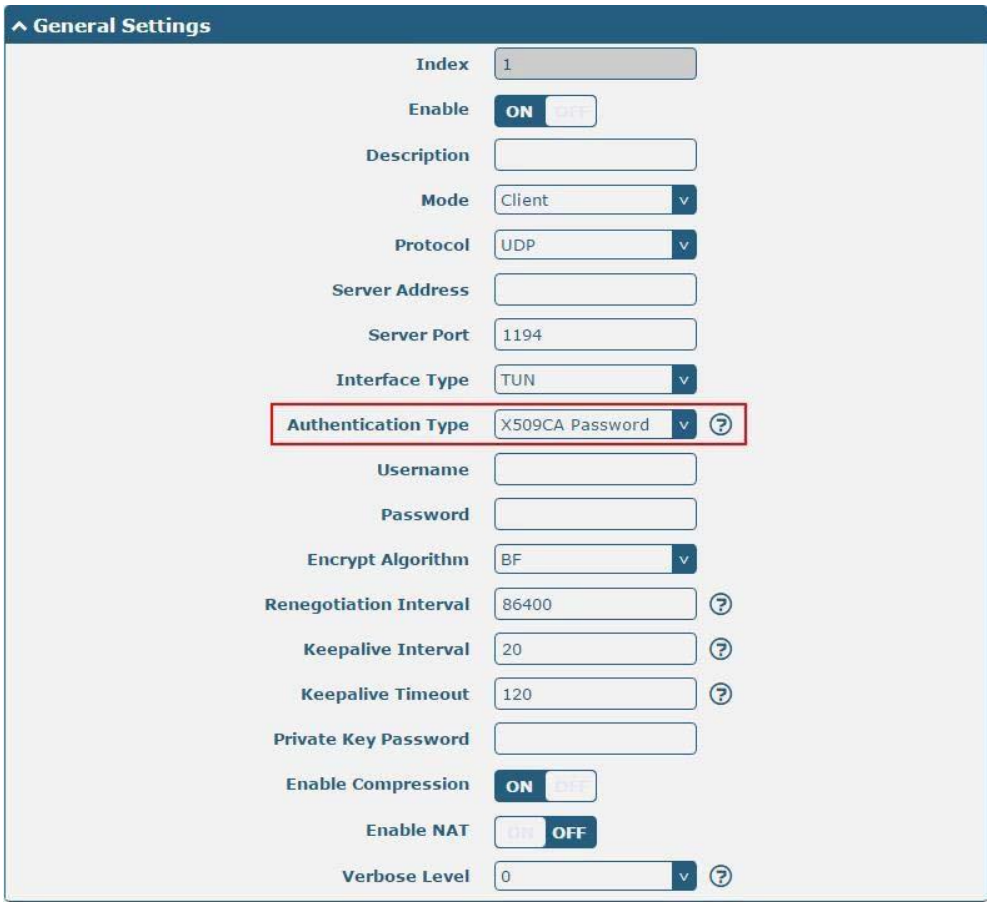
Wenn Sie als Authentifizierung „Password“ wählen, wird das Fenster wie unten dargestellt:



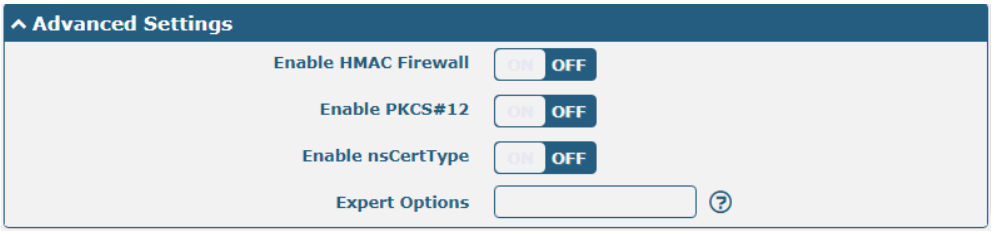
Wenn Sie als Authentifizierungstyp „X509CA“ wählen, wird das Fenster wie unten dargestellt:



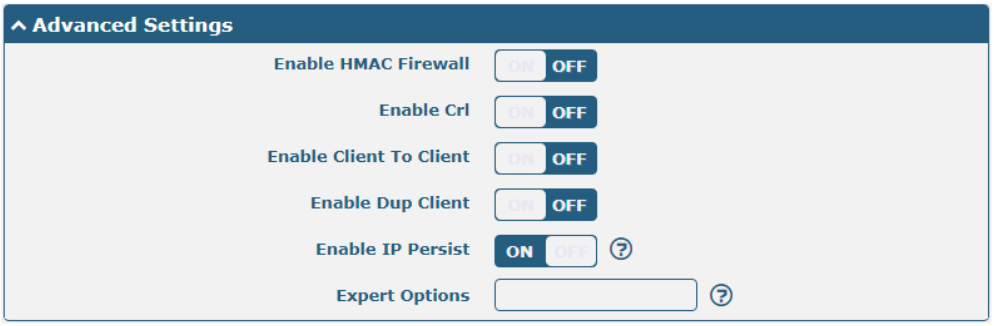
Wenn Sie als Authentifizierungstyp „X509CA Password“ wählen, wird das Fenster wie unten dargestellt:



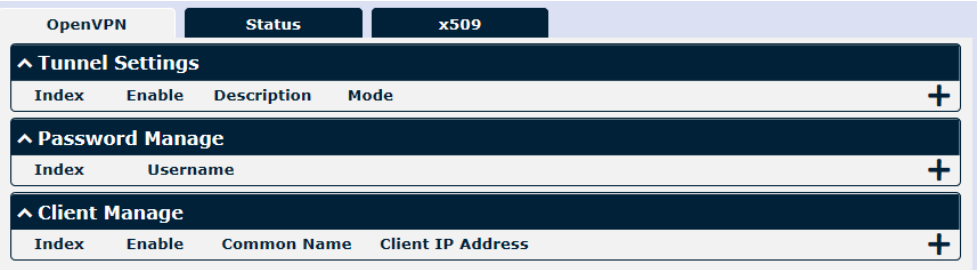
Wenn Sie als Modus „Client“ wählen, wird das Fenster wie unten dargestellt.



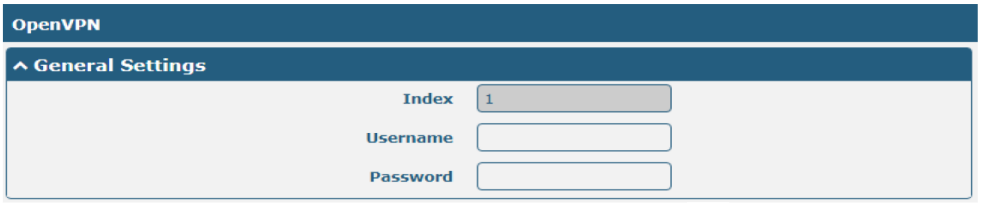
Wenn Sie als Modus „Server“ wählen, wird das Fenster wie unten dargestellt.



Wenn Sie „Server“ als Modus und „X509CA Password“ („X509CA Passwort“) als Authentifizierungstyp wählen, wird das Fenster von „Virtual Private Network > OpenVPN > OpenVPN“ wie unten dargestellt.



Klicken Sie auf „User Password Management“ („Benutzer-Passwortverwaltung“) +, um Benutzername und Passwort hinzuzufügen, wie unten gezeigt:



Klicken Sie auf „Client Management“ („Client-Verwaltung“) +, um Client-Informationen hinzuzufügen, wie unten gezeigt:

General Settings @ OpenVPN (Allgemeine Einstellungen @ OpenVPN)		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Enable (Aktivieren)	Klicken Sie auf den Schalter, um diesen OpenVPN-Tunnel zu aktivieren/ deaktivieren.	ON (EIN)
Enable IPv6 (IPv6 aktivieren)	Klicken Sie auf den Schalter, um diesen OpenVPN-Tunnel für die Verwendung von IPv6 zu aktivieren/ deaktivieren.	OFF (AUS)
Description (Beschreibung)	Geben Sie eine Beschreibung für diesen OpenVPN-Tunnel ein.	Null
Mode (Modus)	Wählen Sie aus „P2P“, „Client“ oder „Server“.	Client
TLS Mode (TLS-Modus)	Wählen Sie aus „None“ („Kein“), „Client“ oder „Server“.	None (Keine)
Protocol (Protokoll)	Wählen Sie aus „UDP“, „TCP-Client“ oder „TCP-Server“.	UDP
Server Address (Server-Adresse)	Geben Sie die End-to-End-IP-Adresse oder die Domäne des entfernten OpenVPN-Servers ein.	Null
Server Port (Server-Port)	Geben Sie den End-to-End-Listener-Port oder den Listener-Port des OpenVPN-Servers ein.	1194
Listening address (Listening-	Lokale Server-Adresse.	Null
Listening port (Listening-	Lokaler Server-Port.	1194
Interface Type (Schnittstellen-Typ)	Wählen Sie aus „TUN“ oder „TAP“, die zwei verschiedene Arten von Geräteschnittstellen für OpenVPN sind. Der Unterschied zwischen TUN- und TAP-Geräten besteht darin, dass ein TUN-Gerät ein virtuelles Punkt-zu-Punkt-Gerät im Netzwerk ist, während ein TAP-Gerät ein virtuelles Gerät im Ethernet ist.	TUN

Authentication Type (Authentifizierungstyp)	Wählen Sie aus „None“ („Keine“), „Preshared“ („Vorab vereinbart“), „Password“, „X509CA“ und „X509CA Password“. Hinweis: Die Authentifizierungstypen „None“ („Keine“) und „Preshared“ („Vorab vereinbart“) funktionieren nur im P2P-Modus.	None (Keine)
Enable IP Address pool (IP-Adress-Pool aktivieren)	Klicken Sie auf den Schalter, um die IP-Adress-Pool-Zuweisungsfunktion zu aktivieren/ deaktivieren.	OFF (AUS)
Starting Address (Startadresse)	Definiert den Beginn eines IP-Adress-Pools, der OpenVPN-Clients Adressen zuweist.	10.8.0.5
End Address (Endadresse)	Definiert das Ende des IP-Adress-Pools für die Zuweisung von Adressen an OpenVPN-Clients.	10.8.0.254
Client Network (Client-Netzwerk)	Geben Sie die Client-Netzwerk-IP ein.	10.8.0.0
Client Netmask (Client-Netzmaske)	Geben Sie die Client-Netzmaske ein.	255.255.255.0
Username (Benutzername)	Geben Sie den Benutzernamen ein, der für die Authentifizierungstypen „Password“ oder „X509CA Password“ verwendet wird.	Null
Password (Passwort)	Geben Sie das Passwort ein, das für die Authentifizierungstypen „Password“ oder „X509CA Password“ verwendet wird.	Null
Local IP (Lokale IP)	Geben Sie die lokale virtuelle IP ein.	10.8.0.1
Remote IP (Remote-IP)	Geben Sie die entfernte virtuelle IP ein.	10.8.0.2
Encrypt Algorithm (Verschlüsselungs-Algorithmus)	Wählen Sie aus „BF“, „DES“, „DES-EDE3“, „AES128“, „AES192“ und „AES256“. BF: 128-Bit-BF-Verschlüsselungsalgorithmus im CBC-Modus verwenden DES: 64-Bit-DES-Verschlüsselungsalgorithmus im CBC-Modus verwenden DES-EDE3: 192-Bit-3DES-Verschlüsselungsalgorithmus im CBC-Modus verwenden AES128: 128-Bit-AES-Verschlüsselungsalgorithmus im CBC-Modus verwenden AES192: 192-Bit-AES-Verschlüsselungsalgorithmus im CBC-Modus verwenden AES256: 256-Bit-AES-Verschlüsselungsalgorithmus im CBC-	BF
Renegotiation Interval (Renegotiation-Intervall)	Legen Sie das Renegotiation-Intervall fest. Wenn die Verbindung fehlgeschlagen ist, wird OpenVPN neu verhandeln, wenn das Renegotiation-Intervall erreicht ist.	86400
Maximum number of clients (Maximale Anzahl von Clients)	Legen Sie die maximale Anzahl von Clients fest, die auf den OpenVPN-Server zugreifen dürfen.	10
Keepalive Interval (Keepalive-Intervall)	Legen Sie ein Keepalive-Intervall (Ping-Intervall) fest, um zu prüfen, ob der Tunnel aktiv ist.	20
Keepalive Timeout (Keepalive-Zeitüberschreitung)	Legen Sie die Keepalive-Zeitüberschreitung fest. Ein OpenVPN-Neustart wird ausgelöst, nachdem n Sekunden verstrichen sind, ohne dass ein Ping oder ein anderes Paket aus der Ferne empfangen wurde.	120
MTU (MÜE)	Stellen Sie die maximale Übertragungseinheit ein.	1500

Data Sharding (Daten-Sharding)	Legen Sie die maximale Frame-Länge fest.	Null
Private Key Password (Passwort für privaten Schlüssel)	Geben Sie das Passwort des privaten Schlüssels unter dem Authentifizierungstyp „X509CA“ und „X509CA Password“ ein.	Null
Enable Compression (Kompression aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option, um den Datenstrom des Headers zu komprimieren.	ON (EIN)
Enable Default Gateway (Standard-Gateway aktivieren)	Einzelner Schalter zum Aktivieren/ Deaktivieren der Standard-Gateway-Funktion. Pushen Sie nach der Aktivierung die lokale Tunneladresse als Standard-Gateway des Peer-Gerätes.	OFF (AUS)
Enable NAT (NAT aktivieren)	Klicken Sie auf den Schalter, um die NAT-Option zu aktivieren /deaktivieren. Wenn diese Funktion aktiviert ist, wird die Quell-IP-Adresse des Hosts hinter dem Router vor dem Zugriff auf den entfernten OpenVPN-Client getarnt.	OFF (AUS)
Receive DNS Push (DNS-Push empfangen)	Einzelner Schalter zum Aktivieren/ Deaktivieren der Funktion DNS-Push empfangen. Nach der Aktivierung ist es erlaubt, DNS-Informationen zu empfangen, die von der Gegenstelle gepusht werden.	OFF (AUS)
Verbose Level (Ausführlichkeit)	Wählen Sie die Ausführlichkeitsstufe des Ausgabeprotokolls mit Werten von 0 bis 11. 0: Keine Ausgabe außer fatalen Fehlern 1~4: Normaler Einsatzbereich 5: Ausgabe von Rand W-Zeichen an die Konsole für jedes gelesene und geschriebene Paket 6~11: Debug-Info-Bereich	0
Advanced Settings @ OpenVPN (Erweiterte Einstellungen @ OpenVPN)		
Enable HMAC Firewall (HMAC-Firewall aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Fügen Sie zum Schutz vor DoS-Angriffen eine zusätzliche Ebene der HMAC-Authentifizierung zum TLS-Kontrollkanal hinzu.	OFF (AUS)
Enable PKCS#12 (PKCS#12 aktivieren)	Klicken Sie auf den Schalter, um das PKCS#12-Zertifikat zu aktivieren/ deaktivieren. Es handelt sich um einen Verschlüsselungsstandard für den Austausch digitaler Zertifikate, die zur Beschreibung persönlicher Identitätsinformationen verwendet werden.	OFF (AUS)
Enable nsCertType (nsCertType aktivieren)	Klicken Sie auf den Schalter, um nsCertType zu aktivieren/ deaktivieren. Dies erfordert, dass das Peer-Zertifikat mit einer expliziten nsCertType-Bezeichnung „Server“ signiert wurde.	OFF (AUS)
Enable Crl (Crl aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, können Client-Zertifikate widerrufen werden.	OFF (AUS)
Enable client to client (Client-zu-Client aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Funktion aktiviert ist, können Clients miteinander kommunizieren.	OFF (AUS)

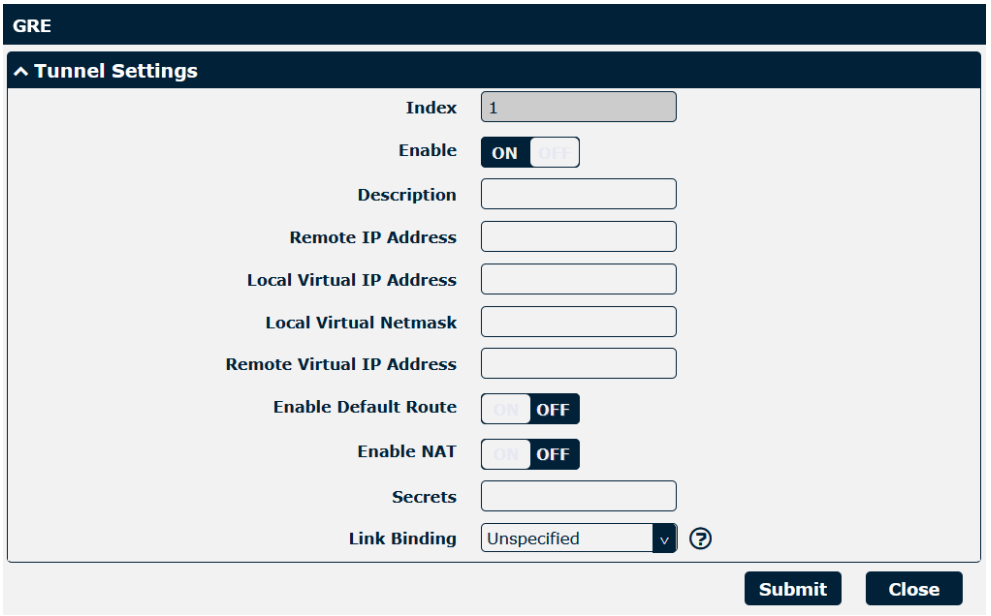
X509		
Punkt	Beschreibung	Standard
X509 Settings (X509-Einstellungen)		
Tunnel Name (Tunnelname)	Wählen Sie einen gültigen Tunnel. Wählen Sie aus „Tunnel 1“, „Tunnel 2“, „Tunnel 3“, „Tunnel 4“, „Tunnel 5“ oder „Tunnel 6“.	Tunnel 1
Tunnel Mode (Tunnel-Modus)	Wählen Sie aus „P2P Mode“ („P2P-Modus“), „Client Mode“ („Client-Modus“) oder „Server Mode“ („Server-Modus“).	Client mode
Root certificate (Root Zertifikat)	Wählen Sie die Root-Datei zum Importieren in den Router.	--
Certificate File (Zertifikat-Datei)	Klicken Sie auf „Durchsuchen“, um die Zertifikatsdatei in den Router hochzuladen.	--
Private Key (Privater Schlüssel)	Klicken Sie auf „ Durchsuchen “, um den privaten Schlüssel in den Router hochzuladen.	--
TLS Auth Key (TLS-Authentifizierungs-Schlüssel)	Klicken Sie auf „ Durchsuchen“, um den TLS-Authentifizierungs-Schlüssel in den Router hochzuladen.	--
PKCS#12 Certificate (PKCS#12-Zertifikat)	Klicken Sie auf „ Durchsuchen “, um das PKCS#12-Zertifikat in den Router hochzuladen.	--
Certificate Files (Zertifikat-Dateien)		
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Filename (Dateiname)	Zeigt den Namen des importierten Zertifikats an.	Null
File Size (Dateigröße)	Zeigt die Größe der Zertifikatsdatei an.	Null
Modification Time (Änderungszeit)	Zeigt den Zeitstempel an, wann die Zertifikatsdatei zuletzt geändert wurde.	Null

3.20 VPN > GRE

In diesem Abschnitt können Sie das GRE und die zugehörigen Parameter einstellen. Generic Routing Encapsulation (GRE) ist ein Tunneling-Protokoll, das eine Vielzahl von Netzwerkschichtprotokollen innerhalb virtueller Punkt-zu-Punkt-Verbindungen über ein Internet-Protokoll-Netzwerk kapseln kann.

GRE

Klicken Sie auf +, um Tunneleinstellungen hinzuzufügen. Die maximale Anzahl beträgt 3.



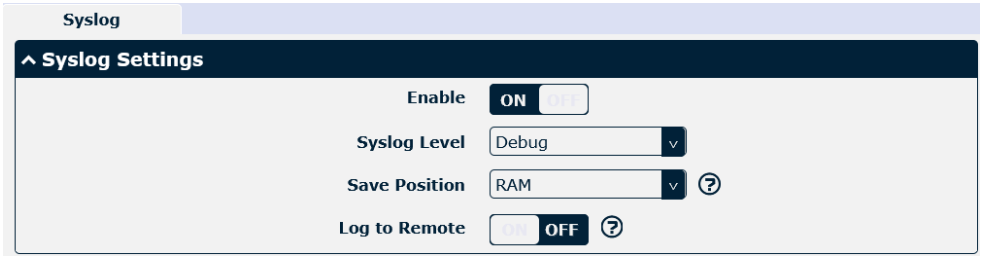
Tunnel Settings @ GRE (Tunneleinstellungen @ GRE)		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Enable (Aktivieren)	Klicken Sie auf den Schalter, um diesen GRE-Tunnel zu aktivieren/ deaktivieren.	ON (EIN)
Beschreibung	Geben Sie eine Beschreibung für diesen GRE-Tunnel ein.	Null
Remote IP Address (Entfernte IP-Adresse)	Stellen Sie die entfernte reale IP-Adresse des GRE-Tunnels ein.	Null
Local Virtual IP Address (Lokale virtuelle IP-Adresse)	Stellen Sie die lokale virtuelle IP-Adresse des GRE-Tunnels ein.	Null
Local Virtual Netmask (Lokale virtuelle Netzmaske)	Stellen Sie die lokale virtuelle Netzmaske des GRE-Tunnels ein.	Null
Remote Virtual IP Address / IPv6 prefix length (Länge virtuelle IP-Adresse / IPv6-Präfix)	Legen Sie die virtuelle Remote-IP-Adresse des GRE-Tunnels fest.	Null
Enable Default Route (Standard-Route aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, läuft der gesamte Datenverkehr des DSR-211 Routers über das GRE-VPN.	OFF (AUS)
Enable NAT (NAT aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Diese Option muss aktiviert werden, wenn der Router in einer NAT-Umgebung arbeitet.	Disable (Deaktiviert)
Secrets	Legen Sie den Schlüssel des GRE-Tunnels fest.	Null
Link Binding	Wählen Sie aus „WWAN1“, „WWAN2“, „WAN“ oder „WLAN“.	Not bound (Nicht gebunden)

Status

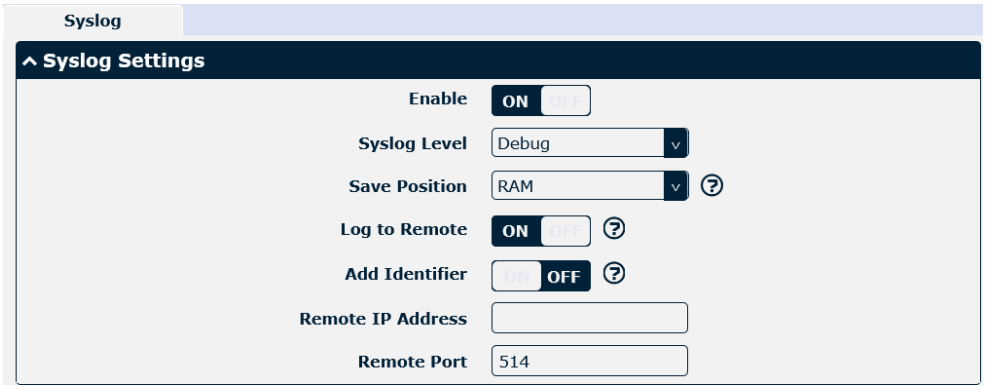
In diesem Abschnitt können Sie den Status des GRE-Tunnels einsehen.

3.21 Services > Syslog

In diesem Abschnitt können Sie die Syslog-Parameter einstellen. Das Systemprotokoll des DSR-211 Routers kann lokal gespeichert werden; es unterstützt auch das Senden an einen entfernten Protokollserver und spezifiziertes Anwendungs-Debugging. Standardmäßig ist die Option „Log to Remote“ („Auf Remote-Server protokollieren“) deaktiviert.



Bei Aktivierung der Option „Log to Remote“ („Auf Remote-Server protokollieren“) wird das Fenster wie unten dargestellt.

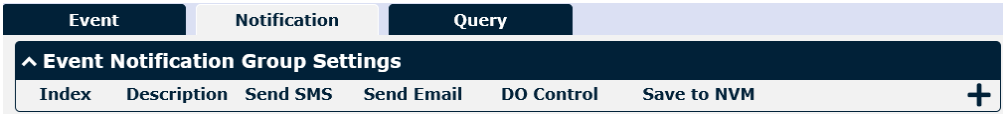


Syslog Settings (Syslog-Einstellungen)		
Punkt	Beschreibung	Standard
Enable (Aktivieren)	Klicken Sie auf den Schalter, um die Option Syslog-Einstellungen zu aktivieren/ deaktivieren.	OFF (AUS)
Syslog Level (Syslog-Ebene)	Wählen Sie aus „Debug“ („Debugging“), „Info“ („Information“), „Notice“ („Hinweis“), „Warning“ („Warnung“) oder „Error“ („Fehler“), die von niedrig bis hoch reichen. Die untere Ebene wird im Syslog mehr Details ausgeben.	Debug (Debugging)
Save Position (Speicherort)	Wählen Sie den Speicherort aus „RAM“, „NVM“ oder „Console“ („Konsole“). Wenn Sie „RAM“ wählen, werden die Daten nach dem Neustart gelöscht. Hinweis: Es wird nicht empfohlen, das Syslog lange Zeit im NVM (Non-Volatile Memory, nicht-flüchtiger Speicher) zu speichern.	RAM
Log to Remote (Auf Remote-Server protokollieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option, damit der Router das Syslog an den entfernten Syslog-Server senden kann. Sie müssen die IP und den Port des Syslog-Servers eingeben.	OFF (AUS)
Add Identifier (Bezeichner hinzufügen)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, können Sie der Syslog-Meldung eine Seriennummer hinzufügen.	OFF (AUS)
Remote IP Address (Remote-IP-Adresse)	Geben Sie die IP-Adresse des Syslog-Servers ein, wenn Sie die Option „Log to Remote“ („An Remote-Server protokollieren“) aktivieren.	Null
Remote Port (Remote-Port)	Geben Sie den Port des Syslog-Servers ein, wenn Sie die Option „Log to Remote“ („An Remote-Server protokollieren“) aktivieren.	514

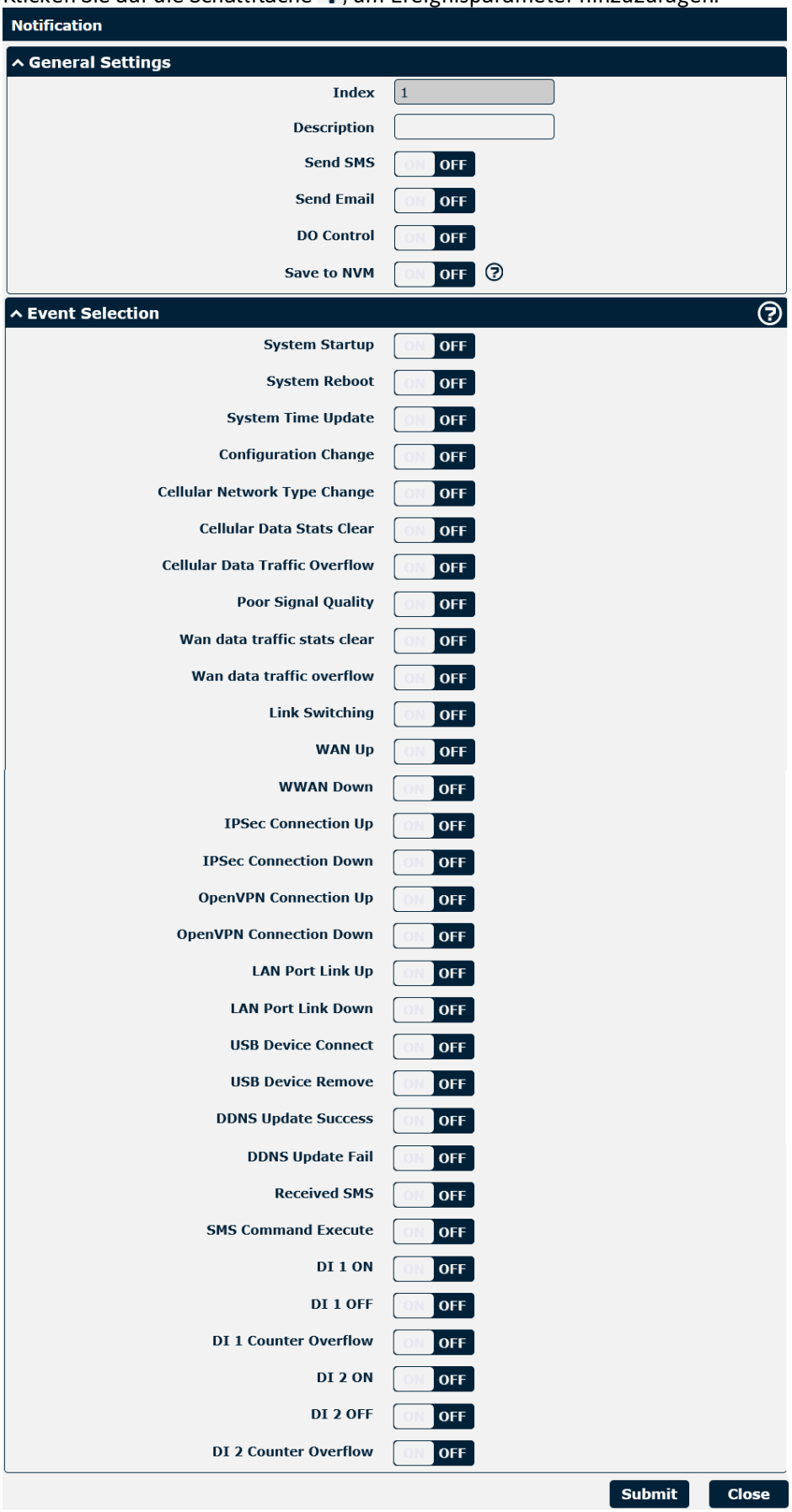
3.22 Services > Event

In diesem Abschnitt können Sie die Ereignisparameter einstellen. Die Ereignisfunktion bietet die Möglichkeit, Alarme per SMS oder E-Mail zu versenden, wenn bestimmte Systemereignisse auftreten.

General Settings @ Event (Allgemeine Einstellungen unter Ereignisse)		
Punkt	Beschreibung	Standard
Signal Quality Threshold (Signalqualitäts-Schwellenwert)	Legen Sie den Schwellenwert für die Signalqualität fest. Der Router erzeugt ein Protokollereignis, wenn der tatsächliche Wert unter dem angegebenen Schwellenwert liegt. 0 bedeutet, dass diese Option deaktiviert ist.	0

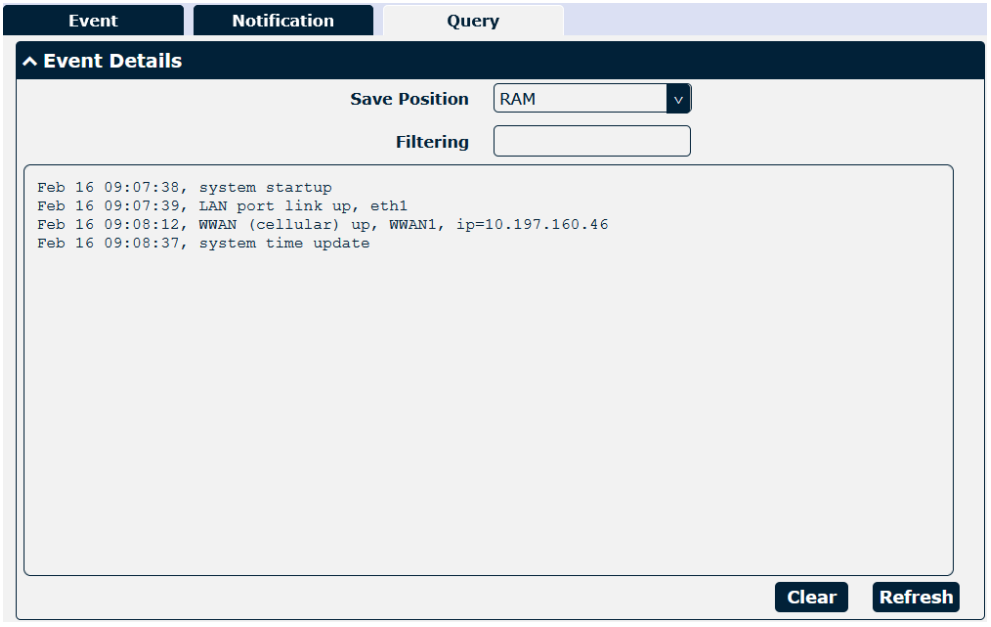


Klicken Sie auf die Schaltfläche +, um Ereignisparameter hinzuzufügen.



General Settings @ Notification (Allgemeine Einstellungen @ Benachrichtigungen)		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Description (Beschreibung)	Geben Sie eine Beschreibung für diese Gruppe ein.	Null
Sent SMS (SMS senden)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, sendet der Router bei Eintreten eines Ereignisses eine Benachrichtigung per SMS an die angegebenen Telefonnummern. Stellen Sie die zugehörige Telefonnummer unter „3.24 Services > SMS“ ein und verwenden Sie das Zeichen „;“ zum Trennen der Nummern.	OFF (AUS)
Send Email (E-Mail senden)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Wenn diese Option aktiviert ist, sendet der Router bei Eintreten eines Ereignisses eine Benachrichtigung per E-Mail an das angegebene E-Mail-Postfach. Stellen Sie die zugehörige E-Mail-Adresse unter „3.25 Services > E-Mail“ ein.	OFF (AUS)
DO Control (DO-Steuerung)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/deaktivieren. Nach dem Einschalten sendet der Ereignis-Router es in Form von Low/High Level an den entsprechenden DO.	OFF (AUS)
Save to NVM (Im NVM speichern)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option, um das Ereignis im nichtflüchtigen Speicher zu speichern.	OFF (AUS)

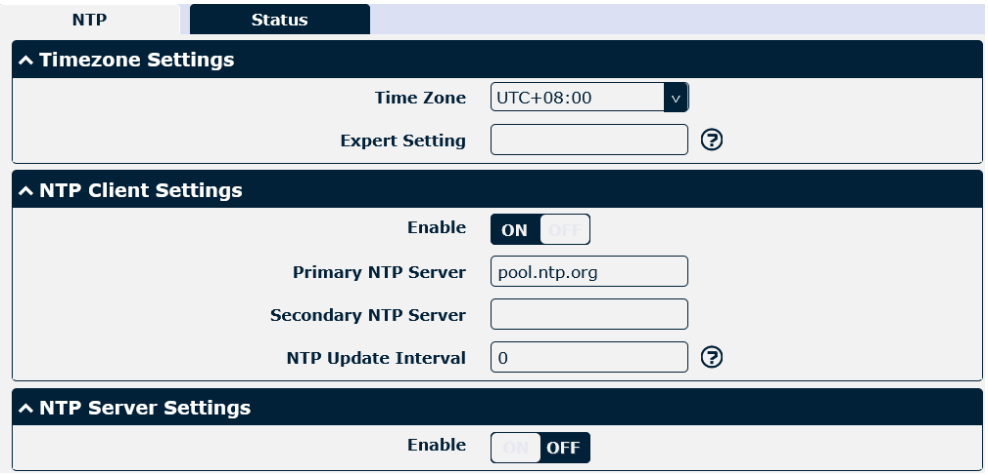
Im folgenden Fenster können Sie verschiedene Arten von Ereignisaufzeichnungen abfragen. Klicken Sie auf **Refresh**, um gefilterte Ereignisse abzufragen; klicken Sie auf **Clear**, um die Ereignisaufzeichnungen im Fenster zu löschen.



Event Details (Ereignisdetails)		
Punkt	Beschreibung	Standard
Save Position (Speicherort)	Wählen Sie den Speicherort aus „RAM“ oder „NVM“. RAM: Random-access memory (Flüchtiger Speicher) NVM: Non-Volatile Memory (Nichtflüchtiger Speicher)	RAM
Filter Message (Filternachricht)	Das Ereignis wird entsprechend der vom Benutzer eingestellten Filternachricht gefiltert. Klicken Sie auf die Schaltfläche „Refresh“ („Aktualisieren“), das gefilterte Ereignis wird in der folgenden Box angezeigt. Verwenden Sie „&“, um Filternachrichten zu trennen, z. B. Nachricht1& Nachricht2.	Null

3.23 Services > NTP

In diesem Abschnitt können Sie die zugehörigen NTP-Parameter (Network Time Protocol) einstellen, einschließlich Zeitzone, NTP-Client und NTP-Server.

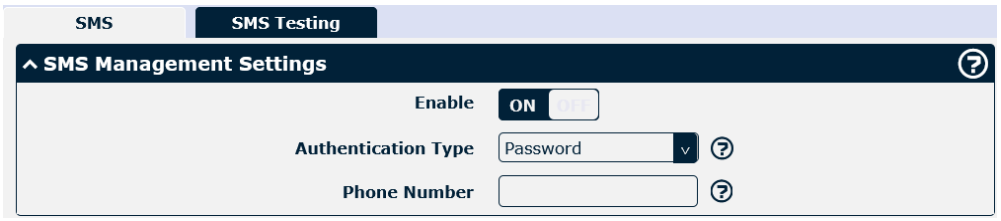


NTP		
Punkt	Beschreibung	Standard
Timezone Settings (Zeitzonen-Einstellungen)		
Time Zone (Zeitzone)	Klicken Sie auf die Dropdown-Liste, um die Zeitzone auszuwählen, in der Sie sich befinden.	MEZ+08:00
Expert Setting (Experteneinstellung)	Geben Sie die Zeitzone mit Sommerzeit im Format der Zeitzonen-Umgebungsvariablen an. Die Option Time Zone (Zeitzone) wird in diesem Fall ignoriert.	Null
NTP Client Settings (NTP-Client-Einstellungen)		
Enable (Aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren/ deaktivieren. Aktivieren Sie diese Option, um die Zeit mit dem NTP-Server zu synchronisieren.	ON (EIN)
Primary NTP Server (Primärer NTP-Server)	Geben Sie die IP-Adresse oder den Domänennamen des primären NTP-Servers ein.	pool.ntp.org
Secondary NTP Server (Sekundärer NTP-Server)	Geben Sie die IP-Adresse oder den Domänennamen des sekundären NTP-Servers ein.	Null
NTP Update interval (NTP-Aktualisierungs intervall)	Geben Sie das Intervall (Minuten) ein, in dem der NTP-Client die Zeit vom NTP-Server synchronisiert. Eine Einstellung in Minuten gibt das Warten auf die nächste Aktualisierung an; 0 bedeutet eine einmalige Synchronisierung.	0
NTP Server Settings (NTP-Server-Einstellungen)		
Enable (Aktivieren)	Klicken Sie auf den Schalter, um die Option NTP-Server zu aktivieren.	OFF (AUS)

In diesem Fenster können Sie die aktuelle Zeit des Routers anzeigen und auch die Router-Zeit synchronisieren. Klicken Sie auf die Schaltfläche Sync (Synchronisieren), um die Router-Zeit mit der Zeit des PC zu synchronisieren.

3.24 Services > SMS

In diesem Abschnitt können Sie die SMS-Parameter einstellen. Der DSR-211 Router unterstützt die SMS-Verwaltung. Die Benutzer können ihre Router durch den Versand von SMS steuern und konfigurieren. Weitere Einzelheiten zur SMS-Steuerung finden Sie unter 4.2.2 SMS Remote Control (SMS-Fernsteuerung).



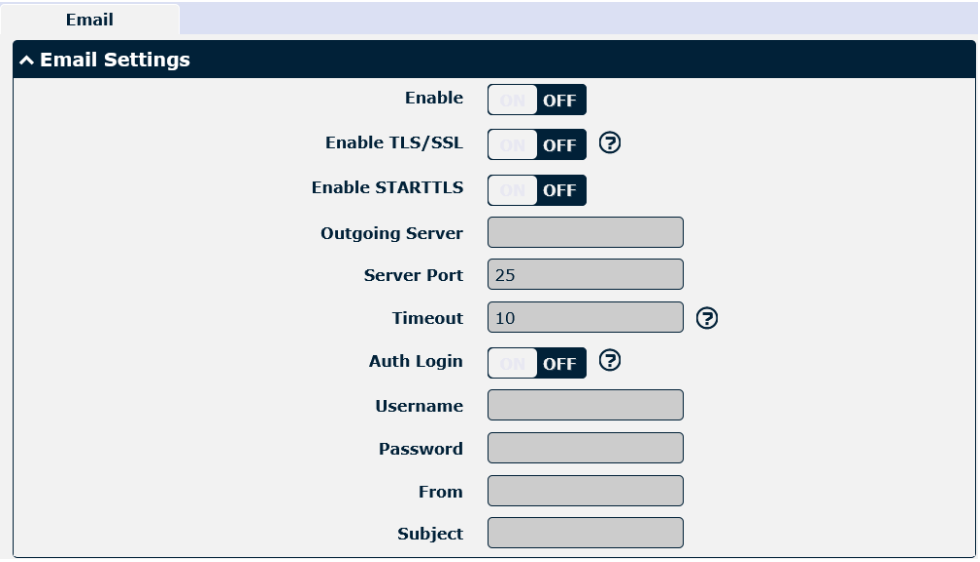
SMS Management Settings (SMS-Verwaltungseinstellungen)		
Punkt	Beschreibung	Standard
Enable (Aktivieren)	Klicken Sie auf den Schalter, um die Option SMS Management (SMS-Verwaltung) zu aktivieren/deaktivieren. Hinweis: Wenn diese Option deaktiviert ist, ist die SMS-Konfiguration ungültig.	ON (EIN)
Authentication Type (Authentifizierungstyp)	Wählen Sie den Authentifizierungstyp aus „Password“ („Passwort“), „Phonenum“ („Telefonnummer“) oder „Both“ („Beide“). Password (Passwort) Verwenden Sie zur Authentifizierung denselben Benutzernamen und dasselbe Passwort wie für den WEB-Manager. Zum Beispiel sollte das Format der SMS lauten: „Benutzername: Passwort; cmd1; cmd2; ...“. Hinweis: Legen Sie das WEB-Manager-Passwort im Abschnitt System > User Management (Benutzerverwaltung) fest. Phonenum (Telefonnummer: Verwenden Sie die Telefonnummer zur Authentifizierung. Der Benutzer sollte die Telefonnummer einstellen, die für die SMS-Verwaltung erlaubt ist. Das Format der SMS sollte „cmd1; cmd2;“ sein. Both (Beides): Verwenden Sie zur Authentifizierung sowohl das Passwort als auch die Telefonnummer. Der Benutzer sollte die Telefonnummer einstellen, die für die SMS-Verwaltung erlaubt ist. Das Format der SMS sollte „Benutzername: Passwort; cmd1; cmd2; ...“ lauten.	Password (Passwort)
Phone Number (Telefonnummer)	Stellen Sie die Telefonnummer ein, die für die SMS-Verwaltung verwendet wird, und verwenden Sie das Zeichen „;“ zum Trennen der Nummern. Hinweis: Sie kann null sein, wenn als Authentifizierungstyp „Password“ („Password“) gewählt wird.	Null

In diesem Abschnitt können Sie prüfen, ob der aktuelle SMS-Dienst verfügbar ist.

SMS Testing (SMS-Prüfung)		
Punkt	Beschreibung	Standard
Phone Number (Telefonnummer)	Geben Sie die spezifizierte Telefonnummer ein, die die SMS vom Router empfangen kann.	Null
Message (Nachricht)	Geben Sie die Nachricht ein, die der Router an die angegebene Telefonnummer senden soll.	Null
Result (Ergebnis)	Das Ergebnis des SMS-Tests wird im Ergebnisfeld angezeigt.	Null
Send	Klicken Sie auf die Schaltfläche, um die Testnachricht zu senden.	--

3.25 Services > E-Mail

Die E-Mail-Funktion unterstützt den Versand der Ereignisbenachrichtigungen an den angegebenen Empfänger per E-Mail.

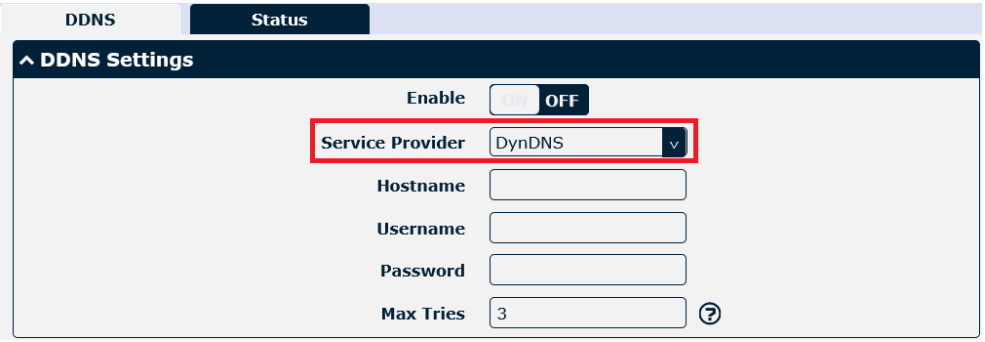


Email Settings (E-Mail-Einstellungen		
Punkt	Beschreibung	Standard
Enable (Aktivieren)	Klicken Sie auf den Schalter, um die Option E-Mail zu aktivieren/ deaktivieren.	OFF (AUS)
Enable TLS/ SSL (TLS/SSL aktivieren)	Klicken Sie auf den Schalter, um die TLS/SSL-Option zu aktivieren/ deaktivieren.	OFF (AUS)
Enable STARTTLS (STARTTLS aktivieren)	Klicken Sie auf den Schalter, um die STARTTLS-Verschlüsselung zu aktivieren/deaktivieren.	OFF (AUS)
Outgoing server (Ausgangsserver)	Geben Sie die IP-Adresse oder den Domänennamen des SMTP-Servers ein.	Null
Server port (Server-Port)	Geben Sie den SMTP-Server-Port ein.	25

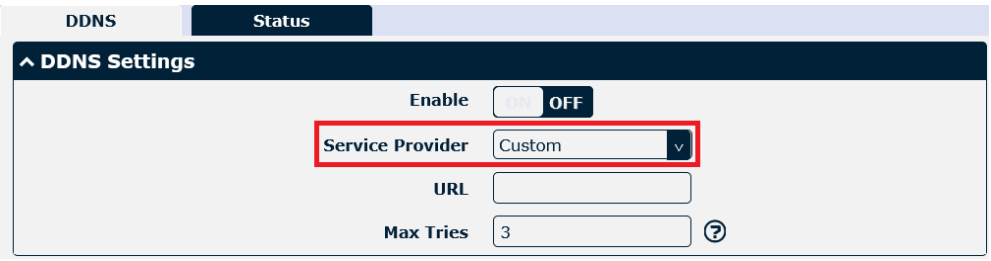
Timeout (Zeitüberschreitung)	Legen Sie die maximale Zeit für das Senden von E-Mails an den SMTP-Server fest. Wenn der Server die E-Mail in dieser Zeit nicht erhält, wird ein erneuter Sendeversuch erfolgen.	10
Auth Login (Auth-Anmeldung)	Wenn der Mail-Server AUTH-Login unterstützt, müssen Sie diese Schaltfläche aktivieren und einen Benutzernamen und ein Passwort festlegen.	OFF (AUS)
Username (Benutzername)	Geben Sie den Benutzernamen ein, der vom SMTP-Server registriert wurde.	Null
Password (Passwort)	Geben Sie das Passwort des obigen Benutzernamens ein.	Null
From (Von)	Geben Sie die Quelladresse der E-Mail ein.	Null
Subject (Betreff)	Geben Sie den Betreff dieser E-Mail ein.	Null

3.26 Services > DDNS

In diesem Abschnitt können Sie die DDNS-Parameter einstellen. Die Dynamic-DNS-Funktion ermöglicht es Ihnen, eine dynamische IP-Adresse mit einem statischen Domänennamen zu pseudonymisieren. Damit können Sie einen Domänennamen nutzen, auch wenn der ISP keine statische IP-Adresse zuweist. Dies ist besonders nützlich für das Hosting von Servern über Ihre Verbindung, so dass jeder, der sich mit Ihnen verbinden möchte, Ihren Domänennamen verwenden kann, anstatt Ihre dynamische IP-Adresse verwenden zu müssen, die sich von Zeit zu Zeit ändert. Diese dynamische IP-Adresse ist die WAN-IP-Adresse des Routers, die Ihnen von Ihrem ISP zugewiesen wird. Der Dienstanbieter ist standardmäßig auf „DynDNS“ eingestellt, wie unten dargestellt.

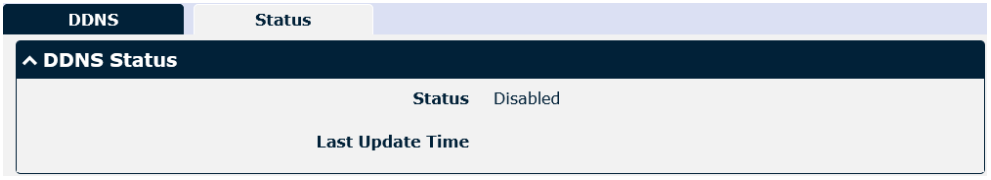


Wenn Sie als Dienstanbieter „Custom“ („Benutzerdefiniert“) gewählt haben, wird das Fenster wie unten dargestellt.



DDNS Settings (DDNS-Einstellungen)		
Punkt	Beschreibung	Standard
Enable (Aktivieren)	Klicken Sie auf den Schalter, um die DDNS-Option zu aktivieren/ deaktivieren.	OFF (AUS)
Service Provider (Dienstanbieter)	Wählen Sie den DDNS-Dienst aus „DynDNS“, „NO-IP“ oder „3322“ Hinweis: Der DDNS-Dienst kann nur nach Registrierung durch den entsprechenden Dienstanbieter genutzt werden.	DynDNS
Hostname (Host-Name)	Geben Sie den vom DDNS-Server bereitgestellten Host-Namen ein.	Null
Username (Benutzername)	Geben Sie den vom DDNS-Server bereitgestellten Benutzernamen ein.	Null
Password (Passwort)	Geben Sie das vom DDNS-Server bereitgestellte Passwort ein.	Null
URL	Geben Sie die vom Benutzer angepasste URL ein.	Null

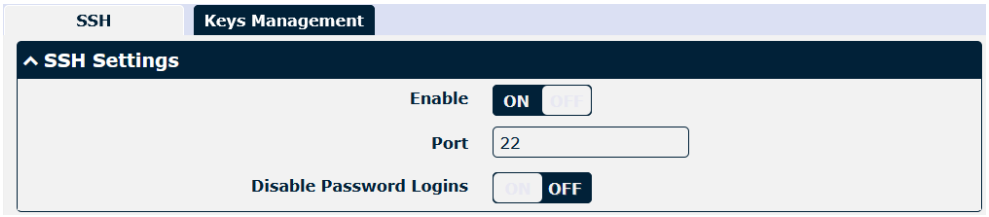
Klicken Sie auf die „Status“-Leiste, um den Status des DDNS anzuzeigen.



DDNS Status	
Punkt	Beschreibung
Status	Zeigt den aktuellen Status des DDNS an.
Last Update Time (Letzte Aktualisierungszeit)	Zeigt das Datum und die Uhrzeit an, zu denen das DDNS zuletzt aktualisiert wurde.

3.27 Services > SSH

Der DSR-211 Router unterstützt SSH-Passwort-Zugang und Zugang mit geheimen Schlüsseln.

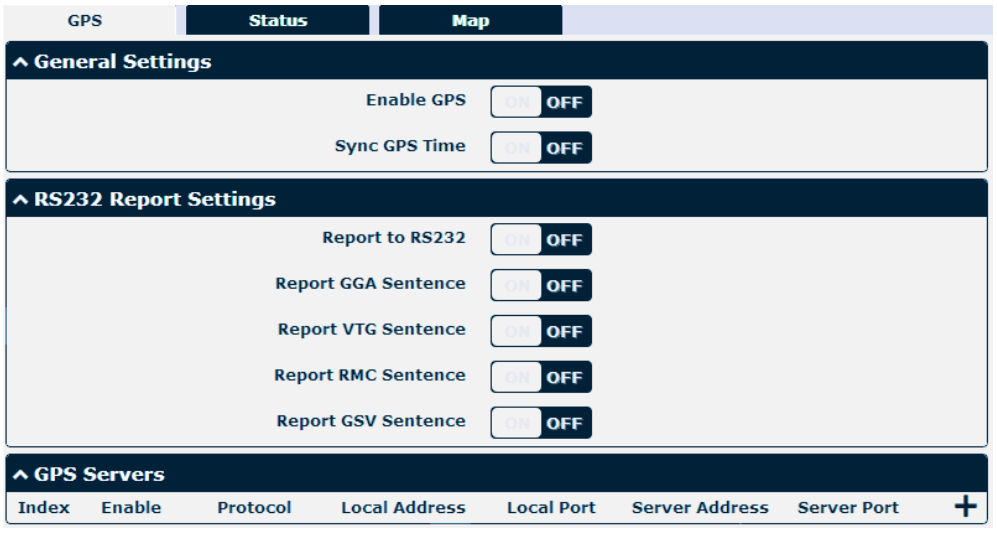


SSH Settings (SSH-Einstellungen)		
Punkt	Beschreibung	Standard
Enable (Aktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren /deaktivieren. Wenn diese Option aktiviert ist, können Sie über SSH auf den DSR-211 Router zugreifen.	OFF (AUS)
Port	Legen Sie den Port des SSH-Zugriffs fest.	22
Disable Password Logins (Passwort-Logins deaktivieren)	Klicken Sie auf den Schalter, um diese Option zu aktivieren /deaktivieren. Wenn diese Option aktiviert ist, können Sie Benutzername und Passwort nicht für den Zugriff auf den Router über SSH verwenden. In diesem Fall kann nur der Schlüssel für die Anmeldung verwendet werden.	OFF (AUS)

Keys Management (Verwaltung von Schüsseln)	
Punkt	Beschreibung
Authorized Keys (Autorisierte Schlüssel)	Klicken Sie auf „Durchsuchen“, um einen autorisierten Schlüssel auf Ihrem Computer zu lokalisieren, und klicken Sie dann auf „Import“ („Importieren“), um diesen Schlüssel in Ihren Router zu importieren. Hinweis: Diese Option ist gültig, wenn die Option für Passwort-Logins aktiviert ist.

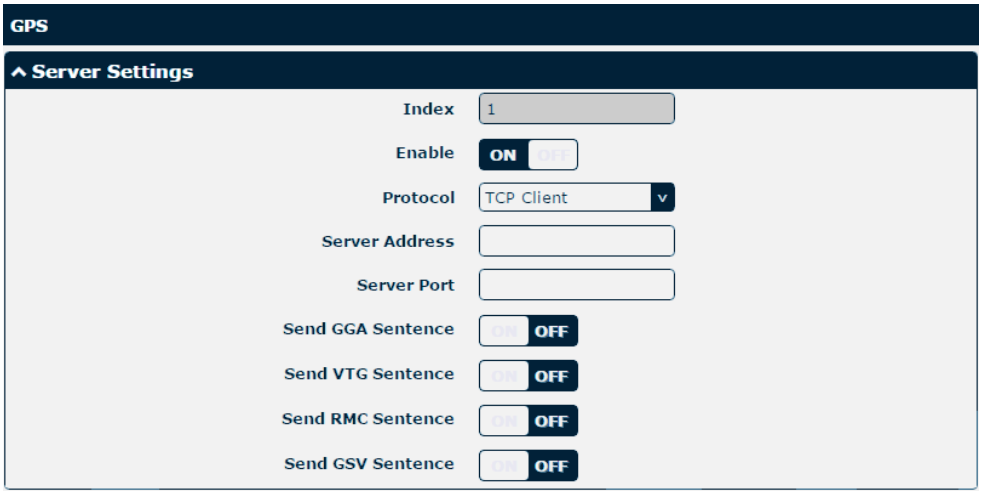
3.28 Services > GPS

In diesem Abschnitt können Sie die GPS-Parameter einstellen.

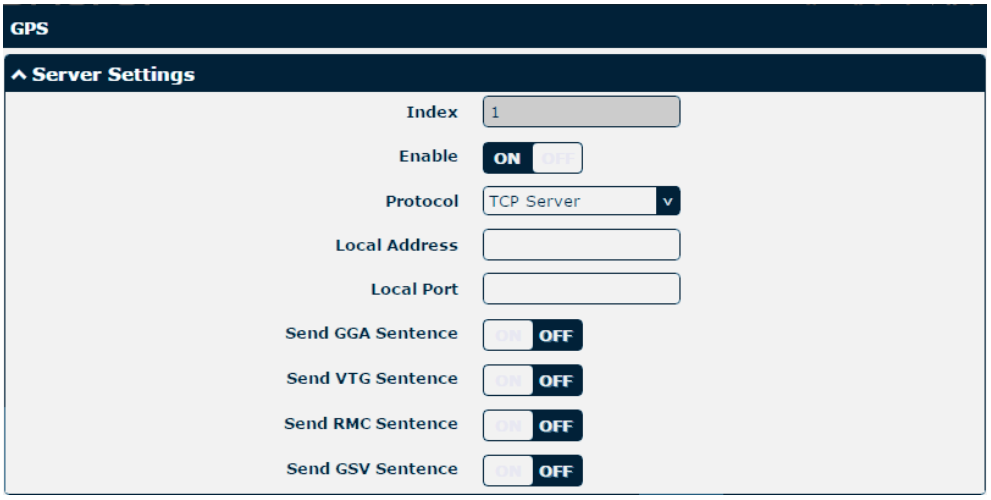


General Settings @ GPS (Allgemeine Einstellungen @ GPS)		
Punkt	Beschreibung	Standard
Enable GPS (GPS aktivieren)	Klicken Sie auf den Schalter, um die GPS-Option zu aktivieren/ deaktivieren.	OFF (AUS)
Sync GPS Time (GPS-Zeit synchronisieren)	Klicken Sie auf den Schalter, um die GPS-Zeit zu synchronisieren.	OFF (AUS)
RS 232 Report Settings (RS-232-Berichtseinstellungen)		
Report to RS 232 (Bericht an RS-232)	Klicken Sie auf den Schalter, um an RS-232 zu berichten.	OFF (AUS)
Report GGA Sentence (GGA-Satz berichten)	Klicken Sie auf den Schalter, um den GGA-Satz zu berichten.	OFF (AUS)
Report VTG Sentence (VTG-Satz berichten)	Klicken Sie auf den Schalter, um den VTG-Satz zu berichten.	OFF (AUS)
Report RMC Sentence (RMC-Satz berichten)	Klicken Sie auf den Schalter, um den RMC-Satz zu berichten.	OFF (AUS)
Report GSV Sentence (GSV-Satz berichten)	Klicken Sie auf den Schalter, um den GSV-Satz zu berichten.	OFF (AUS)

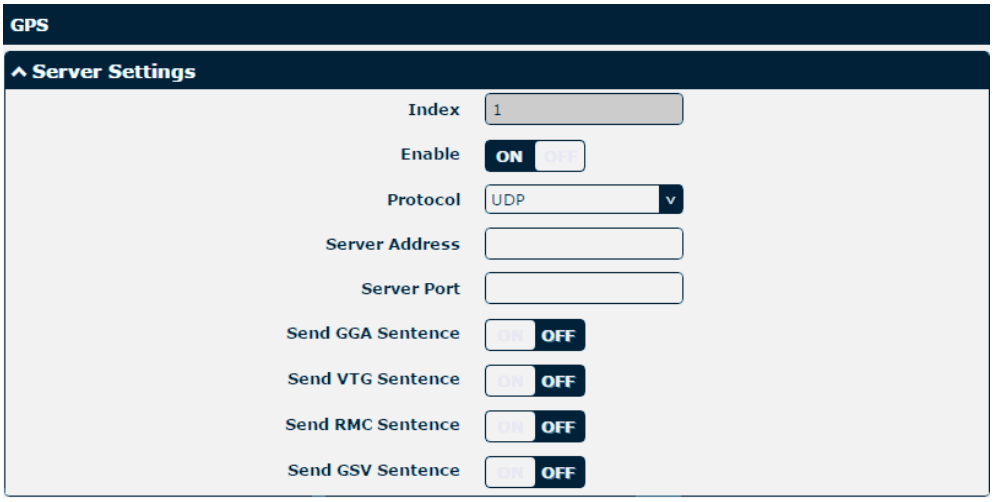
Wenn Sie als Protokoll „TCP Client“ wählen, wird das Fenster wie unten dargestellt.



Wenn Sie als Protokoll „TCP Server“ wählen, wird das Fenster wie unten dargestellt:



Wenn Sie als Protokoll „UDP“ wählen, wird das Fenster wie unten dargestellt:



Server Settings (Server-Einstellungen)		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Enable (Aktivieren)	Klicken Sie auf den Schalter, um die GPS-Servereinstellungen zu aktivieren/ deaktivieren.	ON (EIN)
Protocol (Protokoll)	Wählen Sie aus „TCP Client“, „TCP Server“ oder „UDP“.	TCP Client
Server Address @TCP Client	Legen Sie die Adresse des TCP-Clients fest.	Null
Server Port @TCP Client	Legen Sie den Port des entfernten TCP-Servers fest.	Null
Local Address	Legen Sie die lokale Adresse fest, wenn der Router als TCP-Server eingestellt ist.	Null
Local Port (Lokaler Port)	Legen Sie den lokalen Port fest, wenn der Router als TCP-Server eingestellt ist.	Null

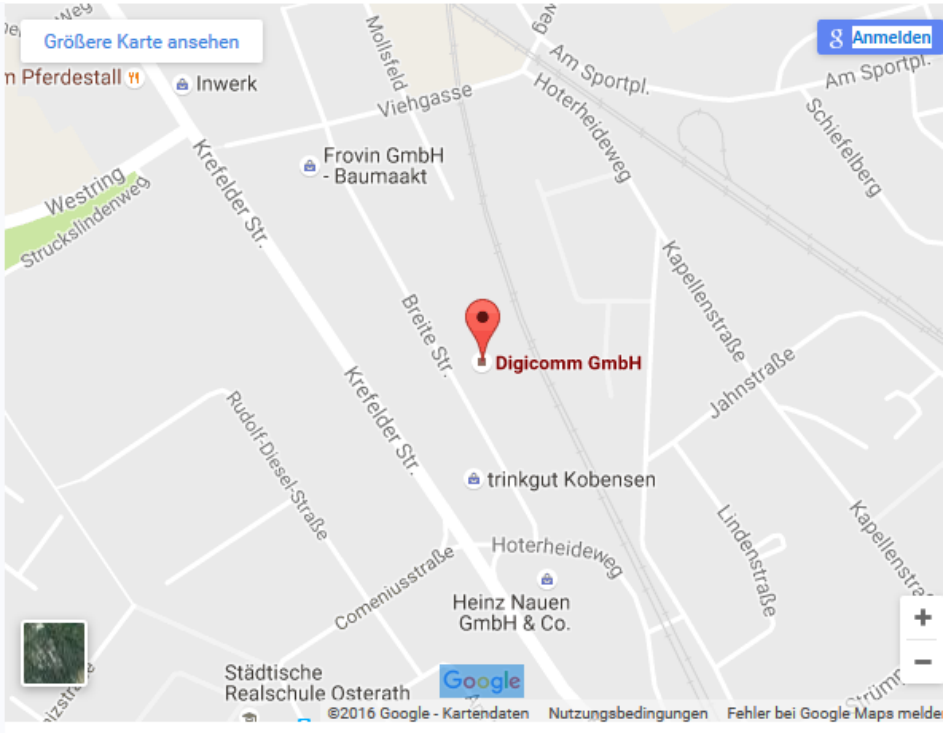
Server Address @ UDP	Legen Sie die Adresse des UDP-Servers fest.	Null
Server Port @ UDP (Server-Port @ UDP)	Legen Sie den Port des entfernten UDP-Servers fest.	Null
Send GGA Sentence (GGA-Satz senden)	Senden Sie GGA-Informationen im NMEA-Format.	OFF (AUS)
Send VTG Sentence (VTG-Satz senden)	Senden Sie VTG-Informationen im NMEA-Format.	OFF (AUS)
Send RMC Sentence (RMC-Satz senden)	Senden Sie RMC-Informationen im NMEA-Format.	OFF (AUS)
Send GSV Sentence (GSV-Satz senden)	Senden Sie GSV-Informationen im NMEA-Format.	OFF (AUS)

Klicken Sie auf die Spalte Status, um den Status des GPS anzuzeigen.

GPS Status	
Punkt	Beschreibung
Status	Zeigt den GPS-Status an. Der GPS-Status umfasst: „NO Fix“ („KEIN Fix“), „2D Fix“ and „3D Fix“.
UTC Time (UTC-Zeit)	Zeigt die UTC der Satelliten an. Dabei handelt es sich um die koordinierte Weltzeit, nicht die Lokalzeit.
Last Fixed Time (Zeit des letzten Fix)	Zeigt die letzte Positionierungszeit an.
Satellites In Use (Genutzte Satelliten)	Zeigt die Anzahl der genutzten Satelliten an.
Satellite In View (Satelliten in Sicht)	Zeigt die Anzahl der Satelliten in Sicht an.
Latitude (Breitengrad)	Zeigt den Breitengradstatus des Routers an.
Longitude (Längengrad)	Zeigt den Längengradstatus des Routers an.
Altitude (Höhe)	Zeigt den Höhenstatus des Routers an.

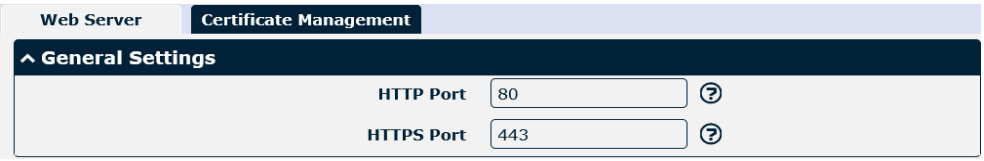
Speed (Geschwindigkeit)	Zeigt die horizontale Geschwindigkeit des Routers an.

Klicken Sie auf die Spalte Map (Karte), um den aktuellen Standort des Routers anzuzeigen.



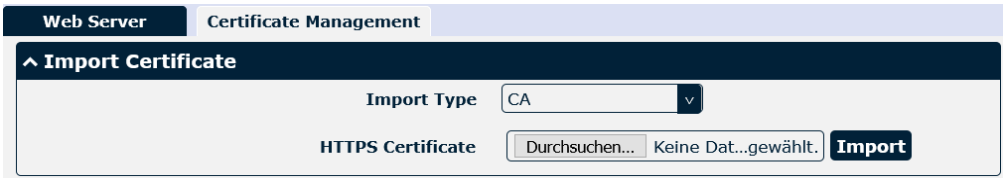
3.29 Services > Web-Server

In diesem Abschnitt können Sie die Parameter des Web-Servers ändern.



Basic @ Web Server (Grundlagen @ Web-Server)		
Punkt	Beschreibung	Standard
HTTP Port	Geben Sie die HTTP-Portnummer ein, die Sie im Web-Server des Routers ändern möchten. Auf einem Web-Server ist Port 80 der Port, auf dem der Server „lauscht“ bzw. auf dem er Nachrichten eines Web-Clients erwartet. Wenn Sie den Router mit einer anderen HTTP-Port-Nummer als 80 konfigurieren, können Sie sich nur am Web-Server des Routers anmelden, wenn Sie diese Port-Nummer hinzufügen.	80
HTTPS Port	Geben Sie die HTTPS-Portnummer ein, die Sie im Web-Server des Routers ändern möchten. Auf einem Web-Server ist Port 443 der Port, auf dem der Server „lauscht“ bzw. auf dem er Nachrichten eines Web-Clients erwartet. Wenn Sie den Router mit einer anderen HTTPS-Port-Nummer als 443 konfigurieren, können Sie sich nur am Web-Server des DSR-211 anmelden, wenn Sie diese Port-Nummer hinzufügen. Hinweis: HTTPS ist sicherer als HTTP. In vielen Fällen tauschen Clients möglicherweise vertrauliche Informationen mit einem Server aus, der gesichert werden muss, um unbefugten Zugriff zu verhindern. Aus diesem Grund wurde HTTPS von der Netscape Corporation entwickelt, um Autorisierung und sichere Transaktionen zu ermöglichen.	443

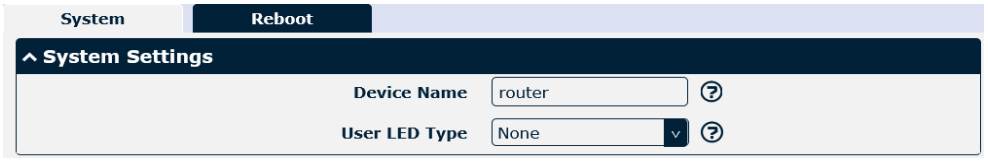
In diesem Abschnitt können Sie die Zertifikatsdatei in den Router importieren.

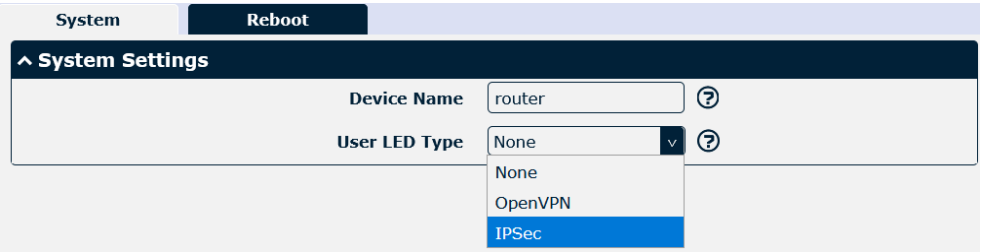


Certificate Management (Verwaltung von Zertifikaten)		
Punkt	Beschreibung	Standard
Import Type (Import-Typ)	Wählen Sie aus „CA“ und „Private Key“ („Privater Schlüssel“). CA: ein vom CA-Zentrum ausgestelltes digitales Zertifikat Private Key (Privater Schlüssel): eine Datei mit privatem Schlüssel	CA
HTTPS Certificate (HTTPS-Zertifikat)	Klicken Sie auf „Durchsuchen“, um die Zertifikatsdatei auf Ihrem Computer zu lokalisieren, und klicken Sie dann auf „Import“ („Importieren“), um diese Datei in Ihren Router zu importieren.	--

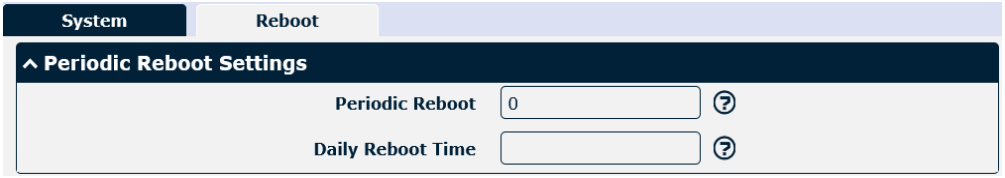
3.30 Services > Advanced

In diesem Abschnitt können Sie die erweiterten Parameter einstellen.





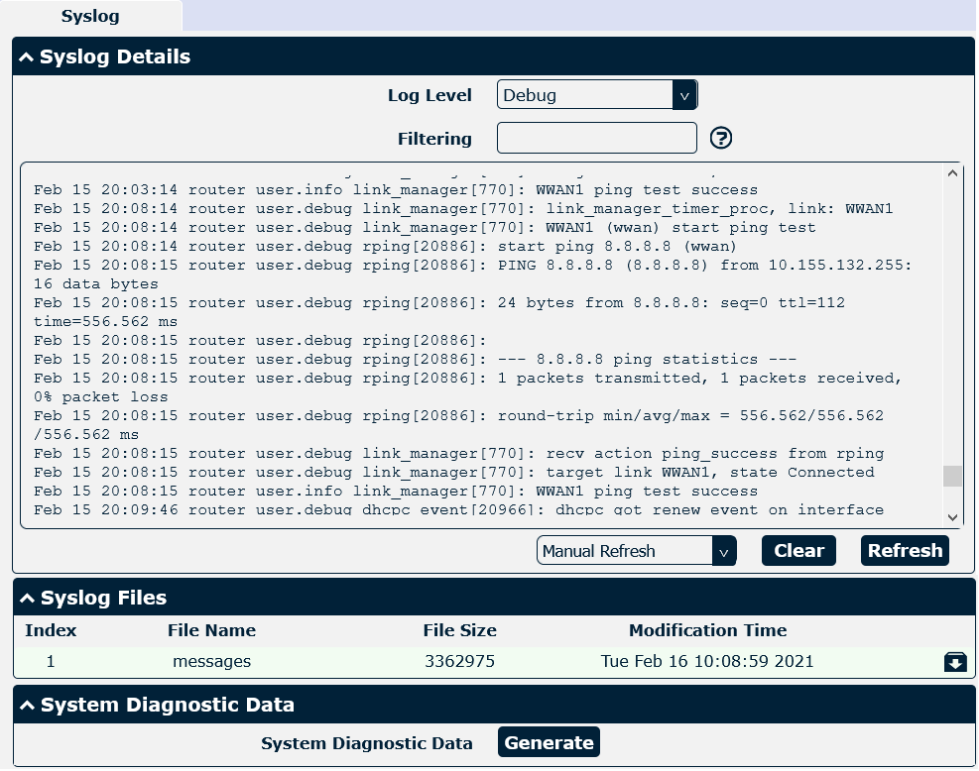
System Settings (Systemeinstellungen)		
Punkt	Beschreibung	Standard
Device Name (Gerätename)	Stellen Sie den Gerätenamen so ein, dass verschiedene von Ihnen installierte Geräte unterschieden werden können; gültige Zeichen sind a–z, A–Z, 0–9, @, ., -, #, $ und * .	router
User LED Type (Benutzer-LED-Typ)	Legen Sie den Anzeigetyp Ihrer USR-LED fest. Wählen Sie aus „None“ („Keine“), „OpenVPN“, „IPsec“ oder „WiFi“. None: Bedeutungslose Anzeige, die LED ist aus OpenVPN: USR-Indikator, der den OpenVPN-Status anzeigt IPsec: USR-Indikator, der den IPsec-Status anzeigt WiFi: USR-Indikator, der den WiFi-Status anzeigt Hinweis: Weitere Einzelheiten zum USR-Indikator finden Sie unter „2.2 LED Indicators“ („LED-Anzeigen“).	None (Keine)



Reboot (Neustart)		
Punkt	Beschreibung	Standard
Periodic Reboot (Periodischer Neustart)	Legen Sie die Neustartperiode des Routers fest. 0 bedeutet deaktiviert.	0
Daily Reboot Time (Tägliche Neustartzeit)	Stellen Sie die tägliche Neustartzeit des Routers ein. Nutzen Sie das Format HH:MM in einem 24-Stunden-Zeitraum, da die Angaben sonst ungültig sind. Wenn Sie das Feld leer lassen, bedeutet dies deaktivieren.	Null

3.31 System > Debug

In diesem Abschnitt können Sie die Syslog-Details überprüfen und herunterladen.



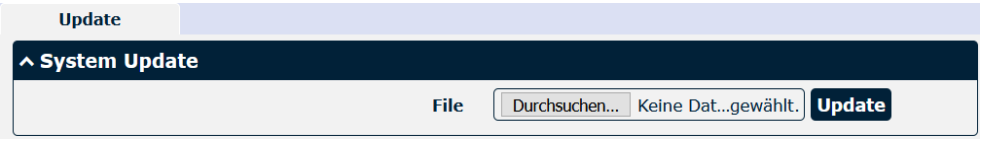
Syslog (Systemprotokoll)		
Punkt	Beschreibung	Standard
Syslog Details		
Log Level (Protokoll-Ebene)	Wählen Sie aus „Debug“ („Debugging“), „Info“ („Information“), „Notice“ („Hinweis“), „Warn“ („Warnung“) oder „Error“ („Fehler“), die von niedrig bis hoch reichen. Die untere Ebene wird im Syslog mehr Details ausgeben.	Debug (Debugging)
Filtering (Filterung)	Geben Sie die Filternachricht basierend auf den Schlüsselwörtern ein. Verwenden Sie „&“, um mehrere Filternachrichten zu trennen, z. B. „Schlüsselwort1&Schlüsselwort2“.	Null
Refresh (Aktualisierung)	Wählen Sie aus „Manual Refresh“ („Manuelle Aktualisierung“), „5 Seconds“ („5 Sekunden“), „10 Seconds“ („10 Sekunden“), „20 Seconds“ („20 Sekunden“) oder „30 Seconds“ („30 Sekunden“). Sie können diese Intervalle auswählen, um die im folgenden Feld angezeigten Protokollinformationen zu aktualisieren. Wenn Sie „Manuel Refresh“ („Manuelle Aktualisierung“) wählen, sollten Sie auf die Aktualisierungs-Schaltfläche klicken, um das Syslog zu aktualisieren.	Manual Refresh (Manuelle Aktualisierung)
Clear	Klicken Sie auf die Schaltfläche, um das Syslog zu löschen.	--

Refresh	Klicken Sie auf die Schaltfläche, um das Syslog zu aktualisieren.	--
Syslog Files (Syslog-Dateien)		
Syslog Files List (Liste der Syslog-Dateien)	Es können maximal 5 Syslog-Dateien in der Liste angezeigt werden. Die Dateinamen reichen von message 0 bis message 4. Die neueste Syslog-Datei wird an den Anfang der Liste gestellt.	/
System Diagnosing Data (Daten zur Systemdiagnose)		
Generate	Klicken Sie auf die Schaltfläche, um die Syslog-Diagnosedatei zu generieren.	/
Download	Klicken Sie auf die Schaltfläche, um die generierten Systemdiagnosedaten herunterzuladen.	/

3.32 System > Update

In diesem Abschnitt können Sie die Firmware Ihres DSR-211 aktualisieren. Klicken Sie auf System > Update (Aktualisierung) > System Update (Systemaktualisierung) und dann auf „Durchsuchen“, um die Firmware-Datei für das Upgrade zu lokalisieren. Sobald die neueste Firmware ausgewählt wurde, klicken Sie auf **Update**, um den Upgrade-Prozess zu starten. Der Upgrade-Prozess kann mehrere Minuten dauern. Schalten Sie Ihren Router während des Firmware-Upgrade-Prozesses nicht aus.

Hinweis: Um auf die neueste Firmware-Datei zuzugreifen, wenden Sie sich bitte an Ihren technischen Support.



Update		
Punkt	Beschreibung	Standard
System Update (System-Aktualisierung)	Klicken Sie auf „Durchsuchen“, um die richtige Firmware auf Ihrem PC auszuwählen, und klicken Sie dann auf die Schaltfläche **Update** zum Aktualisieren. Nach erfolgreicher Aktualisierung klicken Sie auf „Save and Apply“ („Speichern und Übernehmen“) und dann den Router neu starten, damit die Änderungen wirksam werden.	Null

3.33 System > App Center

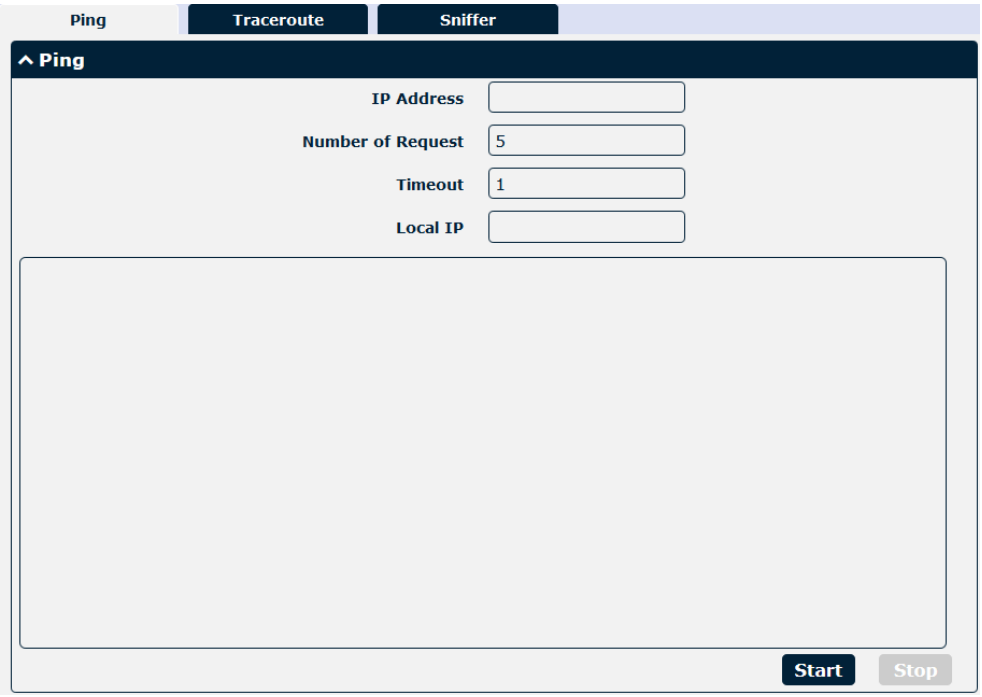
In diesem Abschnitt können Sie dem Router einige erforderliche oder benutzerspezifische Anwendungen hinzufügen. Importieren und installieren Sie Ihre Anwendungen in das App Center, und starten Sie das Gerät entsprechend den Systemaufforderungen neu. Die installierten Anwendungen werden unter dem Menü „Services“ („Dienste“) angezeigt. Anwendungen im Zusammenhang mit VPN werden unter dem Menü „VPN“ angezeigt.

Hinweis: Nach dem Import der Anwendungen in den Router kann die Seitenanzeige aufgrund des Browser-Caches eine leichte Verzögerung aufweisen. Es wird empfohlen, zuerst den Cache des Browsers zu leeren und sich dann erneut am Router anzumelden.

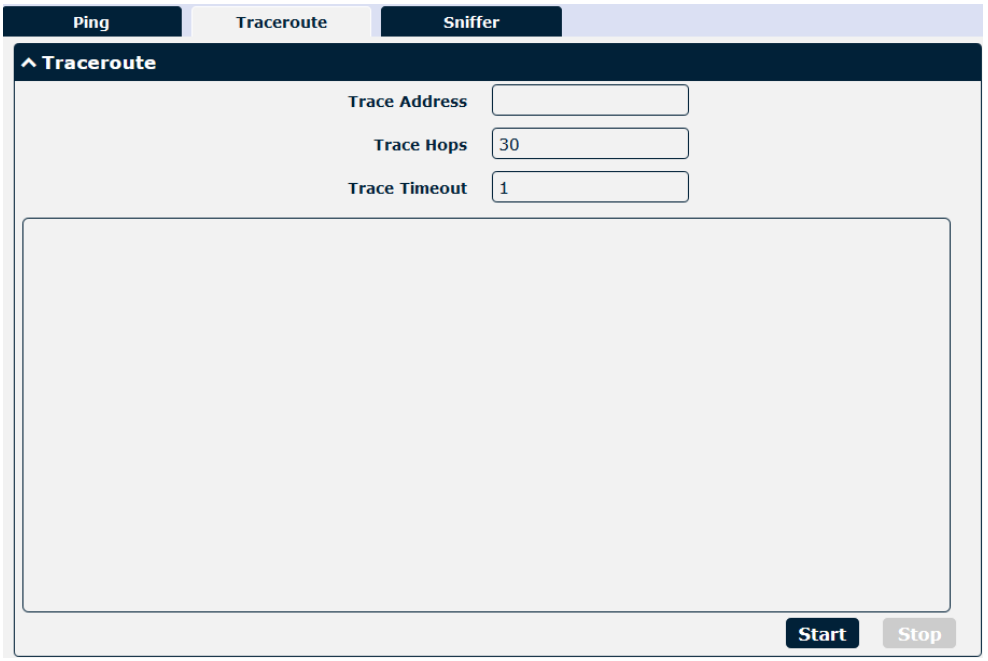
App Center		
Punkt	Beschreibung	Standard
App Install (App installieren)		
File (Datei)	Klicken Sie auf „Durchsuchen“, um die App-Datei auf Ihrem Computer zu lokalisieren, und klicken Sie dann auf Install (installieren), um diese Datei in Ihren Router zu importieren. Hinweis: Das Dateiformat sollte xxx.rpk sein	--
Installed Apps (Installierte Anwendungen)		
Index	Gibt die Ordinalzahl der Liste an.	--
Name	Zeigt den Namen der App an.	Null
Version	Zeigt die Version der App an.	Null
Status	Zeigt den Status der App an.	Null
Description (Beschreibung)	Zeigt die Beschreibung für diese App an.	Null

3.34 System > Tools

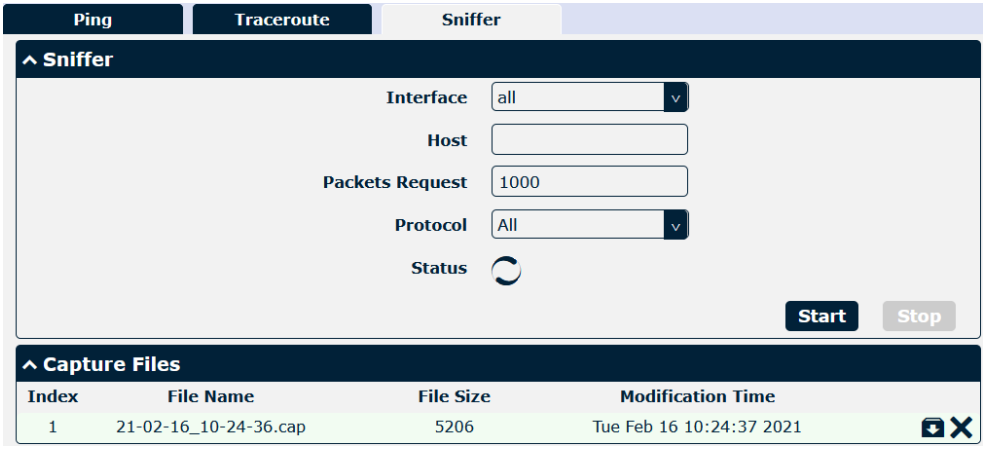
Dieser Abschnitt stellt den Benutzern drei Werkzeuge zur Verfügung: Ping, Traceroute und Sniffer.



Ping		
Punkt	Beschreibung	Standard
IP address (IP-Adresse)	Geben Sie die Ziel-IP-Adresse oder Zieldomäne des Pings ein.	Null
Number of Requests (Anzahl der Anfragen)	Geben Sie die Anzahl der Ping-Anfragen ein.	5
Timeout (Zeitüberschreitung)	Geben Sie die Zeitüberschreitung der Ping-Anfragen an.	1
Local IP (Lokale IP)	Geben Sie die lokale IP des Mobilfunk-WAN, Ethernet-WAN oder Ethernet-LAN an. Null steht für die automatische Auswahl einer lokalen IP-Adresse aus diesen drei Möglichkeiten.	Null
Start	Klicken Sie auf diese Schaltfläche, um die Ping-Anforderung zu starten, und das Protokoll wird in der folgenden Box angezeigt.	Null
Stop	Klicken Sie auf diese Schaltfläche, um die Ping-Anforderung zu beenden.	--



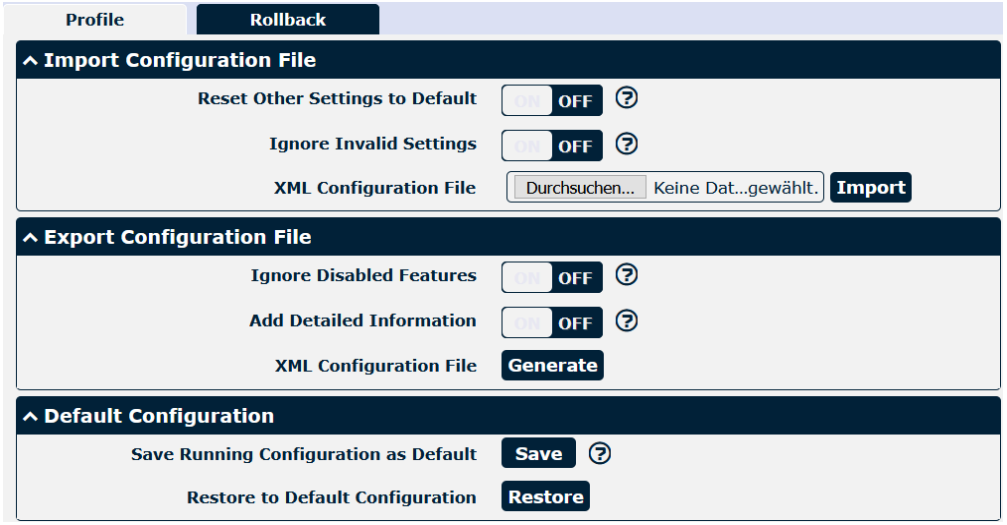
Traceroute		
Punkt	Description (Beschreibung)	Standard
Trace Address (Trace-Adresse)	Geben Sie die Ziel-IP-Adresse oder Zieldomäne des Trace ein.	Null
Trace Hops	Geben Sie die maximale Anzahl Trace Hops an. Der Router stoppt das Tracing, wenn die Anzahl der Trace Hops den Maximalwert erreicht hat, unabhängig davon, ob das Ziel erreicht wurde oder nicht.	30
Trace Timeout (Trace-Zeitüberschreitung)	Geben Sie die Zeitüberschreitung der Traceroute-Anfrage an.	1
Start	Klicken Sie auf diese Schaltfläche, um die Traceroute-Anfrage zu starten, und das Protokoll wird in der folgenden Box angezeigt.	--
Stop	Klicken Sie auf diese Schaltfläche, um die Traceroute-Anfrage zu stoppen.	--



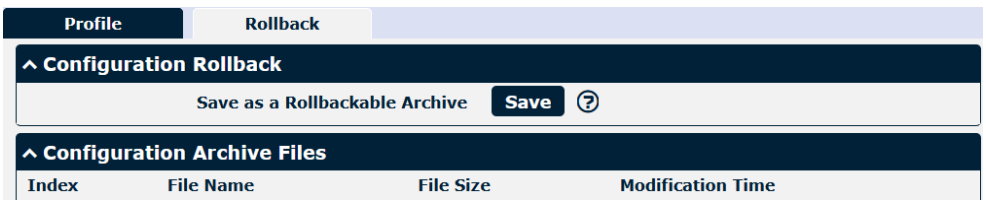
Sniffer		
Punkt	Beschreibung	Standard
Interface (Schnittstelle)	Wählen Sie die Schnittstelle entsprechend Ihrer Ethernet-Konfiguration.	All (Alle)
Host	Filtern Sie das Paket, das die angegebene IP-Adresse enthält.	Null
Packets Request (Paketan-forderungen)	Legt die Anzahl der Pakete fest, die Router zu einem Zeitpunkt aufzeichnen kann.	1000
Protocol (Protokoll)	Wählen Sie aus „Alle“, „IP“, „TCP“, „UDP“ und „ARP“.	All (Alle)
Port	Legen Sie die Port-Nummer für TCP oder UDP fest, die in Sniffer verwendet wird.	Null
Status	Zeigt den aktuellen Status von Sniffer an.	Null
Start	Klicken Sie auf diese Schaltfläche, um den Sniffer zu starten.	--
Stop	Klicken Sie auf diese Schaltfläche, um den Sniffer zu stoppen. Sobald Sie auf diese Schaltfläche klicken, wird eine neue Protokolldatei in der folgenden Liste angezeigt.	--
Capture Files (Erfassungsdateien)	Jeder Zeitpunkt des Sniffer-Protokolls wird automatisch als neue Datei gespeichert. Sie finden die Datei in dieser Sniffer-Verkehrsdaten-Liste und klicken auf, um das Protokoll herunterzuladen. Klicken Sie auf ✕, um die Protokolldatei zu löschen. Es können maximal 5 Dateien zwischengespeichert werden.	Null

3.35 System > Profile

In diesem Abschnitt können Sie die Konfigurationsdatei importieren oder exportieren und den Router auf die Werkseinstellung zurücksetzen.



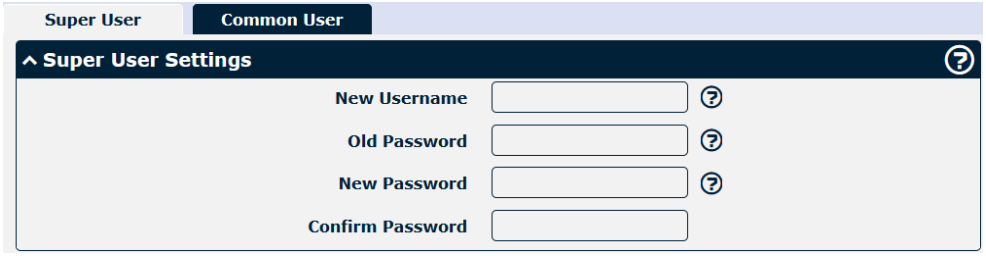
Profile		
Punkt	Beschreibung	Standard
Import Configuration File (Konfigurationsdatei importieren)		
Reset Other Settings to Default (Andere Einstellungen auf Standard zurücksetzen)	Klicken Sie den Schalter auf Stellung „ON“ („EIN“), um andere Parameter auf Standardeinstellungen zurückzusetzen.	OFF (AUS)
Ignore Invalid Settings (Ungültige Einstellungen ignorieren)	Klicken Sie den Schalter auf Stellung „OFF“ („AUS“), um ungültige Einstellungen zu ignorieren.	OFF (AUS)
XML Configuration File (XML-Konfigurationsdatei)	Klicken Sie auf „Durchsuchen“, um die XML-Konfigurationsdatei auf Ihrem Computer zu lokalisieren, und klicken Sie dann auf Import, um diese Datei in Ihren Router zu importieren.	--
Export Configuration File (Konfigurationsdatei exportieren)		
Ignore Disabled Features (Deaktivierte Funktionen ignorieren)	Klicken Sie den Schalter auf Stellung „OFF“ („AUS“), um die deaktivierten Funktionen zu ignorieren.	OFF (AUS)
Add Detailed Information (Detaillierte Informationen hinzufügen)	Klicken Sie den Schalter auf Stellung „ON“ („EIN“), um detaillierte Informationen hinzuzufügen.	OFF (AUS)
Encrypt Secret Data (Geheime Daten verschlüsseln)	Klicken Sie den Schalter auf Stellung „ON“ („EIN“), um die geheimen Daten zu verschlüsseln.	OFF (AUS)
XML Configuration File (XML-Konfigurationsdatei)	Klicken Sie auf die Schaltfläche Generate, um die XML Konfigurationsdatei zu erzeugen.	--
Default Configuration (Standardkonfiguration)		
Save Running Configuration as Default (Laufende Konfiguration als Standard speichern)	Klicken Sie auf Save, um die aktuellen Betriebsparameter als Standardkonfiguration zu speichern.	--
Restore to Default Configuration (Standardkonfiguration wiederherstellen)	Klicken Sie auf die Schaltfläche Restore, um die Werkseinstellungen wiederherzustellen.	--



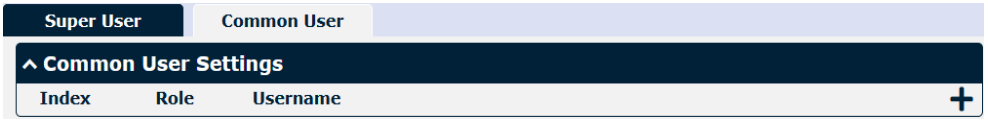
Rollback		
Punkt	Beschreibung	Standard
Configuration Rollback (Konfigurations-Rollback)		
Save as a Rollbackable Archive (Als Rollback-fähiges Archiv speichern)	Erstellen Sie manuell einen Sicherungspunkt. Zusätzlich erstellt das System jeden Tag automatisch einen Sicherungspunkt, wenn sich die Konfiguration ändert.	--
Configuration Archive Files (Konfigurations-Archivdateien)		
Configuration Archive Files (Konfigurations-Archivdateien)	Zeigt die zugehörigen Informationen über Konfigurations-Archivdateien an, einschließlich Name, Größe und Änderungszeit.	--

3.36 System > User Management

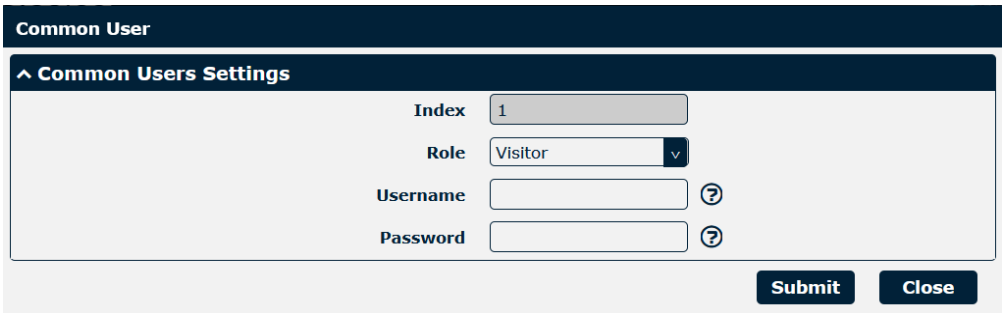
Jeder Router hat nur einen Superuser, der die höchste Autorität zum Ändern, Hinzufügen und Verwalten anderer allgemeiner Benutzer hat.



Super User Settings (Superuser-Einstellungen)		
Punkt	Beschreibung	Standard
New Username (Neuer Benutzername)	Geben Sie einen neuen Benutzernamen ein, den Sie erstellen möchten; gültige Zeichen sind a–z, A–Z, 0–9, @, ., -, #, $ und *.	Null
Old Password (Altes Passwort)	Geben Sie das alte Passwort Ihres Routers ein. Der Standardwert ist „admin“.	Null
New Password (Neues Passwort)	Geben Sie ein neues Passwort ein, das Sie erstellen möchten; gültige Zeichen sind a–z, A–Z, 0–9, @, ., -, #, $ und *.	Null
Confirm Password (Passwort bestätigen)	Geben Sie zur Bestätigung das neue Passwort erneut ein.	Null



Klicken Sie auf die Schaltfläche +, um einen neuen allgemeinen Benutzer hinzuzufügen.
Die maximale Anzahl beträgt 5.



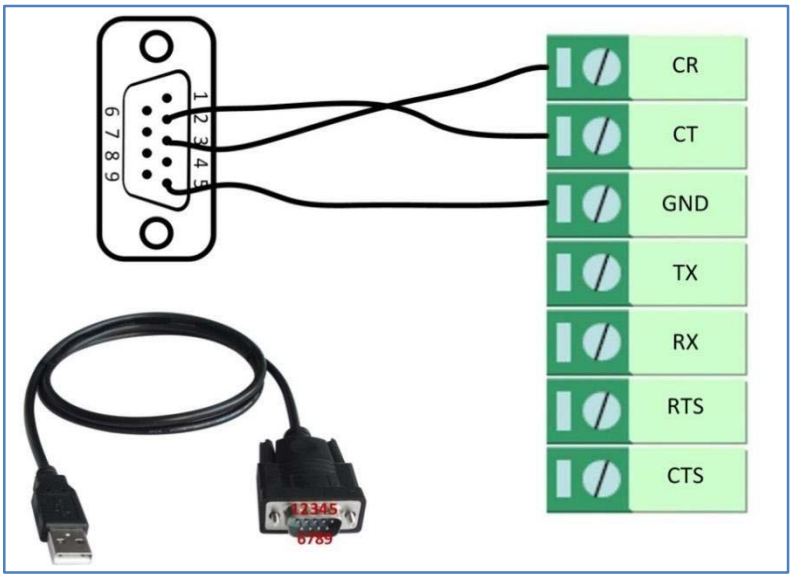
Common User Settings (Allgemeine Benutzer Einstellungen)		
Punkt	Beschreibung	Standard
Index (Index)	Gibt die Ordinalzahl der Liste an.	--
Role (Rolle)	Wählen Sie aus „Visitor“ („Besucher“) und „Editor“ („Bearbeiter“). Visitor (Besucher): Auf dieser Ebene können Benutzer lediglich die Konfiguration des Routers einsehen. Editor (Bearbeiter): Auf dieser Ebene können Benutzer die Konfiguration des Routers einsehen und bearbeiten.	Visitor (Besucher)
Username (Benutzername)	Legen Sie den Benutzernamen fest; gültige Zeichen sind a–z, A–Z, 0–9, @, ., -, #, $ und *.	Null
Password (Passwort)	Legen Sie das Passwort fest, das mindestens 5 Zeichen enthält; gültige Zeichen sind a–z, A–Z,0–9, @, ., -, #, $ und *.	Null

4. Konfigurationsbeispiele

4.1 Schnittstellen

4.1.1 Konsolenanschluss

Sie können den Konsolenanschluss verwenden, um den Router über CLI-Befehle zu verwalten. Siehe bitte Kapitel 5 für eine Einführung in CLI.



4.1.2 Digitaleingang

Der DSR-211 unterstützt Digitaleingänge mit potenzialfreien Kontakten. Bitte überprüfen Sie die Anschlussschnittstelle des Routers, Sie können leicht eine Markierung „V-“ an einem Pin des Stromanschlusses finden.

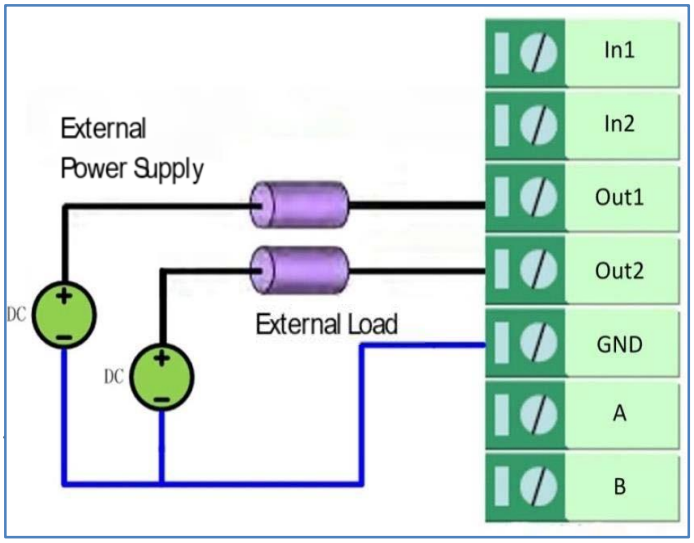
Hinweis: Schließen Sie In1/ In2 nicht direkt an und schieben Sie den Schalter nicht auf den mit „GND“ gekennzeichneten Anschluss am Klemmenblock. Andernfalls kann die DI nicht ordnungsgemäß funktionieren.

4.1.3 Digitalausgang

Der DSR-211 unterstützt Digitalausgänge mit stromführenden Kontakten.
Bitte beachten Sie die Abbildung auf der rechten Seite, um den negativen Pol der Stromversorgung an den mit „GND“ gekennzeichneten Anschluss anzuschließen.

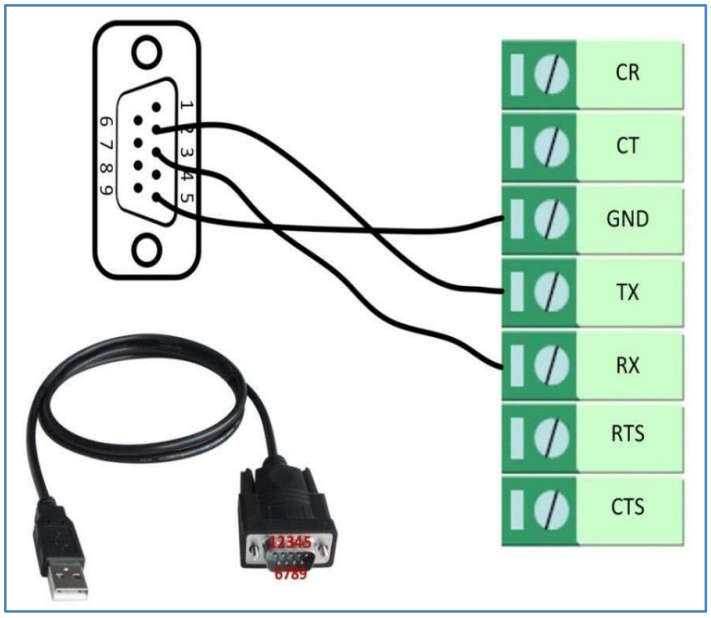
Die maximale Ausgangsspannung, der maximale Ausgangsstrom und die maximale Ausgangsleistung von DO betragen 30 V DC, 0,3 A bzw. 0,3 W.

Das bedeutet, dass die Spannungsdifferenz zwischen Out1, Out2 und GND nicht mehr als 30 V DC und der Stromwert durch Out1 und Out2 nicht mehr als 300 mA betragen darf, während die von Out1 und Out2 abgeführte Ausgangsleistung nicht mehr als 0,3 W betragen darf. Andernfalls wird der DO beschädigt.



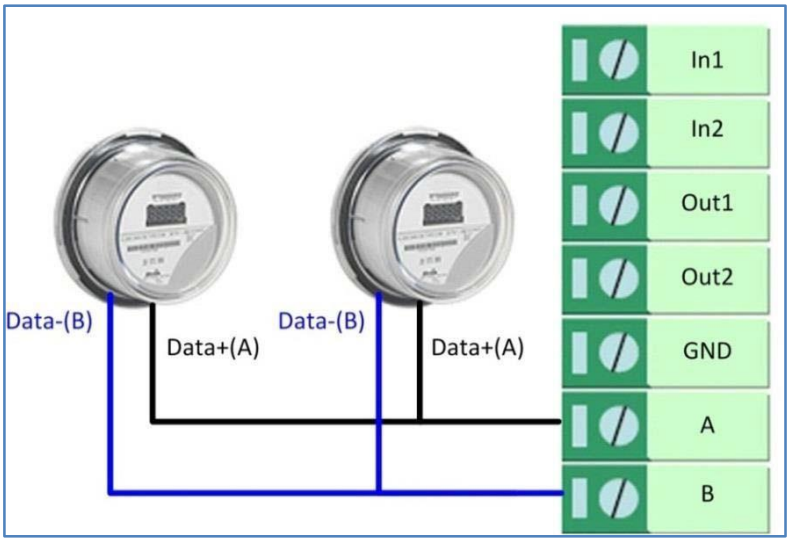
4.1.4 RS-232

Der DSR-211 unterstützt eine RS-232-Schnittstelle für serielle Datenkommunikation. Bitte beachten Sie das folgende Anschlussschema:



4.1.5 RS-485

Der DSR-211 unterstützt eine RS-485-Schnittstelle für serielle Datenkommunikation.
Bitte beachten Sie das folgende Anschlussschema.



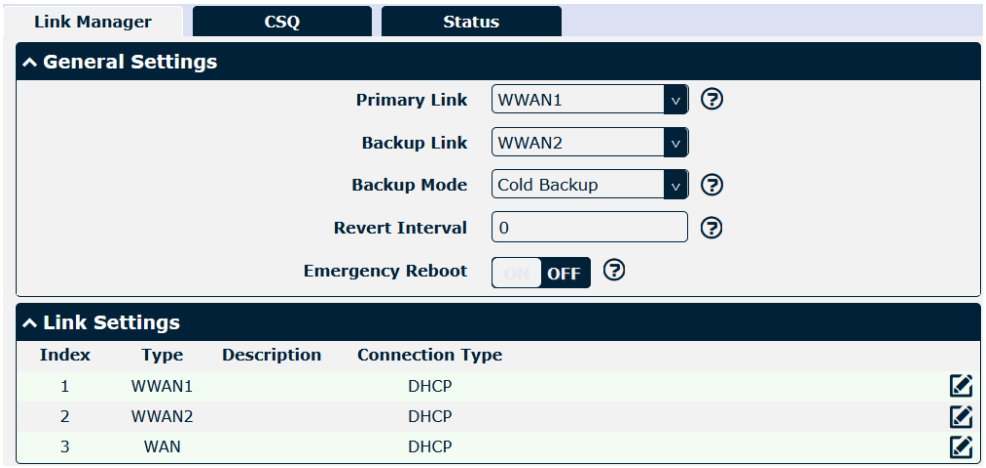
4.2 Mobilfunk

4.2.1 Mobilfunk-Einwahl

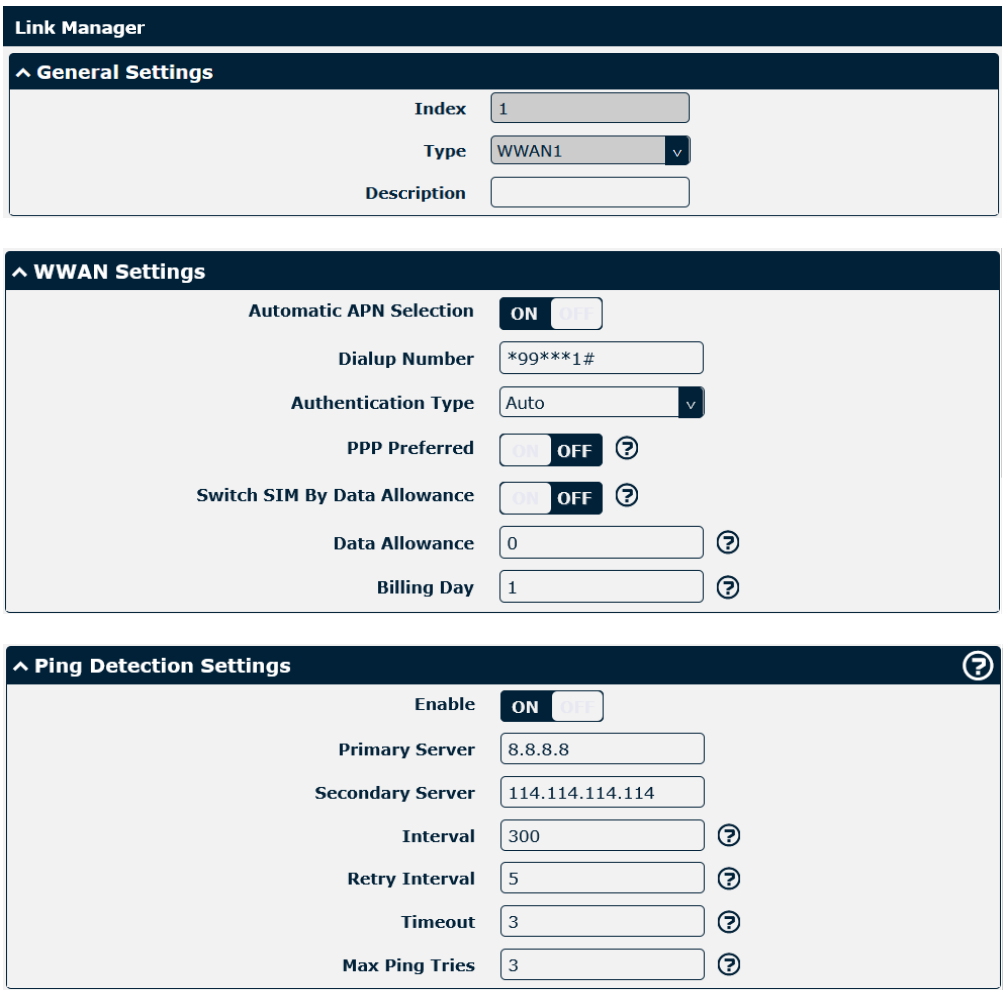
Dieser Abschnitt zeigt Ihnen, wie Sie die Primär- und Backup-SIM-Karte für die Mobilfunk-Einwahl konfigurieren. Schließen Sie den Router korrekt an, legen Sie zwei SIM-Karten ein und öffnen Sie dann die

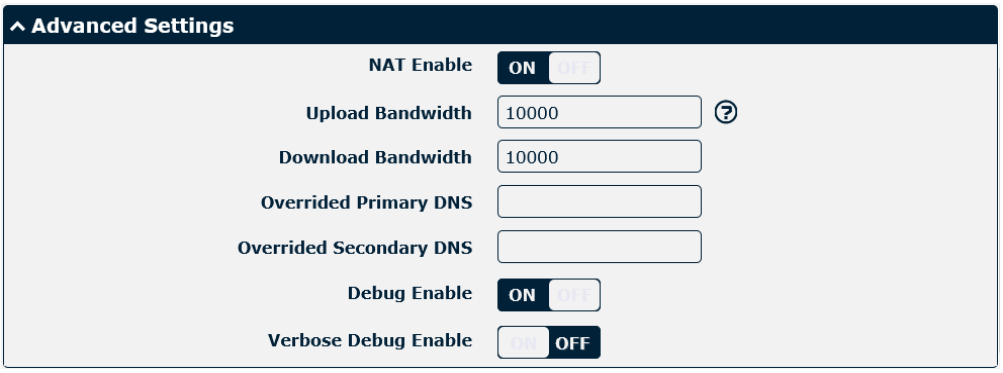
Konfigurationsseite. Klicken Sie im Menü der Startseite auf Interface (Schnittstelle) > Link Manager (Link-Manager) > General Settings (Allgemeine Einstellungen), wählen Sie „WWAN1“ als Primärlink, „WWAN2“ als Backup-Link und „Cold Backup“ als Backup-Modus. Klicken Sie dann auf Submit (Übermitteln).

Hinweis: Alle Daten werden über WWAN1 übertragen, wenn Sie WWAN1 als primären Link wählen und den Backup-Modus als „Cold Backup“ einstellen. Gleichzeitig ist WWAN2 als Backup-Link immer offline. Die gesamte Datenübertragung wird auf WWAN2 umgestellt, wenn der Link zum WWAN1 getrennt wird.



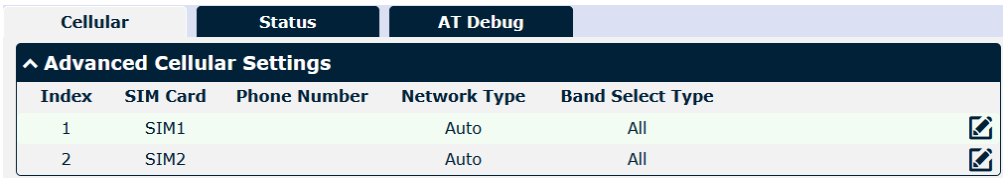
Klicken Sie auf die Schaltfläche des WWAN1, um dessen Parameter entsprechend dem aktuellen ISP einzustellen.



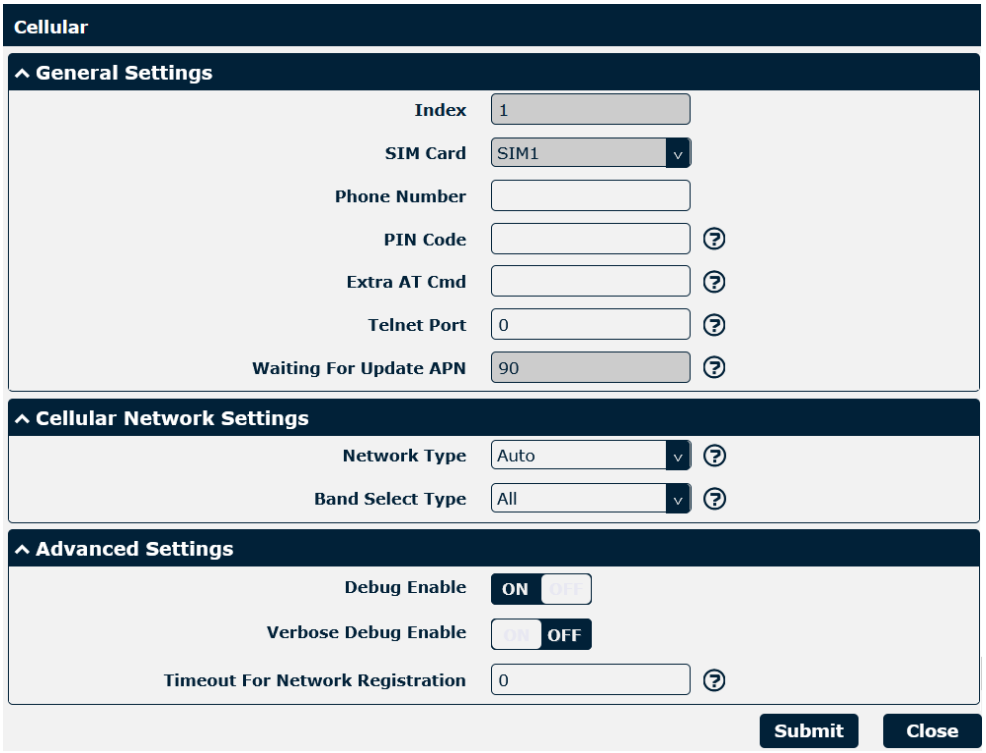


Wenn Sie fertig sind, klicken Sie auf Submit (Übermitteln) > Save & Apply (Speichern & Übernehmen) damit die Konfiguration wirksam wird.

Das Fenster wird wie unten angezeigt, wenn Sie auf Interface (Schnittstelle) > Cellular (Mobilfunk) > Advanced Cellular Settings (Erweiterte Mobilfunkeinstellungen) klicken:



Klicken Sie auf die Bearbeiten-Schaltfläche von SIM1, um die Parameter entsprechend Ihrer Anwendungsanforderung einzustellen.



Wenn Sie fertig sind, klicken Sie auf Submit (Übermitteln) > Save & Apply (Speichern & Übernehmen), damit die Konfiguration wirksam wird.

4.2.2 SMS-Fernsteuerung

Der DSR-211 unterstützt die Fernsteuerung per SMS. Sie können die folgenden Befehle nutzen, um den Status des DSR-211 abzurufen und alle Parameter des DSR-211 einzustellen. Es gibt drei Authentifizierungstypen für die SMS-Steuerung. Sie können zwischen „Password“ („Passwort“), „Phonenum“ („Telefonnummer“) oder „Both“ („Beides“) wählen.

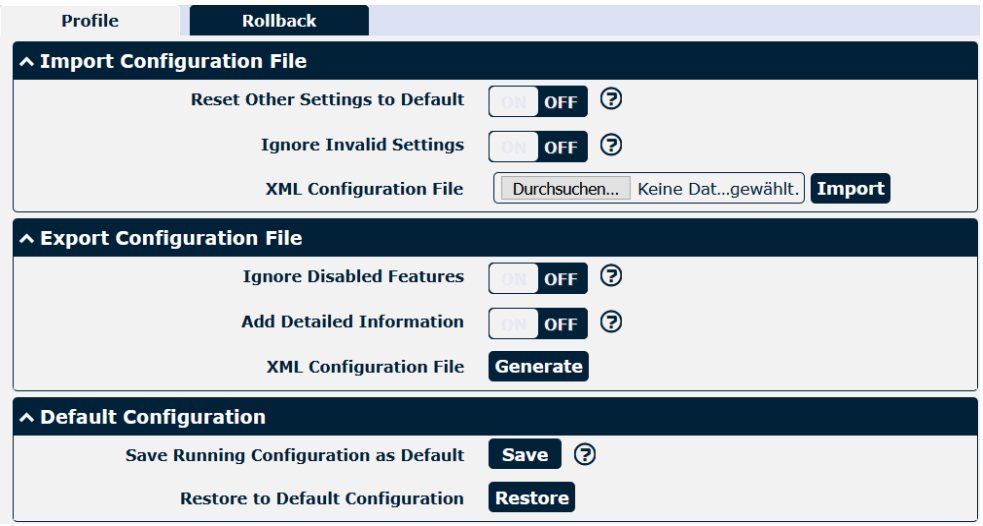
Ein SMS-Befehl hat den folgenden Aufbau:

1. „Password“-Modus – Benutzername Passwort;cmd1;cmd2;cmd3; …cmdn (für alle Telefonnummern verfügbar).
2. „Phonenum“-Modus – Passwort;cmd1; cmd2; cmd3; ...cmdn (verfügbar, wenn die SMS von der Telefonnummer gesendet wurde, die in der Telefongruppe des DSR-211 hinzugefügt wurde).“
3. „Both“-Modus – Benutzername: Passwort;cmd1;cmd2;cmd3; …cmdn (verfügbar, wenn die SMS von der Telefonnummer gesendet wurde, die in der Telefongruppe des DSR-211 hinzugefügt wurde).

Erläuterung der SMS-Befehle:

1. Benutzername und Passwort: Verwenden Sie zur Authentifizierung denselben Benutzernamen und dasselbe Passwort wie der WEB-Manager.
2. cmd1, cmd2, cmd3 bis cmdn, das Befehlsformat ist das gleiche wie beim CLI-Befehl. Weitere Einzelheiten zu CLI cmd finden Sie im Kapitel 5 Einführung zu CLI.

Hinweis: Laden Sie die XML-Konfigurationsdatei aus dem konfigurierten Webbrowser herunter. Das Format des SMS-Steuerbefehls kann sich auf die Daten der XML-Datei beziehen.
Gehen Sie zu System > Profile (Profil) > Export Configuration File (Konfigurationsdatei exportieren), klicken Sie auf **Generate**, um die XML-Datei zu erzeugen und klicken Sie auf **Export**, um die XML-Datei zu exportieren.



XML-Befehl:
<lan >
<network max_entry_num="2" >
<id > 1</id >
<interface > lan0</interface >
<ip > 172.16.24.24</ip >
<netmask > 255.255.0.0</netmask >
<mtu > 1500</mtu >
SMS cmd:
set lan network 1 interface lan0 set lan network 1 ip 172.16.24.24
set lan network 1 netmask 255.255.0.0 set lan network 1 mtu 1500

Das Semikolon-Zeichen („;“) wird verwendet, um mehrere in einer einzigen SMS verpackten Befehle zu trennen.

Beispiel:
admin:admin;status system
In diesem Befehl ist der Benutzername „admin“, das Passwort ist „admin“, und die Funktion des Befehls besteht darin, den Systemstatus zu erhalten.

SMS received: hardware_version = 1.2 firmware_version = "3.0.0" kernel_version = 4.1.0
device_model = DSR-211 serial_number = 201612221052
uptime = "0 days, 00:39:31"
system_time = "Mon Feb 27 09:52:52 2017 admin: admin;reboot
In diesem Befehl ist der Benutzername „admin“, das Passwort ist „admin“, und der Befehl lautet, den Router neu zu starten.
SMS received:
OK

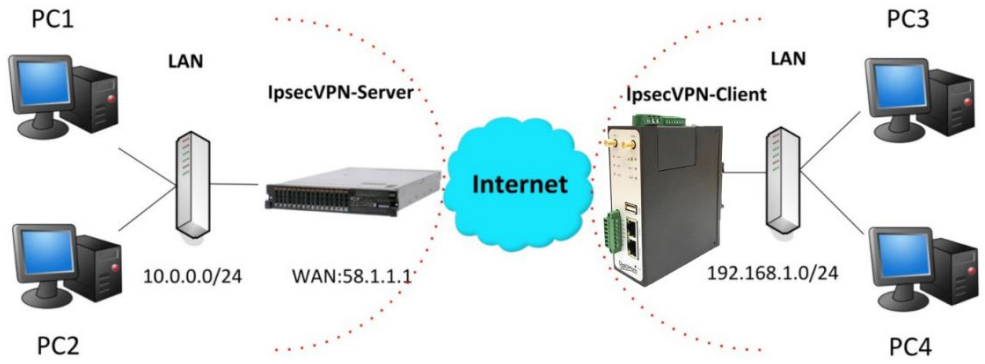
admin:admin;set firewall remote_ssh_access false;set firewall remote_telnet _access false
In diesem Befehl ist der Benutzername „admin“, das Passwort ist „admin“, und der Befehl dient zum Deaktivieren des remote_ssh- und remote_telnet-Zugriffs.
SMS received
OK
OK

admin:admin; set lan net work 1 interface lan0;set lan network 1 ip 172.16.24.24; set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500
In diesem Befehl ist der Benutzername „admin“, das Passwort ist „admin“, und der Befehl dient zur Konfiguration der LAN-Parameter.

SMS received: OK
OK OK OK

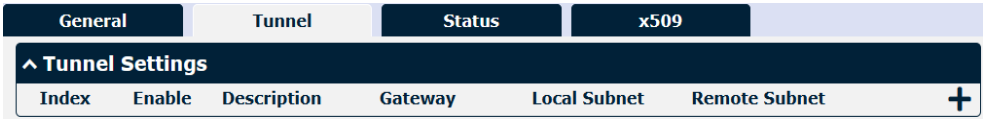
4.3 Netzwerk

4.3.1 IPsec VPN

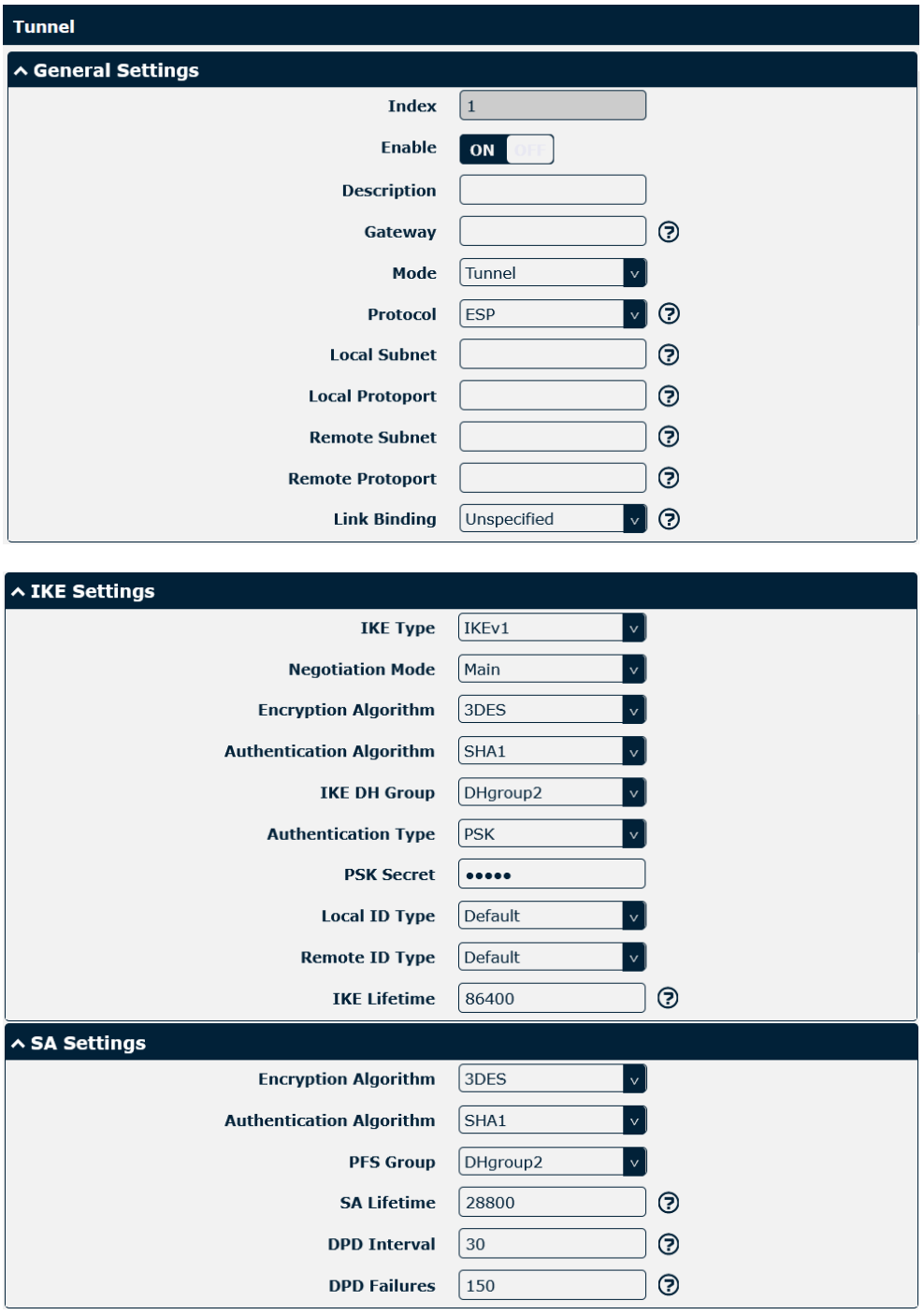


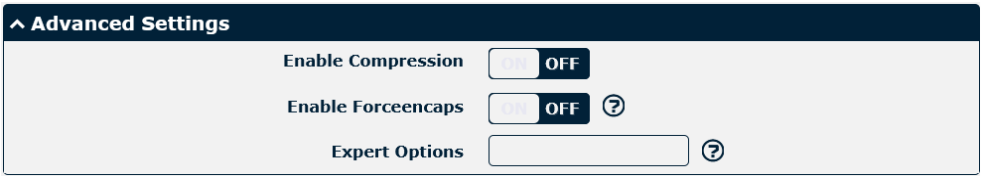
IPsec VPN_CLIENT:

Wenn Sie auf VPN > IPsec > Tunnel klicken, wird das Fenster wie unten dargestellt.

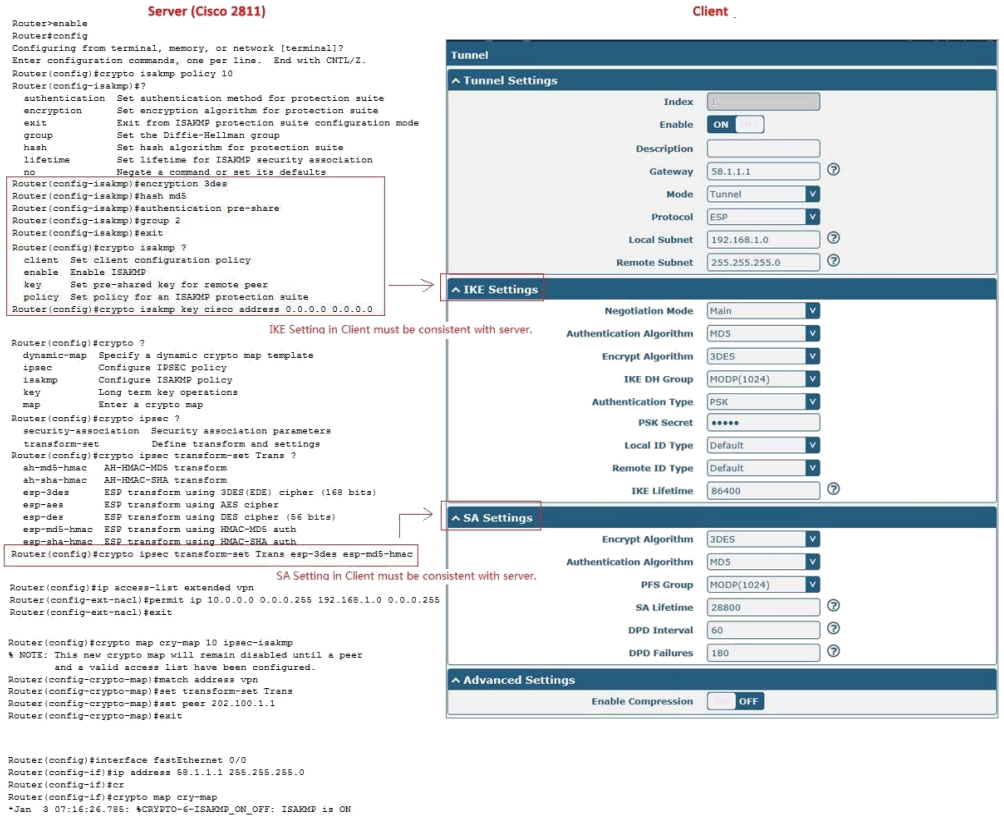


Klicken Sie auf die Schaltfläche + und stellen Sie die Parameter des IPsec-Clients wie unten beschrieben ein:



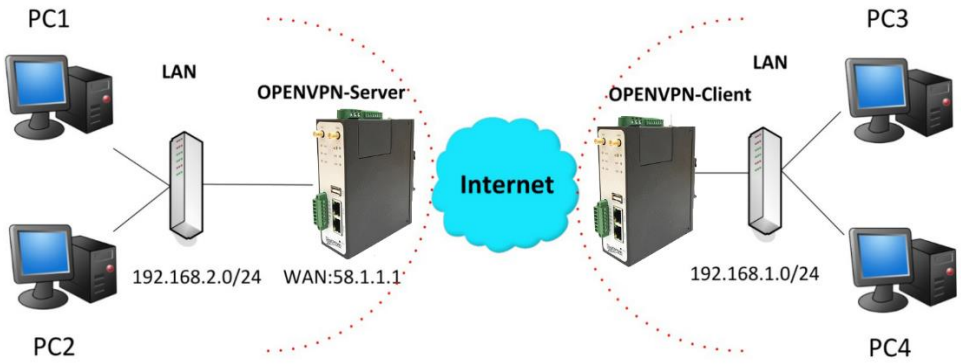


Wenn Sie fertig sind, klicken Sie auf Submit (Übermitteln) > Save & Apply (Speichern & Übernehmen), damit die Konfiguration wirksam wird. Der Vergleich zwischen Server und Client ist wie unten dargestellt:



4.3.2 Open VPN

OpenVPN unterstützt zwei Modi, Client und P2P. Als Beispiel sei hier P2P genannt.



Die Konfiguration von zwei Punkten ist wie folgt

OPENVPN_Server

Erzeugen Sie zuerst das entsprechende OpenVPN-Zertifikat auf der Serverseite und beziehen Sie sich auf die folgenden Befehle zur Konfiguration des Servers:

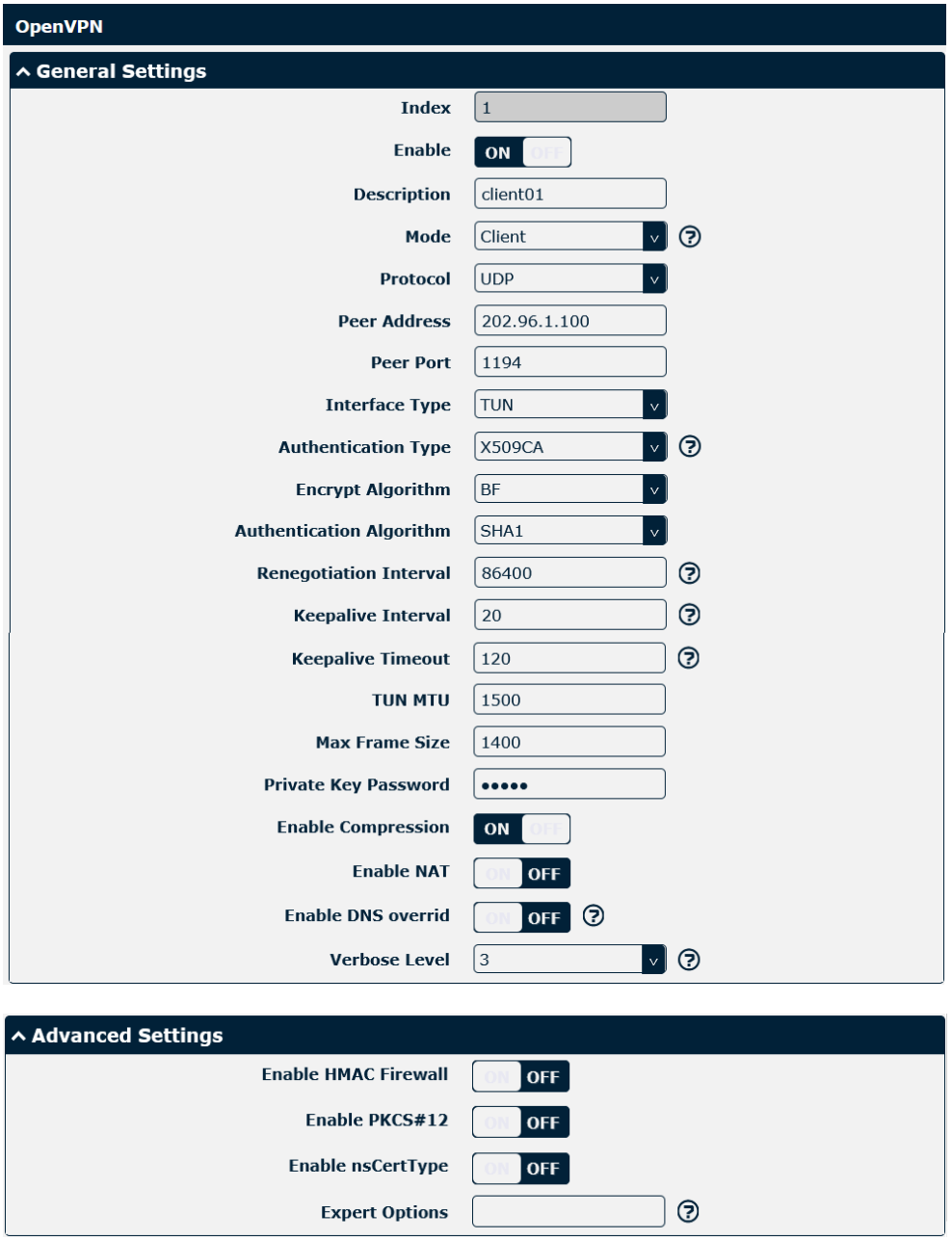
```
local 202.96.1.100
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert Server01.crt
key Server01.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.3.0 255.255.255.0"
client-config-dir ccd
route 192.168.1.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Hinweis: Für weitere Konfigurationsdetails wenden Sie sich bitte an Ihren Support-Techniker.

OpenVPN_Client:

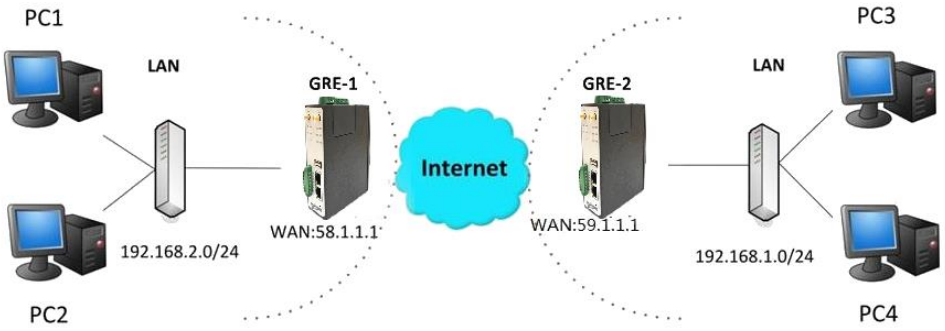
Klicken Sie wie unten angegeben auf VPN > OpenVPN > OpenVPN.

Klicken Sie auf +, um den Client01 wie unten beschrieben zu konfigurieren.



Wenn Sie fertig sind, klicken Sie auf Submit (Übermitteln) > Save & Apply (Speichern & Übernehmen), damit die Konfiguration wirksam wird.

4.3.3 GRE-VPN

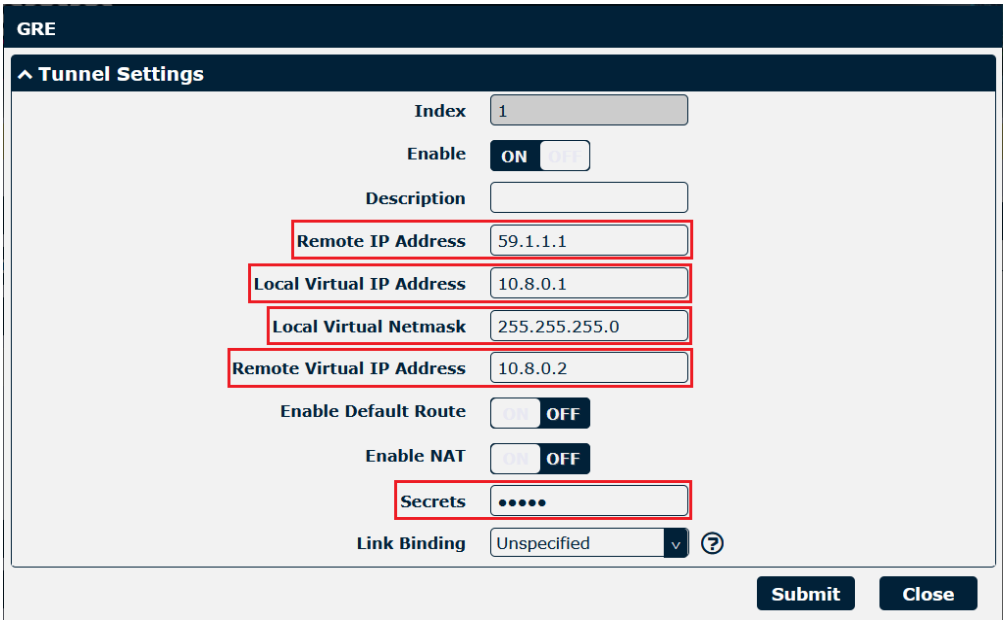


Die Konfiguration von zwei Punkten ist wie folgt

Wenn Sie auf VPN > GRE> GRE klicken, wird das Fenster wie unten dargestellt:

GRE-1

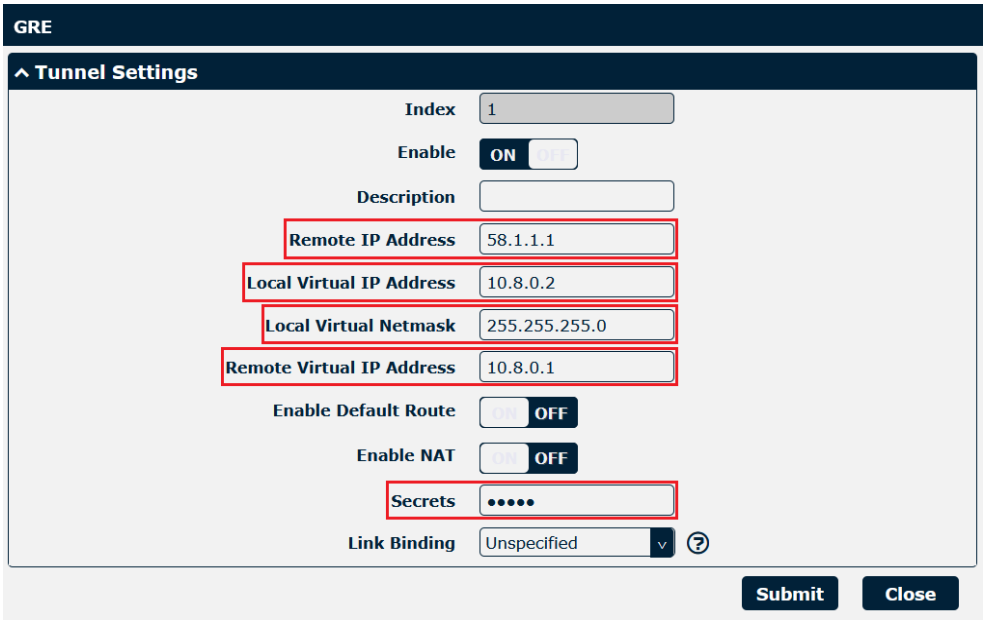
Klicken Sie auf die Schaltfläche + und stellen Sie die Parameter von GRE-1 wie folgt ein:



Wenn Sie fertig sind, klicken Sie auf Submit (Übermitteln) > Save & Apply (Speichern & Übernehmen), damit die Konfiguration wirksam wird.

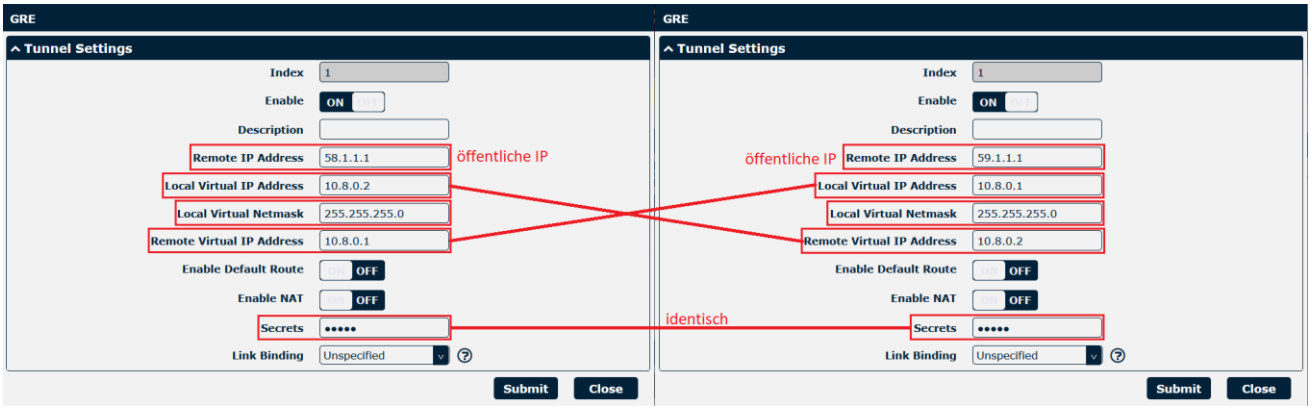
GRE-2:

Klicken Sie auf die Schaltfläche + und stellen Sie die Parameter von GRE-1 wie folgt ein.



Wenn Sie fertig sind, klicken Sie auf Submit (Übermitteln) > Save & Apply (Speichern & Übernehmen), damit die Konfiguration wirksam wird.

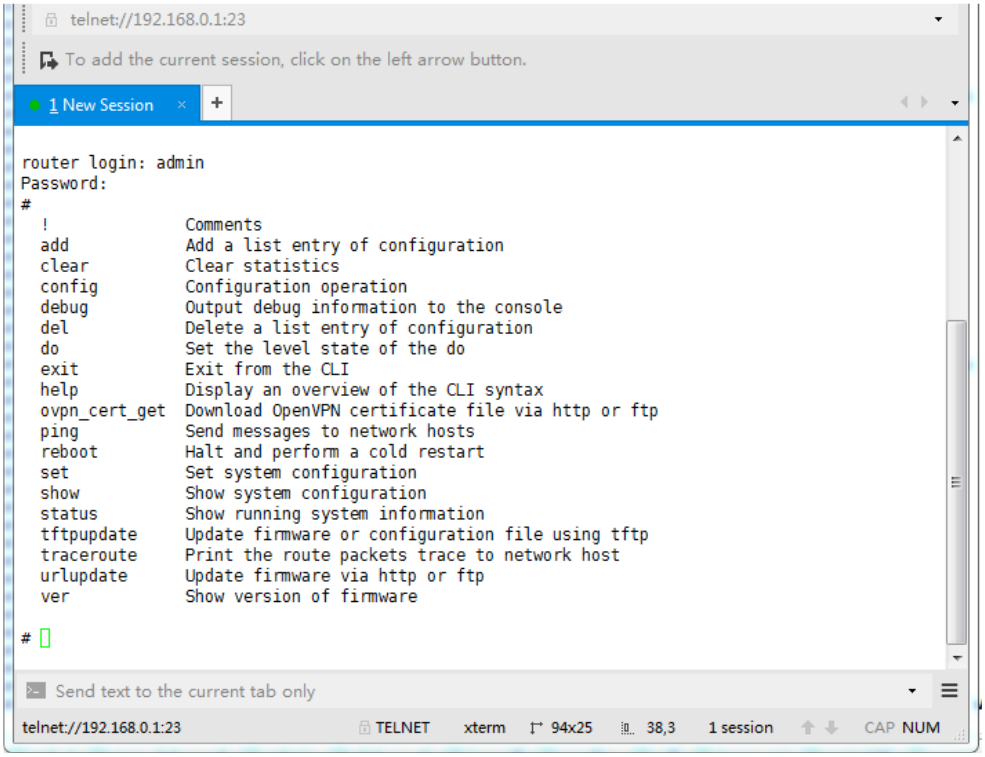
Der Vergleich zwischen GRE-1 und GRE-2 ist wie folgt:



5. Einführung zu CLI

5.1 Was ist die CLI?

Die DSR-211-Befehlszeilenschnittstelle (CLI) ist eine Softwareschnittstelle, die eine weitere Möglichkeit bietet, die Parameter von Geräten über SSH oder über eine Telnet-Netzwerkverbindung einzustellen.



Router-Anmeldung

Router-Anmeldung: admin

Passwort: admin

#

CLI-Befehle:

? (Hinweis: das „?“ wird auf der Seite nicht angezeigt.)

!	Anmerkungen
add	Einen Listeneintrag der Konfiguration hinzufügen
clear	Statistik löschen
config	Konfigurationsvorgang
debug	Debug-Informationen auf die Konsole ausgeben
del	Löschen eines Listeneintrags der Konfiguration
exit	Verlassen der CLI
help	Einen Überblick über die CLI-Syntax anzeigen
ovpn_cert_get	OpenVPN-Zertifikatsdatei über https oder ftp herunterladen
ping	Senden von Nachrichten an Netzwerk-Hosts
reboot	Halt und Durchführung eines kalten Neustarts
route	Statische Route dynamisch ändern, diese Einstellung wird nicht gespeichert
set	Systemkonfiguration einstellen

show Systemkonfiguration anzeigen
status Laufende Systeminformationen anzeigen
tftpupdate Firmware mit tftp aktualisieren
traceroute Drucken der Routenpaket-Verfolgung zum Netzwerk urlupdate Firmware mit https oder ftp aktualisieren
ver Version der Firmware anzeigen

5.2 CLI Konfiguration

Im Folgenden finden Sie eine Tabelle mit Beschreibungen/ Hilfestellungen sollten im Konfigurationsprogramm Fehler auftreten:

Befehle/Tipps	Beschreibung
?	Wenn Sie ein Fragezeichen „?“ eingeben, werden Ihnen die Hilfeinformationen angezeigt. Beispiel: # config (? drücken) config Konfigurationsvorgang #config Drücken (Leertaste+?) commit Konfigurationsänderungen speichern und geänderte Konfiguration wirksam werden lassen save_and_apply Konfigurationsänderungen speichern und geänderte Konfiguration wirksam werden lassen loaddefault Werkskonfiguration wiederherstellen
Strg+C	Drücken Sie diese beiden Tasten gleichzeitig, neben der Kopierfunktion können diese auch genutzt werden, um das Einstellprogramm zu verlassen.
Syntaxfehler: Der Befehl ist nicht abgeschlossen	Der Befehl ist nicht abgeschlossen.
Leertaste + Tabulatortaste drücken	Dies kann Ihnen helfen, den Befehl zu beenden. Beispiel: # config (Drücken Sie die Eingabetaste) Syntaxfehler: Der Befehl ist nicht abgeschlossen # config (Leertaste + Tabulatortaste drücken) commit save_and_apply loaddefault
# config commit # config save_and_apply /	Wenn Ihre Einstellung abgeschlossen ist, sollten Sie diese Befehle eingeben, damit Ihre Einstellung auf dem Gerät wirksam wird. Hinweis: Commit und save_and_apply führen den selben Befehl aus.

5.3 Befehlsreferenz

Befehle	Syntax	Beschreibung
Debug	Debugging-Parameter	Ein- oder Ausschalten der Debugging-Funktion
Show (Anzeigen)	Parameter anzeigen	Zeigt die aktuelle Konfiguration jeder Funktion; um alle zu sehen, benutzen Sie bitte „show running“.
Set (Einstellen)	Parameter einstellen	Alle Funktionsparameter werden durch die Befehle set und add gesetzt, der Unterschied ist, dass set für den Einzelparameter und add für den Listenparameter steht.
Add (Hinzufügen)	Parameter hinzufügen	

Hinweis: Laden Sie die Datei config.XML aus dem Webbrowser herunter. Das Befehlsformat kann sich auf das Dateiformat config.XML beziehen.

5.4 Schnellstart mit Konfigurationsbeispielen

Der beste und schnellste Weg, die CLI zu beherrschen, besteht darin, sich zunächst alle Funktionen auf der Webseite anzusehen, dann alle CLI-Befehle einmal zu lesen und schließlich anhand einiger Referenzbeispiele die Konfiguration zu erlernen.

Beispiel 1: Aktuelle Version anzeigen

```
# status system
hardware_version = 1.2
firmware_version = "3.0.0" (
kernel_version = 4.1.0
device_model = DSR-211
serial_number = 201612221052
uptime = "0 days, 00:40:31"
system_time = " Feb 27 09:52:52 2019“
```

Beispiel 2: Firmware über tftp aktualisieren

```
# tftpupdate (Leertaste + ?)
firmware          Neue Firmware
# tftpupdate firmware (Leertaste + ?)
 String   Firmware-Name
# tftpupdate firmware DSR-211-firmware-sysupgrade-unknown.bin host 192.168.100.99
 / / Geben Sie einen neuen Firmware-Namen ein
Downloading
DSR-211-firmware-s 100%| * * * * * *** *** * * * *** ** **** * *** *** * |  5018k   0:00:00 ETA
Flashing
Checking 100%
Decrypting 100%
Flashing 100%
Verifying 100% Verify Success
upgrade success          / / Update erfolgreich
# config save_and_apply
OK       / / Speichern und Anwenden der aktuellen Konfiguration, damit die Konfiguration wirksam wird
```

Beispiel 3: Link-Manager einstellen

```
# set
# set
at_over_telnet          AT über Telnet
cellular          Mobilfunk
ddns                    Dynamisches DNS
ethernet                Ethernet
event                   Ereignis-Management
firewall          Firewall
gre                     GRE
ipsec                   IPsec
lan                     Local Area Network
link_manager            Link-Manager
ntp                     NTP
openvpn                 OpenVPN
reboot                  Automatischer Neustart
route                   Route
sms                     SMS
snmp                    SNMP-Agent
ssh                     SSH
syslog                  Syslog
system                  System
```

```
user_management      Benutzerverwaltung
vrrp                 VRRP
web_server           Webserver
# set link_manager
primary_link         Primärer Link
backup_link          Backup-Link
backup_mode          Backup-Modus
emergency_reboot     Notfall-Neustart
link                 Link-Einstellungen
# set link_manager primary_link (Leertaste + ?)
Enum    Primärer Link (wwan1/ wwan2/ wan)
# set link_manager primary_link wwan1/ / Wählen Sie „wwan1“ als primären Link
OK                                          / / Einstellung erfolgreich
# set link_manager link 1
type                 Typ
desc                 Beschreibung
connection_type      Verbindungstyp
wwan                 WWAN-Einstellungen
static_addr          Statische Adresseinstellungen
pppoe                PPPoE-Einstellungen
ping                 Ping-Einstellungen
mtu                  MÜE
dns1_overrided Überschriebenes primäres DNS
dns2_overrided Überschriebenes sekundäres DNS
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan
auto_apn             Automatische APN-Auswahl
apn      APN
username             Benutzername
password             Passwort
dialup_number Einwahlnummer
auth_type            Authentifizierungstyp
aggressive_reset     Aggressiver Reset
switch_by_data_allowance      SIM nach verbrauchten Datenkontingent wechseln
data_allowance       Datenkontingent
billing_day          Tag der Rechnungsstellung
# set link_manager link 1 wwan switch_by_data_allowance true
OK
#
# set link_manager link 1 wwan data_allowance 100     / / open cellular switch_by_data_traffic
OK                                                    / / Einstellung erfolgreich
# set link_manager link 1 wwan billing_day 1    / / Einstellung gibt den Tag des Monats für die Abrechnung an
OK                                                    / / Einstellung erfolgreich
…
# config save_and_apply
OK      / / Speichern und Anwenden der aktuellen Konfiguration, damit die Konfiguration wirksam wird
```

Beispiel 4: Ethernet einstellen

```
# set Ethernet port_setting 2 port_assignment lan0                    //Set Table 2 (eth1) to lan0
OK
# config save_and_apply                                               // Einstellung erfolgreich
OK
```

Beispiel 5: LAN-IP-Adresse einstellen

```
# show lan all
network {
id = 1
interface = lan0
ip = 192.168.0.1
netmask = 255.255.255.0
mtu = 1500
dhcp {
enable = true
mode = server relay_server = ""
pool_start = 192.168.0.2
pool_end = 192.168.0.100
netmask = 255.255.255.0
gateway = ""
primary_dns = ""
secondary_dns = ""
wins_server = ""
lease_time = 120
expert_options = ""
debug_enable = false
}
}
multi_ip {
id = 1
interface = lan0
ip = 172.16.24.24 netmask = 255.255.0.0
}
#
# set lan
network          Netzwerkeinstellungen
multi_ip         Multiple IP-Adresseinstellungen
vlan     VLAN
# set lan network 1(Leertaste + ?)
interface        Schnittstelle
ip       IP-Adresse
netmask          Netzmaske
 mtu     MÜE
dhcp     DHCP-Einstellungen
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.99.22        / / Einstellung IP-Adresse für LAN
OK       / / Einstellung erfolgreich
# set lan network 1 netmask 255.255.0.0
OK
#
…
# config save_and_applyOK      / / Speichern und Anwenden der aktuellen Konfiguration, damit die
                               Konfiguration wirksam wird
```

Beispiel 6: CLI zur Mobilfunkeinstellung

```
# show cellular all
sim {
id = 1
card = sim1
phone_number = ""
extra_at_cmd = ""
network_type = auto
band_select_type = all
band_gsm_850 = false
band_gsm_900 = false
band_gsm_1800 = false
band_gsm_1900 = false
band_wcdma_850 = false
band_wcdma_900 = false
band_wcdma_1900 = false
band_wcdma_2100 = false
band_lte_800 = false
band_lte_850 = false
band_lte_900 = false
band_lte_1800 = false
band_lte_1900 = false
band_lte_2100 = false
band_lte_2600 = false
band_lte_1700 = false
band_lte_700 = false
band_tdd_lte_2600 = false
band_tdd_lte_1900 = false
band_tdd_lte_2300 = false
band_tdd_lte_2500 = false

}
sim {

id = 2
card = sim2
phone_number =
extra_at_cmd = ""
network_type = auto
band_select_type = all
band_gsm_850 = false
band_gsm_900 = false
band_gsm_1800 = false
band_gsm_1900 = false
band_wcdma_850 = false
band_wcdma_900= false
band_wcdma_1900 = false
band_wcdma_2100 = false
band_lte_800 = false
band_lte_850 = false
band_lte_900 = false
band_lte_1800 = false
band_lte_1900 = false
band_lte_2100 = false
band_lte_2600 = false
band_lte_1700 = false
band_lte_700 = false
band_tdd_lte_2600 = false
band_tdd_lte_1900 = false
```

band_tdd_lte_2300 = false
band_tdd_lte_2500 = false
}
# set(Leertaste + ?)
at_over_telnet cellular ddns dhcp dns
event firewall ipsec lan link_manager ntp openvpn reboot route serial_port
sms snmp syslog system user_management vrrp
set cellular(Leertaste + ?)
sim SIM Settings
set cellular sim(Leertaste + ?)
Integer Index (1..2)

set cellular sim 1(Leertaste + ?)

card	SIM-Karte
phone_number	Telefonnummer
extra_at_cmd	Extra-AT-Befehl
network_type	Netzwerktyp
band_select_type	Bandwahltyp
band_gsm_850	GSM 850
band_gsm_900	GSM 900
band_gsm_1800	GSM 1800
band_gsm_1900	GSM 1900
band_wcdma_850	WCDMA 850
band_wcdma_900	WCDMA 900
band_wcdma_1900	WCDMA 1900
band_wcdma_2100	WCDMA 2100
band_lte_800	LTE800 (Band 20)
band_lte_850	LTE850 (Band 5)
band_lte_900	LTE900 (Band 8)
band_lte_1800	LTE1800 (Band 3)
band_lte_1900	LTE1900 (Band 2)
band_lte_2100	LTE2100 (Band 1)
band_lte_2600	LTE2600 (Band 7)
band_lte_1700	LTE1700 (Band 4)
band_lte_700	LTE700 (Band 17)
band_tdd_lte_2600	TDD LTE2600 (Band 38)
band_tdd_lte_1900	TDD LTE1900 (Band 39)
band_tdd_lte_2300	TDD LTE2300 (Band 40)
band_tdd_lte_2500	TDD LTE2500 (Band 41)

set cellular sim 1 phone_number 017*********
OK
…
config save_and_apply / / Speichern und Anwenden der aktuellen Konfiguration, damit die Konfiguration wirksam wird
OK

6. Glossar

Akronym	Beschreibung
AC	Alternating Current (Wechselstrom)
APN	Access Point Name (Name des Zugangspunkts)
ASCII	American Standard Code for Information Interchange (Amerikanischer Standard-Code für den Informationsaustausch)
CE	Conformité Européenne (Europäische Konformität)
CHAP	Challenge Handshake Authentication Protocol (Authentifizierungsprotokoll)
CLI	Command Line Interface for batch scripting (Befehlszeilenschnittstelle für Batch-Skripting)
CSD	Circuit Switched Data (Leitungsvermittelte Daten)
CTS	Clear to Send (Frei zum Senden)
dB	Dezibel
dBi	Dezibel relativ zu einem isotropen Strahler
DC	Direct Current (Gleichstrom)
DCD	Data Carrier Detect (Trägerkennung)
DCE	Data Communication Equipment (Datenkommunikationsausrüstung (typischerweise Modems)
DCS 1800	Digital Cellular System, auch als PCN (Personal Communications Network) bezeichnet
DI	Digital Input (Digitaleingang)
DO	Digital Output (Digitalausgang)
DSR	Data Set Ready (Datensatz bereit)
DTE	Data Terminal Equipment (Datenendgerät)
DTMF	Dual Tone Multi-frequency (Zweiton-Mehrfrequenz)
DTR	Data Terminal Ready (Datenterminal bereit)
EDGE	Enhanced Data rates for Global Evolution of GSM and IS-136 (Verbesserte Datenraten für die globale Entwicklung von GSM und IS-136)
EMC	Electromagnetic Compatibility (Elektromagnetische Verträglichkeit)
EMI	Electro-Magnetic Interference (Elektromagnetische Interferenz)
ESD	Electrostatic Discharges (Elektrostatische Entladungen)
ETSI	European Telecommunications Standards Institute (Europäisches Institut für Telekommunikationsnormen)
EVDO	Evolution-Data Optimized (Evolutionsdaten-optimiert)
FDD LTE	Frequency Division Duplexing Long Term Evolution (Frequenzteilungs-Duplexing Langfristentwicklung)
GND	Ground (Elektrische Erde)
GPRS	General Packet Radio Service (Allgemeiner Paketfunkdienst)
GRE	generic route encapsulation (Generische Routenkapselung)
GSM	Global System for Mobile Communications (Globales System für mobile Kommunikation)
HSPA	High Speed Packet Access (Hochgeschwindigkeits-Paketzugriff)
ID	identification data (Identifikationsdaten)
IMEI	International Mobile Equipment Identity (Internationale Identität von Mobilgeräten)
IP	Internet Protocol (Internet-Protokoll)
IPsec	Internet Protocol Security (Internet-Protokollsicherheit)
kbps / kbit/s	Kilobit pro Sekunde
L2TP	Layer 2 Tunneling Protocol (Schicht-2-Tunnelprotokoll)
LAN	Local Area Network (Lokalbereichsnetzwerk)
LED	Light Emitting Diode (Lichtemittierende Diode)
M2M	Machine to Machine (Maschine zu Maschine)

MAX	Maximum
Min	Minimum
MO	Mobile Originated (Mobiler Ursprung)
MS	Mobile Station (Mobile Station)
MT	Mobile Terminated (Mobil terminiert)
OpenVPN	Open Virtual Private Network (Offenes virtuelles privates Netzwerk)
PAP	Password Authentication Protocol (Passwort-Authentifizierungsprotokoll)
PC	Personal Computer
PCN	Personal Communications Network (Persönliches Kommunikationsnetzwerk, auch als DCS1800 bezeichnet)
PCS	Personal Communication System (Persönliches Kommunikationssystem, auch als GSM 1900 bezeichnet)
PDU	Protocol Data Unit (Protokoll-Dateneinheit)
PIN	Personal Identity Number (Persönliche Identitätsnummer)
PLC	Program Logic Control System (Speicherprogrammierbare Steuerung, SPS)
PPP	Point-to-point Protocol (Punkt-zu-Punkt-Protokoll)
PPTP	Point to Point Tunneling Protocol (Punkt-zu-Punkt-Tunnelprotokoll)
PSU	Power Supply Unit (Stromversorgungseinheit)
PUK	Personal Unblocking Key (Persönlicher Freigabeschlüssel)
R&TTE	Radio and Telecommunication Terminal Equipment (Funk- und Telekommunikationsendgeräte)
RF	Radio Frequency (Hochfrequenz, HF)
RTC	Real Time Clock (Echtzeituhr)
RTS	Request to Send (Anforderung zum Senden)
RTU	Remote Terminal Unit (Fernwirkgerät)
Rx	Receive Direction (Empfangsrichtung)
SDK	Software Development Kit (Software-Entwicklungs-Kit)
SIM	Subscriber Identification Module (Teilnehmer-Identifizierungsmodul)
SMA-Antenne	Stummelantenne oder Magnetantenne
SMS	Short Message Service (Kurznachrichtendienst)
SNMP	Simple Network Management Protocol (Einfaches Netzwerk-Managementprotokoll)
TCP/ IP	Transmission Control Protocol / Internet Protocol (Übertragungssteuerungsprotokoll /
TE	Terminal Equipment (Endgerät, auch als DTE bezeichnet)
Tx	Transmit Direction (Senderichtung)
UART	Universal Asynchronous Receiver-transmitter (Universal-Asynchron-Empfänger-Sender)
UMTS	Universal Mobile Telecommunications System (Universelles Mobiltelekommunikationssystem)
USB	Universal Serial Bus (Universeller serieller Bus)
USSD	Unstructured Supplementary Service Data (Unstrukturierte Ergänzungs-Servicedaten)
VDC	Volts Direct current (Volt Gleichstrom)
VLAN	Virtual Local Area Network (Virtuelles Nahbereichsnetzwerk)
VPN	Virtual Private Network (Virtuelles privates Netzwerk)
VSWR	Voltage Stationary Wave Ratio (Spannung Stationäres Wellenverhältnis)
WAN	Wide Area Network (Weitbereichsnetzwerk)

Sie brauchen technische Unterstützung?

Unser Support-Team hilft Ihnen gerne weiter:

Telefon +49 (0)2159/ 693 75-50
E-Mail: support@digicomm.de

AddSecure GmbH
Breite Str. 10
40670 Meerbusch