Industrieller Router Pro-Serie UR35

Benutzerhandbuch

Vorwort

Vielen Dank, dass Sie sich für den industriellen Mobilfunkrouter UR35 von Milesight entschieden haben. Der industrielle Mobilfunkrouter UR35 bietet eine stabile Netzwerkverbindung mit umfassenden Funktionen wie automatischem Failover/Failback, erweitertem Betriebstemperaturbereich, zwei SIM-Karten, Hardware-Watchdog, VPN, Fast Ethernet und vielem mehr.

Dieses Handbuch beschreibt die Konfiguration und Bedienung des industriellen Mobilfunk-Routers UR35. Hier finden Sie detaillierte Informationen zu den Funktionen und zur Konfiguration des Routers.

Leser

Dieses Handbuch richtet sich in erster Linie an folgende Benutzer:

- Netzwerkplaner
- Technisches Support- und Wartungspersonal vor Ort
- Netzwerkadministratoren, die für die Netzwerkkonfiguration und -wartung verantwortlich sind

Sicherheitshinweise

Milesight übernimmt keine Verantwortung für Verluste oder Schäden, die durch Nichtbeachtung der Anweisungen in dieser Bedienungsanleitung entstehen.

- Das Gerät darf in keiner Weise zerlegt oder umgebaut werden.
- Um Brandgefahr und Stromschlag zu vermeiden, halten Sie das Produkt vor der Installation von Regen und Feuchtigkeit fern.
- Stellen Sie das Gerät nicht an Orten auf, an denen die Temperatur oder Luftfeuchtigkeit unterhalb/oberhalb des Betriebsbereichs liegt.
- Das Gerät darf niemals Stürzen, Stößen oder Schlägen ausgesetzt werden.
- Stellen Sie sicher, dass das Gerät bei der Installation fest sitzt.
- Stellen Sie sicher, dass der Stecker fest in die Steckdose eingesteckt ist.
- Ziehen Sie nicht an der Antenne oder dem Netzkabel, sondern lösen Sie diese, indem Sie die Stecker festhalten.

Konformitätserklärung

Das UR35 entspricht den grundlegenden Anforderungen und anderen relevanten Bestimmungen der CE, FCC und RoHS.

Für Unterstützung wenden Sie sich bitte an den technischen Support von Milesight:
E-Mail:iot.support@milesight.com Support-Portal: support.milesight-iot.com Tel.: 86-592-5085280
Fax: 86-592-5023065
Adresse: Gebäude C09, Software Park III, Xiamen 361024, China

Revisionsverlauf

Datum	Dokumentversion	Beschreibung
19. Juli 2019	V 1.1	Erstversion
23. September 2019	V 1.2	Unterstützung von Sprachanrufen
14. November 2019	V 1.3	Python-, SMS- und IP-Passthrough-Funktionen hinzugefügt
11. Mai 2020	V 1.4	Aktualisierung der Webschnittstellen
9. Dezember 2020	V 2.0	Layout ersetzen
17. September 2021	V 2.1	1. Mobilfunk- und Ping-Erkennung unterstützen IPv6; 2. WAN-Verbindungstyp hinzufügen: DHCPv6-Client, DS-Lite 3. DHCPv6-Server-Funktion hinzugefügt; 4. IPv6-Statisches-Routing-Feature hinzugefügt; 5. Expertenoption in IPsec-Einstellungen hinzugefügt; 6. Unterstützung für das Löschen von SMS-Eingangs- und Ausgangsmappen.
30. Juni 2023	V 2.2	1. Funktion zum Zurücksetzen von Verbindungen mit hoher Priorität hinzufügen; 2. Funktion für MQTT und TR069 hinzufügen; 3. Unterstützung für benutzerdefinierte Mobilfunk-MTU und IMS; 4. Unterstützung für den Import von OpenVPN-Dateikonfigurationen, Hinzufügen des TLS-Crypt-Modus und des Authentifizierungsmodus; 5. Aktualisierung von Modbus Master/Slave zu Modbus Client/Server; 6. Unterstützung für die Konfiguration des L2TP-Hostnamens.
5. Juli 2024	V 2.3	1. Hinzufügen der WireGuard-VPN-Funktion; 2. Hinzufügen der Auswahl des Mobilfunkbands und der Anpassung der Subnetzmaske; 3. Unterstützung für die Zeitsynchronisation mit dem Mobilfunkbetreiber; 4. Unterstützung für die Anzeige des Verbindungsstatus des Ethernet-Ports und die Konfiguration der PoE-Einstellungen; 5. Unterstützung der MQTT-Funktion im DI- und seriellen DTU-Modus Downlink;

		6. Aktualisierung der standardmäßigen sekundären ICMP- und DNS-Serveradresse; 7. WPA/WPA2-Enterprise-Verschlüsselungsmodus für den WLAN-Client-Modus hinzufügen; 8. Optimierung der IPsec-Einstellungen in der Web-GUI.

Inhalt

Kapitel 1 Produktvorstellung

1.1 Übersicht

Der UR35 ist ein industrieller Mobilfunkrouter mit integrierten intelligenten Softwarefunktionen, der für vielfältige M2M/IoT-Anwendungen entwickelt wurde. Der UR35 unterstützt globale WCDMA- und 4G LTE-Standards, bietet Betreibern sofortige Konnektivität und sorgt für eine enorme Steigerung der Betriebszeit.

Durch den Einsatz einer leistungsstarken und stromsparenden CPU in Industriequalität und eines Funkmoduls bietet der UR35 eine Netzwerkverbindung mit Wire-Speed bei geringem Stromverbrauch und extrem kompakter Bauweise, um eine äußerst sichere und zuverlässige Verbindung zum Funknetzwerk zu gewährleisten.

Gleichzeitig unterstützt der UR35 auch Fast-Ethernet-Ports, serielle Ports (RS232/RS485) und I/O (Ein-/Ausgänge), sodass Sie M2M-Anwendungen, die Daten und Videos kombinieren, in begrenzter Zeit und mit begrenztem Budget skalieren können.

Das UR35 eignet sich besonders für Smart Grids, digitale Medieninstallationen, industrielle Automatisierung, Telemetriegeräte, medizinische Geräte, digitale Fabriken, Finanzwesen, Zahlungsgeräte, Umweltschutz, Wasserwirtschaft und vieles mehr.

Einzelheiten zur Hardware und Installation finden Sie in der UR35-Schnellstartanleitung.

1.2 Vorteile

Vorteile

- Integrierte industrielle leistungsstarke NXP-CPU, großer Speicher
- Fast Ethernet für schnelle Datenübertragung
- Zwei SIM-Karten für die Sicherung zwischen mehreren Netzbetreibern und globale 2G/3G/LTE-Optionen erleichtern die Verbindung
- Ausgestattet mit Ethernet, E/A, serieller Schnittstelle, WLAN und GPS für die Verbindung verschiedener Feldgeräte
- Eingebettetes Python SDK für die Weiterentwicklung
- Robustes Gehäuse, optimiert für DIN-Schienen- oder Regalmontage
- 3 Jahre Garantie inklusive

Sicherheit und Zuverlässigkeit

- Automatisches Failover/Failback zwischen Ethernet und Mobilfunk (Dual-SIM)
- Aktivierung des Geräts mit Sicherheitsframeworks wie IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN/WirGuard
- Integrieren Sie einen Hardware-Watchdog, der automatisch verschiedene Fehler behebt und ein Höchstmaß an Verfügbarkeit gewährleistet.
- Einrichtung eines sicheren Mechanismus für die zentralisierte Authentifizierung und Autorisierung des Gerätezugriffs durch Unterstützung von AAA (TACACS+, Radius, LDAP, lokale Authentifizierung) und mehreren Benutzerebenen

Einfache Wartung

- Milesight DeviceHub bietet eine einfache Einrichtung, Massenkonfiguration und zentralisierte Verwaltung von Remote-Geräten
- Das benutzerfreundliche Design der Weboberfläche und mehrere Upgrade-Optionen helfen Administratoren dabei, das Gerät kinderleicht zu verwalten.
- Die Web-GUI und die CLI ermöglichen dem Administrator eine einfache Verwaltung und schnelle Konfiguration einer großen Anzahl von Geräten.
- Effiziente Verwaltung der Remote-Router auf der bestehenden Plattform durch den Industriestandard SNMP und TR069.

Funktionen

- Verbinden Sie Remote-Geräte in einer Umgebung, in der sich die Kommunikationstechnologien ständig ändern.
- Industrieller 32-Bit-ARM-Cortex-A7-Prozessor, hohe Leistung mit bis zu 528 MHz und 128 MB Speicher für die Unterstützung weiterer Anwendungen
- Unterstützt zahlreiche Protokolle wie SNMP,TR069, MQTT,Modbus-Bridging, RIP, OSPF
- Unterstützt einen breiten Betriebstemperaturbereich von -40 °C bis 70 °C/-40 °F bis 158 °F

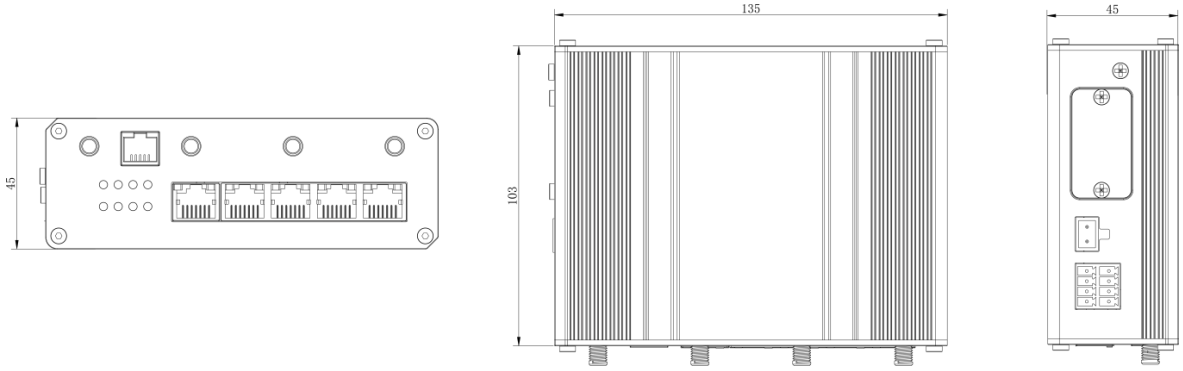
1.3 Technische Daten

Hardware-System	
CPU	528 MHz, 32-Bit-ARM-Cortex-A7
Speicher	128 MB Flash, 128 MB DDR3 RAM
Speicher	1 × Micro SD
Mobilfunk-Schnittstellen	
Anschlüsse	2 × 50 Ω SMA (Mittelstift: SMA-Buchse)
SIM-	2
WLAN-Schnittstelle	
Anschlüsse	1 × 50 Ω SMA (Mittelstift: RP-SMA-Buchse)
Standards	IEEE 802.11 b/g/n
Sendeleistung	802.11b: 16 dBm +/-1,5 dBm (11 Mbit/s) 802.11g: 14 dBm +/-1,5 dBm (54 Mbit/s) 802.11n: 13 dBm +/-1,5 dBm (65 Mbit/s, HT20/40 MCS7)
Modi	Unterstützt AP- und Client-Modus, mehrere SSIDs
Sicherheit	WPA/WPA2-Authentifizierung, WEP/TKIP/AES-Verschlüsselung
GPS (optional)	

Anschlüsse	1 × 50 Ω SMA (Mittelstift: SMA-Buchse)
Protokolle	NMEA 0183, PMTK
Ethernet	
Anschlüsse	5 × RJ-45 (PoE PSE optional)
Physikalische Schicht	10/100 Base-T (IEEE 802.3)
Datenrate	10/100 Mbit/s (automatische Erkennung)
Schnittstelle	Auto MDI/MDIX
Modus	Vollduplex oder Halbduplex (automatische Erkennung)
Serielle Schnittstelle	
Anschlüsse	1 × RS232 + 1 × RS485 (2 × RS485 optional)
Anschluss	Anschlussblock
Baudrate	300 bps bis 230400 bps
E/A	
Steckverbinder	Anschlussblock
Digital	1 × DI + 1 × DO
Software	
Netzwerkprotokolle	IPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH, MQTT, MQTTS, TR069 usw.
VPN-Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE/WirGuard
Firewall	ACL/DMZ/Port-Zuordnung/MAC-Bindung/SPI/DoS- und DDoS-Schutz /IP-Passthrough
Verwaltungs–	Web, CLI, SMS, On-Demand-Einwahl, DeviceHub AAA
Radius, TACACS+, LDAP, lokale Authentifizierung Mehrstufige Berechtigungsverwaltung Mehrere Ebenen von Benutzerberechtigungen	
Zuverlässigkeit	VRRP, WAN-Failover, Dual-SIM-Backup
Serieller Anschluss	Transparent (TCP-Client/Server, UDP), Modbus-Gateway (Modbus RTU zu Modbus TCP)
Stromversorgung und Verbrauch	
Anschluss	2-polig mit 5,08-mm-Klemmenblock
Eingangsspannung	9–48 VDC
Leistungsaufnahme	Typisch 3,9 W, max. 4,6 W (im Nicht-PoE-Modus)
Leistungsabgabe (optional)	4 × 802.3 af/at PoE-Ausgang
Physikalische Eigenschaften	

Schutzart	IP30
Gehäuse und Gewicht	Metall, 485 g
Abmessungen	135 x 100 x 45 mm (5,31 x 4,06 x 1,77 Zoll)
Befestigung	Tisch-, Wand- oder DIN-Schienenmontage
Sonstiges	
Reset-Taste	1 × RESET
LED-Anzeigen	1 × POWER, 1 × SYSTEM, 1 × SIM, 1 × Wi-Fi, 1 × VPN, 3 × Signalstärke
Integrier	Watchdog, Timer
Umgebung	
Betriebstemperatur	-40 °C bis +70 °C (-40 °F bis +158 °F) Reduzierte Zellleistung bei über 60 °C
Lagertemperatur	-40 °C bis +85 °C (-40 °F bis +185 °F)
Ethernet-Isolation	1,5 kV RMS
Relative Luftfeuchtigkeit	0 % bis 95 % (nicht kondensierend) bei 25 °C/77 °F

1.4 Abmessungen (mm)

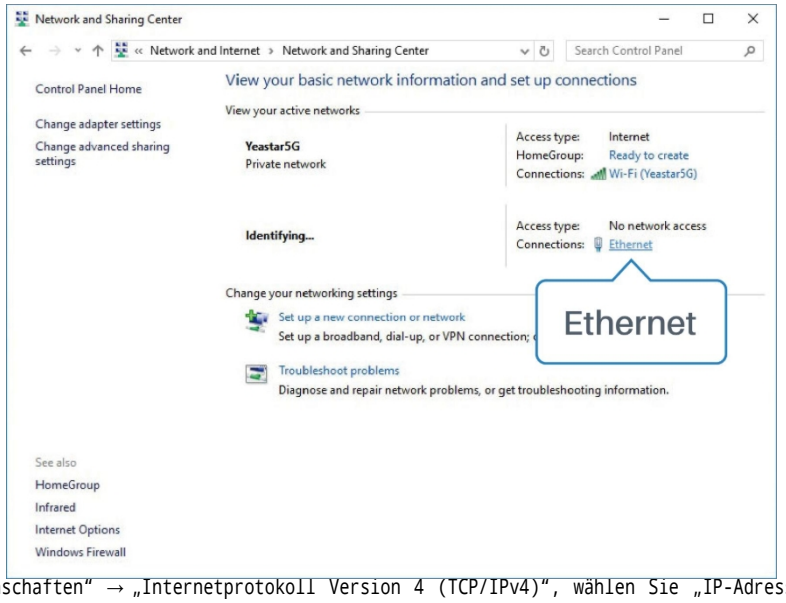


Kapitel 2 Zugriff auf die Web-GUI

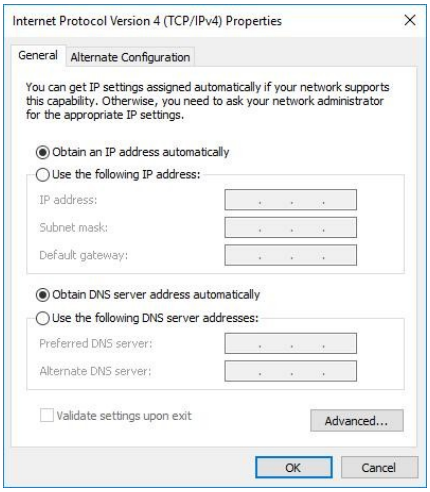
In diesem Kapitel wird erläutert, wie Sie auf die Web-GUI des UR35-Routers zugreifen können. Verbinden Sie den PC direkt mit dem LAN-Anschluss des UR35-Routers. Die folgenden Schritte basieren auf dem Betriebssystem Windows 10 und dienen als Referenz.

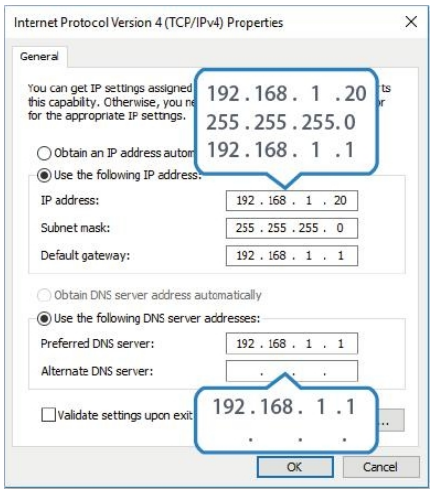
Benutzername: **admin**
Passwort: **password**
IP-Adresse: **192.168.1.1**

1. Gehen Sie zu „Systemsteuerung“ → „Netzwerk und Internet“ → „Netzwerk- und Freigabecenter“ und klicken Sie dann auf „Ethernet“ (kann auch anders heißen).



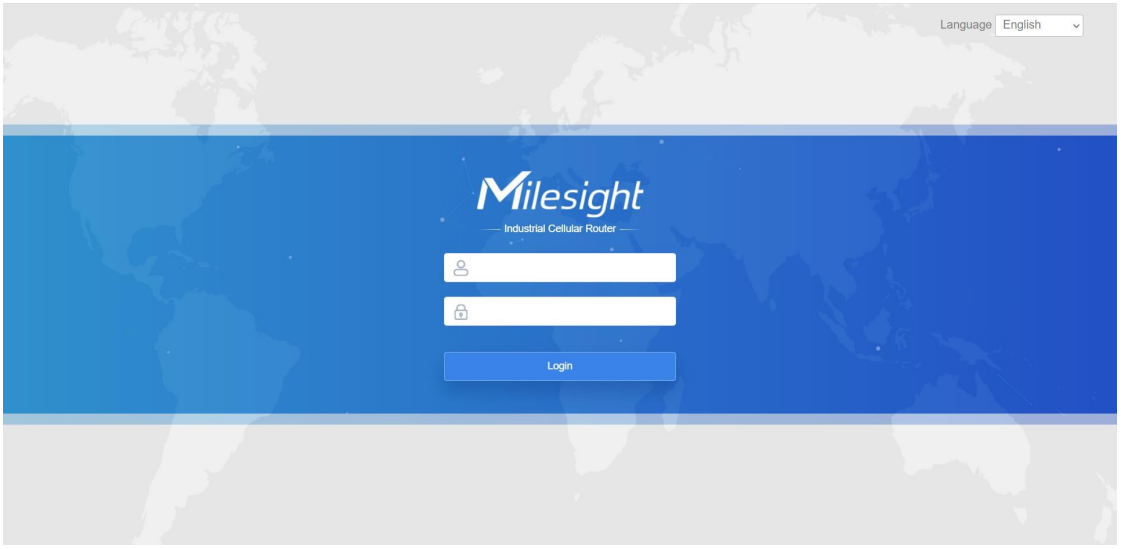
2. Gehen Sie zu „Eigenschaften“ → „Internetprotokoll Version 4 (TCP/IPv4)“, wählen Sie „IP-Adresse automatisch beziehen“ oder „Folgende IP-Adresse verwenden“ und weisen Sie dann manuell eine statische IP-Adresse innerhalb desselben Subnetzes des Geräts zu.





3. Öffnen Sie einen Webbrowser auf Ihrem PC (Chrome wird empfohlen), geben Sie die IP-Adresse 192.168.1.1 ein und drücken Sie die Eingabetaste auf Ihrer Tastatur.

4. Geben Sie den Benutzernamen und das Passwort ein und klicken Sie auf „Anmelden“.



Wenn Sie den Benutzernamen oder das Passwort mehr als fünfmal falsch eingeben, wird die Anmeldeseite für 10 Minuten gesperrt.

5. Wenn Sie sich mit dem Standardbenutzernamen und -kennwort anmelden, werden Sie aufgefordert, das Kennwort zu ändern. Aus Sicherheitsgründen wird empfohlen, das Kennwort zu ändern. Klicken Sie auf die Schaltfläche „Abbrechen“, wenn Sie es später ändern möchten.

6. Nachdem Sie sich bei der Web-GUI angemeldet haben, können Sie Systeminformationen anzeigen und Konfigurationen am Router vornehmen.

Kapitel 3 Webkonfiguration

3.1 Status

3.1.1 Übersicht

Auf dieser Seite können Sie die Systeminformationen des Routers anzeigen.

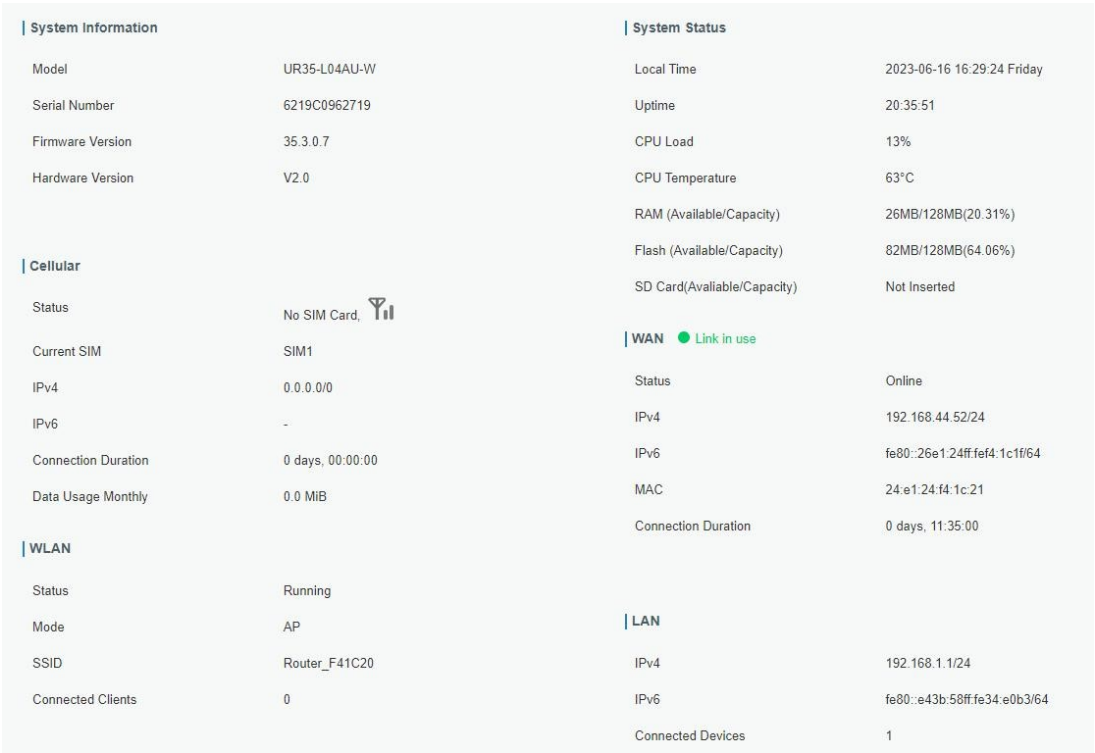


Abbildung 3-1-1-1

Systeminformationen	
Element	**Beschreibung**
Modell	Zeigt den Modellnamen des Routers an.
Seriennummer	Zeigt die Seriennummer des Routers an.
Firmware-Version	Zeigt die aktuelle Firmware-Version des Routers an.
Hardware-Version	Zeigt die aktuelle Hardwareversion des Routers an.

Tabelle 3-1-1-1 Systeminformationen

Systemstatus	
Element	**Beschreibung**
Lokale Zeit	Zeigt die aktuelle Ortszeit des Systems an.
Betriebszeit	Zeigen Sie die Informationen darüber an, wie lange der Router bereits in Betrieb ist.
CPU-Auslastung	Zeigt die aktuelle CPU-Auslastung des Routers an.
CPU-Temperatur	Aktuelle CPU-Temperatur anzeigen.
RAM (verfügbar/Kapazität)	Zeigt die RAM-Kapazität und den verfügbaren RAM-Speicher an.
Flash (verfügbar/Kapazität)	Zeigt die Flash-Kapazität und den verfügbaren Flash-Speicher an.
SD-Karte (Verfügbar/Kapazität)	Zeigt die Kapazität und den verfügbaren Speicher der Micro-SD-Karte an , sofern diese eingelegt ist.

Tabelle 3-1-1-2 Systemstatus

Mobilfunk	
Element	**Beschreibung**
Status	Zeigen Sie den Echtzeitstatus der aktuellen SIM-Karte an
Aktuelle SIM	Zeigt die SIM-Karte an, die derzeit für die Datenverbindung verwendet wird.
IPv4/IPv6	Zeigen Sie die vom Mobilfunkanbieter erhaltene IPv4/IPv6-Adresse an.

Verbindungsdauer	Zeigt die Verbindungsdauer der aktuellen SIM-Karte an.
Monatliche Datennutzung	Zeigt die monatliche Datenverbrauchsstatistik der aktuell verwendeten SIM-Karte an. .

Tabelle 3-1-1-3 Mobilfunkstatus

WAN	
Element	**Beschreibung**
Status	Zeigt den aktuellen Status des WAN-Ports an.
IPv4/IPv6	Die für den WAN-Port konfigurierte IPv4/IPv6-Adresse.
MAC	Die MAC-Adresse des Ethernet-Ports.
Verbindungsdauer	Zeigt die Verbindungsdauer des WAN-Ports an.

Tabelle 3-1-1-4 WAN-Status

WLAN	
Element	**Beschreibung**
Status	Zeigt den aktuellen Status des WLAN an.
IP	Zeigt den WLAN-Modus (AP oder Client) an.
SSID	Zeigt die SSID des WLAN-AP oder Clients an.
Verbundene Clients	Zeigt die Anzahl der verbundenen Geräte an, wenn der Modus AP ist.

Tabelle 3-1-1-5 WLAN-Status

LAN	
Element	**Beschreibung**
IP4/IPv6	Zeigt die IP4/IPv6-Adresse des LAN-Ports an.
Angeschlossene Geräte	Anzahl der Geräte, die mit dem LAN des Routers verbunden sind.

Tabelle 3-1-1-6 LAN-Status

3.1.2 Mobilfunk

Auf dieser Seite können Sie den Mobilfunknetzstatus des Routers anzeigen.

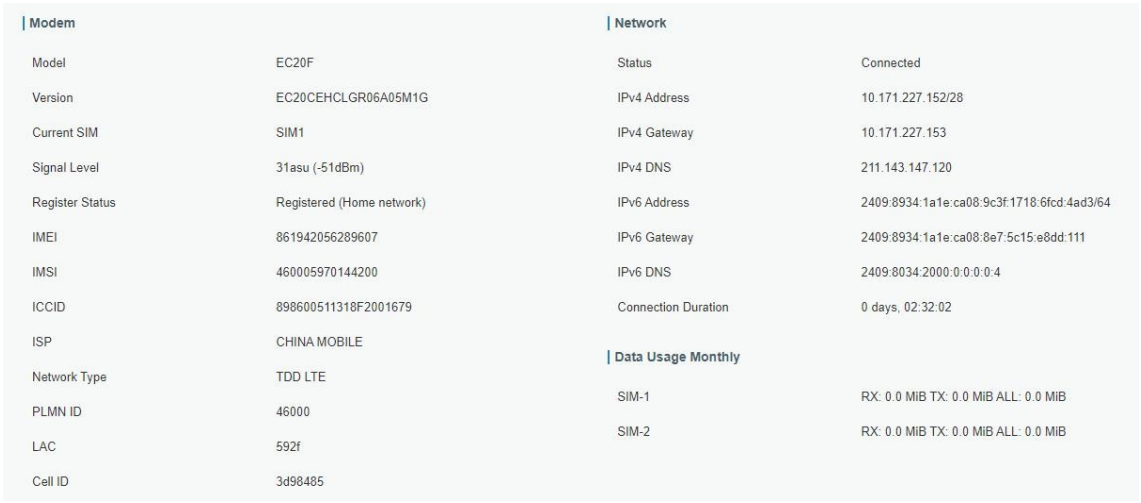


Abbildung 3-1-2-1

Modem-Informationen	
Element	**Beschreibung**

Status	Zeigt den entsprechenden Erkennungsstatus des Moduls und der SIM-Karte an.
Version	Zeigt die Firmware-Version des Mobilfunkmoduls an.
Aktuelle SIM	Zeigt die aktuell verwendete SIM-Karte an.
Signalpegel	Zeigt die Mobilfunksignalstärke an.
Registrierungsstatus	Zeigt den Registrierungsstatus der SIM-Karte an.
IMEI	Zeigen Sie die IMEI des Moduls an.
IMSI	Zeigen Sie die IMSI der SIM-Karte an.
ICCID	Zeigen Sie die ICCID der SIM-Karte an.
ISP	Zeigt den Netzbetreiber an, bei dem die SIM-Karte registriert ist.
Netzwerktyp	Zeigt den verbundenen Netzwerktyp an, z. B. LTE, 3G usw.
PLMN-ID	Zeigt die aktuelle PLMN-ID an, einschließlich MCC,MNC,LAC und Cell ID.
LAC	Zeigt den Standortbereichscode der SIM-Karte an.
Cell-ID	Zeigen Sie die Zell-ID des SIM-Kartenstandorts an.

Tabelle 3-1-2-1 Modem-Informationen

Netz	
Element	**Beschreibung**
Status	Zeigt den Verbindungsstatus des Mobilfunknetzes an.
IPv4/IPv6-Adresse	Zeigt die IPv4/IPv6-Adresse und die Netzmaske des Mobilfunknetzes an.
IPv4/IPv6-Gateway	Zeigt das IPv4/IPv6-Gateway und die Netzmaske des Mobilfunknetzes an.
IPv4/IPv6-DNS	Zeigt die IPv4/IPv6-DNS des Mobilfunknetzes an.
Verbindungsdauer	Zeigt Informationen darüber an, wie lange das Mobilfunknetz verbunden ist verbunden ist.

Tabelle 3-1-2-2 Netzwerkstatus

Datenverbrauch monatlich	
Element	**Beschreibung**
SIM-1	Zeigen Sie die monatlichen Datenverbrauchsstatistiken von SIM-1 an.
SIM-2	Zeigen Sie die monatlichen Datenverbrauchsstatistiken von SIM-2 an.

Tabelle 3-1-2-3 Informationen zur Datennutzung

3.1.3 Netz

Auf dieser Seite können Sie den WAN- und LAN-Status des Routers überprüfen.

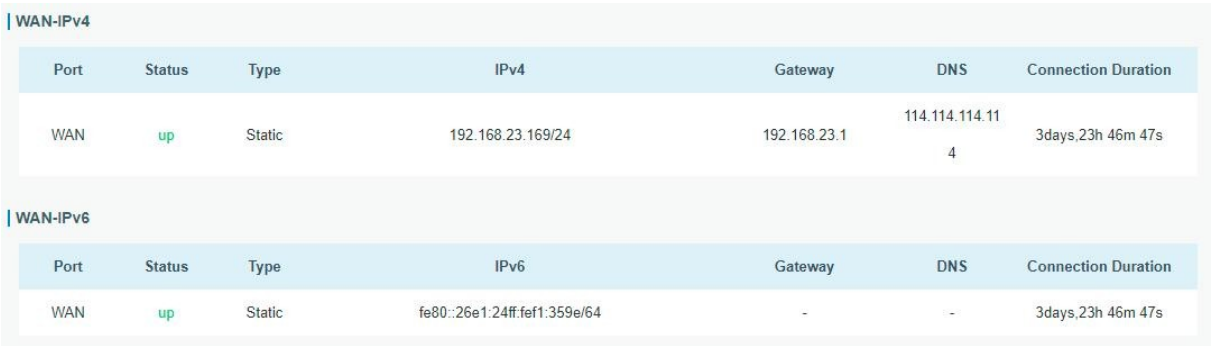


Abbildung 3-1-3-1

WAN-Status

Element	Beschreibung
Port	Zeigt den Namen des WAN-Ports an.
Status	Zeigt den Status des WAN-Ports an. „up“ bedeutet, dass WAN aktiviert und das Ethernet-Kabel angeschlossen ist. „down“ bedeutet, dass das Ethernet-Kabel getrennt ist oder die WAN-Funktion deaktiviert ist.
Typ	Zeigt den Typ der DFÜ-Verbindung des WAN-Ports an.
IPv4/IPv6	Zeigt die IPv4-Adresse mit Netzmaske oder die IPv6-Adresse mit Präfixlänge des WAN-Ports an.
Gateway	Zeigt das Gateway des WAN-Ports an.
DNS	Zeigt das DNS des WAN-Ports an.
Verbindungsdauer	Zeigen Sie die Informationen darüber an, wie lange das Ethernet-Kabel angeschlossen war am WAN-Port angezeigt, wenn die WAN-Funktion aktiviert ist. Sobald die WAN-Funktion deaktiviert oder die Ethernet-Verbindung getrennt wird, wird die Zeitmessung beendet.

Tabelle 3-1-3-1 WAN-Status

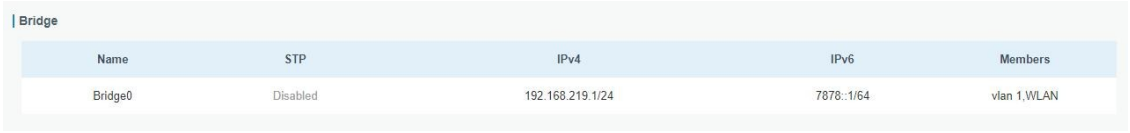


Abbildung 3-1-3-2

Bridge	
Element	**Beschreibung**
Name	Zeigt den Namen der Bridge-Schnittstelle an.
STP	Zeigt an, ob STP aktiviert ist.
IPv4/IPv6	Zeigt die IPv4/IPv6-Adresse und die Netzmaske der Bridge-Schnittstelle an.
Netzmaske	Zeigt die Netzmaske der Bridge-Schnittstelle an.
Mitglieder	Zeigen Sie die Mitglieder der Bridge-Schnittstelle an.

Tabelle 3-1-3-2 Bridge-Status

3.1.4 WLAN

Auf dieser Seite können Sie den WLAN-Status überprüfen, einschließlich der Informationen zum Zugangspunkt und zum Client.

Abbildung 3-1-4-1

WLAN-Status

Element	Beschreibung
WLAN-Status	
Name	Zeigt den Namen der WLAN-Schnittstelle an.
Status	Zeigt den Status der WLAN-Schnittstelle an.
Typ	Zeigt den Typ der WLAN-Schnittstelle an.
SSID	Zeigt die SSID des Routers an, wenn der Schnittstellentyp AP ist. Zeigen Sie die SSID des AP an, mit dem der Router verbunden ist, wenn der Schnittstellentyp „Client“ ist.
IP-Adresse	Zeigt die IP-Adresse des Routers an, wenn der Schnittstellentyp „AP“ ist. Zeigt die IP-Adresse des AP an, mit dem der Router verbunden ist , wenn der Schnittstellentyp „Client“ ist.
Netzmaske	Zeigt die Netzmaske des Routers an, wenn der Schnittstellentyp „AP“ ist. Zeigt die Netzmaske des AP an, mit dem der Router verbunden ist, wenn der Schnittstellentyp Client ist.
Verbundene Stationen	
SSID	Zeigt die SSID des Routers an, wenn der Schnittstellentyp AP ist. Zeigt die SSID des AP an, mit dem der Router verbunden ist, wenn der Schnittstellentyp „Client“ ist.
MAC-Adresse	Zeigt die MAC-Adresse des Clients an, der mit dem Router verbunden ist, wenn der Schnittstellentyp AP ist. Zeigt die MAC-Adresse des AP an, mit dem der Router verbunden ist, wenn der Schnittstellentyp Client ist.
IP-Adresse	Zeigen Sie die IP-Adresse des Clients an, der mit dem Router verbunden ist, wenn der Schnittstellentyp AP ist. Zeigen Sie die IP-Adresse des AP an , mit dem der Router verbunden ist, wenn der Schnittstellentyp „Client“ ist.
Verbindungsdauer	Zeigen Sie die Verbindungsdauer zwischen dem Client-Gerät und dem Router an, wenn der Schnittstellentyp AP ist. Zeigen Sie die Verbindungsdauer zwischen dem Router und dem AP anzeigen, wenn der Schnittstellentyp Client ist.

Tabelle 3-1-4-1 WLAN-Status

3.1.5 VPN

Auf dieser Seite können Sie den VPN-Status überprüfen, einschließlich PPTP, L2TP, IPsec, OpenVPN und DMVPN.

Abbildung 3-1-5-1

VPN-Status	
Element	**Beschreibung**
Clients	
Name	Zeigt den Namen der aktivierten VPN-Clients an.
Status	Zeigt den Status des Clients an. „Verbunden" bedeutet, dass der Client mit dem Server verbunden ist. „Getrennt" bedeutet, dass , dass der Client vom Server getrennt ist.
Lokale IP	Zeigt die lokale IP-Adresse des Tunnels an.
Remote-IP	Zeige die echte Remote-IP-Adresse des Tunnels an.
Server	
Name	Zeigt den Namen des aktivierten VPN-Servers an.
Status	Zeigt den Status des Servers an.
Verbindungsliste	
Servertyp	Zeigt den Typ des Servers an.
Client-IP	Zeigt die IP-Adresse des Clients an, der mit dem Server verbunden hat.
Dauer	Zeigt die Informationen darüber an, wie lange der Client mit diesem Server verbunden war, wenn der Server aktiviert ist. Sobald der Server deaktiviert oder die Verbindung getrennt wird, wird die Die Dauer wird nicht mehr gezählt.

Tabelle 3-1-5-1 VPN-Status

3.1.6 Routing

Auf dieser Seite können Sie den Routing-Status überprüfen, einschließlich der Routing-Tabelle und des ARP-Caches.

| Routing Table

Destination	Netmask/Prefix Length	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.22.1	WAN	1
127.0.0.0	255.0.0.0	-	Loopback	-
192.168.1.0	255.255.255.0	-	Bridge0	-
192.168.22.0	255.255.255.0	-	WAN	-
::	0	2408:844b:1a20:fc0:1d0a:9a67:4a3:3b5a	Cellular 0	-
::1	128	-	Loopback	-
2001:4860:4860::8888	128	2408:844b:1a20:fc0:1d0a:9a67:4a3:3b5a	Cellular 0	1
2004::	64	-	Bridge0	-
2400:3200::1	128	2408:844b:1a20:fc0:1d0a:9a67:4a3:3b5a	Cellular 0	1
2408:844b:1a20:fc0::	64	-	Cellular 0	-

| ARP Cache

IP	MAC	Interface
192.168.1.113	c8:5b:76:b2:56:1f	Bridge0
192.168.22.127	24:e1:24:f0:47:e1	WAN
192.168.22.1	5c:dd:70:6c:46:3d	WAN
192.168.22.6	f4:b5:49:f1:1b:1f	WAN
192.168.23.77	24:4b:fe:8d:95:ab	WAN

Manual Refresh

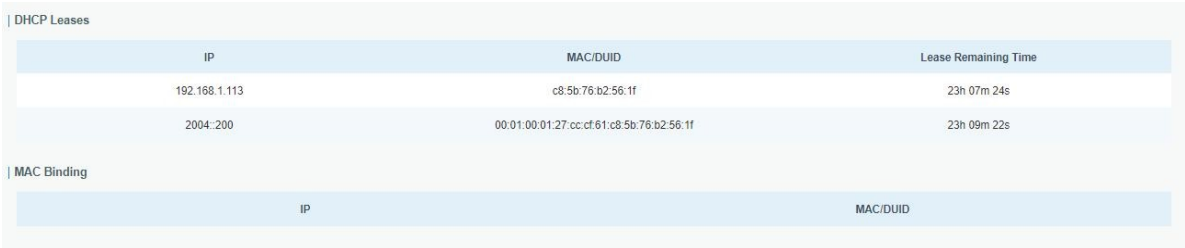
Abbildung 3-1-6-1

Element	Beschreibung
Routing-Tabelle	
Ziel	Zeigt die IP-Adresse des Zielhosts oder des Zielnetzwerks an.
Netzmaske/Präfix Länge	Zeigt die Netzmaske oder Präfixlänge des Zielhosts oder Zielnetzwerks an. Netzwerks.
Gateway	Zeigt die IP-Adresse des Gateways an.
Schnittstelle	Zeigt die ausgehende Schnittstelle der Route an.
Metrik	Zeige die Metrik der Route an.
ARP-Cache	
IP	Zeigen Sie die IP-Adresse des ARP-Pools an.
MAC	Zeigen Sie die der IP-Adresse entsprechende MAC-Adresse an.
Schnittstelle	Zeigt die zugehörige Schnittstelle von ARP an.

Tabelle 3-1-6-1 Routing-Informationen

3.1.7 Host-Liste

Auf dieser Seite können Sie die Host-Informationen anzeigen.



| DHCP Leases

IP	MAC/DUID	Lease Remaining Time
192.168.1.113	c8:5b:76:b2:56:1f	23h 07m 24s
2004::200	00:01:00:01:27:cc:cf:61:c8:5b:76:b2:56:1f	23h 09m 22s

| MAC Binding

IP	MAC/DUID

Abbildung 3-1-7-1

Hostliste	
Element	**Beschreibung**
DHCP-Leases	
IP-Adresse	IP-Adresse des DHCP-Clients anzeigen
MAC/DUID	MAC-Adresse des DHCPv4-Clients oder DUID des DHCPv6-Clients anzeigen.
Verbleibende Lease-Zeit	Die verbleibende Leasingdauer des DHCP-Clients anzeigen.
MAC-Bindung	
IP & MAC	Zeigen Sie die IP-Adresse und MAC-Adresse an, die in der Liste „Statische IP“ des DHCP-Dienst.

Tabelle 3-1-7-1 Hostliste Beschreibung

3.1.8 GPS (gilt nur für GPS-Version)

Wenn die GPS-Funktion aktiviert ist und die GPS-Informationen erfolgreich abgerufen wurden, können Sie auf dieser Seite die aktuellen GPS-Informationen anzeigen, darunter GPS-Zeit, Breiten- und Längengrad sowie Geschwindigkeit.

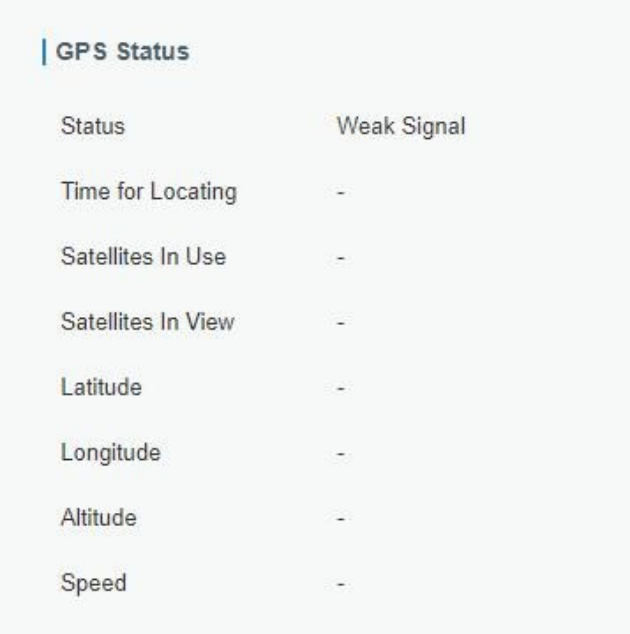


Abbildung 3-1-8-1

GPS-Status	
Element	**Beschreibung**
Status	Zeigt den Status des GPS an.
Zeit für die Ortung	Zeigt die Zeit für die Ortung an.
Verwendete Satelliten	Zeigt die Anzahl der verwendeten Satelliten an.
Sichtbare Satelliten	Zeigt die Anzahl der sichtbaren Satelliten an.
Breitengrad	Zeigt den Breitengrad des Standorts an.
Längengrad	Zeigt den Längengrad des Standorts an.
Höhe	Zeigt die Höhe des Standorts an.
Geschwindigkeit	Zeigt die Bewegungsgeschwindigkeit an.

Tabelle 3-1-8-1 GPS-Status Beschreibung

3.2 Netz

3.2.1 Schnittstelle

3.2.1.1 Verbindungsausfall

In diesem Abschnitt wird beschrieben, wie Sie Link-Failover-Strategien, deren Priorität und die Ping-Einstellungen konfigurieren. Jede Regel verfügt standardmäßig über eigene Ping-Regeln. Der Router wählt gemäß der Priorität die nächste verfügbare Schnittstelle für den Internetzugang aus. Stellen Sie sicher, dass Sie hier die gesamte Schnittstelle aktiviert haben, die Sie verwenden möchten. Wenn Priorität 1 nur IPv4 verwenden kann, wählt UR35 einen zweiten Link aus, bei dem IPv6 als primärer IPv6-Link fungiert, und umgekehrt.

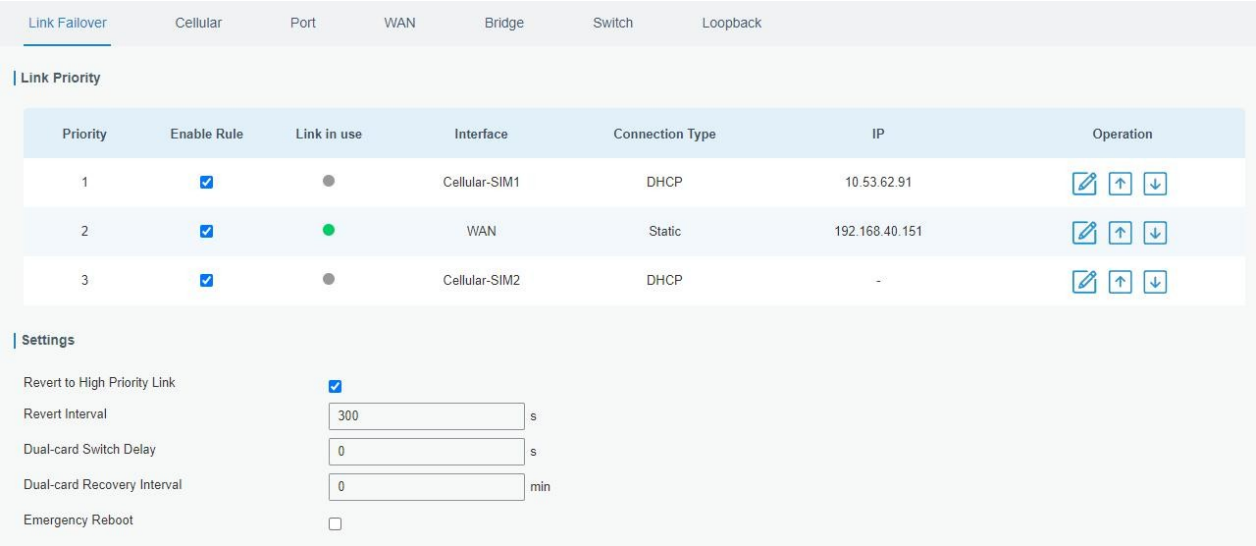


Abbildung 3-2-1-1

Link-Failover	
Element	**Beschreibung**
Link-Priorität	
Priorität	Zeigt die Priorität jeder Schnittstelle an. Sie können sie mit den Aufwärts- und Abwärts-Schaltflächen der Operation ändern.
Regel aktivieren	Wenn diese Option aktiviert ist, nimmt der Router diese Schnittstelle in seine Switching-Regel auf. Wenn die Mobilfunkschnittstelle hier nicht aktiviert ist, wird die Schnittstelle ebenfalls deaktiviert.
Verbindung in Gebrauch	Markieren Sie mit grüner Farbe, ob diese Schnittstelle verwendet wird
Schnittstelle	Zeigen Sie den Namen der Schnittstelle an.
Verbindungstyp	Zeigen Sie an, wie die IP-Adresse in dieser Schnittstelle abgerufen werden kann, z. B. statisch IP oder DHCP.
IP	Zeigen Sie die IP-Adresse der Schnittstelle an.
Betrieb	Sie können die Priorität der Regeln ändern und die Ping-Erkennungsregeln hier konfigurieren. Erkennungsregeln konfigurieren.
Einstellungen	
Zurück zu Hoch Prioritätsverbindung	Wenn die Verbindung der Verbindung mit hoher Priorität wiederhergestellt ist, wird zur Verbindung mit hoher Priorität zurück.
Rückstellintervall	Geben Sie die Anzahl der Sekunden an, die gewartet werden soll, bevor zur

	Verbindung mit höherer Priorität, 0 bedeutet, dass die Funktion deaktiviert ist.
Dual-Karten-Schalter Verzögerung	Die Verzögerungszeit für den Wechsel zur Karte mit niedriger Priorität, wenn die Verbindung zur Karte mit hoher Priorität unterbrochen ist. Mobilfunkverbindung mit hoher Priorität fehlschlägt. 0 bedeutet sofortiges Umschalten.
Wiederherstellung bei zwei Karten Intervall	Das Intervall zur Erkennung einer Mobilfunkverbindung mit hoher Priorität. Wenn die Verbindung wiederhergestellt ist, wird wieder auf die Mobilfunkverbindung mit hoher Priorität umgeschaltet.
Notfall-Neustart	Aktivieren Sie diese Option, um das Gerät neu zu starten, wenn keine Verbindung verfügbar ist.

Tabelle 3-2-1-1 Parameter für die Verbindungsausfallsicherung

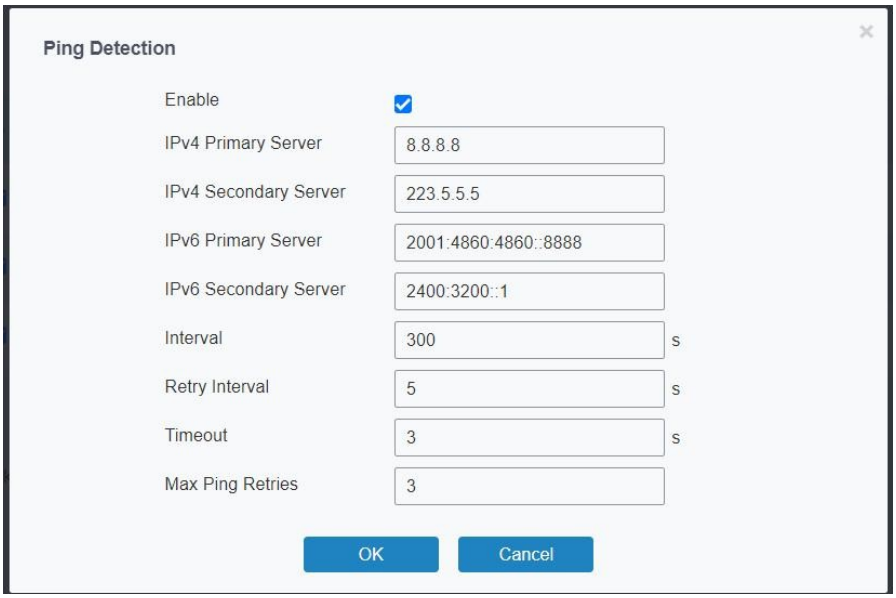


Abbildung 3-2-1-2

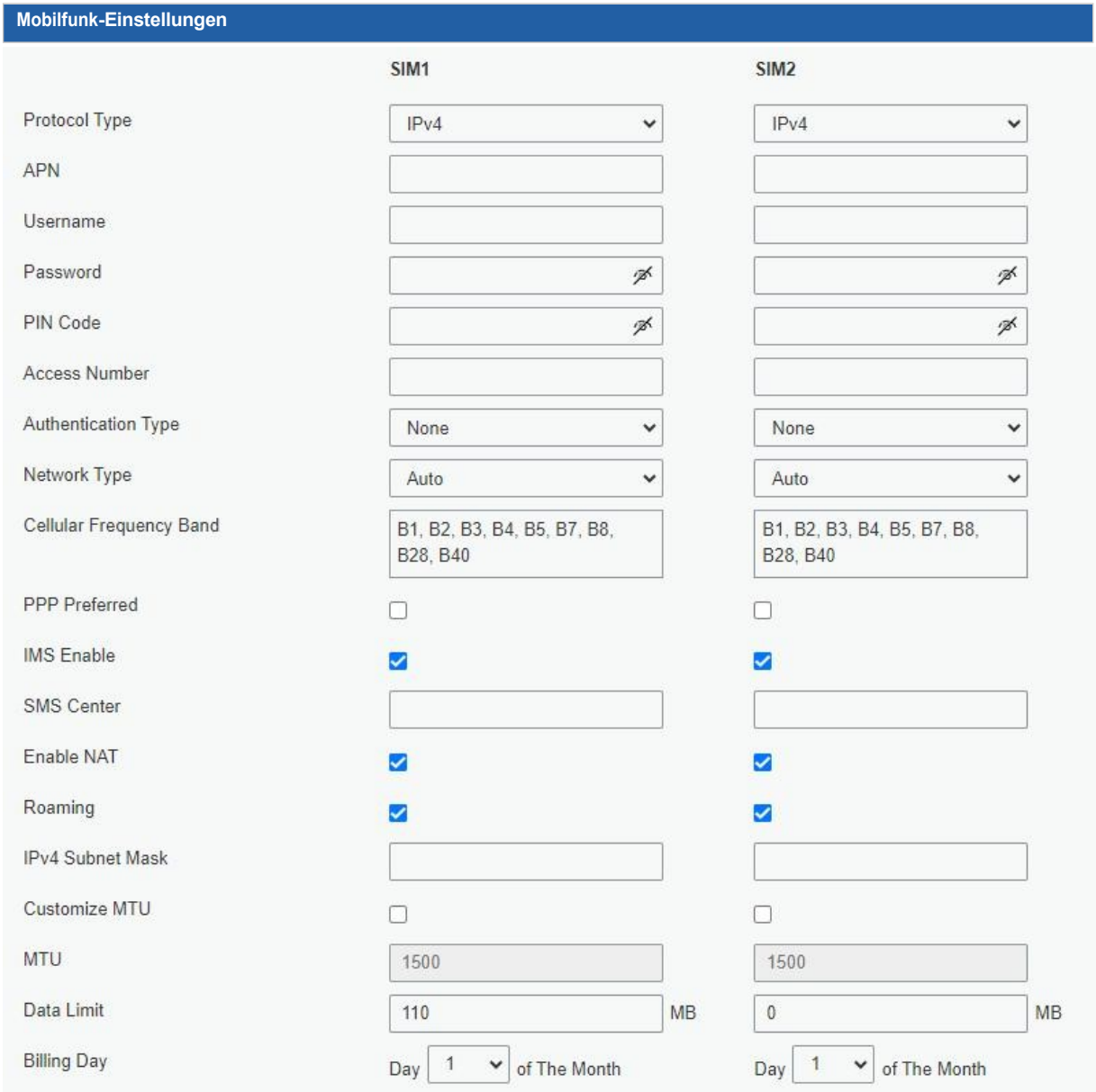
Ping-Erkennung	
Artikel	**Beschreibung**
Aktivieren	Wenn diese Option aktiviert ist, überprüft der Router regelmäßig den Verbindungsstatus des Links.
IPv4/IPv6-Primärserver	Der Router sendet ein ICMP-Paket an die IPv4/IPv6-Adresse oder den Hostnamen, um festzustellen, ob die Internetverbindung noch verfügbar ist oder nicht.
IPv4/IPv6-Sekundärserver Server	Der Router versucht, den sekundären Servernamen anzupingen, wenn Primärserver nicht verfügbar ist.
Intervall	Zeitintervall (in Sekunden) zwischen zwei Pings.
Wiederholungsintervall	Legen Sie das Ping-Wiederholungsintervall fest. Wenn der Ping fehlschlägt, in jedem Wiederholungsintervall erneut einen Ping-Versuch.
Zeitlimit	Die maximale Zeit, die der Router auf eine Antwort auf eine Ping-Anfrage wartet. Wenn er innerhalb der in diesem Feld definierten Zeit keine Antwort erhält, gilt die Ping-Anfrage als fehlgeschlagen betrachtet.
Maximale Ping-Wiederholungen	Die Anzahl der Wiederholungsversuche, die der Router unternimmt, um eine Ping-Anfrage zu senden, bis Feststellung, dass die Verbindung fehlgeschlagen ist.

Tabelle 3-2-1-2 Ping-Erkennungsparameter

3.2.1.2 Mobilfunk

In diesem Abschnitt wird erläutert, wie Sie die entsprechenden Parameter für das Mobilfunknetz einstellen. Der UR35-Mobilfunkrouter verfügt über zwei Mobilfunkschnittstellen, nämlich SIM1 und SIM2. Es ist jeweils nur eine Mobilfunkschnittstelle aktiv. Wenn beide Mobilfunkschnittstellen aktiviert sind, gilt die auf der Seite „Link Failover“ konfigurierte Prioritätsregel.

Abbildung 3-2-1-3



Element	Beschreibung
Protokolltyp	Wählen Sie zwischen „IPv4“, „IPv6“ und „IPv4/IPv6“.
APN	Geben Sie den Zugangspunktnamen für die Mobilfunk-Einwahlverbindung , den Sie von Ihrem lokalen Internetdienstanbieter erhalten haben.
Benutzername	Geben Sie den Benutzernamen für die vom lokalen Internetdienstanbieter bereitgestellte Mobilfunk-Einwahlverbindung ein lokalen Internetdienstanbieters bereitgestellt wird.
Passwort	Geben Sie das Passwort für die vom lokalen Internetdienstanbieter bereitgestellte Mobilfunk-Einwahlverbindung ein.

	lokalen Internetdienstanbieters.
PIN-Code	Geben Sie einen 4-8-stelligen PIN-Code ein, um die SIM-Karte zu entsperren.
Zugangsnummer	Geben Sie die Nummer der Einwahlzentrale für die vom lokalen ISP bereitgestellt wird.
Authentifizierungstyp	Wählen Sie zwischen „Keine", „PAP" oder „CHAP".
Netzwerktyp	Wählen Sie zwischen „Auto", „Nur 4G", „Nur 3G" und „Nur 2G". Auto: Verbindet sich automatisch mit dem Netzwerk mit dem stärksten Signal. Nur 4G: Verbindet sich nur mit dem 4G-Netzwerk. Und so weiter.
Mobilfunkfrequenz Band	Wählen Sie die Mobilfunkbänder aus, die zur Registrierung des Mobilfunknetzes verwendet werden. Dies kann zur Optimierung der Mobilfunkgeschwindigkeit durch Auswahl bestimmter Frequenzbänder verwendet werden.
PPP bevorzugt	Die PPP-Einwahlmethode wird bevorzugt.
IMS aktivieren	IMS-Funktion aktivieren oder deaktivieren.
SMS-Zentrum	Geben Sie die Nummer der lokalen SMS-Zentrale ein, um SMS zu speichern, weiterzuleiten, zu konvertieren und Zustellung von SMS-Nachrichten.
NAT aktivieren	Aktivieren oder deaktivieren Sie die NAT-Funktion.
Roaming	Roaming aktivieren oder deaktivieren.
IPv4-Subnetzmaske	Passen Sie die Mobilfunk-Subnetzmaske an. Wenn dieses Feld leer ist, verwendet das Gerät die von der Mobilfunkbasisstation bereitgestellte Subnetzmaske.
MTU anpassen	Aktivieren oder deaktivieren Sie diese Option, um die maximalen Übertragungseinheiten anzupassen. Wenn deaktiviert, verwendet das Gerät die MTU-Einstellungen des Betreibers.
MTU	Passen Sie die maximalen Übertragungseinheiten an.
Datenlimit	Wenn Sie das festgelegte Datenvolumen erreicht haben, wird die Datenverbindung der aktuell verwendeten SIM-Karte deaktiviert. 0 bedeutet, dass die Funktion deaktiviert wird Funktion deaktiviert.
Abrechnungstag	Wählen Sie den Abrechnungstag der SIM-Karte. Der Router setzt die verwendeten Daten auf 0 zurück.

Tabelle 3-2-1-3 Mobilfunkparameter

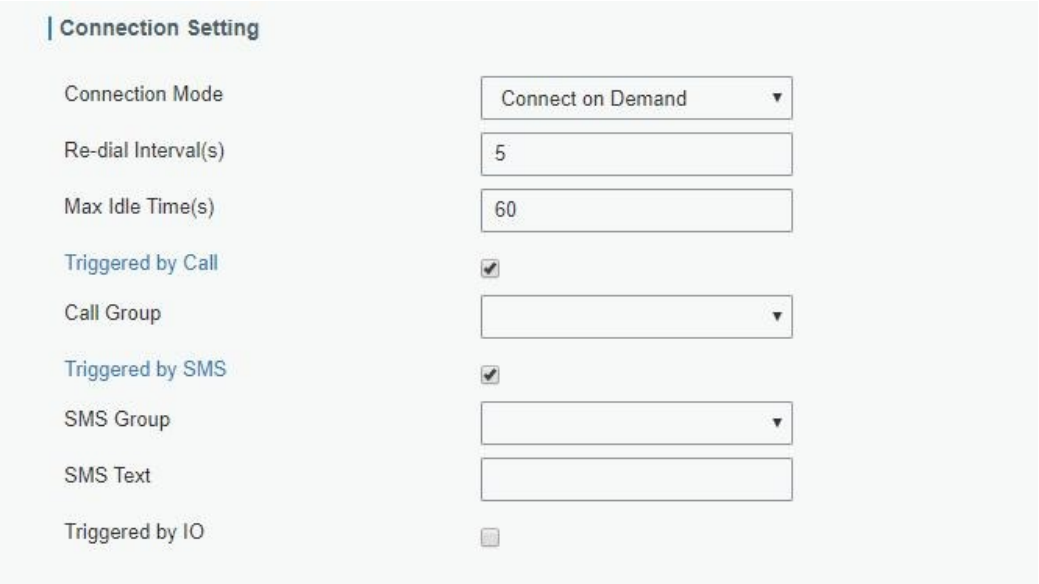


Abbildung 3-2-1-4

Verbindungseinstellungen	
Element	**Beschreibung**
Verbindungsmodus	Wählen Sie „Immer online“ und „Bei Bedarf verbinden“.
Wählintervall(e)	Stellen Sie das Intervall ein, nach dem die Verbindung zum ISP hergestellt werden soll, wenn die Verbindung unterbrochen wird. Der Standardwert beträgt 5 Sekunden.
Maximale Leerlaufzeiten	Legen Sie die maximale Dauer fest, die der Router im Leerlaufzustand der aktuellen Verbindung verbleiben soll . Bereich: 10-3600
Durch Anruf ausgelöst	Der Router wechselt automatisch vom Offline-Modus in den Mobilfunknetzmodus , wenn er einen Anruf von einer bestimmten Telefonnummer erhält.
Anrufgruppe	Wählen Sie eine Anrufgruppe für den Anrufauslöser aus. Gehen Sie zu **System > Telefon & SMS > Telefon,** um Telefon-Gruppe einrichten.
Ausgelöst durch SMS	Der Router wechselt automatisch vom Offline-Modus in den Mobilfunknetzmodus , wenn er eine bestimmte SMS von einem bestimmten Mobiltelefon empfängt.
SMS-Gruppe	Wählen Sie eine SMS-Gruppe für den Auslöser aus. Gehen Sie zu **System > Telefon & SMS > SMS,** um eine SMS-Gruppe einrichten.
SMS-Text	Geben Sie den SMS-Inhalt für die Auslösung ein.
Ausgelöst durch IO	Der Router wechselt automatisch vom Offline-Modus in den Mobilfunkmodus, wenn sich der DI-Status ändert. Gehen Sie zu „Industrial > I/O > DI“, um die Auslösebedingung zu konfigurieren.

Tabelle 3-2-1-4 Mobilfunkparameter

Verwandte Themen

Mobilfunknetzverbindung
Telefongruppe
DI-Einstellung

3.2.1.3 Port

In diesem Abschnitt wird beschrieben, wie Sie die Ethernet-Port-Parameter konfigurieren. Der Mobilfunkrouter UR35 unterstützt 5 Fast-Ethernet-Ports.

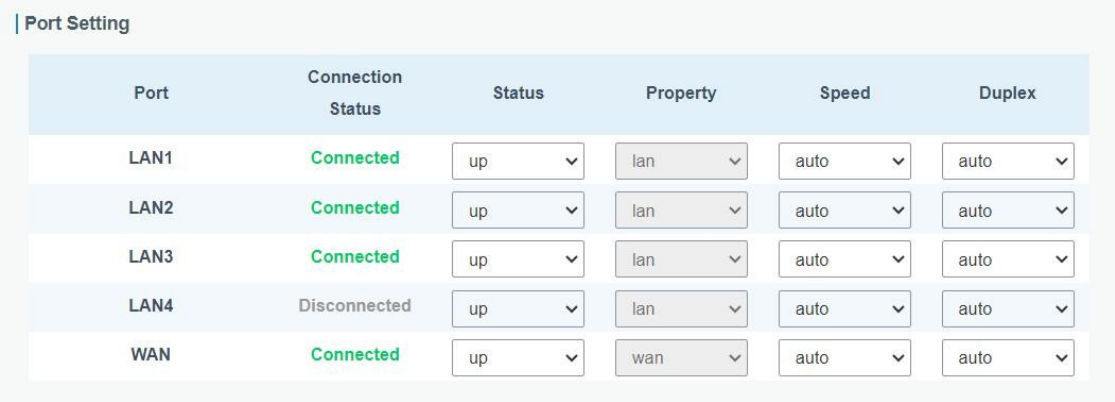


Abbildung 3-2-1-5

Port-Einstellung	
Element	**Beschreibung**

Port	Benutzer können die Ethernet-Ports entsprechend ihren Anforderungen definieren.
Verbindung Status	Zeigt den Verbindungsstatus dieses Ethernet-Ports an.
Status	Legen Sie den Status des Ethernet-Ports fest; wählen Sie „up“, um ihn zu aktivieren, und „down“, , um ihn zu deaktivieren.
Eigenschaft	Zeigt den Typ des Ethernet-Ports an, entweder als WAN-Port oder als LAN-Port.
Geschwindigkeit	Legen Sie die Geschwindigkeit des Ethernet-Ports fest. Die Optionen sind „auto“, „100 Mbps“ und „10 Mbps“.
Duplex	Stellen Sie den Modus des Ethernet-Ports ein. Die Optionen sind „auto“, „full“ und „half“.

Tabelle 3-2-1-5 Port-Parameter

Hinweis:

- **Nur die PoE-Version (Modellname enthält „-P“) unterstützt die folgenden Einstellungen.**
- **Diese Einstellungen funktionieren nur, wenn dieser Router mit 48 V betrieben wird.**
- **Nur Geräte mit Hardwareversion 3.0 und höher unterstützen diese Funktionen.**

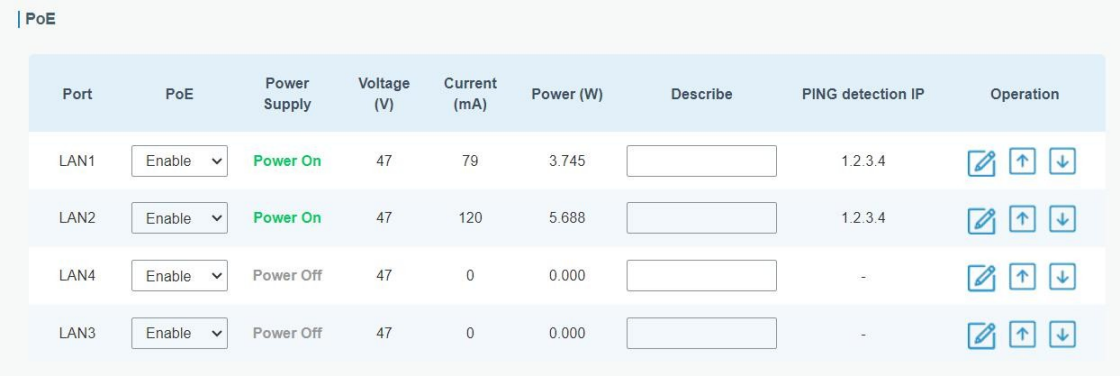


Abbildung 3-2-1-6

PoE-Einstellung	
Element	**Beschreibung**
Port	Benutzer können die Ethernet-Ports entsprechend ihren Anforderungen definieren.
PoE	Aktivieren oder deaktivieren Sie diesen Ethernet-Anschluss, um Strom zu liefern.
Stromversorgung	Zeigen Sie den Status der Stromversorgung dieses Ethernet-Ports an.
Spannung	Zeigen Sie die aktuelle Ausgangsspannung dieses Ethernet-Ports an.
Strom	Zeigt den aktuellen Ausgangsstrom dieses Ethernet-Ports an.
Leistung	Zeigt die aktuelle Ausgangsleistung dieses Ethernet-Ports an.
Beschreibung	Fügen Sie die Beschreibung dieses Ethernet-Ports hinzu.
Ping-Erkennung IP	Zeigen Sie die IP-Adresse an, an die das ICMP-Paket gesendet werden soll, um den Verbindungsstatus zu erkennen. .
Betrieb	Sie können die Priorität der Stromversorgung der Ports ändern und die Ping-Erkennungsregeln konfigurieren.

Tabelle 3-2-1-6 PoE-Parameter

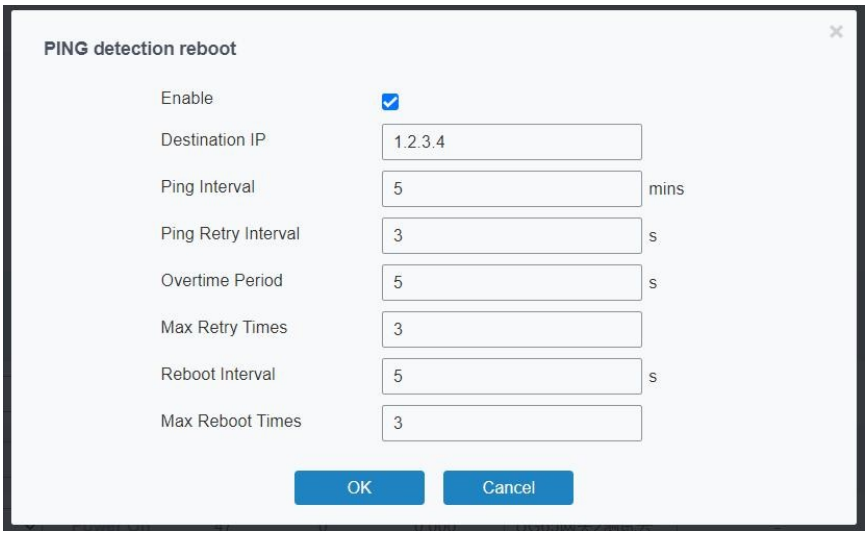


Abbildung 3-2-1-7

Ping-Erkennung Neustart	
Element	**Beschreibung**
Aktivieren	Wenn diese Option aktiviert ist, überprüft der Router regelmäßig den Verbindungsstatus des Ports. Wenn die Erkennung fehlschlägt, startet der Router diesen Port neu.
Ziel-IP	Der Router sendet ein ICMP-Paket an die IPv4-Adresse, um festzustellen, ob die Verbindung noch verfügbar ist oder nicht.
Intervall	Zeitintervall (in Sekunden) zwischen zwei Pings.
Ping-Wiederholungsintervall	Legen Sie das Ping-Wiederholungsintervall fest. Wenn der Ping fehlschlägt, sendet der Router erneut in jedem Wiederholungsintervall.
Zeitüberschreitungszeitraum	Die maximale Zeit, die der Router auf eine Antwort auf eine Ping-Anfrage wartet. Wenn er innerhalb der in diesem Feld definierten Zeit keine Antwort erhält, gilt die Ping-Anfrage als fehlgeschlagen betrachtet.
Maximale Anzahl von Ping-Wiederholungen	Die Anzahl der Wiederholungsversuche des Routers beim Senden von Ping-Anfragen, bis feststellt, dass die Verbindung fehlgeschlagen ist.
Neustart-Intervall	Das Ausschaltintervall dieses Ethernet-Ports.
Maximale Neustartzeiten	Die Anzahl der Wiederholungsversuche, die der Router unternimmt, um diesen Port neu zu starten. 0 bedeutet keine Begrenzung.

Tabelle 3-2-1-7 Ping-Erkennungsparameter

3.2.1.4 WAN

Der WAN-Port kann mit einem Ethernet-Kabel verbunden werden, um einen Internetzugang zu erhalten.

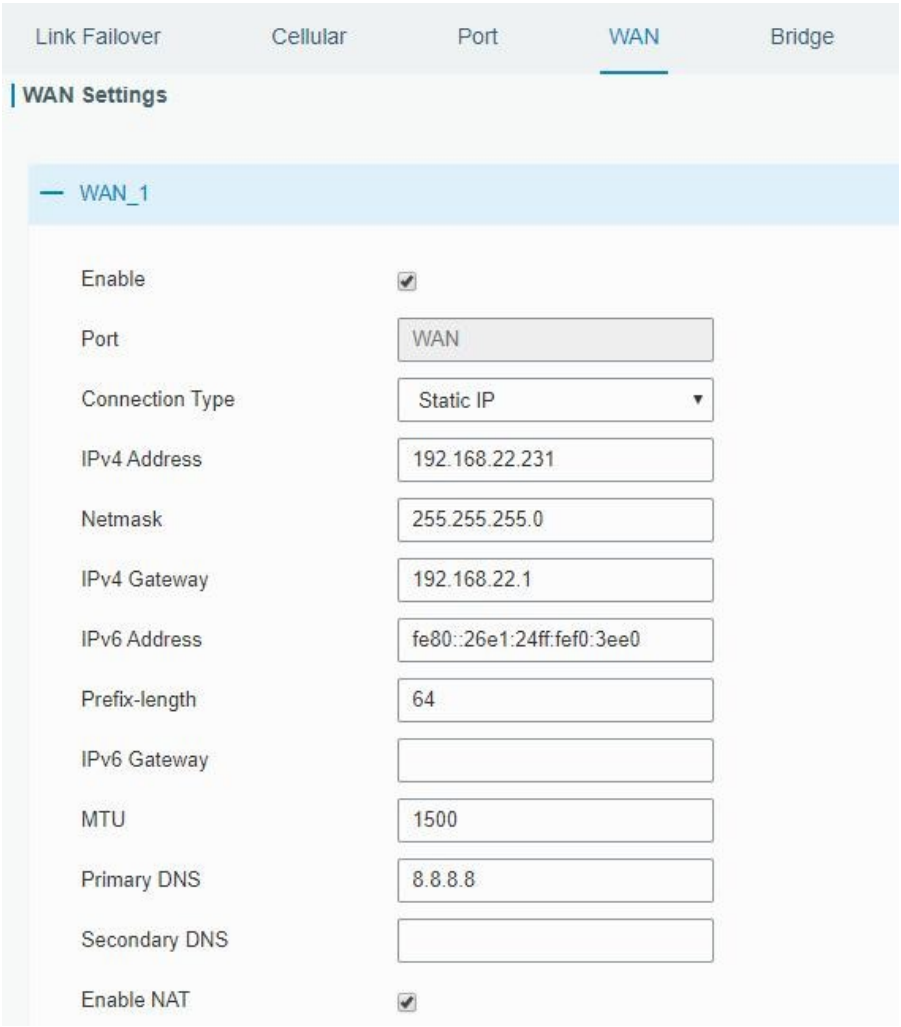


Abbildung 3-2-1-8

WAN-Einstellung		
Element	**Beschreibung**	**Standard**
Aktivieren	WAN-Funktion aktivieren.	Aktivieren
Port	Der Port, der derzeit als WAN-Port festgelegt ist.	WAN
Verbindungstyp	Wählen Sie den gewünschten Verbindungstyp aus. **Statische IP**: Weisen Sie der Ethernet-WAN-Schnittstelle eine statische IP-Adresse, Netzmaske und Gateway zu. **DHCP-Client**: Konfigurieren Sie die Ethernet-WAN-Schnittstelle als DHCP-Client, um automatisch eine IP-Adresse zu erhalten. **PPPoE**: Konfigurieren Sie die Ethernet-WAN-Schnittstelle als PPPoE-Client. **DHCPv6-Client**: Konfigurieren Sie die Ethernet-WAN-Schnittstelle als DHCP-Client, um automatisch eine IPv6-Adresse zu erhalten. **Dual-Stack Lite**: Verwendung von IPv4-in-IPv6-Tunneling zum Senden	IPv4-Paket des statischen IP

	IPv4-Paket des Endgeräts über einen Tunnel im IPv6-Zugangsnetzwerk an den ISP.	
MTU	Legen Sie die maximale Übertragungseinheit fest.	1500
IPv4 Primär DNS	Legen Sie den primären IPv4-DNS-Server fest.	8.8.8.8
Sekundärer IPv4-DNS DNS	Sekundären IPv4-DNS-Server festlegen.	-- --
IPv6 Primär DNS	Legen Sie den primären IPv6-DNS-Server fest.	-- --
Sekundärer IPv6-DNS DNS	Legen Sie den sekundären IPv6-DNS-Server fest.	-- --
NAT aktivieren	Aktivieren oder deaktivieren Sie die NAT-Funktion. Wenn diese Funktion aktiviert ist, kann eine private IP-Adresse in eine öffentliche IP-Adresse übersetzt werden.	Aktivieren

Tabelle 3-2-1-8 WAN-Parameter

1. Statische IP-Konfiguration

Wenn das externe Netzwerk eine feste IP für die WAN-Schnittstelle zuweist, wählen Sie den Modus „Statische IP".

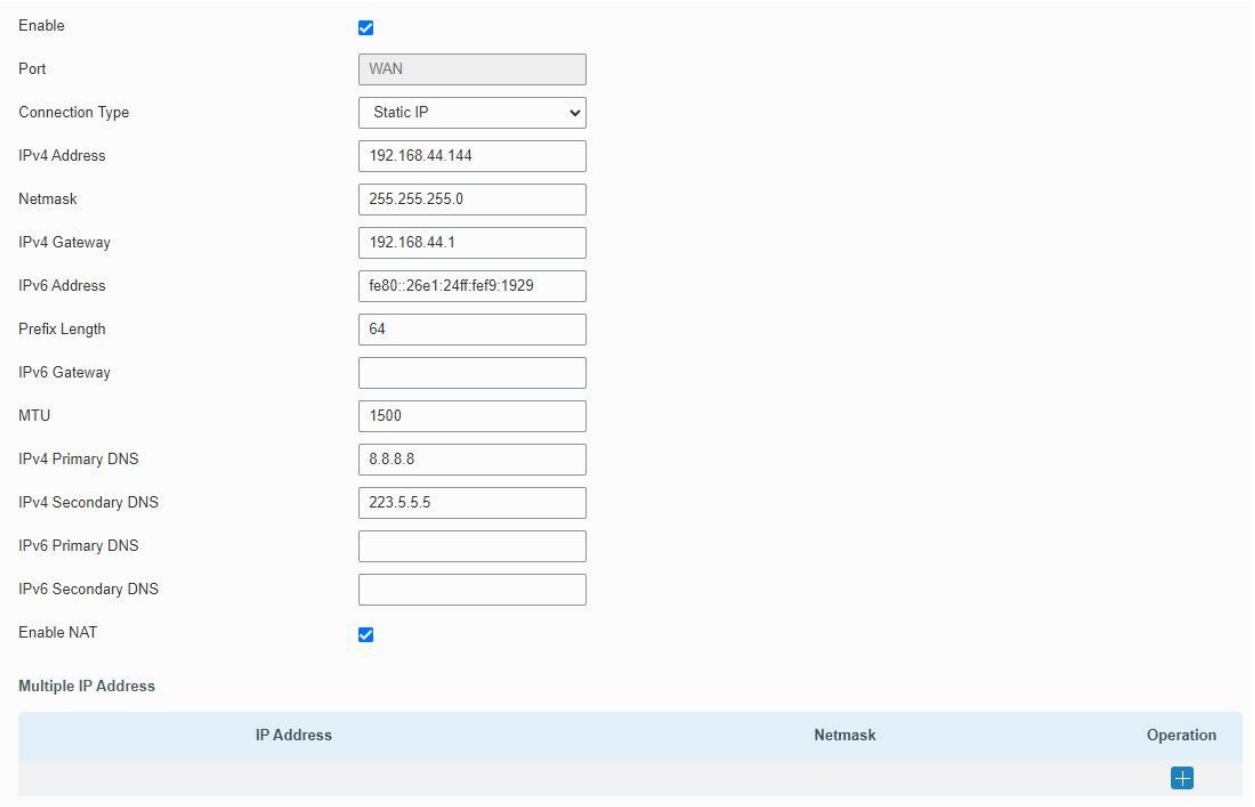


Abbildung 3-2-1-9

Statische IP		
Element	**Beschreibung**	**Standard**
IPv4 Adresse	Legen Sie die IPv4-Adresse des WAN-Ports fest.	192.168.0.1
Netzmaske	Legen Sie die Netzmaske für den WAN-Port fest.	255.255.255.0

IPv4 Gateway	Legen Sie das Gateway für die IPv4-Adresse des WAN-Ports fest.	192.168.0.2
IPv6 Adresse	Legen Sie die IPv6-Adresse fest, die auf das Internet zugreifen kann.	Generiert aus Mac-Adresse
Präfixlänge	Legen Sie die IPv6-Präfixlänge fest, um anzugeben, wie viele Bits einer globalen Unicast-IPv6-Adresse im Netzwerkteil enthalten sind. Beispielsweise wird in 2001:0DB8:0000:000b::/64 die Zahl 64 verwendet , um anzugeben, dass sich die ersten 64 Bits im Netzwerkteil befinden.	64
IPv6 Gateway	Legen Sie das Gateway für die IPv6-Adresse des WAN-Ports fest. Beispiel: 2001:DB8:ACAD:4::2.	--
Mehrere IP-Adressen Adresse	Legen Sie mehrere IP-Adressen für den WAN-Port fest.	Null

Tabelle 3-2-1-9 Statische Parameter

2. DHCP-Client/DHCPv6-Client

Wenn im externen Netzwerk ein DHCP-Server aktiviert ist und der Ethernet-WAN-Schnittstelle IP-Adressen zugewiesen wurden, wählen Sie den DHCP/DHCPv6-Client-Modus, um die IP-Adresse automatisch zu beziehen.

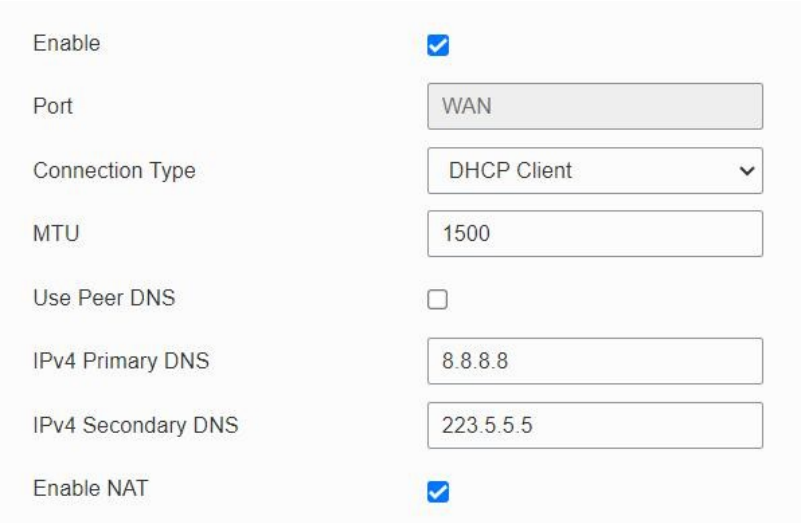


Abbildung 3-2-1-10

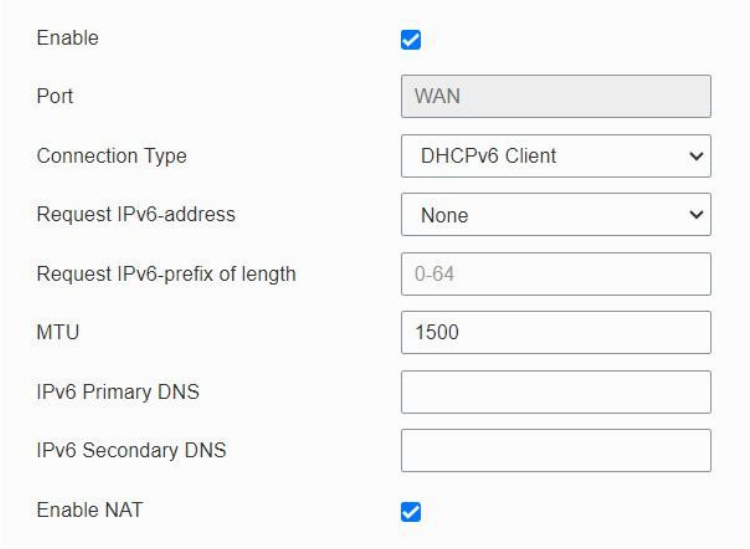


Abbildung 3-2-1-11

DHCP-Client	
Element	**Beschreibung**
Peer-DNS verwenden	Peer-DNS während PPP-Einwahl automatisch beziehen. DNS ist erforderlich, wenn Sie eine Domain aufrufen.
DHCPv6-Client	
IPv6-Adresse anfordern	Wählen Sie die Methode zum Abrufen der IPv6-Adresse vom DHCP-Server aus. Wählen Sie zwischen „Versuchen“, „Erzwingen“ und „Keine“. Versuchen: Der DHCP-Server weist bestimmte Adressen mit Priorität zu. Erzwingen: Der DHCP-Server weist nur bestimmte Adressen zu. Keine: Der DHCP-Server weist die Adresse nach dem Zufallsprinzip zu. Die bestimmte Adresse hängt von der Präfixlänge der von Ihnen festgelegten IPv6-Adresse ab , die Sie festgelegt haben.
Anfordern der Präfixlänge von IPv6	Legen Sie die Präfixlänge der IPv6-Adresse fest, die der Router erwarten soll. vom DHCP-Server abrufen.

Tabelle 3-2-1-10 DHCP-Client-Parameter

3. PPPoE

PPPoE steht für „Point-to-Point Protocol over Ethernet”. Der Benutzer muss einen PPPoE-Client auf der Grundlage der ursprünglichen Verbindungsart installieren. Mit PPPoE können Fernzugriffsgeräte die Kontrolle über jeden Benutzer übernehmen.

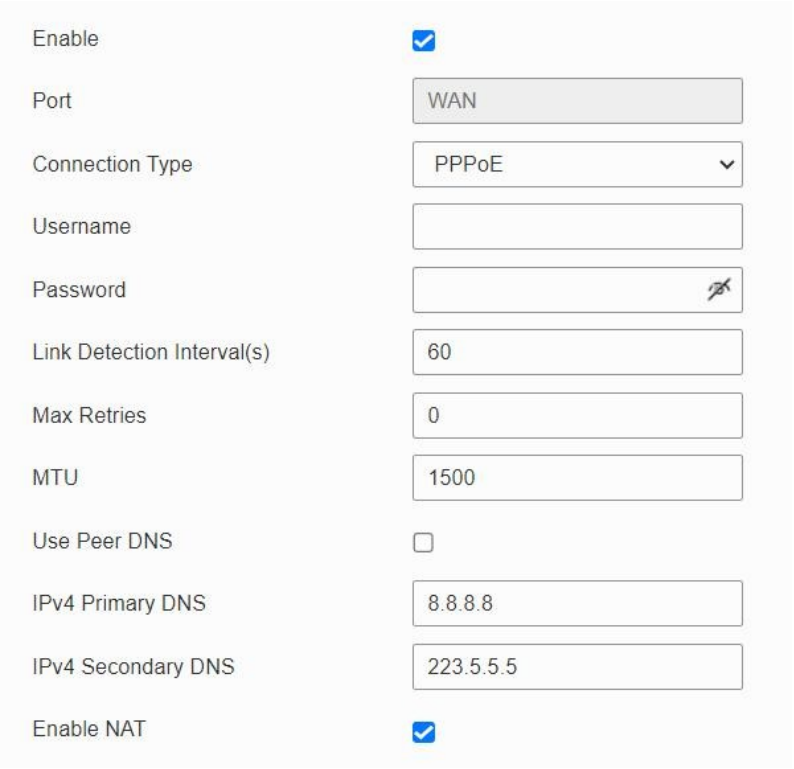


Abbildung 3-2-1-12

PPPoE	
Element	**Beschreibung**
Benutzername	Geben Sie den Benutzernamen ein, den Sie von Ihrem Internetdienstanbieter (ISP) erhalten haben.
Passwort	Geben Sie das Passwort ein, das Sie von Ihrem Internetdienstanbieter (ISP) erhalten haben.
Link-Erkennung Intervall (s)	Legen Sie das Heartbeat-Intervall für die Verbindungserkennung fest. Bereich: 1-600.
Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl der Wiederholungsversuche nach einem fehlgeschlagenen Verbindungsaufbau fest. Bereich: 0-9.
Peer-DNS verwenden	Peer-DNS während des PPP-Wählvorgangs automatisch abrufen. DNS ist erforderlich beim Aufrufen von Domänennamen.

Tabelle 3-2-1-11 PPPoE-Parameter

4. Dual-Stack Lite

Dual-Stack Lite (DS-Lite) verwendet IPv4-in-IPv6-Tunneling, um die IPv4-Pakete eines Teilnehmers über einen Tunnel im IPv6-Zugangsnetzwerk an den ISP zu senden. Das IPv6-Paket wird entkapseln, um das IPv4-Paket des Teilnehmers wiederherzustellen, und dann nach der NAT-Adress- und Portübersetzung und anderen LSN-bezogenen Verarbeitungsvorgängen an das Internet gesendet. Die Antwortpakete durchlaufen denselben Pfad zurück zum Teilnehmer.

Abbildung 3-2-1-13

Dual-Stack Lite	
Element	**Beschreibung**
IPv6-Gateway	Legen Sie das Gateway für die IPv6-Adresse des WAN-Ports fest.
DS-Lite AFTR Adresse	Legen Sie die DS-Lite AFTR-Serveradresse fest.
Lokale IPv6 Adresse	Legen Sie die IPv6-Adresse des WAN-Ports fest, der dasselbe Subnetz wie das IPv6-Gateway verwendet. Gateway verwendet.

Tabelle 3-2-1-12 Dual-Stack Lite-Parameter

Beispiel für die zugehörige Konfiguration

Ethernet-WAN-Verbindung

3.2.1.5 Bridge

Die Brückeneinstellung wird für die Verwaltung von LAN-Geräten verwendet, die an die LAN-Ports des UR35 angeschlossen sind, sodass jedes dieser Geräte auf das Internet zugreifen kann.

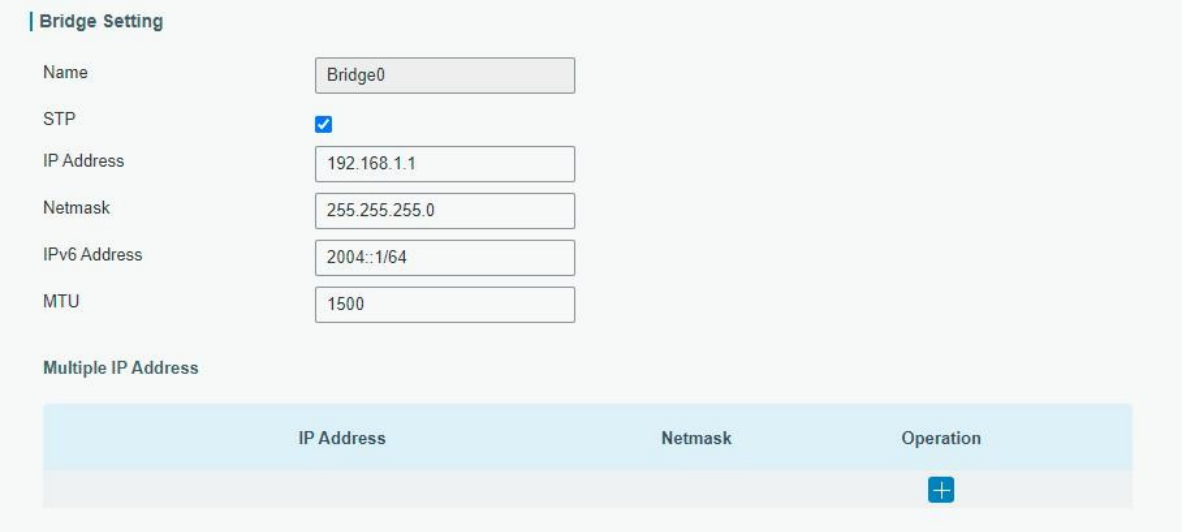


Abbildung 3-2-1-14

Brücke		
Element	**Beschreibung**	**Standard**
Name	Zeigt den Namen der Brücke an. Standardmäßig ist „Bridge0" eingestellt und kann nicht geändert werden.	Bridge0
STP	STP aktivieren/deaktivieren.	Deaktivieren
IP-Adresse	Legen Sie die IP-Adresse für die Bridge fest.	192.168.1.1
Netzmaske	Legen Sie die Netzmaske für die Bridge fest.	255.255.255.0
IPv6-Adresse	Legen Sie die IPv6-Adresse für die Bridge fest.	2004::1/64
MTU	Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500.	1500
Mehrere IP-Adressen	Legen Sie die mehreren IP-Adressen für die Bridge fest.	Null

Tabelle 3-2-1-13 Brückeneinstellungen

3.2.1.6 WLAN

In diesem Abschnitt wird erläutert, wie Sie die entsprechenden Parameter für das WLAN-Netzwerk einstellen. UR35 unterstützt 802.11 b/g/n im AP- oder Client-Modus.

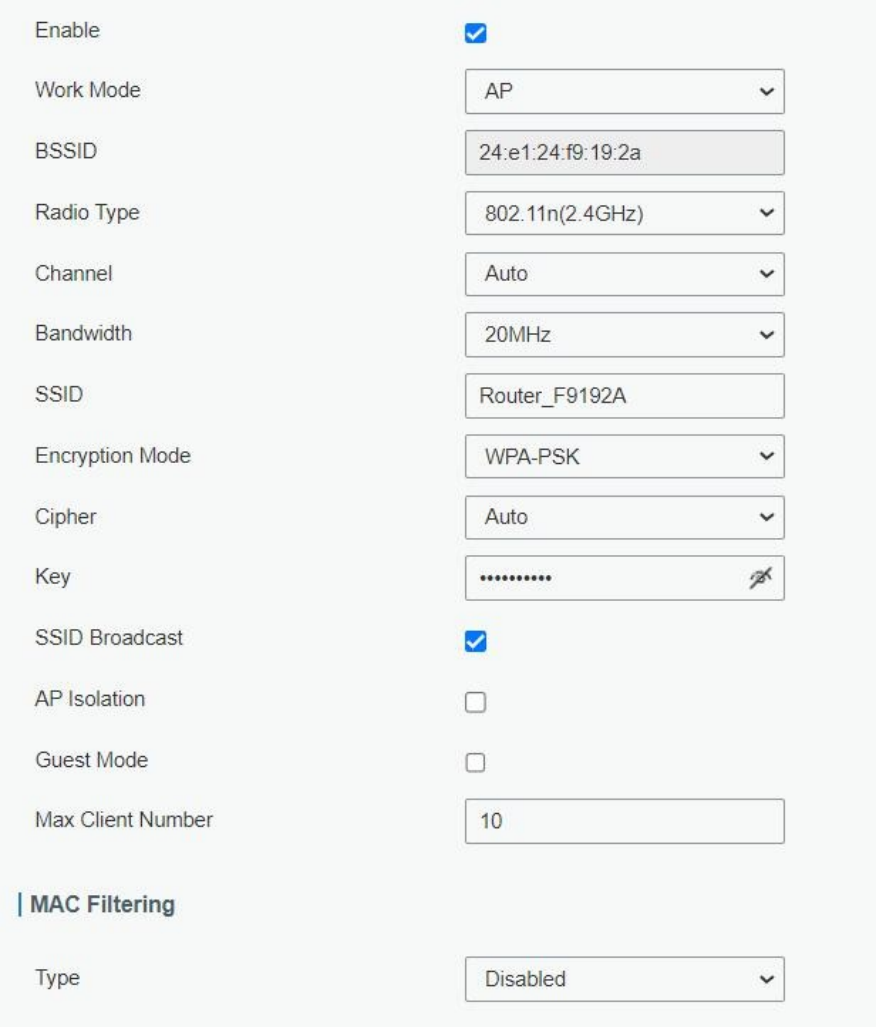


Abbildung 3-2-1-15

WLAN	
Element	**Beschreibung**
Aktivieren	WLAN aktivieren/deaktivieren.
Arbeitsmodus	Wählen Sie den Arbeitsmodus des Routers aus. Die Optionen sind „Client“ oder „AP“.
AP-Modus	
BSSID	Zeigt die MAC-Adresse dieser WLAN-Schnittstelle an.
Funkmodus	Wählen Sie den Funktyp aus. Die Optionen sind „802.11b (2,4 GHz)“, „802.11g (2,4 GHz)“, „802.11n (2,4 GHz)“.
Kanal	Wählen Sie den Funkkanal aus. Die Optionen sind „Auto“, „1“, „2“.....„11“.
Bandbreite	Wählen Sie die Bandbreite aus. Die Optionen sind „20 MHz“ und „40 MHz“.
SSID	Geben Sie die SSID des Zugangspunkts ein.
Verschlüsselungsmodus	Wählen Sie den Verschlüsselungsmodus aus. Die Optionen sind „Keine Verschlüsselung“, „WEP Open System“, „WEP Shared Key“, „WPA-PSK“, „WPA2-PSK“ und „WPA-PSK/WPA2-PSK“.
Verschlüsselung	Wählen Sie die Verschlüsselung für die WPA-Verschlüsselung aus. Die Optionen sind „Auto“, „AES“, „TKIP“ und „AES/TKIP“.
Schlüssel	Geben Sie den Schlüssel ein, um eine Verbindung zu diesem Zugangspunkt herzustellen. Der Standardschlüssel lautet **„iotpassword“**.
SSID	Wenn die SSID-Übertragung deaktiviert ist, können andere drahtlose Geräte die

Broadcast	SSID finden, und Benutzer müssen die SSID manuell eingeben, um auf das drahtlose .
AP-Isolation	Wenn die AP-Isolation aktiviert ist, werden alle Benutzer, die auf den AP zugreifen, voneinander isoliert , ohne miteinander kommunizieren zu können.
Gastmodus	Wenn der Gastmodus aktiviert ist, ist der Zugriff auf das interne Netzwerk nicht möglich.
Max. Clients Anzahl	Legen Sie die maximale Anzahl von Clients fest, auf die zugegriffen werden kann, wenn der Router als AP konfiguriert ist als AP konfiguriert ist.
MAC-Filterung	
Typ	Wählen Sie den Filtertyp für Geräte, die mit dem WLAN-Zugangspunkt dieses Routers verbunden sind. **Deaktivieren:** Allen Benutzern wird die Verbindung zu diesem Zugangspunkt gestattet. **Zulassen und Rest blockieren:** Nur die aufgeführten MAC-Adressen dürfen eine Verbindung zum WLAN-Zugangspunkt des Routers herstellen. **Blockieren und den Rest zulassen:** Die aufgeführten MAC-Adressen dürfen keine Verbindung herstellen. Verbinden Sie sich mit dem WLAN-Zugangspunkt des Routers.
MAC Adresse	Die MAC-Adressen der Geräte, die blockiert oder zugelassen werden sollen.
Beschreibung	Die Beschreibung dieser MAC-Adresse.
Client-Modus	
Scannen	Klicken Sie hier, um die Zugangspunkte in der Umgebung dieses Geräts zu scannen.
SSID	Geben Sie die SSID des Zugangspunkts ein.
BSSID	Geben Sie die MAC-Adresse des Zugangspunkts ein. Entweder die SSID oder die BSSID kann eingegeben werden , um sich mit dem Netzwerk zu verbinden.
Verschlüsselungsmodus	Wählen Sie den Verschlüsselungsmodus aus. Die Optionen sind „Keine Verschlüsselung“, „WEP Open System“, „WEP Shared Key“, „WPA-PSK“, „WPA2-PSK“, „WPA-PSK/WPA2-PSK“, „WPA-Enterprise“, „WPA2-Enterprise“ und „WPA-Enterprise/WPA2-Enterprise“.
Verschlüsselung	Wählen Sie die Verschlüsselung für die WPA-Verschlüsselung aus. Die Optionen sind „Auto“, „AES“, „TKIP“ und „AES/TKIP“.
Schlüssel	Geben Sie den Schlüssel ein, um eine Verbindung zu diesem Zugangspunkt herzustellen.
Xsupplicant Typ	Wählen Sie zwischen „Peap“, „Leap“, „TLS“ und „TTLS“.
Benutzername	Geben Sie den Benutzernamen von WPA/WPA2-Enterprise ein.
Passwort	Geben Sie das Passwort von WPA/WPA2-Enterprise ein.
Anonym Identität	Geben Sie die anonyme Identität von WPA/WPA2-Enterprise ein.
Phase 1/2	Füllen Sie die Phase von WPA/WPA2-Enterprise aus.
CA Zertifikat	Das öffentliche Serverzertifikat, das zur Überprüfung mit WPA/WPA2-Enterprise verwendet wird. Zugangspunkt.
Öffentlicher Schlüssel	Wenn der Xsupplicant-Typ „TLS” ist, importieren Sie den öffentlichen Schlüssel, der für die Überprüfung mit dem WPA/WPA2-Enterprise-Zugangspunkt verwendet wird.
Privater Schlüssel	Wenn der Xsupplicant-Typ „TLS“ ist, importieren Sie den privaten Schlüssel, der für die Überprüfung mit WPA/WPA2-Enterprise-Zugangspunkt verwendet wird.

Privater Schlüssel Entschlüsselung	Legen Sie das Entschlüsselungspasswort für den privaten Schlüssel fest.
IP-Einstellung	
Protokoll	Legen Sie das Protokoll fest, um die WLAN-IP-Adresse zu erhalten.
IP-Adresse	Legen Sie die IP-Adresse im drahtlosen Netzwerk fest, wenn das Protokoll „Statische IP“ lautet.
Netzmaske	Legen Sie die Netzmaske im drahtlosen Netzwerk fest, wenn das Protokoll „Statische IP“ lautet.
Gateway	Stellen Sie das Gateway im drahtlosen Netzwerk ein, wenn das Protokoll „Statische IP“ lautet.

Tabelle 3-2-1-14 WLAN-Parameter

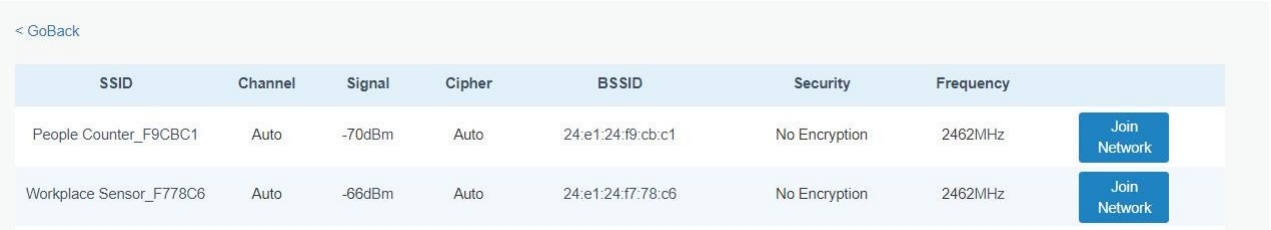


Abbildung 3-2-1-16

WLAN-Scan	
Element	**Beschreibung**
SSID	SSID anzeigen.
Kanal	Drahtlosen Kanal anzeigen.
Signal	Drahtloses Signal anzeigen.
BSSID	Zeigt die MAC-Adresse des Zugangspunkts an.
Verschlüsselung	Zeigt die Verschlüsselung des Zugangspunkts an.
Sicherheit	Zeige den Verschlüsselungsmodus an.
Frequenz	Zeigt die Frequenz des Radios an.
Mit Netzwerk verbinden	Klicken Sie auf die Schaltfläche, um sich mit dem drahtlosen Netzwerk zu verbinden.

Tabelle 3-2-1-15 WLAN-Scan-Parameter

Verwandtes Thema

Beispiel für eine Wi-Fi-Anwendung

3.2.1.7 Switch

VLAN ist eine neue Technologie zum Datenaustausch, die virtuelle Arbeitsgruppen realisiert, indem sie das LAN-Gerät logisch in Netzwerksegmente unterteilt.

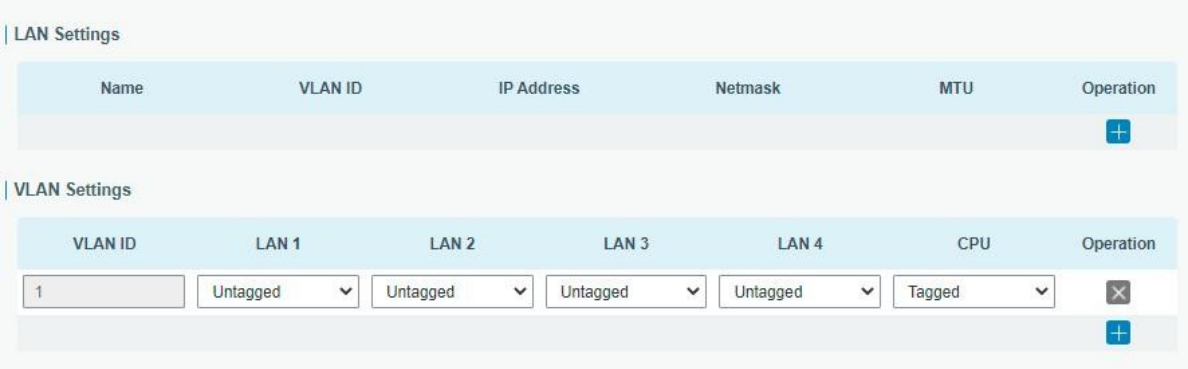


Abbildung 3-2-1-17

Switch	
Element	**Beschreibung**
LAN-Einstellungen	
Name	Legen Sie den Schnittstellennamen des VLAN fest.
VLAN-ID	Wählen Sie die VLAN-ID der Schnittstelle aus.
IP-Adresse	IP-Adresse des LAN-Ports festlegen.
Netzmaske	Netzmaske des LAN-Ports festlegen.
MTU	Legen Sie die maximale Übertragungseinheit des LAN-Ports fest. Bereich: 68-1500.
VLAN-Einstellungen	
VLAN-ID	Legen Sie die Label-ID des VLAN fest. Bereich: 1-4094.
LAN 1/2/3/4	Verbinden Sie das VLAN mit den entsprechenden Ports und wählen Sie den Status aus „Getaggt", „Nicht getaggt" und „Schließen" für Ethernet-Frames auf der Trunk-Verbindung.
CPU	Steuerung der Kommunikation zwischen VLAN und anderen Netzwerken.

Tabelle 3-2-1-16 VLAN-Trunk-Parameter

3.2.1.8 Loopback

Die Loopback-Schnittstelle wird zum Ersetzen der Router-ID verwendet, solange sie aktiviert ist. Wenn die Schnittstelle DOWN istmuss die ID des Routers erneut ausgewählt werden, was zu einer langen Konvergenzzeit von OSPF führt. Daher wird die Loopback-Schnittstelle im Allgemeinen als ID des Routers empfohlen.
Die Loopback-Schnittstelle ist eine logische und virtuelle Schnittstelle auf dem Router. Unter Standardbedingungen gibt es keine Loopback-Schnittstelle auf dem Router, sie kann jedoch bei Bedarf erstellt werden.

Abbildung 3-2-1-18

Loopback		
Element	**Beschreibung**	**Standard**
IP-Adresse	Unveränderlich	127.0.0.1
Netzmaske	Unveränderlich	255.0.0.0
Mehrere IP-Adressen Adressen	Neben der oben genannten IP-Adresse kann der Benutzer weitere IP-Adressen konfigurieren.	Null

Tabelle 3-2-1-17 Loopback-Parameter

3.2.2 DHCP

DHCP verwendet den Client/Server-Kommunikationsmodus. Der Client sendet eine Konfigurationsanfrage an den Server, der die entsprechenden Konfigurationsinformationen zurücksendet und dem Client eine IP-Adresse zuweist, um die dynamische Konfiguration der IP-Adresse und anderer Informationen zu erreichen.

3.2.2.1 DHCP-Server/DHCPv6-Server

Der UR35 kann als DHCP-Server oder DHCPv6-Server eingerichtet werden, um IP-Adressen zu verteilen, wenn sich ein Host anmeldet, und um sicherzustellen, dass jeder Host eine andere IP-Adresse erhält. Der DHCP-Server hat einige bisherige Netzwerkverwaltungsaufgaben, die manuelle Eingriffe erforderten, weitgehend vereinfacht. Der UR35 unterstützt nur Stateful DHCPv6, wenn er als DHCPv6-Server arbeitet.

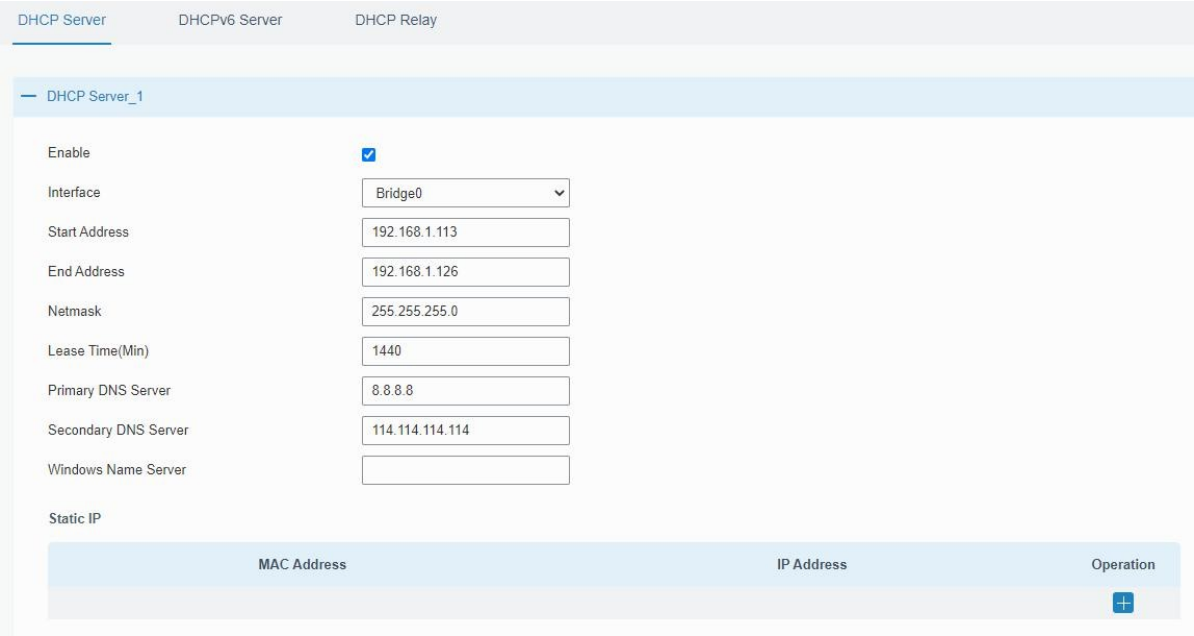


Abbildung 3-2-2-1

Abbildung 3-2-2-2

DHCP/DHCPv6-Server		
Element	**Beschreibung**	**Standard**
Aktivieren	DHCP-Server aktivieren oder deaktivieren.	Aktiv
Schnittstelle	Schnittstelle auswählen.	Bridge0
Startadresse	Definieren Sie den Anfang des Pools von IP-Adressen, die an DHCP-Clients vermietet werden.	192.168.1.0 0
Endadresse	Legen Sie das Ende des Pools von IP-Adressen fest, die an DHCP-Clients vermietet werden.	192.168.1.9 9
Netzmaske	Definieren Sie die Subnetzmaske der IPv4-Adresse, die von DHCP-Clients vom DHCP-Server erhalten haben.	255.255.255 .0
Präfixlänge	Legen Sie die IPv6-Präfixlänge der IPv6-Adresse fest, die von DHCP -Clients vom DHCP-Server erhalten haben.	64
Lease-Zeit (Min)	Legen Sie die Lease-Zeit fest, während der der Client die vom DHCP-Server erhaltene IP-Adresse verwenden kann vom DHCP-Server erhaltene Adresse nutzen kann. Bereich: 1-10080.	1440
Primärer DNS-Server	Legen Sie den primären DNS-Server fest.	192.168.1.1
Sekundärer DNS Server	Sekundärer DNS-Server einstellen.	Null
Windows-Namensserver	Definieren Sie den Windows-Internetnamensdienst, den DHCP-Clients vom DHCP-Server erhalten. Im Allgemeinen können Sie dieses Feld leer lassen.	Null
Statische IP		
MAC-Adresse	Legen Sie eine statische und spezifische MAC-Adresse für den DHCP-Client fest (sie sollte sich von anderen MAC-Adressen unterscheiden, um Konflikte zu vermeiden Konflikte zu vermeiden).	Null
DUID	Legen Sie eine statische und spezifische DUID für den DHCPv6-Client fest (sie sollte sich von anderen DUID unterscheiden, um Konflikte zu vermeiden).	Null
IP-Adresse	Legen Sie eine statische und spezifische IP-Adresse für den DHCP-Client fest (sie	Null

	außerhalb des DHCP-Bereichs liegen).	

Tabelle 3-2-2-1 DHCP-Server-Parameter

3.2.2.2 DHCP-Relay

UR35 kann als DHCP-Relay konfiguriert werden, um einen Relay-Tunnel bereitzustellen und so das Problem zu lösen, dass sich DHCP-Client und DHCP-Server nicht im selben Subnetz befinden.

Abbildung 3-2-2-3

DHCP-Relay	
Element	**Beschreibung**
Aktivieren	DHCP-Relay aktivieren oder deaktivieren.
DHCP-Server	DHCP-Server einstellen, es können bis zu 10 Server konfiguriert werden; trennen Sie diese durch Leerzeichen oder „,“.

Tabelle 3-2-2-2 DHCP-Relay-Parameter

3.2.3 Firewall

In diesem Abschnitt wird beschrieben, wie Sie die Firewall-Parameter einstellen, darunter Sicherheit, ACL, DMZ,Portzuordnung,MAC-Bindung und SPI.

Die Firewall implementiert eine entsprechende Kontrolle des Datenflusses in Eingangsrichtung (vom Internet zum lokalen Netzwerk) und Ausgangsrichtung (vom lokalen Netzwerk zum Internet) entsprechend den Inhaltsmerkmalen der Pakete, wie z. B. Protokollstil, Quell-/Ziel-IP-Adresse usw. Sie stellt sicher, dass der Router in einer sicheren Umgebung und der Host im lokalen Netzwerk betrieben werden.

3.2.3.1 Sicherheit

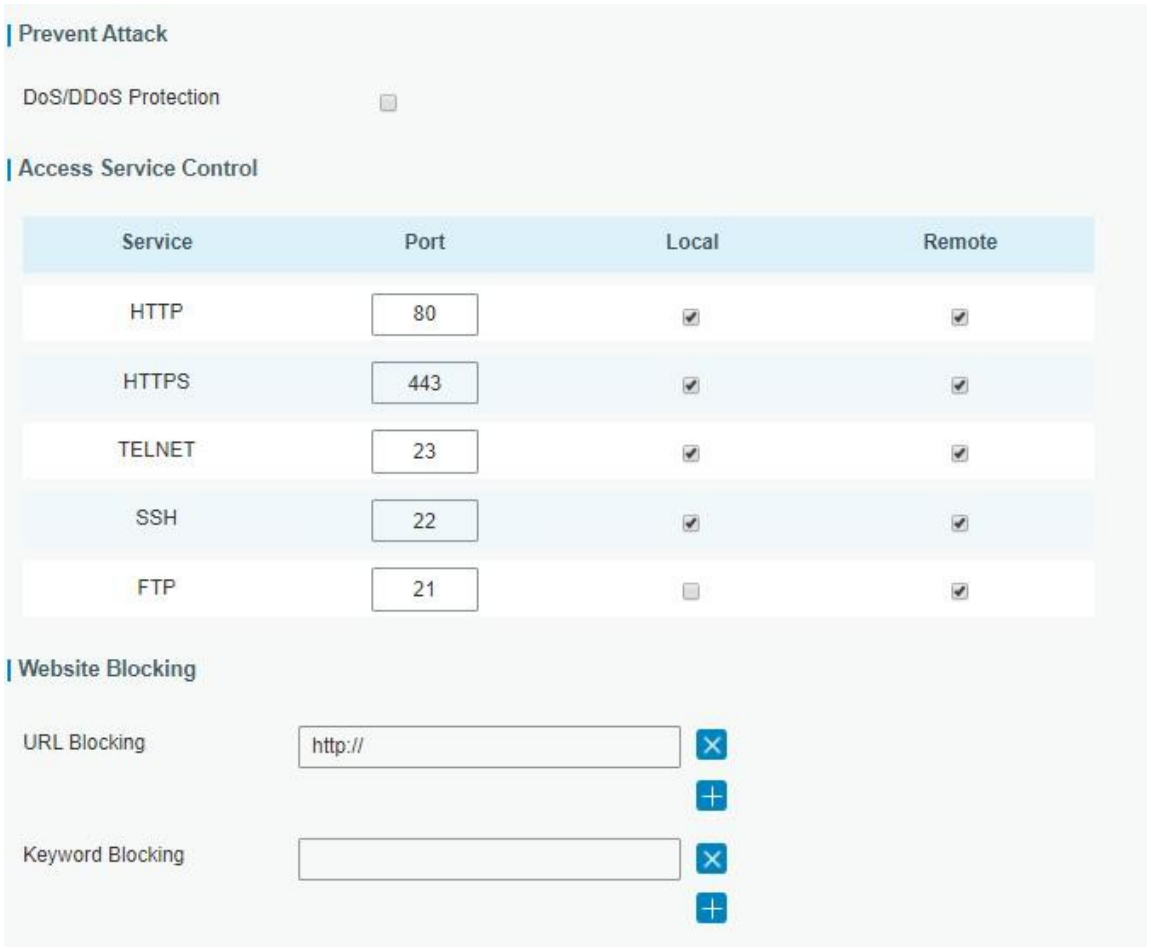


Abbildung 3-2-3-1

Element	Beschreibung	Standard
Angriffe verhindern		
DoS/DDoS-Schutz	Aktivieren/deaktivieren Sie den Schutz vor DoS-/DDoS-Angriffen.	Deaktivieren
Zugriff auf Dienststeuerung		
Port	Legen Sie die Portnummer der Dienste fest. Bereich: 1-65535.	--
Lokal	Greifen Sie lokal auf den Router zu.	Aktivieren
Remote	Greifen Sie remote auf den Router zu.	Deaktivieren
HTTP	Benutzer können sich lokal über HTTP beim Gerät anmelden, um über das Web darauf zuzugreifen und es zu steuern, nachdem die Option aktiviert ist.	80
HTTPS	Benutzer können sich lokal und remote über HTTPS beim Gerät anmelden, um über das Web darauf zuzugreifen und es zu steuern, nachdem die Option aktiviert wurde.	443
TELNET	Benutzer können sich lokal und remote über Telnet beim Gerät anmelden über Telnet, nachdem die Option aktiviert wurde.	23
SSH	Benutzer können sich lokal und remote über SSH, nachdem die Option aktiviert wurde.	22
FTP	Benutzer können sich lokal und remote beim Gerät anmelden über FTP anmelden.	21

Website-Blockierung	
URL-Sperrung	Geben Sie die HTTP-Adresse ein, die Sie blockieren möchten.
Keyword-Blockierung	Sie können bestimmte Websites durch Eingabe eines Stichworts sperren. Die maximal zulässige Zeichenanzahl beträgt 64.

Tabelle 3-2-3-1 Sicherheitsparameter

3.2.3.2 ACL

Die Zugriffskontrollliste, auch ACL genannt, implementiert die Erlaubnis oder Verweigerung des Zugriffs für bestimmten Netzwerkverkehr (z. B. die Quell-IP-Adresse), indem sie eine Reihe von Übereinstimmungsregeln konfiguriert, um den Netzwerk-Schnittstellenverkehr zu filtern. Wenn der Router ein Paket empfängt, wird das Feld gemäß der für die aktuelle Schnittstelle geltenden ACL-Regel analysiert. Nachdem das spezielle Paket identifiziert wurde, wird die Erlaubnis oder Verweigerung des entsprechenden Pakets gemäß der voreingestellten Strategie implementiert.

Die von der ACL definierten Datenpaket-Übereinstimmungsregeln können auch von anderen Funktionen verwendet werden, die eine Unterscheidung des Datenflusses erfordern.

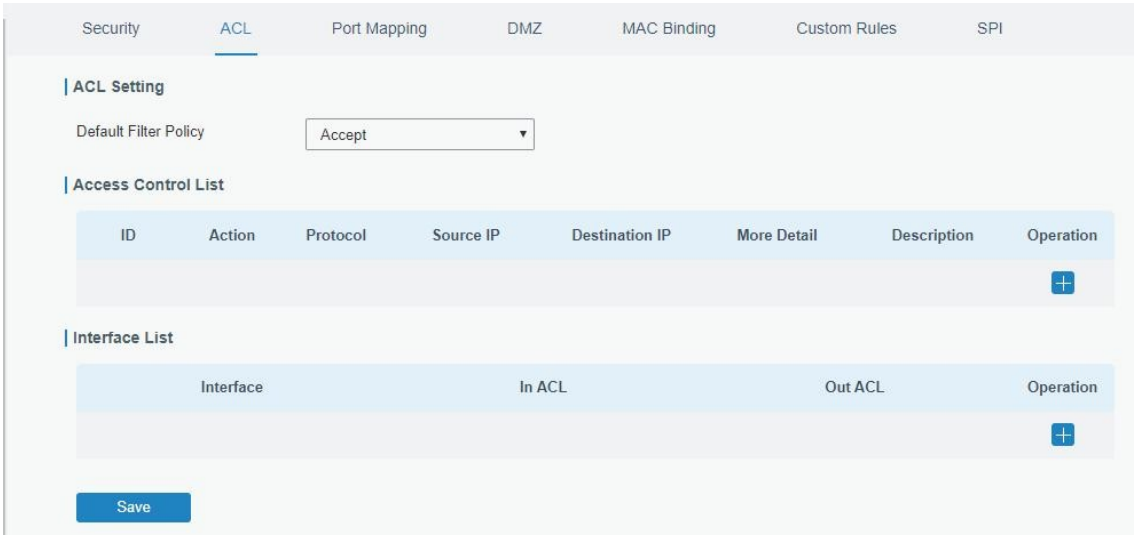


Abbildung 3-2-3-2

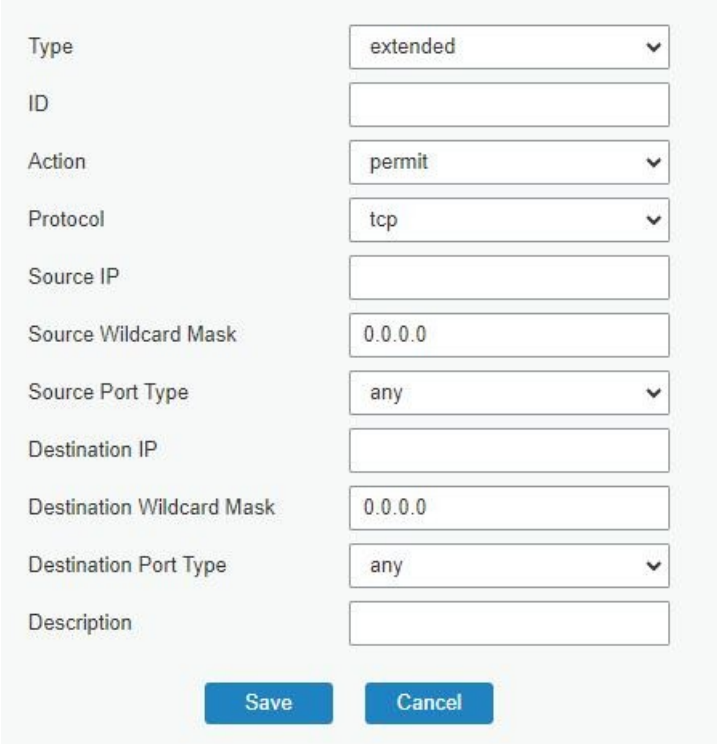


Abbildung 3-2-3-3

Element	Beschreibung
ACL-Einstellung	
Standardfilterrichtlinie	Wählen Sie zwischen „Akzeptieren“ und „Ablehnen“. Die Pakete, die nicht in der Zugriffskontrollliste enthalten sind, werden gemäß der Standardfilterrichtlinie verarbeitet.
Zugriffskontrollliste	
Typ	Wählen Sie den Typ aus „Erweitert“ und „Standard“.
ID	Benutzerdefinierte ACL-Nummer. Bereich: 1-199.
Aktion	Wählen Sie zwischen „Zulassen“ und „Verweigern“.
Protokoll	Wählen Sie das Protokoll aus „ip“, „icmp“, „tcp“, „udp“ und „1-255“ aus.
Quell-IP	Quellnetzwerkadresse (wenn Sie das Feld leer lassen, bedeutet dies „alle“).
Quell-Wildcard-Maske	Wildcard-Maske der Quellnetzwerkadresse.
Ziel-IP	Zielnetzwerkadresse (0.0.0.0 bedeutet alle).
Ziel-Wildcard Maske	Wildcard-Maske der Zieladresse.
Beschreibung	Geben Sie eine Beschreibung für die Gruppen mit derselben ID ein.
ICMP-Typ	Geben Sie den Typ des ICMP-Pakets ein. Bereich: 0-255.
ICMP-Code	Geben Sie den Code des ICMP-Pakets ein. Bereich: 0-255.
Quellporttyp	Wählen Sie den Quellporttyp aus, z. B. angegebener Port, Portbereich usw.
Quellport	Quellportnummer festlegen. Bereich: 1-65535.
Start-Quellport	Startnummer des Quellports festlegen. Bereich: 1-65535.
End-Quellport	Ende der Quellportnummer festlegen. Bereich: 1-65535.
Zielporttyp	Wählen Sie den Zielporttyp aus, z. B. einen bestimmten Port, einen Portbereich, usw.

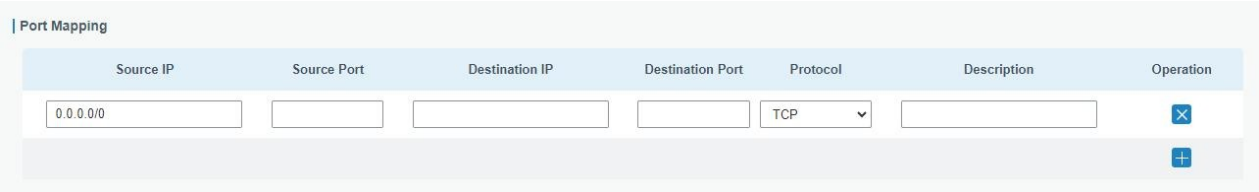
Zielport	Legen Sie die Zielportnummer fest. Bereich: 1-65535.
Startzielport	Legen Sie die Startnummer des Zielports fest. Bereich: 1-65535.
Endzielport	Legen Sie die Endzielportnummer fest. Bereich: 1-65535.
Weitere Details	Informationen zum Port anzeigen.
Schnittstellenliste	
Schnittstelle	Wählen Sie die Netzwerkschnittstelle für die Zugriffskontrolle aus.
In ACL	Wählen Sie eine Regel für eingehenden Datenverkehr aus der ACL-ID aus.
Ausgehende ACL	Wählen Sie eine Regel für ausgehenden Datenverkehr aus der ACL-ID aus.

Tabelle 3-2-3-2 ACL-Parameter

3.2.3.3 Portzuordnung (DNAT)

Wenn externe Dienste intern benötigt werden (z. B. wenn eine Website extern veröffentlicht wird), initiiert die externe Adresse eine aktive Verbindung. Der Router oder das Gateway auf der Firewall empfängt die Verbindung. Anschließend wandelt er die Verbindung in eine interne Verbindung um. Diese Umwandlung wird als DNAT bezeichnet und wird hauptsächlich für externe und interne Dienste verwendet.

Abbildung 3-2-3-3



Port-Zuordnung	
Element	**Beschreibung**
Quell-IP	Geben Sie den Host oder das Netzwerk an, der/das auf die lokale IP-Adresse zugreifen kann. 0.0.0.0/0 bedeutet alle.
Quellport	Geben Sie den TCP- oder UDP-Port ein, von dem aus eingehende Pakete weitergeleitet werden. Bereich: 1-65535.
Ziel-IP	Geben Sie die IP-Adresse ein, an die Pakete weitergeleitet werden, nachdem sie auf der eingehenden Schnittstelle empfangen wurden.
Zielport	Geben Sie den TCP- oder UDP-Port ein, an den Pakete weitergeleitet werden, nachdem Empfang an den eingehenden Ports weitergeleitet werden. Bereich: 1-65535.
Protokoll	Wählen Sie je nach Anforderung Ihrer Anwendung zwischen „TCP" und „UDP".
Beschreibung	Die Beschreibung dieser Regel.

Tabelle 3-2-3-3 Parameter für die Portzuordnung

Beispiel für eine zugehörige Konfiguration

Beispiel für eine NAT-Anwendung

3.2.3.4 DMZ

DMZ ist ein Host innerhalb des internen Netzwerks, bei dem alle Ports offen sind, mit Ausnahme der in der Portzuordnung weitergeleiteten Ports.

Abbildung 3-2-3-4

DMZ	
Element	**Beschreibung**
Aktivieren	DMZ aktivieren oder deaktivieren.
DMZ-Host	Geben Sie die IP-Adresse des DMZ-Hosts im internen Netzwerk ein.
Quelladresse	Legen Sie die Quell-IP-Adresse fest, die auf den DMZ-Host zugreifen kann. „0.0.0.0/0“ bedeutet jede Adresse.

Tabelle 3-2-3-4 DMZ-Parameter

3.2.3.5 MAC-Bindung

Die MAC-Bindung wird verwendet, um Hosts durch Abgleich von MAC-Adressen und IP-Adressen zu spezifizieren, die in der Liste der zulässigen externen Netzwerkzugriffe aufgeführt sind.

Abbildung 3-2-3-5

MAC-Bindungsliste	
Element	**Beschreibung**
MAC-Adresse	Legen Sie die zugeordnete MAC-Adresse fest.
IP-Adresse	Legen Sie die zugeordnete IP-Adresse fest.
Beschreibung	Geben Sie eine Beschreibung ein, um die Bedeutung der Bindungsregel für jedes MAC-IP-Paar zu dokumentieren.

Tabelle 3-2-3-5 MAC-Bindungsparameter

3.2.3.6 Benutzerdefinierte Regeln

Auf dieser Seite können Sie Ihre eigenen benutzerdefinierten Firewall-iptables-Regeln konfigurieren.

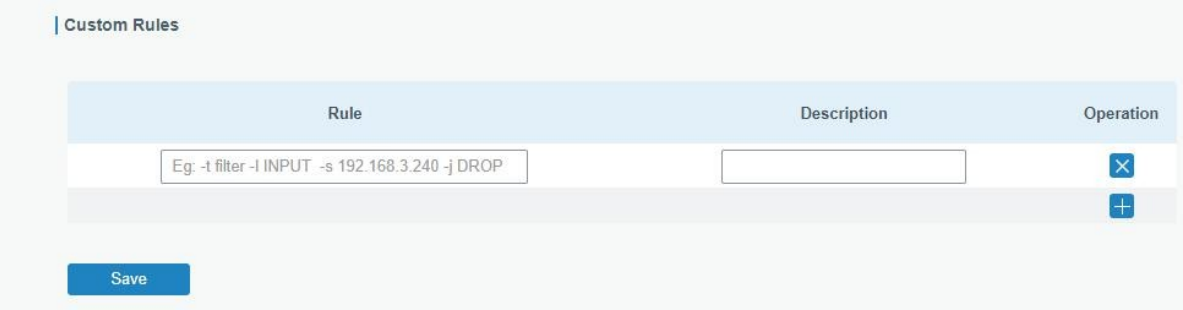


Abbildung 3-2-3-6

Benutzerdefinierte Regeln	
Element	**Beschreibung**
Regel	Geben Sie eine iptables-Regel wie im Beispiel angegeben an. Tipps: Nach dem Ändern oder Löschen der iptables-Regeln müssen Sie das Gerät neu starten, damit die Änderungen wirksam werden.
Beschreibung	Geben Sie die Beschreibung der Regel ein.

Tabelle 3-2-3-6 Parameter für benutzerdefinierte Regeln

3.2.3.7 SPI

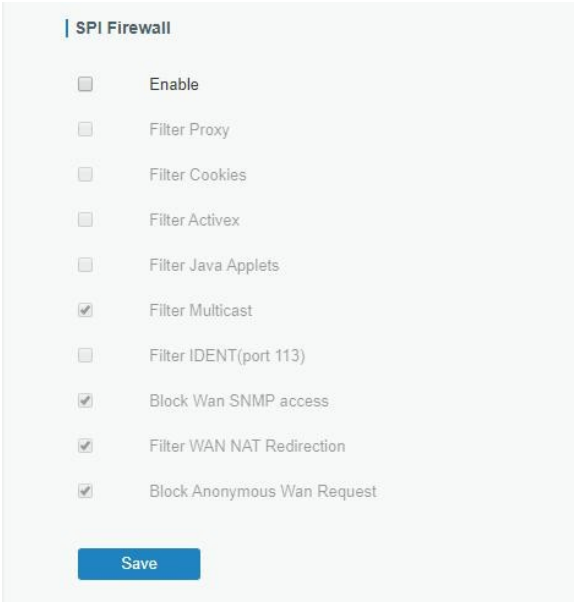


Abbildung 3-2-3-7

SPI-Firewall	
Element	**Beschreibung**
Aktivieren	SPI-Firewall aktivieren/deaktivieren.
Filter-Proxy	Blockiert HTTP-Anfragen, die die Zeichenfolge „Host:“ enthalten.
Cookies filtern	Identifiziert HTTP-Anfragen, die „Cookie” enthalten: String und manipuliert versucht, die Verwendung von Cookies zu verhindern.
ActiveX-Filter	Blockiert HTTP-Anfragen der URL, die auf „.ocx” oder „.cab” endet.
Java-Applets filtern	Blockiert HTTP-Anfragen der URL, die auf „.js“ oder „.class“ endet.
Multicast-Filter	Verhindert, dass Multicast-Pakete das LAN erreichen.

IDENT-Filter (Port 113)	Verhindert den WAN-Zugriff auf Port 113.
Blockiert den WAN-SNMP-Zugriff	Blockieren Sie SNMP-Anfragen aus dem WAN.
Filtern Sie die WAN-NAT-Umleitung.	Verhindern Sie, dass Hosts im LAN die WAN-Adresse des Routers verwenden, um eine Verbindung zu Servern im LAN herzustellen (die mit Portweiterleitung konfiguriert wurden).
Anonyme WAN-Anfragen blockieren Anfragen	Verhindern Sie, dass der Router auf „Pings" aus dem WAN reagiert.

Tabelle 3-2-3-7 SPI-Parameter

3.2.4 QoS

Die Dienstgüte (Quality of Service, QoS) bezieht sich eher auf Mechanismen zur Priorisierung des Datenverkehrs und zur Reservierung von Ressourcen als auf die tatsächlich erreichte Dienstqualität. QoS wurde entwickelt, um unterschiedlichen Anwendungen, Benutzern und Datenflüssen unterschiedliche Prioritäten zuzuweisen oder um ein bestimmtes Leistungsniveau für einen Datenfluss zu gewährleisten.

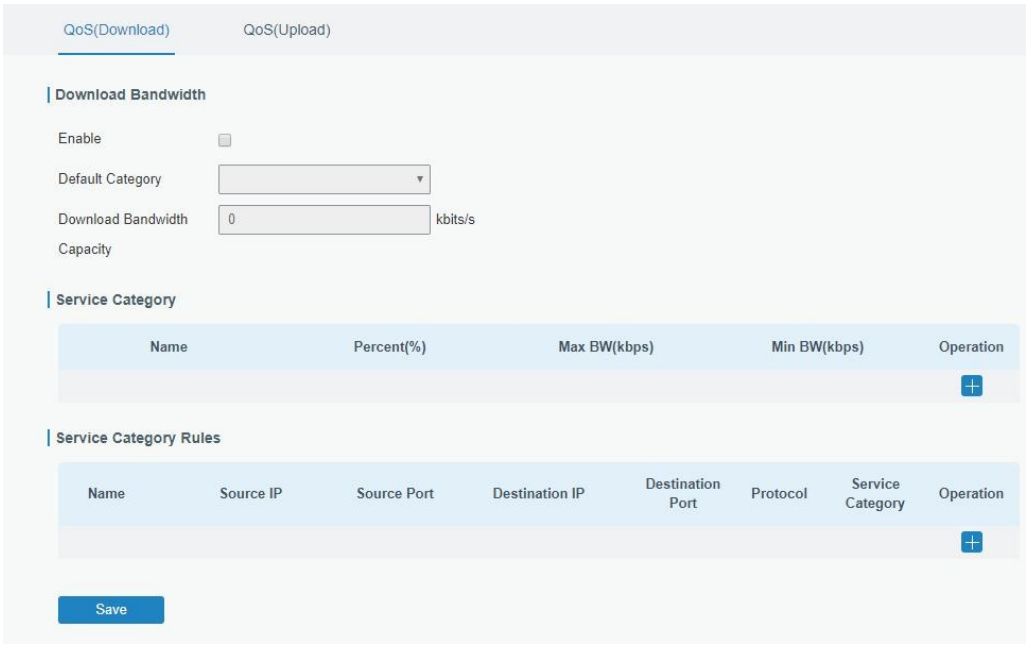


Abbildung 3-2-4-1

QoS	
Element	**Beschreibung**
Download/Upload	
Aktivieren	QoS aktivieren oder deaktivieren.
Standardkategorie	Wählen Sie die Standardkategorie aus der Liste „Dienstkategorie" aus.
Download/Upload Bandbreitenkapazität	Die Download-/Upload-Bandbreitenkapazität des Netzwerks, mit dem der Router verbunden ist, in kbps. Bereich: 1-8000000.
Dienstkategorie	
Name	Sie können Zeichen wie Ziffern, Buchstaben und „-" verwenden.
Prozent (%)	Legen Sie den Prozentsatz für die Dienstkategorie fest. Bereich: 0-100.
Max. Bandbreite (kbps)	Die maximale Bandbreite, die diese Kategorie in kbps. Der Wert sollte kleiner sein als die „Download-/Upload-Bandbreitenkapazität", wenn der Datenverkehr

	gesperrt ist.
Min. BW (kbps)	Die für die Kategorie garantierte Mindestbandbreite in kbps. Der Wert sollte kleiner sein als der Wert „MAX BW“.
Regeln für Dienstkategorien	
Element	**Beschreibung**
Name	Geben Sie der Regel einen aussagekräftigen Namen.
Quell-IP	Quelladresse der Flusskontrolle (wenn Sie das Feld leer lassen, bedeutet dies „beliebig“).
Quellport	Quellport der Flusskontrolle. Bereich: 0-65535 (wenn Sie das Feld leer lassen bedeutet „beliebig“).
Ziel-IP	Zieladresse der Flusskontrolle (leeres Feld bedeutet „beliebig“).
Zielport	Zielport der Flusskontrolle. Bereich: 0-65535 (leer lassen bedeutet „beliebig“).
Protokoll	Wählen Sie das Protokoll aus „ANY“, „TCP“, „UDP“, „ICMP“ und „GRE“ aus.
Dienstkategorie	Legen Sie die Dienstkategorie für die Regel fest.

Tabelle 3-2-4-1 QoS-Parameter (Download/Upload)

Beispiel für eine zugehörige Konfiguration

QoS-Anwendungsbeispiel

3.2.5 VPN

Virtuelle private Netzwerke, auch VPNs genannt, werden verwendet, um zwei private Netzwerke sicher miteinander zu verbinden, sodass Geräte über sichere Kanäle von einem Netzwerk zum anderen Netzwerk verbunden werden können.
Der UR35 unterstützt DMVPN IPsec, GRE, L2TP, PPTP, OpenVPN sowie GRE über IPsec und L2TP über IPsec.

3.2.5.1 DMVPN

Ein dynamisches Multi-Point Virtual Private Network (DMVPN), das mGRE und IPsec kombiniert, ist ein sicheres Netzwerk, das Daten zwischen Standorten austauscht, ohne den Datenverkehr über den VPN-Server oder Router der Unternehmenszentrale zu leiten.

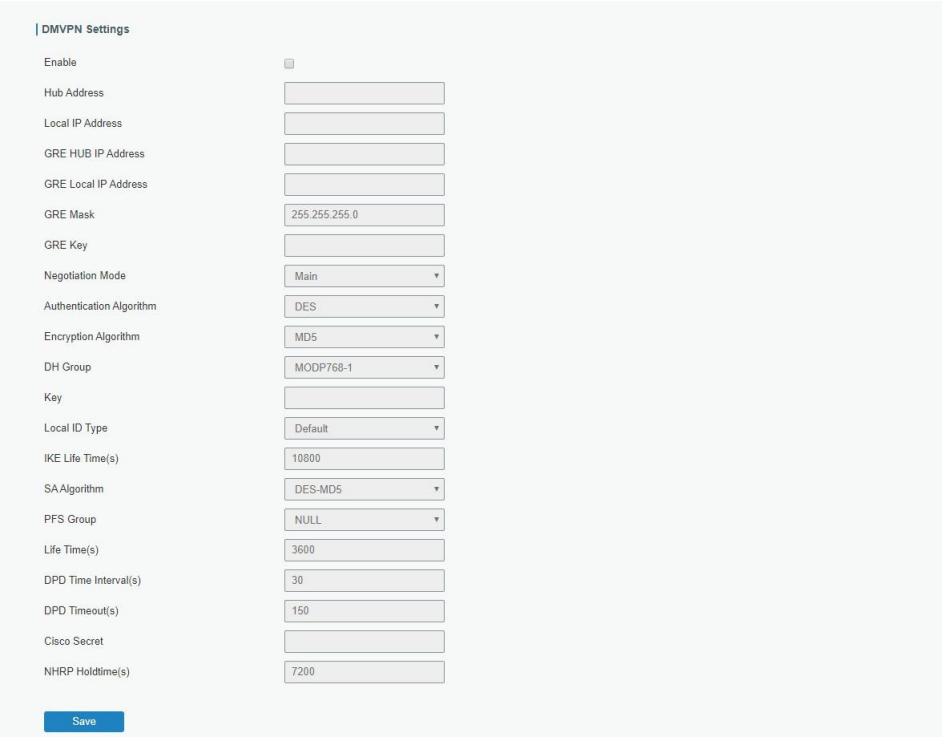


Abbildung 3-2-5-1

DMVPN	
Element	**Beschreibung**
Aktivieren	DMVPN aktivieren oder deaktivieren.
Hub-Adresse	Die IP-Adresse oder der Domänenname des DMVPN-Hubs.
Lokale IP-Adresse	Lokale Tunnel-IP-Adresse von DMVPN.
GRE-Hub-IP-Adresse	IP-Adresse des GRE-Hub-Tunnels.
Lokale GRE-IP-Adresse	Lokale GRE-Tunnel-IP-Adresse.
GRE-Netzmaske	Lokale GRE-Tunnel-Netzmaske.
GRE-Schlüssel	GRE-Tunnels-Schlüssel.
Verhandlungsmodus	Wählen Sie zwischen „Main“ und „Aggressive“.
Authentifizierung Algorithmus	Wählen Sie zwischen „DES“, „3DES“, „AES128“, „AES192“ und „AES256“.
Verschlüsselungsalgorithmus	Wählen Sie zwischen „MD5“ und „SHA1“.
DH-Gruppe	Wählen Sie zwischen „MODP768_1“, „MODP1024_2“ und „MODP1536_5”.
Schlüssel	Geben Sie den vorab vereinbarten Schlüssel ein.
Lokale ID-Art	Wählen Sie zwischen „Standard“, „ID“, „FQDN“ und „Benutzer-FQDN“
IKE-Lebensdauer (s)	Legen Sie die Lebensdauer in der IKE-Verhandlung fest. Bereich: 60-86400.
SA-Algorithmus	Wählen Sie zwischen „DES_MD5“, „DES_SHA1“, „3DES_MD5“, „3DES_SHA1“, „AES128_MD5“, „AES128_SHA1“, „AES192_MD5“, „AES192_SHA1“, „AES256_MD5“ und „AES256_SHA1”.
PFS-Gruppe	Wählen Sie aus „NULL“, „MODP768_1“, „MODP1024_2“ und „MODP1536-5“.

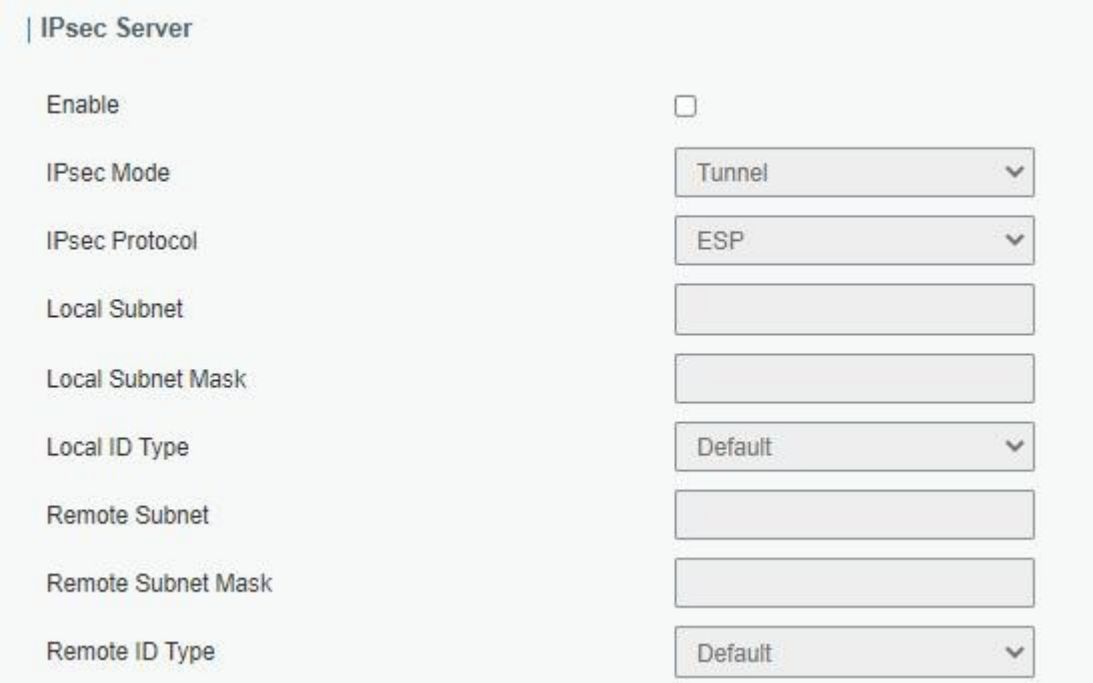
Lebensdauer (s)	Legen Sie die Lebensdauer von IPsec SA fest. Bereich: 60-86400.
DPD-Intervallzeit (s)	DPD-Intervallzeit einstellen
DPD-Zeitlimit (s)	DPD-Zeitüberschreitung festlegen.
Cisco-Geheimnis	Cisco Nhrp-Schlüssel.
NHRP-Haltezeit (s)	Die Haltezeit des NHRP-Protokolls.

Tabelle 3-2-5-1 DMVPN-Parameter

3.2.5.2 IPSec-Server

IPsec ist besonders nützlich für die Implementierung virtueller privater Netzwerke und für den Fernzugriff von Benutzern über eine Einwahlverbindung zu privaten Netzwerken. Ein großer Vorteil von IPsec besteht darin, dass Sicherheitsvorkehrungen getroffen werden können, ohne dass Änderungen an den einzelnen Benutzercomputern erforderlich sind.
IPsec bietet drei Optionen für Sicherheitsdienste: Authentication Header (AH), Encapsulating Security Payload (ESP) und Internet Key Exchange (IKE). AH ermöglicht im Wesentlichen die Authentifizierung der Daten des Absenders. ESP unterstützt sowohl die Authentifizierung des Absenders als auch die Datenverschlüsselung. IKE wird für den Austausch von Verschlüsselungscodes verwendet. Alle drei Dienste können einen oder mehrere Datenflüsse zwischen Hosts, zwischen Host und Gateway sowie zwischen Gateways schützen.

Abbildung 3-2-5-2



IPsec-Server	
Element	**Beschreibung**
Aktivieren	Aktivieren oder deaktivieren Sie den IPsec-Servermodus.
IPsec-Modus	Wählen Sie „Tunnel“ oder „Transport“.
IPsec-Protokoll	Wählen Sie zwischen ESP und AH.
Lokales Subnetz	Geben Sie die lokale LAN-Subnetz-IP-Adresse im IPsec-Tunnel ein.
Lokale Subnetz-Netzmaske	Geben Sie die lokale LAN-Netzmaske im IPsec-Tunnel ein.
Lokaler ID-Typ	Wählen Sie den Identifizierungstyp aus und senden Sie ihn an den Remote-Peer. **Standard:** Keine

	ID: Verwenden Sie die IP-Adresse des lokalen Subnetzes als ID. **FQDN:** Vollständig qualifizierter Domänenname,Beispiel: test.user.com **Benutzer-FQDN:** Vollständig qualifizierte Benutzername-Zeichenfolge im E-Mail-Adressformat, Beispiel: test@user.com
Remote-Subnetz	Legen Sie das Remote-LAN-Subnetz für den IPsec-Tunnel fest.
Remote-Subnetzmaske	Geben Sie die Remote-LAN-Netzmaske im IPsec-Tunnel ein.
Remote-ID-Typ	Wählen Sie den Identifizierungstyp aus, der mit der lokalen ID des Remote-Peers übereinstimmt. **Standard:** Keine **ID:** Remote-Subnetz-IP-Adresse als ID verwenden **FQDN:** Vollständig qualifizierter Domänenname,Beispiel: test.user.com **Benutzer-FQDN:** Vollständig qualifizierte Benutzernamenzeichenfolge im E-Mail-Adressformat, Beispiel: test@user.com

Tabelle 3-2-5-2 IPsec-Serverparameter

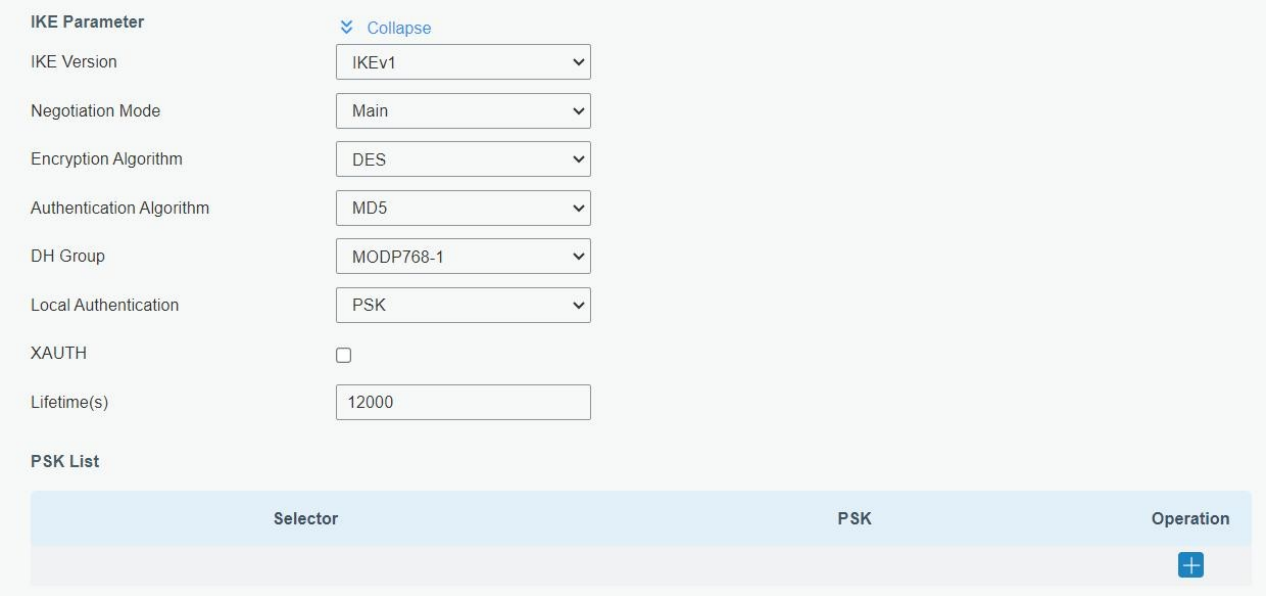


Abbildung 3-2-5-3

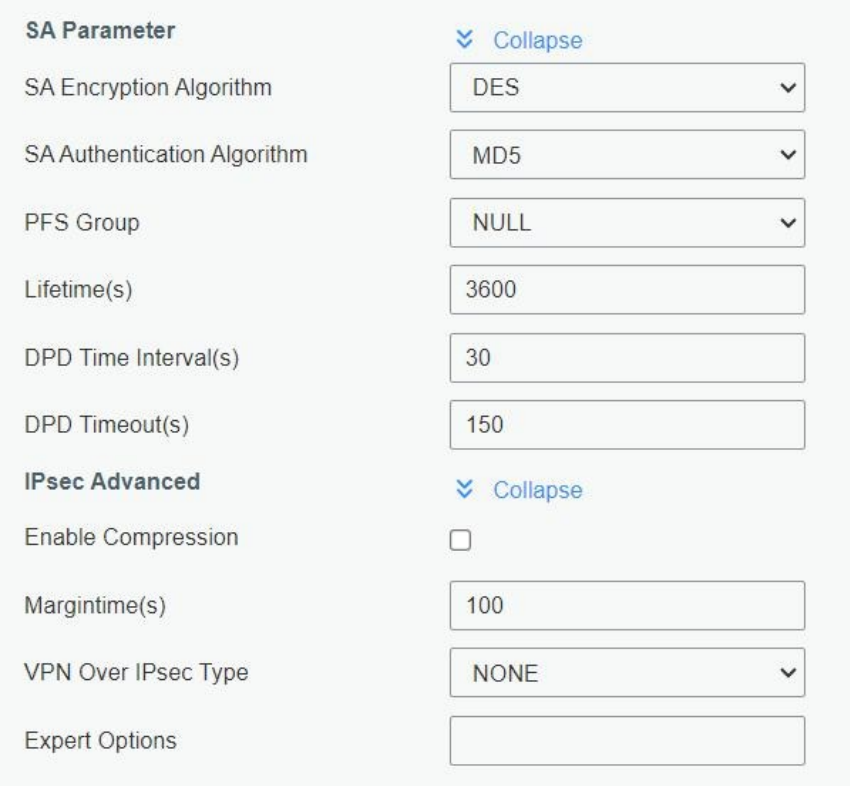


Abbildung 3-2-5-4

IKE-Parameter	
Element	**Beschreibung**
IKE-Version	Wählen Sie die Methode für den Schlüsselaustausch aus IKEv1 und IKEv2 aus.
Verhandlungsmodus	Bei Verwendung von IKEv1 wählen Sie „Main“ oder „Aggressive“.
Verschlüsselungsalgorithmus	Wählen Sie zwischen DES, 3DES, AES128, AES192 oder AES256.
Authentifizierungsalgorithmus	Wählen Sie „MD5“, „SHA1“ oder „SHA2-256“.
DH-Gruppe	Wählen Sie MODP768-1, MODP1024-2, MODP1536-5, MODP2048-14 oder MODP3072-15.
Lokale Authentifizierung	Wählen Sie PSK oder CA. **PSK:** Verwenden Sie einen vorab geteilten Schlüssel, um die Authentifizierung abzuschließen. **CA:** Verwenden Sie das Zertifikat, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **„Netzwerk > VPN > Zertifikate“**, um das CA-Zertifikat, das lokale Zertifikat und den privaten Schlüssel in die entsprechenden Felder zu importieren.
Remote-Authentifizierung	Bei Verwendung von IKEv2 wählen Sie PSK oder CA. **PSK:** Verwenden Sie einen vorab geteilten Schlüssel, um die Authentifizierung abzuschließen. **CA:** Verwenden Sie ein Zertifikat, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **Netzwerk > VPN > > Zertifizierungen**, um das Remote-Zertifikat in die entsprechenden Felder zu importieren.
XAUTH	Bei Verwendung von IKEv1 definieren Sie den XAUTH-Benutzernamen und das Passwort nach XAUTH aktiviert ist.
Lebensdauer (s)	Legen Sie die Lebensdauer in der IKE-Verhandlung fest. Bereich: 60-86400.
XAUTH-Liste	
Benutzername	Geben Sie den Benutzernamen ein, der für die xauth-Authentifizierung verwendet wird.
Passwort	Geben Sie das für die xauth-Authentifizierung verwendete Passwort ein.

PSK-Liste	
Selektor	Geben Sie die entsprechende Identifikationsnummer für die PSK-Authentifizierung ein.
PSK	Geben Sie den vorab geteilten Schlüssel ein.
SA-Parameter	
SA-Verschlüsselungsalgorithmus	Wählen Sie DES, 3DES, AES128, AES192 oder AES256.
SA-Authentifizierung Algorithmus	Wählen Sie MD5, SHA1 oder SHA2-256.
PFS-Gruppe	Wählen Sie NULL, MODP768-1, MODP1024-2 oder MODP1536-5.
Lebensdauer (s)	Legen Sie die Lebensdauer von IPsec SA fest. Bereich: 60-86400 s.
DPD-Zeitintervall(s)	Legen Sie das DPD-Wiederholungsintervall für das Senden von DPD-Anfragen fest. Bereich: 1-86400 s
DPD-Zeitlimit	Legen Sie das DPD-Zeitlimit fest, um Fehler auf der Gegenstelle zu erkennen. Bereich: 10-86400 s.
IPsec erweitert	
Komprimierung aktivieren	Der Kopf des IP-Pakets wird nach der Aktivierung komprimiert.
Marginalzeit	Legen Sie vor Ablauf der Lebensdauer einen Zeitpunkt fest, zu dem die Neuverhandlung zu beginnen.
VPN über IPsec-Typ	Wählen Sie zwischen KEINE, GRE und L2TP.
Expertenoptionen	Der Benutzer kann in diesem Feld einige andere Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen.

Tabelle 3-2-5-3 IPsec-Serverparameter

3.2.5.3 IPSec

UR35 unterstützt die gleichzeitige Ausführung von maximal 3 IPsec-Clients.

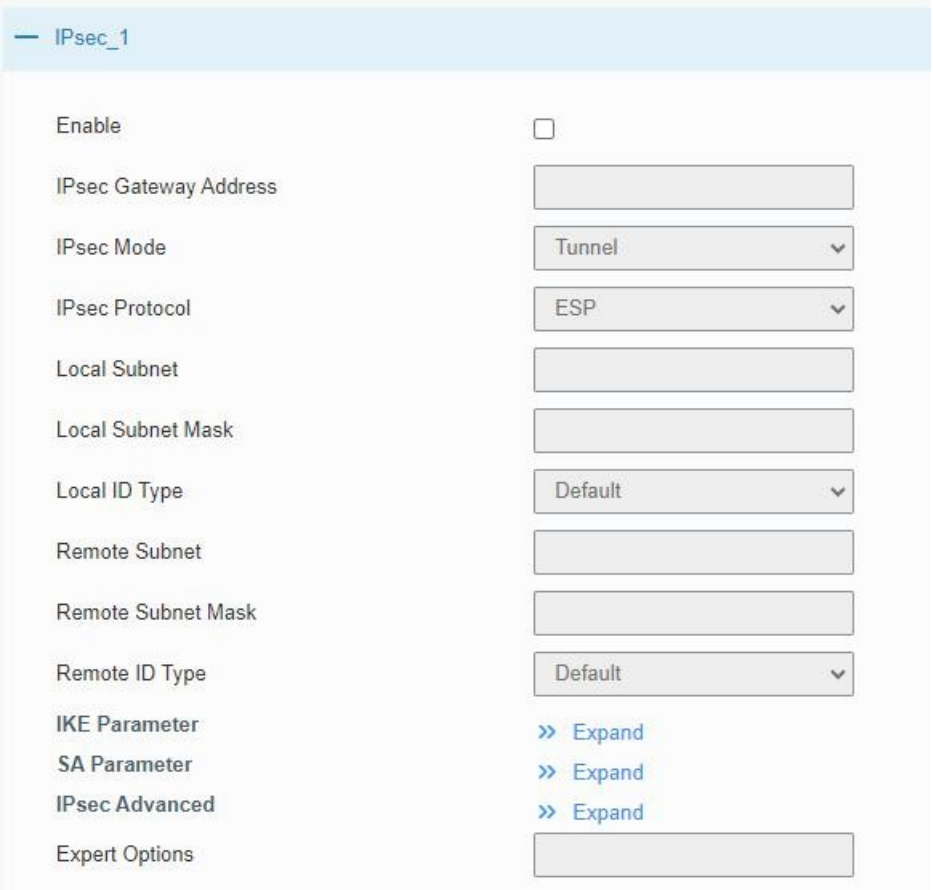


Abbildung 3-2-5-5

IPsec	
Element	**Beschreibung**
Aktivieren	IPsec-Clientmodus aktivieren oder deaktivieren. Maximal 3 Tunnel ist zulässig.
IP-Gateway-Adresse	Geben Sie die Adresse des Remote-IPsec-Servers ein.
IPsec-Modus	Wählen Sie „Tunnel“ oder „Transport“.
IPsec-Protokoll	Wählen Sie zwischen ESP und AH.
Lokales Subnetz	Geben Sie die IP-Adresse des lokalen LAN-Subnetzes im IPsec-Tunnel ein.
Lokale Subnetz-Netzmaske	Geben Sie die lokale LAN-Netzmaske im IPsec-Tunnel ein.
Lokaler ID-Typ	Wählen Sie den Identifizierungstyp aus und senden Sie ihn an den Remote-Peer. **Standard:** Keine **ID:** Verwenden Sie die IP-Adresse des lokalen Subnetzes als ID. **FQDN:** Vollständig qualifizierter Domänenname, Beispiel: test.user.com **Benutzer-FQDN:** Vollständig qualifizierte Benutzernamenzeichenfolge im E-Mail-Adressformat, Beispiel: test@user.com
Remote-Subnetz	Legen Sie das Remote-LAN-Subnetz für den IPsec-Tunnel fest.
Remote-Subnetzmaske	Geben Sie die Remote-LAN-Netzmaske für den IPsec-Tunnel ein.
Remote-ID-Typ	Wählen Sie den Identifizierungstyp aus, der mit der lokalen ID des Remote-Peers übereinstimmt. **Standard:** Keine **ID:** Remote-Subnetz-IP-Adresse als ID verwenden **FQDN:** Vollständig qualifizierter Domänenname, Beispiel: test.user.com **Benutzer-FQDN:** Vollständig qualifizierte Benutzernamenzeichenfolge im E-Mail-Adressformat, Beispiel: test@user.com

Tabelle 3-2-5-4 IPsec-Parameter

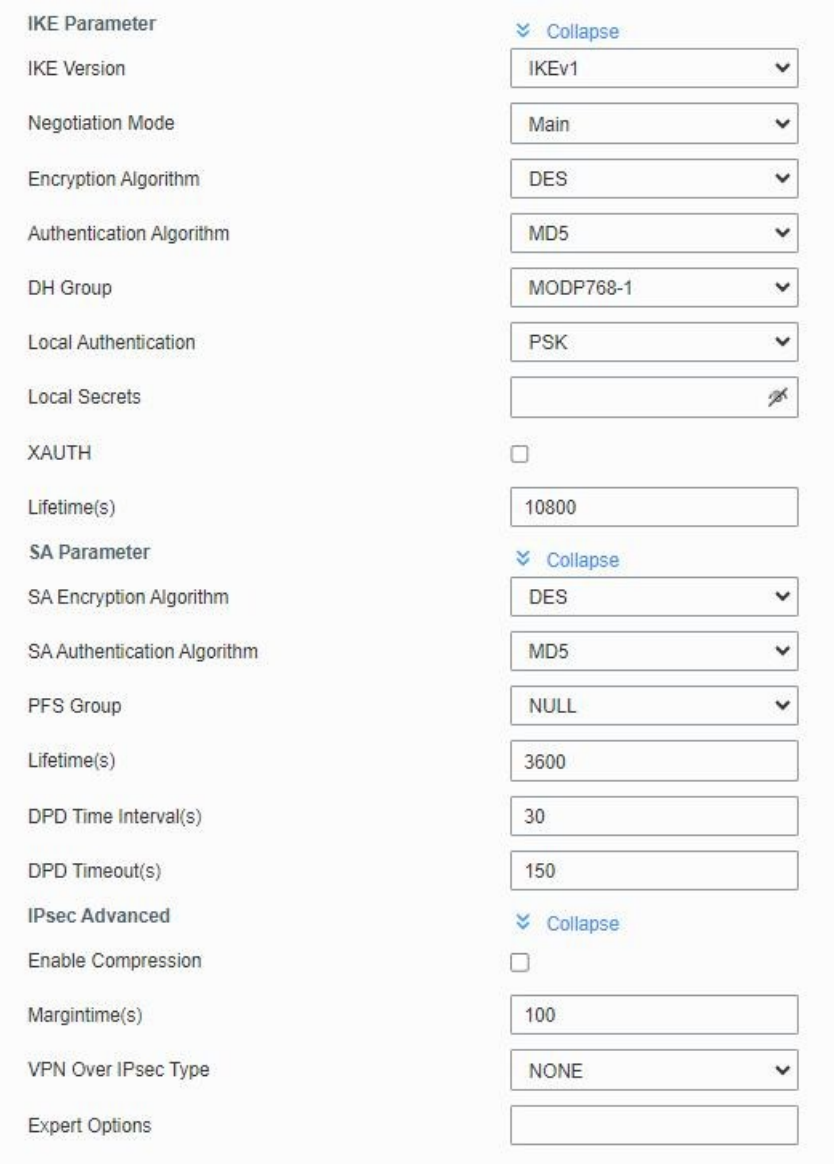


Abbildung 3-2-5-6

IKE-Parameter	
Element	**Beschreibung**
IKE-Version	Wählen Sie die Methode für den Schlüsselaustausch aus IKEv1 und IKEv2 aus.
Verhandlungsmodus	Bei Verwendung von IKEv1 wählen Sie „Main“ oder „Aggressive“.
Verschlüsselungsalgorithmus	Wählen Sie zwischen DES, 3DES, AES128, AES192 oder AES256.
Authentifizierungsalgorithmus	Wählen Sie „MD5“, „SHA1“ oder „SHA2-256“.
DH-Gruppe	Wählen Sie MODP768-1, MODP1024-2, MODP1536-5, MODP2048-14 oder MODP3072-15.
Lokale Authentifizierung	Wählen Sie PSK oder CA. **PSK:** Verwenden Sie einen vorab geteilten Schlüssel, um die Authentifizierung abzuschließen. **CA:** Verwenden Sie ein Zertifikat, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **„Netzwerk > VPN > > Zertifizierungen“**, um das CA-Zertifikat, das lokale Zertifikat und den privaten Schlüssel in die entsprechenden Felder zu importieren.
Lokale Geheimnisse	Geben Sie den vorab geteilten Schlüssel ein, der auf der Serverseite definiert ist.
Remote-Authentifizierung	Bei Verwendung von IKEv2 wählen Sie PSK oder CA.

	PSK: Verwenden Sie den vorab geteilten Schlüssel, um die Authentifizierung abzuschließen. **CA:** Verwenden Sie das Zertifikat, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **„Netzwerk > VPN > Zertifikate“**, um das Remote-Zertifikat in die entsprechenden Felder zu importieren.
Remote-Geheimnisse	Geben Sie den vorab geteilten Schlüssel ein, der auf der Serverseite definiert ist.
XAUTH	Geben Sie den XAUTH-Benutzernamen und das Passwort ein, die auf der Serverseite definiert sind.
Lebensdauer (s)	Legen Sie die Lebensdauer in der IKE-Verhandlung fest. Bereich: 60-86400.
SA-Parameter	
SA-Verschlüsselungsalgorithmus	Wählen Sie DES, 3DES, AES128, AES192 oder AES256.
SA-Authentifizierung Algorithmus	Wählen Sie MD5, SHA1 oder SHA2-256.
PFS-Gruppe	Wählen Sie NULL, MODP768-1, MODP1024-2 oder MODP1536-5.
Lebensdauer (s)	Legen Sie die Lebensdauer von IPsec SA fest. Bereich: 60-86400 s.
DPD-Zeitintervall(s)	Legen Sie das DPD-Wiederholungsintervall für das Senden von DPD-Anfragen fest. Bereich: 1-86400 s
DPD-Zeitlimit	Legen Sie das DPD-Zeitlimit fest, um Fehler auf der Gegenstelle zu erkennen. Bereich: 10-86400 s.
IPsec erweitert	
Komprimierung aktivieren	Der Kopf des IP-Pakets wird nach der Aktivierung komprimiert.
Margintime	Legen Sie vor Ablauf der Lebensdauer einen Zeitpunkt fest, zu dem die Neuverhandlung zu beginnen.
VPN über IPsec-Typ	Wählen Sie zwischen KEINE, GRE und L2TP.
Expertenoptionen	Der Benutzer kann in diesem Feld einige andere Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen.

Tabelle 3-2-5-5 IPsec-Parameter

3.2.5.4 GRE

Generic Routing Encapsulation (GRE) ist ein Protokoll, das Pakete kapselt, um andere Protokolle über IP-Netzwerke zu routen. Es handelt sich um eine Tunneling-Technologie, die einen Kanal bereitstellt, über den gekapselte Datennachrichten übertragen und an beiden Enden gekapselt und entkapselt werden können.

Unter den folgenden Umständen kann die GRE-Tunnelübertragung angewendet werden:

- Der GRE-Tunnel kann Multicast-Datenpakete übertragen, als wäre er eine echte Netzwerkschnittstelle. Mit IPSec allein lässt sich keine Verschlüsselung von Multicast erreichen.
- Ein bestimmtes Protokoll kann nicht geroutet werden.
- Ein Netzwerk mit unterschiedlichen IP-Adressen ist erforderlich, um zwei andere ähnliche Netzwerke zu verbinden.

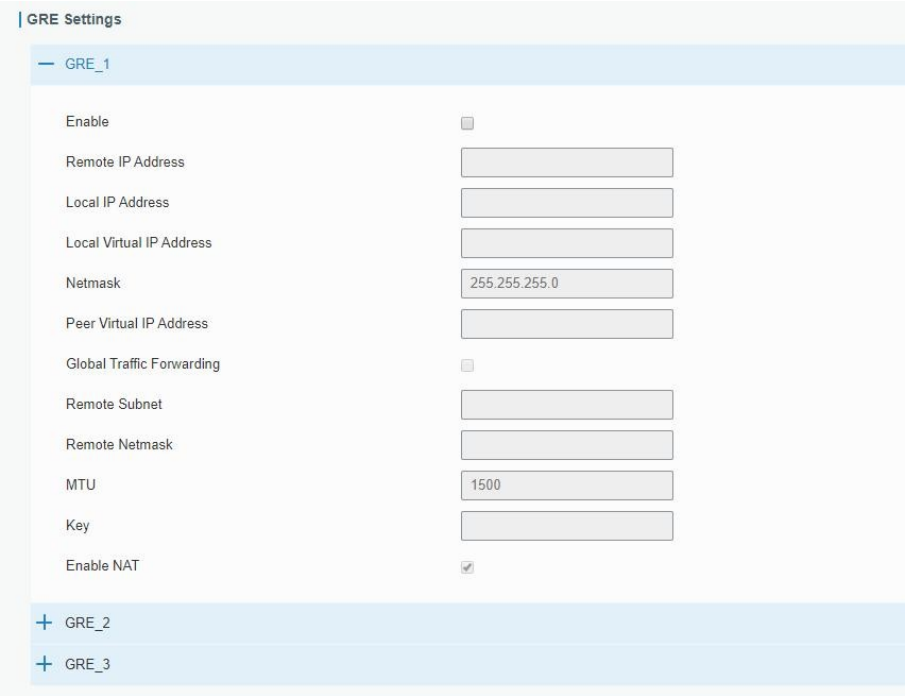


Abbildung 3-2-5-7

GRE	
Element	**Beschreibung**
Aktivieren	Aktivieren Sie diese Option, um die GRE-Funktion zu aktivieren.
Remote-IP-Adresse	Geben Sie die tatsächliche Remote-IP-Adresse des GRE-Tunnels ein.
Lokale IP-Adresse	Legen Sie die lokale IP-Adresse fest.
Lokale virtuelle IP Adresse	Legen Sie die lokale Tunnel-IP-Adresse des GRE-Tunnels fest.
Netzmaske	Legen Sie die lokale Netzmaske fest.
Virtuelle IP-Adresse des Peers	Geben Sie die Remote-Tunnel-IP-Adresse des GRE-Tunnels ein.
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über den GRE-Tunnel gesendet, wenn diese Funktion aktiviert ist.
Remote-Subnetz	Geben Sie die IP-Adresse des Remote-Subnetzes des GRE-Tunnels ein.
Remote-Netzmaske	Geben Sie die Remote-Netzmaske des GRE-Tunnels ein.
MTU	Geben Sie die maximale Übertragungseinheit ein. Bereich: 64-1500.
Schlüssel	Legen Sie den GRE-Tunnelschlüssel fest.
NAT aktivieren	Aktivieren Sie die NAT-Traversal-Funktion.

Tabelle 3-2-5-6 GRE-Parameter

3.2.5.5 L2TP

Das Layer Two Tunneling Protocol (L2TP) ist eine Erweiterung des Point-to-Point Tunneling Protocol (PPTP), das von Internetdienstanbietern (ISP) verwendet wird, um den Betrieb eines virtuellen privaten Netzwerks (VPN) über das Internet zu ermöglichen.

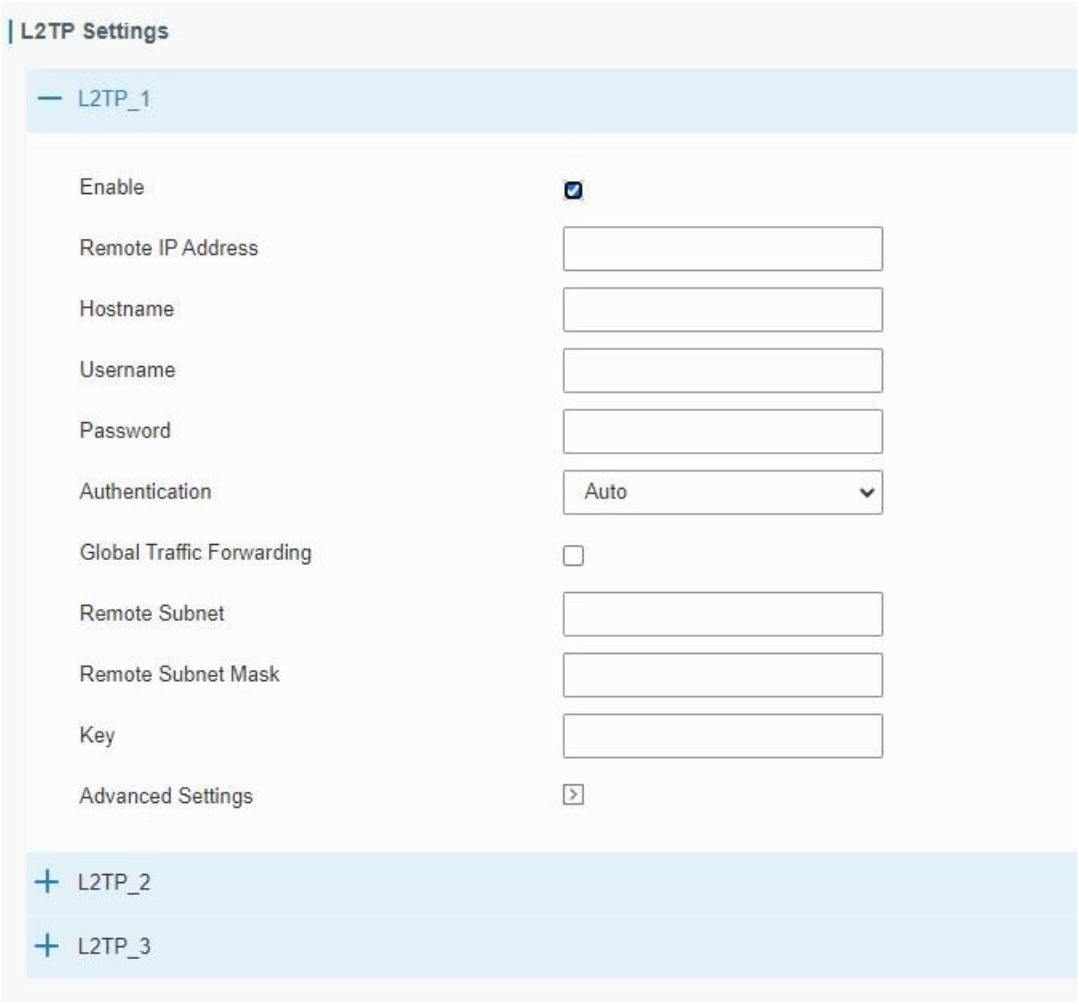


Abbildung 3-2-5-8

L2TP	
Element	**Beschreibung**
Aktivieren	Aktivieren Sie diese Option, um die L2TP-Funktion zu aktivieren.
Remote-IP-Adresse	Geben Sie die öffentliche IP-Adresse oder den Domänennamen des L2TP-Servers ein.
Hostname	Geben Sie den Hostnamen ein, um die Verbindung mit dem L2TP-Server zu überprüfen.
Benutzername	Geben Sie den Benutzernamen ein, den der L2TP-Server bereitstellt.
Passwort	Geben Sie das vom L2TP-Server bereitgestellte Passwort ein.
Authentifizierung	Wählen Sie zwischen „Auto“, „PAP“, „CHAP“, „MS-CHAPv1“ und „MS-CHAPv2“ aus.
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über den L2TP-Tunnel gesendet, nachdem diese Funktion aktiviert ist.
Remote-Subnetz	Geben Sie die Remote-IP-Adresse ein, die L2TP schützt.
Remote-Subnetzmaske	Geben Sie die Remote-Netzwerkmaske ein, die L2TP schützt.
Schlüssel	Geben Sie das Passwort für den L2TP-Tunnel ein.

Tabelle 3-2-5-7 L2TP-Parameter

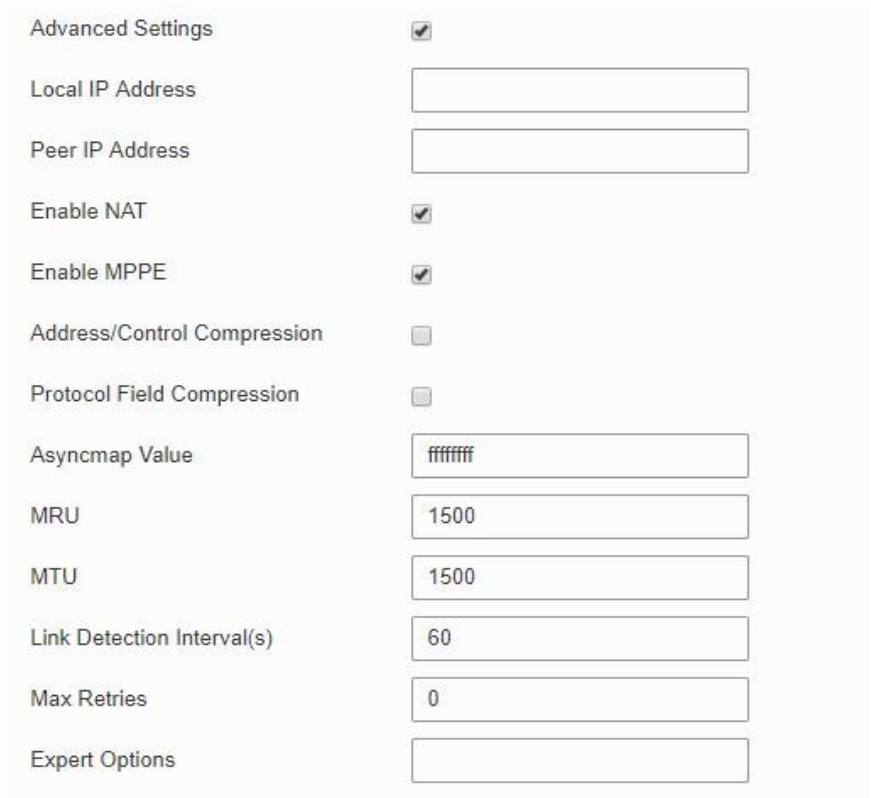


Abbildung 3-2-5-9

Erweiterte Einstellungen	
Element	**Beschreibung**
Lokale IP-Adresse	Legen Sie die Tunnel-IP-Adresse des L2TP-Clients fest. Der Client erhält die Tunnel-IP-Adresse automatisch vom Server, wenn sie null.
Peer-IP-Adresse	Geben Sie die Tunnel-IP-Adresse des L2TP-Servers ein.
NAT aktivieren	Aktivieren Sie die NAT-Traversal-Funktion.
MPPE aktivieren	MPPE-Verschlüsselung aktivieren.
Adresse/Steuerung Komprimierung	Für die PPP-Initialisierung. Der Benutzer kann die Standardoption beibehalten.
Protokollfeld Komprimierung	Für die PPP-Initialisierung. Der Benutzer kann die Standardoption beibehalten.
Asyncmap-Wert	Eine der Initialisierungszeichenfolgen für das PPP-Protokoll. Der Benutzer kann den Standardwert beibehalten. Bereich: 0-ffffffff.
MRU	Legt die maximale Empfangseinheit fest. Bereich: 64-1500.
MTU	Legt die maximale Übertragungseinheit fest. Bereich: 64-1500
Link-Erkennungsintervall (s)	Legen Sie das Verbindungserkennungsintervall fest, um die Tunnelverbindung sicherzustellen Verbindung. Bereich: 0-600.
Max. Wiederholungsversuche	Legen Sie die maximale Anzahl der Wiederholungsversuche fest, um den L2TP-Verbindungsfehler zu erkennen Verbindungsfehler. Bereich: 0-10.
Expertenoptionen	Der Benutzer kann in diesem Feld einige andere PPP-Initialisierungszeichenfolgen eingeben Feld einige andere PPP-Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Leerzeichen trennen.

Tabelle 3-2-5-8 L2TP-Parameter

3.2.5.6 PPTP

Das Point-to-Point Tunneling Protocol (PPTP) ist ein Protokoll, mit dem Unternehmen ihr eigenes Unternehmensnetzwerk über private „Tunnel" über das öffentliche Internet erweitern können. Im Endeffekt nutzt ein Unternehmen ein Weitverkehrsnetzwerk als ein einziges großes lokales Netzwerk.

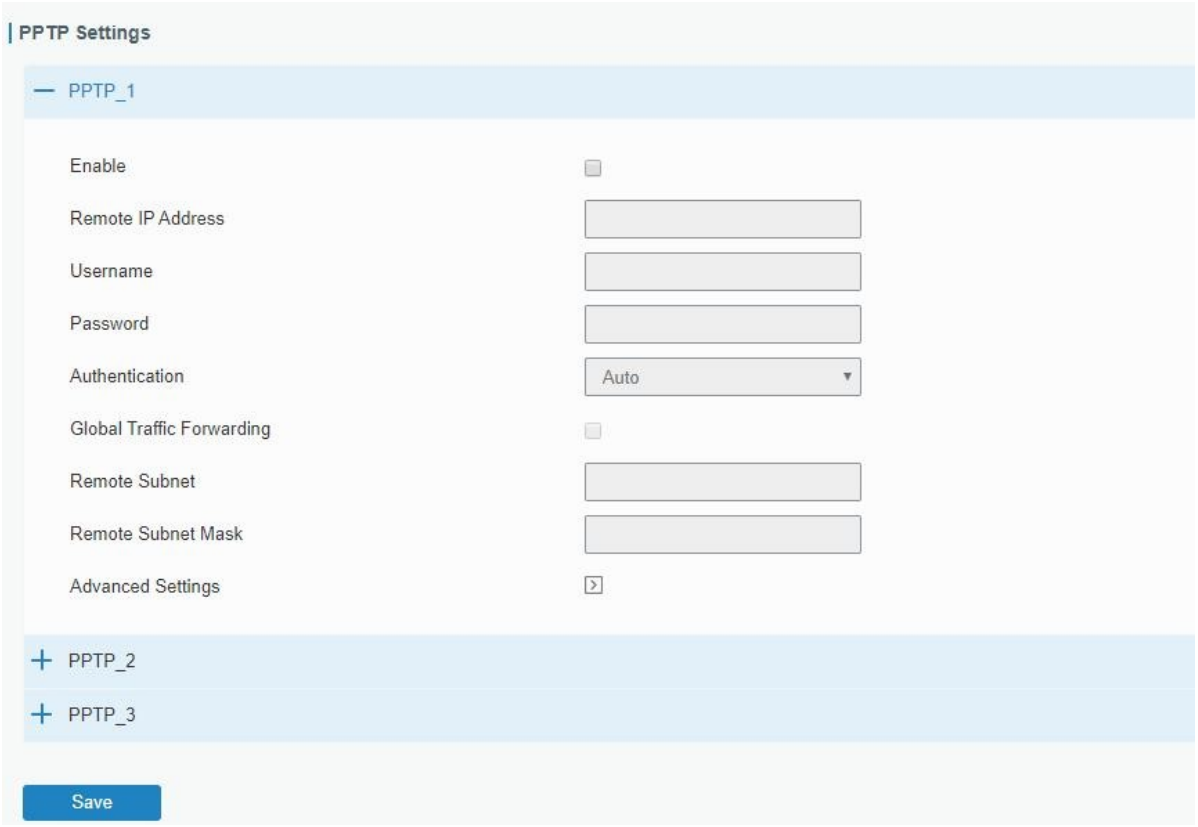


Abbildung 3-2-5-10

PPTP	
Element	**Beschreibung**
Aktivieren	PPTP-Client aktivieren. Es sind maximal 3 Tunnel zulässig.
Remote-IP-Adresse	Geben Sie die öffentliche IP-Adresse oder den Domänennamen des PPTP-Servers ein.
Benutzername	Geben Sie den Benutzernamen ein, den der PPTP-Server bereitstellt.
Passwort	Geben Sie das vom PPTP-Server bereitgestellte Passwort ein.
Authentifizierung	Wählen Sie zwischen „Auto", „PAP", „CHAP", „MS-CHAPv1" und „MS-CHAPv2" aus.
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über den PPTP-Tunnel gesendet, sobald Sie diese Funktion aktivieren.
Remote-Subnetz	Legen Sie das Peer-Subnetz von PPTP fest.
Remote-Subnetzmaske	Legen Sie die Netzmaske des Peer-PPTP-Servers fest.

Tabelle 3-2-5-9 PPTP-Parameter

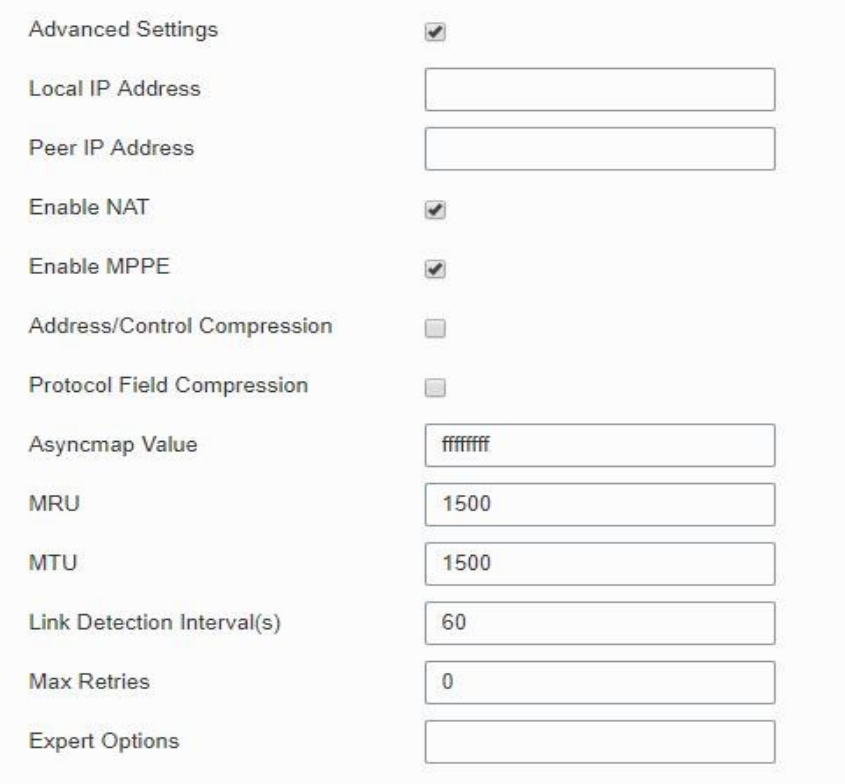


Abbildung 3-2-5-11

Erweiterte PPTP-Einstellungen	
Element	**Beschreibung**
Lokale IP-Adresse	Legen Sie die IP-Adresse des PPTP-Clients fest.
Peer-IP-Adresse	Geben Sie die Tunnel-IP-Adresse des PPTP-Servers ein.
NAT aktivieren	Aktivieren Sie die NAT-Funktion von PPTP.
MPPE aktivieren	MPPE-Verschlüsselung aktivieren.
Adresse/Steuerung Komprimierung	Für die PPP-Initialisierung. Der Benutzer kann die Standardoption beibehalten.
Protokollfeld Komprimierung	Für die PPP-Initialisierung. Der Benutzer kann die Standardoption beibehalten.
Asyncmap-Wert	Eine der Initialisierungszeichenfolgen des PPP-Protokolls. Der Benutzer kann den Standardwert beibehalten. Bereich: 0-ffffffff.
MRU	Geben Sie die maximale Empfangseinheit ein. Bereich: 0-1500.
MTU	Geben Sie die maximale Übertragungseinheit ein. Bereich: 0-1500.
Link-Erkennungsintervall (s)	Stellen Sie das Verbindungserkennungsintervall ein, um die Tunnelverbindung sicherzustellen Verbindung. Bereich: 0-600.
Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl der Wiederholungsversuche fest, um den PPTP-Verbindungsfehler zu erkennen Verbindungsfehler. Bereich: 0-10.
Expertenoptionen	Der Benutzer kann in diesem Feld einige andere PPP-Initialisierungszeichenfolgen eingeben Feld eingeben und die Zeichenfolgen durch Leerzeichen trennen.

Tabelle 3-2-5-10 PPTP-Parameter

3.2.5.7 OpenVPN-Client

OpenVPN ist ein Open-Source-Produkt für virtuelle private Netzwerke (VPN), das eine vereinfachte Sicherheitsarchitektur

, ein modulares Netzwerkdesign und plattformübergreifende Portabilität bietet. Die Standardversion von OpenVPN für den UR35 ist 2.4.9.
UR35 unterstützt die gleichzeitige Ausführung von maximal 3 OpenVPN-Clients. Sie können die ovpn-Datei direkt importieren oder die Parameter auf dieser Seite konfigurieren, um Clients einzurichten.

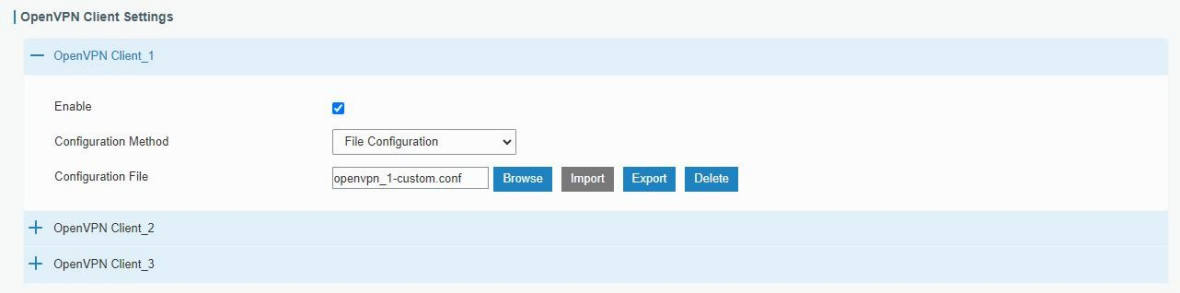


Abbildung 3-2-5-12

OpenVPN-Client – Dateikonfiguration	
Element	**Beschreibung**
Durchsuchen	Klicken Sie hier, um die Client-Konfigurationsdatei im OVPN-Format einschließlich der Einstellungen und Zertifikatsinhalte. Bitte beachten Sie die Client-Konfigurationsdatei gemäß dem Beispiel: client.conf
Bearbeiten	Klicken Sie hier, um die importierte Datei zu bearbeiten.
Export	Exportieren Sie die Serverkonfigurationsdatei.
Löschen	Klicken Sie hier, um die Konfigurationsdatei zu löschen.

Tabelle 3-2-5-11 OpenVPN-Client-Parameter

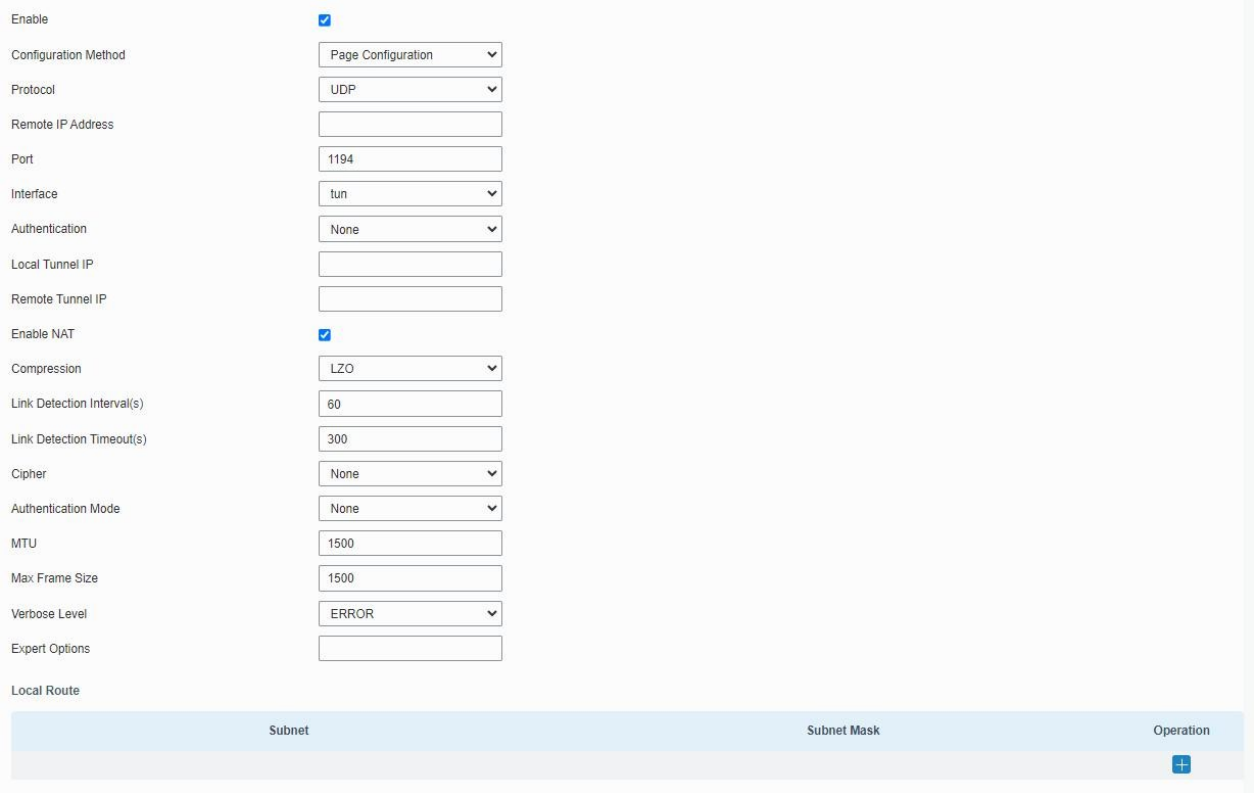


Abbildung 3-2-5-13

OpenVPN-Client – Seitenkonfiguration	
Element	**Beschreibung**
Protokoll	Wählen Sie ein Transportprotokoll aus, das durch die Verbindung von UDP und TCP verwendet wird.
Remote-IP-Adresse	Geben Sie die IP-Adresse oder den Domänennamen des Remote-OpenVPN-Servers ein.
Port	Geben Sie die TCP/UCP-Servicenummer des Remote-OpenVPN-Servers ein. Bereich: 1–65535
Schnittstelle	Wählen Sie den Typ der virtuellen VPN-Netzwerkschnittstelle aus TUN und TAP aus. TUN-Geräte kapseln IPv4 oder IPv6 (OSI-Schicht 3), während TAP-Geräte Ethernet 802.3 (OSI-Schicht 2) kapseln.
Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird. **Vorab geteilt:** Verwenden Sie denselben geheimen Schlüssel wie der Server, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **„Netzwerk > VPN > Zertifizierungen“**, um eine statische Datei in das PSK-Feld zu importieren. **Benutzername/Passwort:** Verwenden Sie den auf der Serverseite voreingestellten Benutzernamen/das voreingestellte Passwort, um die Authentifizierung abzuschließen. **X.509-Zertifikat:** Verwenden Sie ein Zertifikat vom Typ X.509, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **„Netzwerk > VPN > Zertifikate“**, um das CA-Zertifikat, das Client-Zertifikat und den privaten Client-Schlüssel in die entsprechenden Felder zu importieren. **X.509-Zertifikat + Benutzer:** Verwenden Sie sowohl Benutzername/Passwort als auch X.509-Zertifikat als Authentifizierungstyp.
Lokale virtuelle IP	Legen Sie die lokale Tunneladresse fest, wenn der Authentifizierungstyp **„Keine“** oder **„Vorab geteilt“** ist.
Virtuelle Remote-IP	Remote-Tunneladresse festlegen, wenn der Authentifizierungstyp **„Keine“** oder **„Vorab geteilt“**.
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über den OpenVPN-Tunnel gesendet, wenn diese Funktion aktiviert ist.
TLS-Authentifizierung aktivieren Authentifizierung	Wählen Sie zwischen „Keine“, „TLS-Authentifizierung“ und „TLS-Verschlüsselung“. Wenn Sie „TLS-Authentifizierung“ oder „TLS-Verschlüsselung“ auswählen „TLS-Verschlüsselung“ wählen, gehen Sie zur Seite **„Netzwerk > VPN > Zertifikate“**, um eine ta.key-Datei zu importieren.
Komprimierung	Wählen Sie diese Option, um LZO zur Komprimierung von Daten zu aktivieren oder zu deaktivieren.
Link-Erkennungsintervall (s)	Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Wenn dies sowohl auf dem Server als auch auf dem Client eingestellt ist, überschreibt der vom Server übertragene Wert die lokalen Werte des Clients. Bereich: 10–1800 s.
Zeitlimit für die Verbindungserkennung (s)	OpenVPN wird nach Ablauf des Zeitlimits neu aufgebaut. Wenn dies sowohl auf dem Server als auch auf dem Client eingestellt ist, überschreibt der vom Server übermittelte Wert die lokalen Werte des Clients. Bereich: 60–3600 s.
Verschlüsselung	Wählen Sie zwischen NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC, AES-192-CBC und AES-256-CBC.
Authentifizierungsmodus	Wählen Sie zwischen KEINER, MD5, SHA1, SHA256 und SHA512.
MTU	Geben Sie die maximale Übertragungseinheit ein. Bereich: 128–1500.
Maximale Frame-Größe	Legen Sie die maximale Frame-Größe fest. Bereich: 128–1500.
Ausführlichkeitsstufe	Wählen Sie zwischen ERROR, WARING, NOTICE und DEBUG.
Expertenoptionen	Der Benutzer kann in diesem Feld einige Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen. **Beispiel:** ncp-ciphers AES-128-GCM, Schlüsselrichtung 1
Lokale Route	

Subnetz	Legen Sie die IP-Adresse der lokalen Route fest.
Subnetzmaske	Legen Sie die Netzmaske der lokalen Route fest.

Tabelle 3-2-5-12 OpenVPN-Client-Parameter

Verwandtes Thema

Beispiel für eine OpenVPN-Client-Anwendung

3.2.5.8 OpenVPN-Server

Der UR35 unterstützt OpenVPN-Server zum Erstellen sicherer Punkt-zu-Punkt- oder Standort-zu-Standort-Verbindungen in gerouteten oder gebrückten Konfigurationen und Fernzugriffsfunktionen. Sie können die ovpn-Datei direkt importieren oder die Parameter auf dieser Seite konfigurieren, um diesen Server einzurichten. Der UR35 unterstützt maximal 20 OpenVPN-Client-Verbindungen.

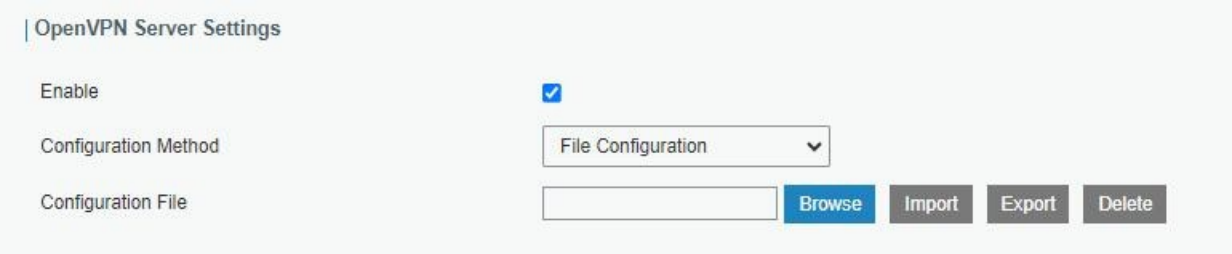


Abbildung 3-2-5-14

OpenVPN-Server – Dateikonfiguration	
Element	**Beschreibung**
Durchsuchen	Klicken Sie hier, um die OVPN-Konfigurationsdatei des Servers mit den Einstellungen und Zertifikatsinhalte. Bitte beachten Sie die Serverkonfigurationsdatei gemäß dem Beispiel: server.conf
Bearbeiten	Klicken Sie hier, um die importierte Datei zu bearbeiten.
Export	Exportieren Sie die Serverkonfigurationsdatei.
Löschen	Klicken Sie hier, um die Konfigurationsdatei zu löschen.

Tabelle 3-2-5-13 OpenVPN-Serverparameter

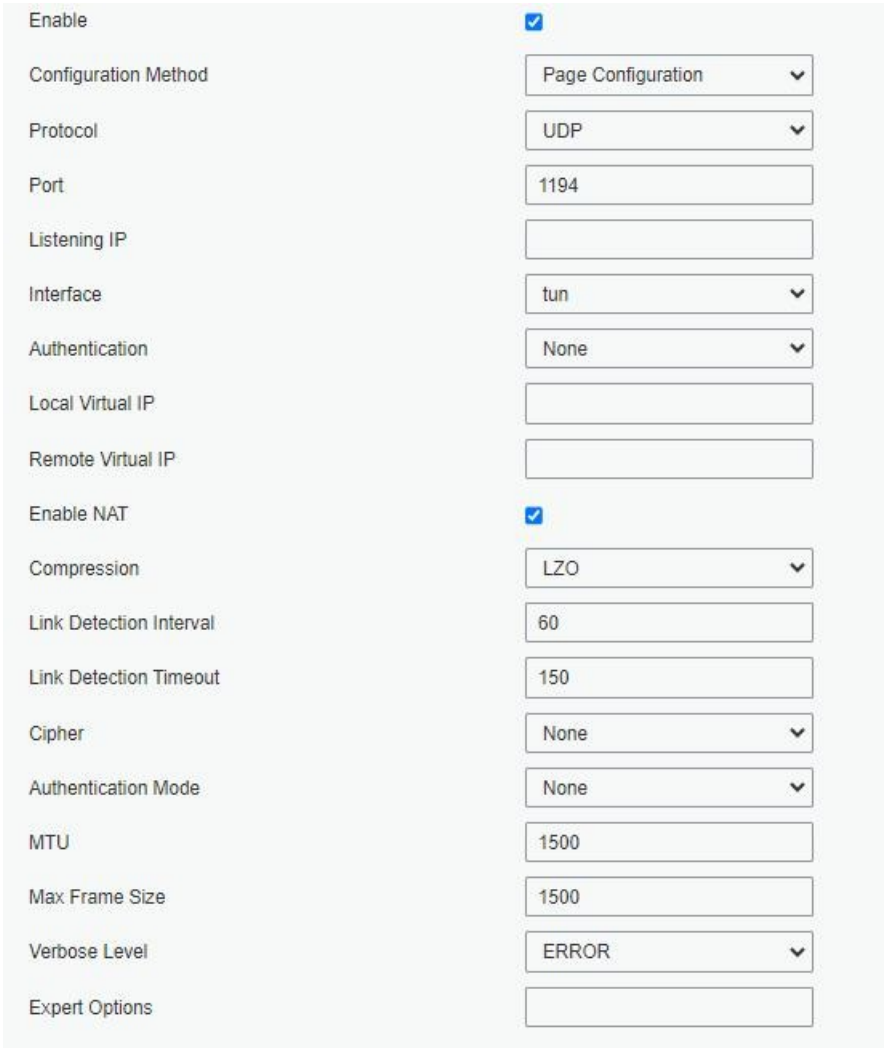


Abbildung 3-2-5-15

Abbildung 3-2-5-16

OpenVPN-Server – Seitenkonfiguration	
Element	**Beschreibung**
Protokoll	Wählen Sie ein Transportprotokoll für die Verbindung aus UDP und TCP aus.
Zuhörende IP	Geben Sie den lokalen Hostnamen oder die IP-Adresse für die Bindung ein. Wenn das Feld leer bleibt, verbindet sich der OpenVPN-Server Server an alle Schnittstellen gebunden.
Port	Geben Sie die TCP/UCP-Servicenummer für die OpenVPN-Clientverbindung ein. Bereich: 1-65535.

Schnittstelle	Wählen Sie den Typ der virtuellen VPN-Netzwerkschnittstelle aus TUN und TAP aus. TUN-Geräte kapseln IPv4 oder IPv6 (OSI-Schicht 3), während TAP-Geräte Ethernet 802.3 (OSI-Schicht 2) kapseln.
Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird. **Vorab geteilt:** Verwenden Sie denselben geheimen Schlüssel wie der Server, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **„Netzwerk > VPN > Zertifikate“**, um eine statische Datei („static.key“) in das Feld **„PSK“** zu importieren. **Benutzername/Passwort:** Verwenden Sie den auf der Serverseite voreingestellten Benutzernamen/das Passwort, um die Authentifizierung abzuschließen. **X.509-Zertifikat:** Verwenden Sie ein Zertifikat vom Typ X.509, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **„Netzwerk > VPN > Zertifizierungen“**, um das CA-Zertifikat, das Client-Zertifikat und den privaten Client-Schlüssel in die entsprechenden Felder zu importieren. **X.509-Zertifikat + Benutzer:** Verwenden Sie sowohl Benutzername/Passwort als auch X.509-Zertifikat als Authentifizierungstyp verwenden.
Lokale virtuelle IP	Legen Sie die lokale Tunneladresse fest, wenn der Authentifizierungstyp **„Keine“** oder **„Vorab geteilt“** ist.
Virtuelle Remote-IP	Legen Sie die Remote-Tunneladresse fest, wenn der Authentifizierungstyp **„Keine“** oder „Vorab geteilt“ lautet. **„Vorab geteilt“ ist.**
Client-Subnetz	Definieren Sie einen IP-Adresspool für den OpenVPN-Client.
Client-Netzmaske	Legen Sie die Netzmaske des Client-Subnetzes fest, um den IP-Adressbereich zu begrenzen.
Neuverhandlungsintervall	Verhandeln Sie den Datenkanalschlüssel nach diesem Intervall neu. 0 bedeutet deaktivieren.
Maximale Anzahl von Clients	Begrenzen Sie den Server auf eine maximale Anzahl gleichzeitiger Clients, Bereich: 1-20. **Hinweis:** Bitte stellen Sie die Protokollierungsstufe auf „Info“ ein, wenn Sie viele Clients verbinden müssen.
CRL aktivieren	CRL-Überprüfung aktivieren oder deaktivieren.
Client-zu-Client aktivieren	Wenn diese Option aktiviert ist, können OpenVPN-Clients miteinander kommunizieren.
Dup-Client aktivieren	Ermöglicht mehreren Clients, sich mit demselben gemeinsamen Namen oder derselben gemeinsamen Zertifizierung zu verbinden. Zertifizierung verbinden.
TLS-Authentifizierung aktivieren Authentifizierung	Wählen Sie zwischen „Keine“, „TLS-Authentifizierung“ und „TLS-Verschlüsselung“. Wenn Sie „TLS-Authentifizierung“ oder „TLS-Verschlüsselung“ auswählen, gehen Sie zu „Netzwerk > VPN > Zertifikate“, um eine ta „TLS-Verschlüsselung“ wählen, gehen Sie zur Seite **„Netzwerk > VPN > Zertifikate“**, um eine ta.key-Datei zu importieren.
Komprimierung	Wählen Sie diese Option, um LZO zur Komprimierung von Daten zu aktivieren oder zu deaktivieren.
Link-Erkennungsintervall (s)	Legen Sie das Verbindungserkennungsintervall fest, um die Tunnelverbindung sicherzustellen. Wenn dies sowohl auf dem Server als auch auf dem Client festgelegt ist, überschreibt der vom Server übertragene Wert die lokalen Werte des Clients. Bereich: 10–1800 s.
Zeitlimit für Verbindungserkennung (s)	OpenVPN wird nach Ablauf des Zeitlimits neu aufgebaut. Wenn dies sowohl auf dem Server als auch auf dem Client eingestellt ist, überschreibt der vom Server übermittelte Wert die lokalen Werte des Clients . Bereich: 60–3600 s.
Verschlüsselung	Wählen Sie zwischen NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC, AES-192-CBC und AES-256-CBC.
Authentifizierungsmodus	Wählen Sie zwischen KEINE, MD5, SHA1, SHA256 und SHA512.
MTU	Geben Sie die maximale Übertragungseinheit ein. Bereich: 64–1500.
Maximale Frame-Größe	Legen Sie die maximale Frame-Größe fest. Bereich: 64–1500.
Ausführlichkeitsstufe	Wählen Sie zwischen ERROR, WARING, NOTICE und DEBUG.
Expertenoptionen	Der Benutzer kann in diesem Feld einige Initialisierungszeichenfolgen eingeben und die Zeichenfolgen mit Semikolons trennen.

	Beispiel: ncp-ciphers AES-128-GCM Schlüsselrichtung 1
Konto	
Benutzername und Passwort	Legen Sie Benutzername und Passwort für den OpenVPN-Client fest, wenn der Authentifizierungstyp Benutzername/Passwort ist.
Lokale Route	
Subnetz	Legen Sie die IP-Adresse der lokalen Route fest.
Subnetzmaske	Legen Sie die Netzmaske der lokalen Route fest.
Client-Subnetz	
Name	Legen Sie den Namen als allgemeinen Namen des OpenVPN-Client-Zertifikats fest.
Subnetz	Legen Sie das Subnetz des OpenVPN-Clients fest.
Subnetzmaske	Legen Sie die Subnetzmaske des OpenVPN-Clients fest.

Tabelle 3-2-5-14 OpenVPN-Serverparameter

3.2.5.9 Zertifikate

Auf dieser Seite können Benutzer Zertifikats- und Schlüsseldateien für OpenVPN und IPsec importieren/exportieren.

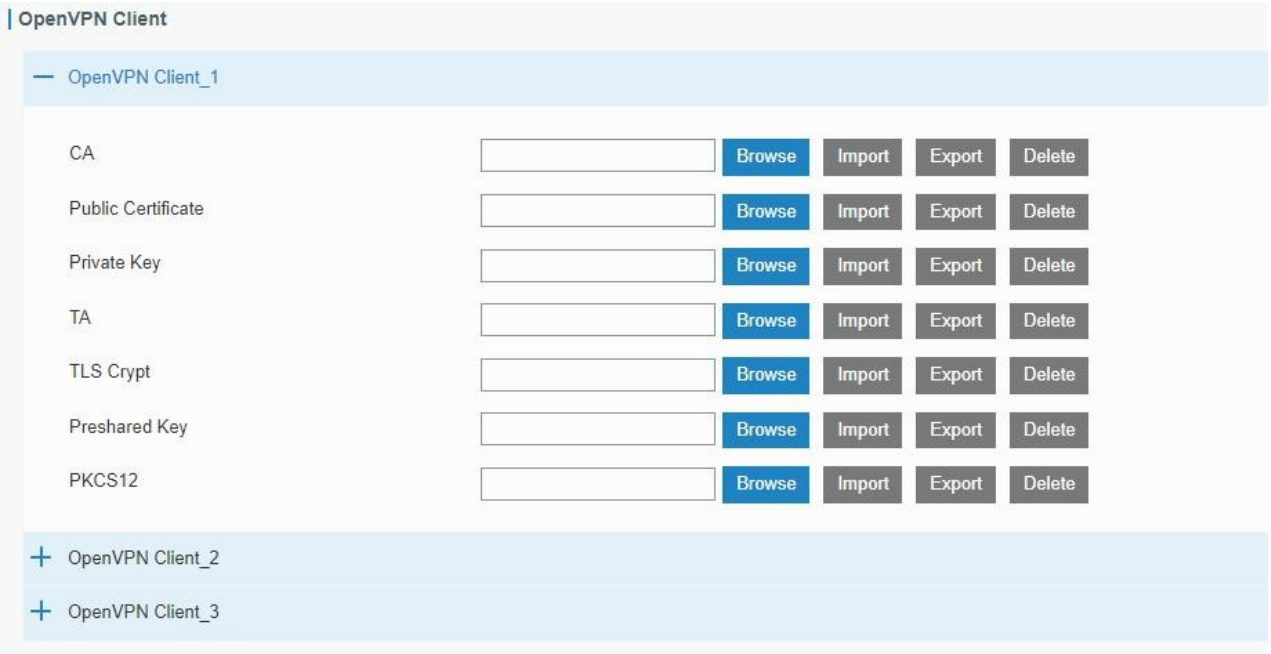


Abbildung 3-2-5-17

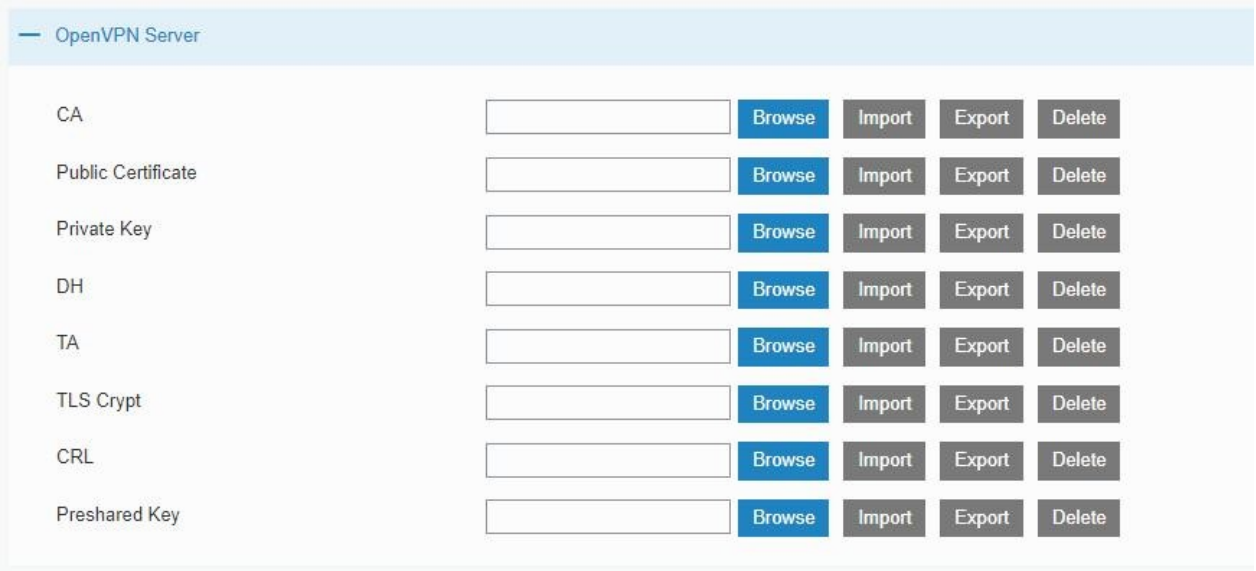


Abbildung 3-2-5-18

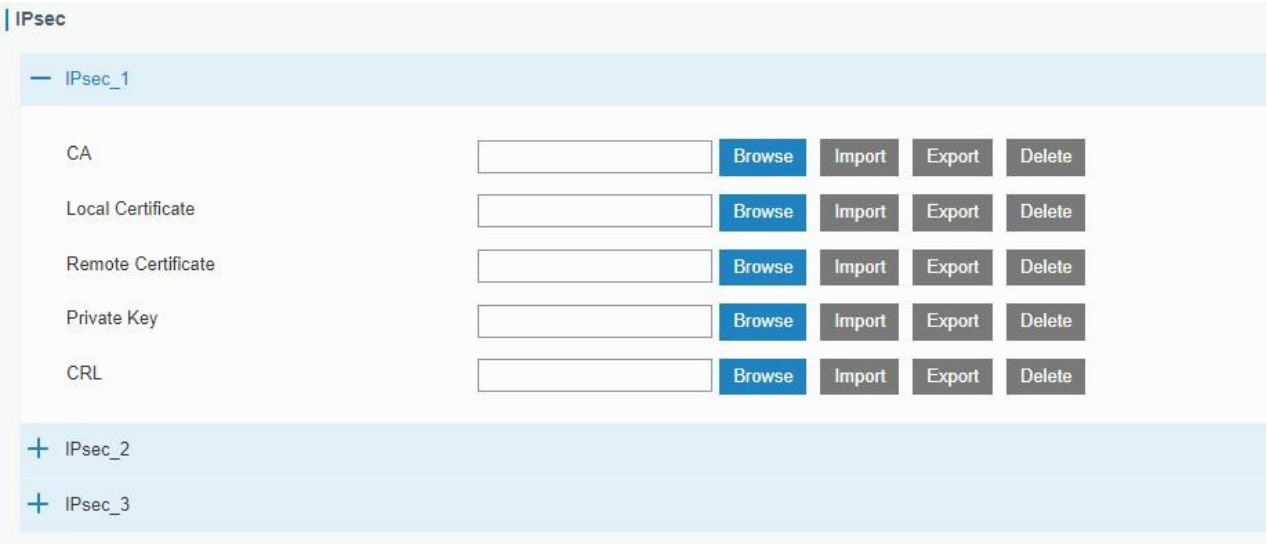


Abbildung 3-2-5-19

Abbildung 3-2-5-20

3.2.5.10 WireGuard

WireGuard ist ein extrem einfaches, aber schnelles und modernes VPN, das modernste Kryptografie nutzt. WireGuard leitet den Datenverkehr über das UDP-Protokoll weiter.

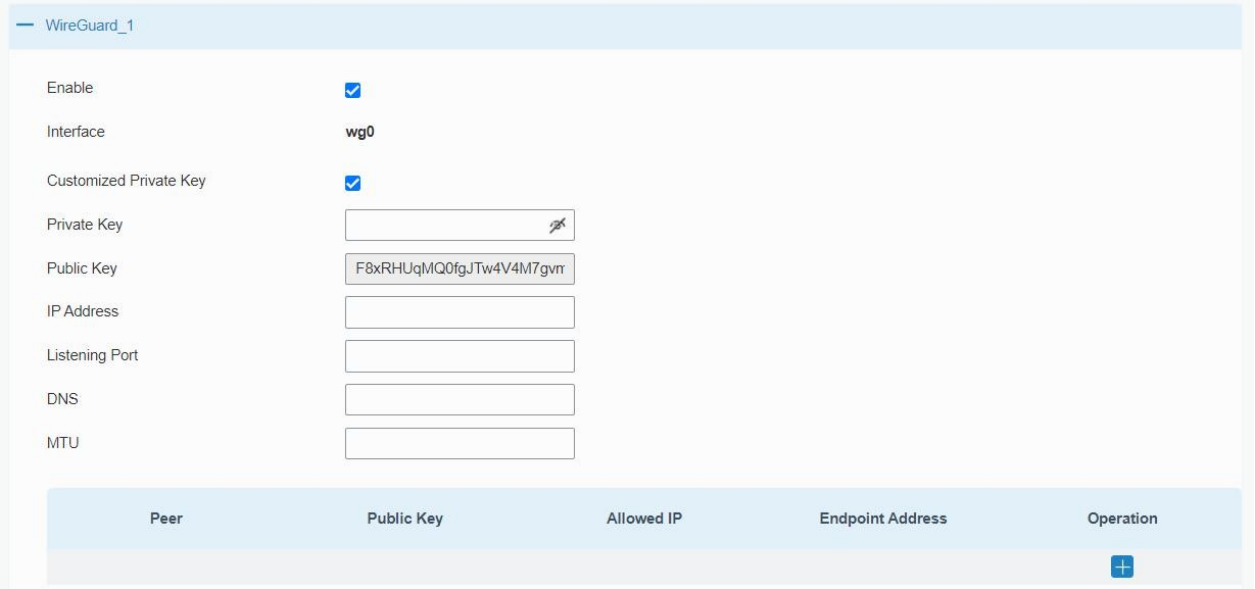


Abbildung 3-2-5-21

WireGuard	
Element	**Beschreibung**
Aktivieren	Aktivieren Sie die WireGuard-Schnittstelle. Es sind maximal 3 WireGuard-Schnittstellen sind zulässig.
Schnittstelle	Zeigt den Namen der WireGuard-Schnittstelle an.
Benutzerdefinierter privater Schlüssel	Aktivieren oder deaktivieren Sie diese Option, um den privaten Schlüssel dieser WireGuard-Schnittstelle anzupassen Schnittstelle anzupassen. Wenn diese Option deaktiviert ist, verwendet der Client den von diesem Router generierten privaten Schlüssel.
Öffentlicher Schlüssel	Zeigen Sie den mit dem privaten Schlüssel generierten öffentlichen Schlüssel an.
IP-Adresse	Legen Sie die lokale virtuelle IP-Adresse und die Netzmaske fest. Beispiel: 10.8.0.2/24
Empfangsport	Legen Sie den Port zum Senden oder Empfangen von WireGuard-Paketen fest. Die Portnummern verschiedener WireGuard-Schnittstellen sollten unterschiedlich sein.
DNS	Legen Sie die DNS-Serveradresse dieser WireGuard-Schnittstelle fest. Wenn dieses Feld leer bleibt, verwendet der Router die DNS-Serveradresse der gemeinsamen Netzwerkschnittstellen (WAN Mobilfunk usw.).
MTU	Legen Sie die maximale Übertragungseinheit dieser WireGuard-Schnittstelle fest. Wenn dieses Feld leer bleibt, verwendet der Router die MTU der gängigen Netzwerkschnittstellen (WAN Mobilfunk usw.).
Peer-Tabelle	Klicken Sie auf „+“, um WireGuard-Peers dieser WireGuard-Schnittstelle hinzuzufügen. Eine WireGuard-Schnittstelle können maximal 20 Peers hinzugefügt werden.

Tabelle 3-2-5-15 WireGuard-Parameter

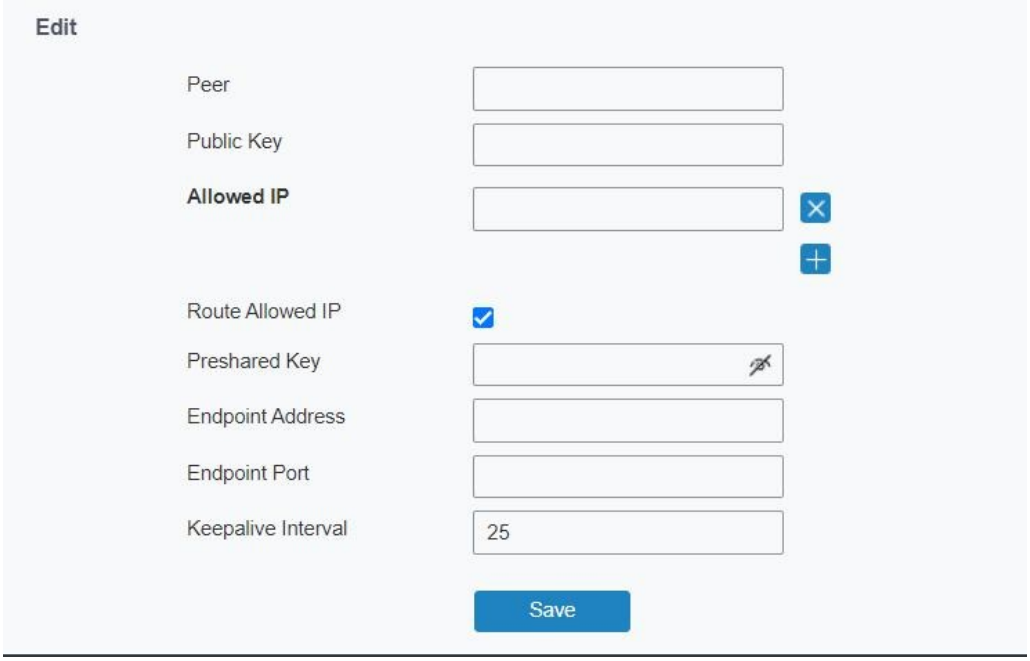


Abbildung 3-2-5-22

WireGuard-Peer	
Element	**Beschreibung**
Peer	Legen Sie einen WireGuard-Peer-Namen fest. Dieser Name sollte in diesem WireGuard-Client eindeutig sein.
Öffentlicher Schlüssel	Legen Sie den öffentlichen Schlüssel des WireGuard-Peer-Servers/Clients fest.
Zulässige IP	Legen Sie die tatsächliche IP-Adresse und Netzmaske des LAN-Netzwerks des WireGuard-Peers fest. Beispiel: 192.168.1.0/24 Ein WireGuard-Peer unterstützt das Hinzufügen von 8 zulässigen IP-Adressen.
Zulässige IP-Adresse weiterleiten	Aktivieren oder deaktivieren Sie diese Option, um statische Routings für zugelassene IP-Adressen hinzuzufügen.
Vorab geteilter Schlüssel	Legen Sie den vorab geteilten Schlüssel fest. Sowohl diese Schnittstelle als auch die Peer-Schnittstelle sollten denselben Schlüsselwert haben.
Endpunktadresse	Legen Sie die IP-Adresse oder den Domänennamen des WireGuard-Peer-Servers/Clients fest.
Endpunkt-Port	Legen Sie den Zielport des WireGuard-Peer-Servers/Clients fest.
Keepalive-Intervall	Nachdem die Verbindung hergestellt wurde, sendet diese WireGuard-Schnittstelle regelmäßig ein Heartbeat-Paket, um die Verbindung aufrechtzuerhalten. 0 bedeutet deaktiviert.

Tabelle 3-2-5-16 WireGuard-Peer-Parameter

3.2.6 IP-Passthrough

Der IP-Passthrough-Modus teilt die vom Internetprovider zugewiesene IP-Adresse mit einem einzelnen LAN-Client-Gerät, das mit dem Router verbunden ist, oder „leitet“ sie weiter.

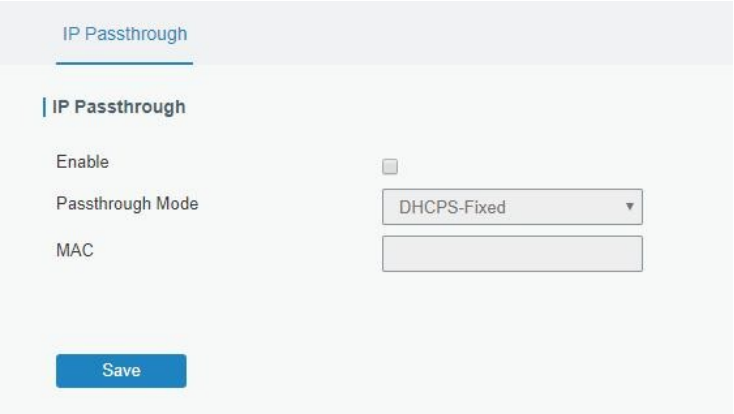


Abbildung 3-2-6-1

IP-Passthrough	
Element	**Beschreibung**
Aktivieren	IP-Passthrough aktivieren oder deaktivieren.
Passthrough-Modus	Wählen Sie den Passthrough-Modus aus DHCPS-Fixed und DHCPS-Dynamic aus.
MAC	Legen Sie die MAC-Adresse fest, wenn der Modus „DHCPS-Fixed“ ist.

Tabelle 3-2-6-1 IP-Passthrough-Parameter

3.2.7 Routing

3.2.7.1 Statisches Routing

Ein statisches Routing ist ein manuell konfigurierter Routing-Eintrag. Die Informationen zum Routing werden manuell eingegeben und nicht aus dem dynamischen Routing-Verkehr abgerufen. Nach dem Einrichten des statischen Routings wird das Paket für das angegebene Ziel an den vom Benutzer festgelegten Pfad weitergeleitet.

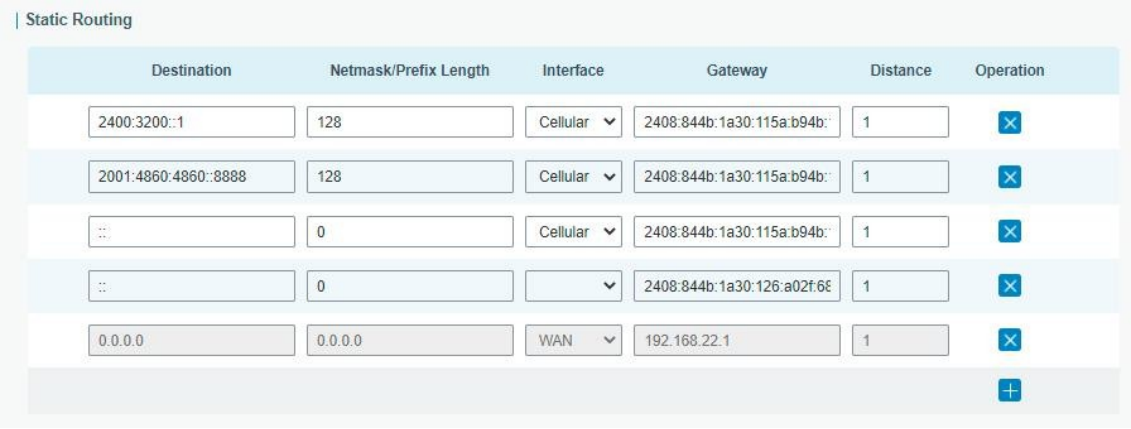


Abbildung 3-2-7-1

Statisches Routing	
Element	**Beschreibung**
Ziel	Geben Sie die Ziel-IP-Adresse ein.
Netzmaske/Präfix Länge	Geben Sie die Subnetzmaske oder Präfixlänge der Zieladresse ein.
Schnittstelle	Die Schnittstelle, über die die Daten die Zieladresse erreichen können.

Gateway	IP-Adresse des nächsten Routers, der passiert wird, bevor die Eingabedaten die Zieladresse erreichen.
Priorität	Priorität, kleinerer Wert bedeutet höhere Priorität. Bereich: 1-255.

Tabelle 3-2-7-1 Statische Routing-Parameter

3.2.7.2 RIP

RIP ist hauptsächlich für kleine Netzwerke konzipiert. RIP verwendet die Hop-Anzahl, um die Entfernung zur Zieladresse zu messen, was als Metrik bezeichnet wird. In RIP beträgt die Hop-Anzahl vom Router zu seinem direkt verbundenen Netzwerk 0 und die Hop-Anzahl des über einen Router zu erreichenden Netzwerks 1 usw. Um die Konvergenzzeit zu begrenzen, ist die angegebene Metrik von RIP eine ganze Zahl im Bereich von 0 bis 15, und eine Hop-Count von größer oder gleich 16 wird als unendlich definiert, was bedeutet, dass das Zielnetzwerk oder der Zielhost nicht erreichbar ist. Aufgrund dieser Einschränkung ist RIP nicht für große Netzwerke geeignet. Um die Leistung zu verbessern und Routing-Schleifen zu verhindern, unterstützt RIP die Split-Horizon-Funktion. RIP führt auch Routing ein, das durch andere Routing-Protokolle erhalten wird.

Jeder Router, auf dem RIP läuft, verwaltet eine Routing-Datenbank, die Routing-Einträge enthält, um alle erreichbaren Ziele zu erreichen.

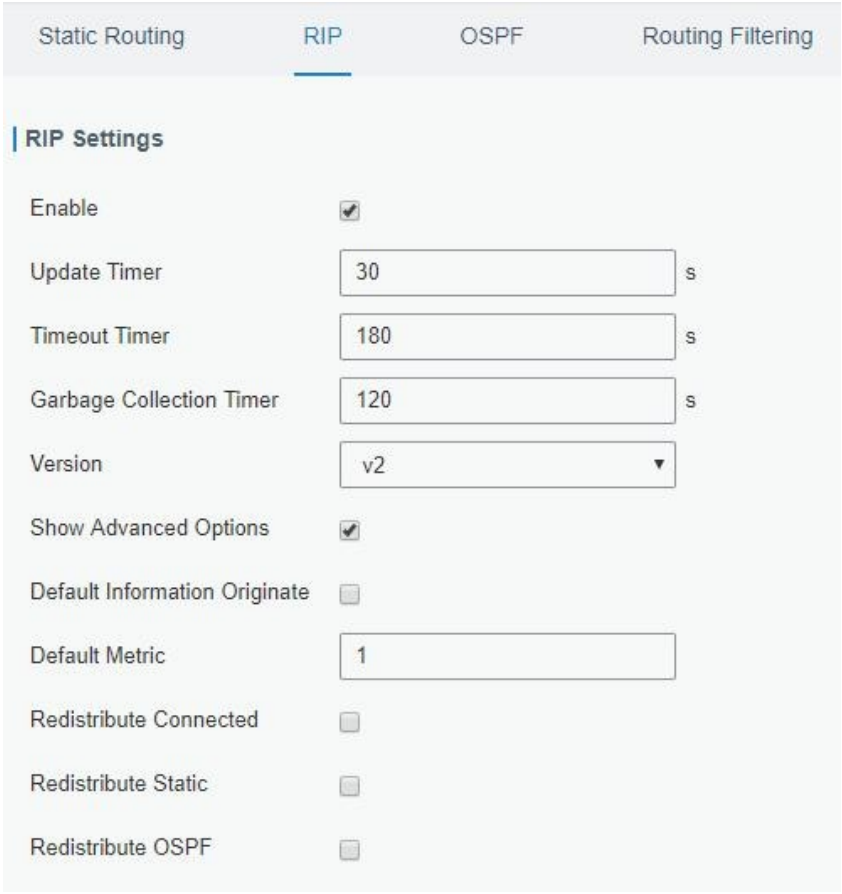


Abbildung 3-2-7-2

RIP	
Element	**Beschreibung**

Aktivieren	RIP aktivieren oder deaktivieren.
Aktualisierungs-Timer	Legt das Intervall für das Senden von Routing-Aktualisierungen fest. Bereich: 5–2147483647, in Sekunden.
Zeitüberschreitungs-Timer	Legt die Routing-Verfallszeit fest. Wenn innerhalb der Verfallszeit kein Aktualisierungspaket für ein Routing empfangen wird innerhalb der Verfallszeit empfangen wird, wird der Routing-Kostenwert des Routings in der Routing-Tabelle auf 16 gesetzt. Bereich: 5–2147483647, in Sekunden.
Garbage Collection-Timer	Es definiert den Zeitraum, in dem die Routingkosten einer Route 16 betragen, bis sie aus der Routingtabelle gelöscht wird. Während der Garbage Collection verwendet RIP 16 als Routingkosten für das Senden von Routing-Updates. Wenn die Garbage Collection zeitlich begrenzt ist und das Routing noch nicht aktualisiert wurde, wird das Routing vollständig aus der Routingtabelle entfernt. Bereich: 5-2147483647, in Sekunden.
Version	RIP-Version. Die Optionen sind v1 und v2.
Erweiterte Einstellungen	
Standardinformationen erstellen	Standardinformationen werden veröffentlicht, wenn diese Funktion aktiviert ist.
Standardmetrik	Die Standardkosten für den Router, um das Ziel zu erreichen. Bereich: 0–16
Verbundene neu verteilen	Zum Aktivieren ankreuzen.
Metrik	Legen Sie die Metrik fest, nachdem „Verbundene neu verteilen“ aktiviert wurde. Bereich: 0–16.
Statisch neu verteilen	Aktivieren Sie diese Option.
Metrik	Legen Sie die Metrik fest, nachdem „Redistribute Static“ (Statisch neu verteilen) aktiviert wurde. Bereich: 0–16.
OSPF neu verteilen	Aktivieren Sie diese Option.
Metrik	Legen Sie die Metrik fest, nachdem „OSPF neu verteilen“ aktiviert wurde. Bereich: 0–16.

Tabelle 3-2-7-2 RIP-Parameter

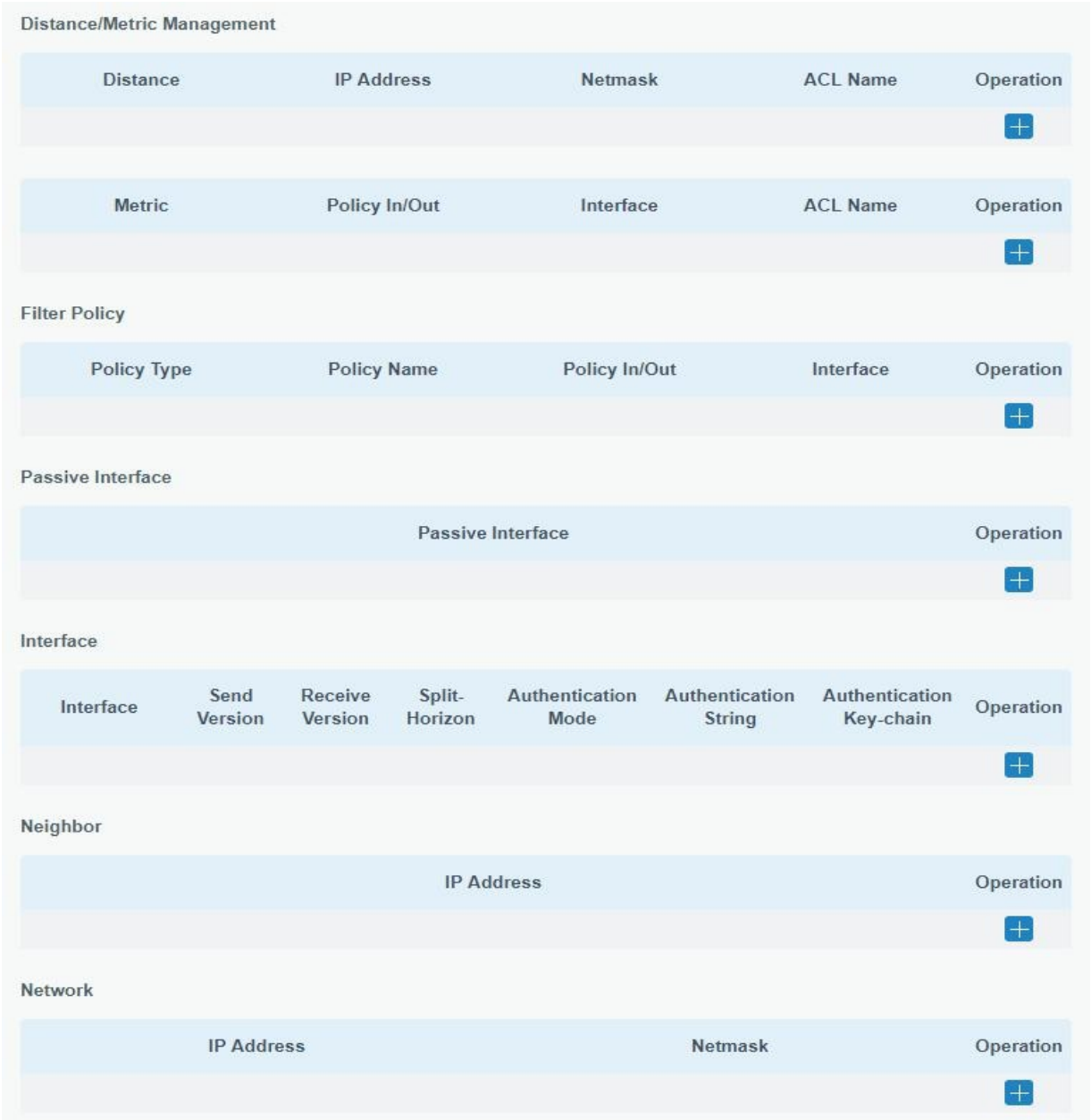


Abbildung 3-2-7-3

Element	Beschreibung
Entfernungs-/Metrikverwaltung	
Entfernung	Legen Sie die administrative Entfernung fest, die eine RIP-Route lernt. Bereich: 1–255
IP-Adresse	Legen Sie die IP-Adresse der RIP-Route fest.
Netzmaske	Legen Sie die Netzmaske der RIP-Route fest.
ACL-Name	Legen Sie den ACL-Namen der RIP-Route fest.
Metrik	Die Metrik der empfangenen oder gesendeten Route von der Schnittstelle. Bereich: 0–16.
Richtlinie Ein/Aus	Wählen Sie zwischen „in" und „out".

Schnittstelle	Wählen Sie die Schnittstelle der Route aus.
ACL-Name	Name der Zugriffskontrollliste der Routing-Strategie.
Filterrichtlinie	
Richtlinientyp	Wählen Sie zwischen „access-list“ und „prefix-list“.
Name der Richtlinie	Benutzerdefinierter Name der Präfixliste.
Richtlinie Ein/Aus	Wählen Sie zwischen „in“ und „out“.
Schnittstelle	Wählen Sie die Schnittstelle aus „cellular0“, „WAN“ und „Bridge0“ aus.
Passive Schnittstelle	
Passive Schnittstelle	Wählen Sie die Schnittstelle aus „cellular0“, „WAN“ und „Bridge0“ aus.
Schnittstelle	
Schnittstelle	Wählen Sie die Schnittstelle aus „cellular0“, „WAN“ und „Bridge0“ aus.
Version senden	Wählen Sie zwischen „default“, „v1“ und „v2“.
Empfangsversion	Wählen Sie zwischen „default“, „v1“ und „v2“.
Split-Horizon	Wählen Sie zwischen „Aktivieren“ und „Deaktivieren“.
Authentifizierungsmodus	Wählen Sie zwischen „Text“ und „md5“.
Authentifizierungszeichenfolge	Der Authentifizierungsschlüssel für die Paketinteraktion in RIPV2.
Authentifizierung Schlüsselkette	Der Authentifizierungsschlüsselbund für die Paketinteraktion in RIPV2.
Nachbar	
IP-Adresse	Legen Sie die IP-Adresse des RIP-Nachbarn manuell fest.
Netzwerk	
IP-Adresse	Die IP-Adresse der Schnittstelle für die RIP-Veröffentlichung.
Netzmaske	Die Netzmaske der Schnittstelle für die RIP-Veröffentlichung.

Tabelle 3-2-7-3

3.2.7.3 OSPF

OSPF, kurz für Open Shortest Path First, ist ein Linkstatus, der auf dem von der IETF entwickelten Interior Gateway Protocol basiert.

Wenn ein Router das OSPF-Protokoll ausführen möchte, sollte eine Router-ID vorhanden sein, die manuell konfiguriert werden kann. Wenn keine Router-ID konfiguriert ist, wählt das System automatisch eine IP-Adresse der Schnittstelle als Router-ID aus. Die Auswahlreihenfolge ist wie folgt:

- Wenn eine Loopback-Schnittstellenadresse konfiguriert ist, wird die zuletzt konfigurierte IP-Adresse der Loopback-Schnittstelle als Router-ID verwendet.
- Wenn keine Loopback-Schnittstellenadresse konfiguriert ist, wählt das System die Schnittstelle mit der größten IP-Adresse als Router-ID aus.

Fünf Arten von OSPF-Paketen:

- **Hello-Paket**

- **DD-Paket** (Database Description Packet)
- **LSR-Paket** (Link-State Request Packet)
- **LSU-Paket** (Link-State Update Packet)
- **LSAck-Paket** (Link-State Acknowledgment Packet)

Nachbar und Nachbarschaft

Nach dem Start des OSPF-Routers sendet dieser Hello-Pakete über die OSPF-Schnittstelle. Nach dem Empfang eines Hello-Pakets überprüft der OSPF-Router die im Paket definierten Parameter. Wenn diese übereinstimmen, wird eine Nachbarbeziehung hergestellt. Nicht alle übereinstimmenden Seiten in einer Nachbarbeziehung können eine Adjazenzbeziehung bilden. Dies wird durch den Netzwerktyp bestimmt. Nur wenn beide Seiten erfolgreich DD-Pakete austauschen und eine LSDB-Synchronisation erreicht wird, kann eine echte Nachbarschaftsbeziehung hergestellt werden. LSA beschreibt die Netzwerktopologie um einen Router herum, LSDB beschreibt die gesamte Netzwerktopologie.

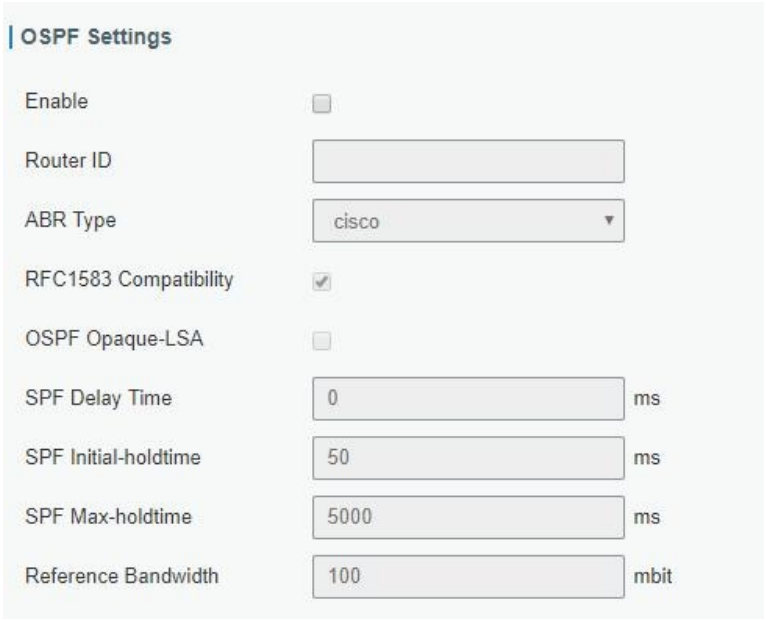


Abbildung 3-2-7-4

OSPF	
Element	**Beschreibung**
Aktivieren	OSPF aktivieren oder deaktivieren.
Router-ID	Router-ID (IP-Adresse) des ursprünglichen LSA.
ABR-Typ	Wählen Sie zwischen Cisco, IBM, Standard und Shortcut.
RFC1583-Kompatibilität	Aktivieren/Deaktivieren.
OSPF Opaque-LSA	Aktivieren/Deaktivieren LSA: ein grundlegendes Kommunikationsmittel des OSPF-Routingprotokolls für das Internetprotokoll (IP).
SPF-Verzögerungszeit	Legen Sie die Verzögerungszeit für OSPF-SPF-Berechnungen fest. Bereich: 0-6000000, in Millisekunden.

SPF-Anfangs-Haltezeit	Legen Sie die Initialisierungszeit von OSPF SPF fest. Bereich: 0-6000000, in Millisekunden.
SPF-Maximalhaltezeit	Legen Sie die maximale Zeit für OSPF SPF fest. Bereich: 0-6000000, in Millisekunden.
Referenzbandbreite	Bereich: 1-4294967, in Mbit.

Tabelle 3-2-7-4 OSPF-Parameter

Abbildung 3-2-7-5

Element	Beschreibung
Schnittstelle	
Schnittstelle	Wählen Sie die Schnittstelle aus „cellular0", „WAN" und „Bridge0" aus.
Hello-Intervall (s)	Sendeintervall für Hello-Pakete. Wenn die Hello-Zeit zwischen zwei benachbarten Routern unterschiedlich ist, kann keine Nachbarbeziehung hergestellt werden. Bereich: 1-65535.
Dead Interval (s)	Totzeit. Wenn innerhalb der Totzeit kein Hello-Paket von den Nachbarn empfangen wird, gilt der Nachbar als ausgefallen. Wenn die Totzeiten zweier benachbarter Router unterschiedlich sind, kann keine Nachbarbeziehung hergestellt werden hergestellt werden.
Wiederholungsintervall (s)	Wenn der Router seinem Nachbarn eine LSA meldet, muss er eine Bestätigung senden. Wenn innerhalb des Wiederholungsintervalls kein Bestätigungspaket empfangen wird, wird diese LSA erneut an den Nachbarn gesendet. Bereich: 3-65535.
Übertragungsverzögerung (s)	Die Übertragung von OSPF-Paketen über die Verbindung dauert einige Zeit. Daher sollte vor der Übertragung eine bestimmte Verzögerungszeit zur Alterungszeit der LSA hinzugefügt werden. Diese Konfiguration muss bei Verbindungen mit geringer Geschwindigkeit besonders berücksichtigt werden. Bereich: 1-65535.
Erweiterte Optionen der Schnittstelle	
Schnittstelle	Schnittstelle auswählen.
Netzwerk	Wählen Sie den OSPF-Netzwerktyp aus.
Kosten	Legen Sie die Kosten für die Ausführung von OSPF auf einer Schnittstelle fest. Bereich: 1-65535.
Priorität	Legen Sie die OSPF-Priorität der Schnittstelle fest. Bereich: 0-255.
Authentifizierung	Legen Sie den Authentifizierungsmodus fest, der vom OSPF-Bereich verwendet wird.

	Einfach: Ein einfaches Authentifizierungskennwort sollte konfiguriert und erneut bestätigt werden. MD5: MD5-Schlüssel und -Passwort sollten konfiguriert und erneut bestätigt werden.
Schlüssel-ID	Es wird nur wirksam, wenn MD5 ausgewählt ist. Bereich 1-255.
Schlüssel	Der Authentifizierungsschlüssel für die OSPF-Paketinteraktion.

Tabelle 3-2-7-5 OSPF-Parameter

Abbildung 3-2-7-6

Element	Beschreibung
Passive Schnittstelle	
Passive Schnittstelle	Wählen Sie die Schnittstelle aus „cellular0“, „WAN“ und „Bridge0“ aus.
Netzwerk	
IP-Adresse	Die IP-Adresse des lokalen Netzwerks.
Netzmaske	Die Netzmaske des lokalen Netzwerks.
Bereichs-ID	Die Bereichs-ID des Routers des ursprünglichen LSA.
Bereich	
Bereichs-ID	Legen Sie die ID des OSPF-Bereichs (IP-Adresse) fest.
Bereich	Wählen Sie zwischen „Stub“ und „NSSA“. Der Backbone-Bereich (Bereichs-ID 0.0.0.0) kann nicht als „Stub“ oder „NSSA“ festgelegt werden.
Keine Zusammenfassung	Verhindern Sie die Zusammenfassung von Routen.
Authentifizierung	Wählen Sie die Authentifizierung aus „simple“ und „md5“ aus.

Tabelle 3-2--7-6 OSPF-Parameter

Abbildung 3-2-7-7

Erweiterte Optionen für den Bereich	
Element	**Beschreibung**
Bereichsbereich	
Bereichs-ID	Die Bereichs-ID der Schnittstelle, wenn OSPF ausgeführt wird (IP-Adresse).
IP-Adresse	Legen Sie die IP-Adresse fest.
Netzmaske	Legen Sie die Netzmaske fest.
Keine Bekanntgabe	Verhindern Sie, dass die Routeninformationen zwischen verschiedenen Bereichen bekannt gegeben werden.
Kosten	Bereich: 0-16777215
Bereichsfilter	
Gebiets-ID	Wählen Sie eine Bereichs-ID für den Bereichsfilter aus.
Filtertyp	Wählen Sie zwischen „Importieren“, „Exportieren“, „Ein-Filtern“ und „Aus-Filtern“.
ACL-Name	Geben Sie einen ACL-Namen ein, der auf der Webseite „Routing > Routing-Filterung“ festgelegt ist.
Virtuelle Bereichsverbindung	
Bereichs-ID	Legen Sie die ID-Nummer des OSPF-Bereichs fest.
ABR-Adresse	ABR ist der Router, der mit mehreren äußeren Bereichen verbunden ist.
Authentifizierung	Wählen Sie zwischen „simple“ und „md5“.
Schlüssel-ID	Dies ist nur wirksam, wenn MD5 ausgewählt ist. Bereich 1-15.
Schlüssel	Der Authentifizierungsschlüssel für die OSPF-Paketinteraktion.
Hello-Intervall	Legen Sie das Intervall für das Senden von Hello-Paketen über die Schnittstelle fest. Bereich: 1-65535
Dead-Intervall	Die Dead-Intervallzeit für das Senden von Hello-Paketen über die Schnittstelle. Bereich: 1-65535
Wiederholen Intervall	Die Intervallzeit für die erneute Übertragung von LSA. Bereich: 1-65535.
Übertragungsverzögerung	Die Verzögerungszeit für die LSA-Übertragung. Bereich: 1-65535.

Tabelle 3-2-7-7 OSPF-Parameter

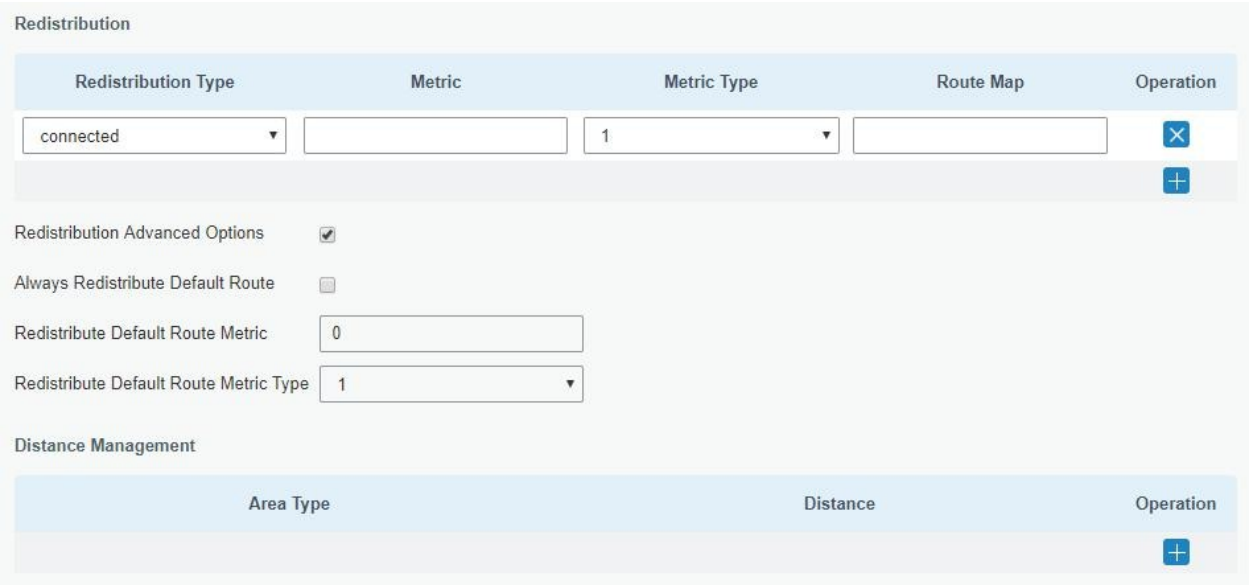


Abbildung 3-2-7-8

Element	Beschreibung
Umverteilung	
Umverteilungstyp	Wählen Sie zwischen „verbunden“, „statisch“ und „rip“.
Metrik	Die Metrik des Umverteilungsrouters. Bereich: 0-16777214.
Metriktyp	Wählen Sie den Metriktyp aus „1“ und „2“ aus.
Routenplan	Wird hauptsächlich zur Verwaltung der Route für die Umverteilung verwendet.
Erweiterte Optionen für die Umverteilung	
Immer neu verteilen Standardroute	Standardroute für die Umverteilung nach dem Start senden.
Standard neu verteilen Routenmetrik	Standard-Routenmetrik für die Neuverteilung senden. Bereich: 0-16777214.
Standard neu verteilen Routenmetriktyp	Wählen Sie zwischen „0“, „1“ und „2“.
Entfernungsmanagement	
Gebietstyp	Wählen Sie zwischen „innerhalb des Bereichs“, „zwischen Bereichen“ und „außerhalb“.
Entfernung	Legen Sie die OSPF-Routing-Entfernung für das Bereichslernen fest. Bereich: 1-255.

Tabelle 3-2-7-8 OSPF-Parameter

3.2.7.4 Routing-Filterung

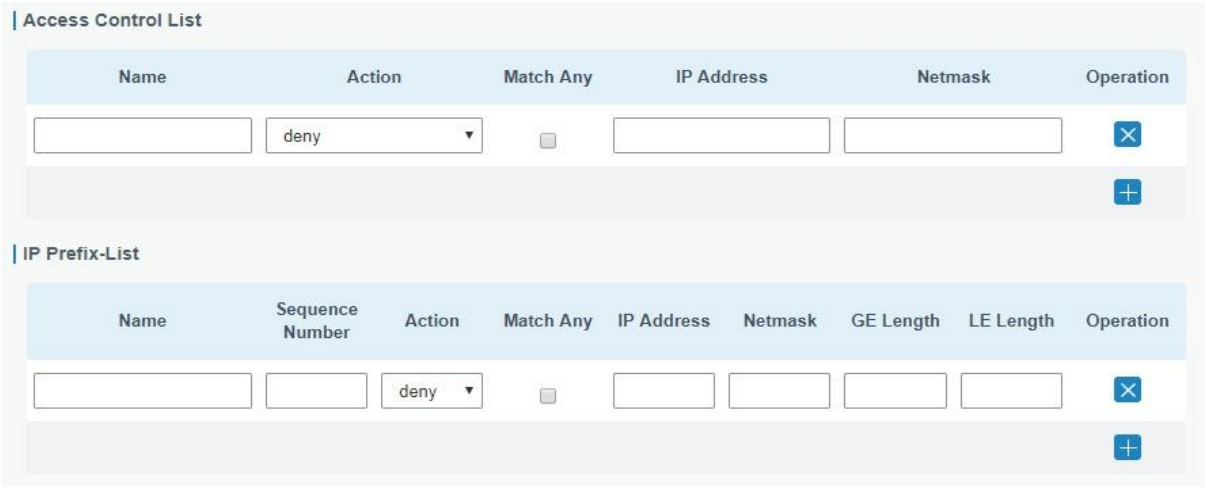


Abbildung 3-2-7-9

Routing-Filterung	
Element	**Beschreibung**
Zugriffskontrollliste	
Name	Benutzerdefinierter Name muss mit einem Buchstaben beginnen. Nur Buchstaben, Ziffern und Unterstrich (_) sind erlaubt.
Aktion	Wählen Sie zwischen „zulassen" und „verweigern".
Beliebig	Es ist nicht erforderlich, die IP-Adresse und die Subnetzmaske festzulegen.
IP-Adresse	Benutzerdefiniert.
Netzmaske	Benutzerdefiniert.
IP-Präfixliste	
Name	Benutzerdefinierter Name muss mit einem Buchstaben beginnen. Es sind nur Buchstaben, Ziffern und Unterstriche (_) sind zulässig.
Sequenz Nummer	Eine Präfixnamenliste kann mit mehreren Regeln abgeglichen werden. Eine Regel wird mit eine Sequenznummer ab. Bereich: 1-4294967295.
Aktion	Wählen Sie zwischen „zulassen" und „verweigern".
Beliebige Übereinstimmung	Es ist nicht erforderlich, die IP-Adresse, die Subnetzmaske, die FE-Länge und die LE-Länge festzulegen.
IP-Adresse	Benutzerdefiniert.
Netzmaske	Benutzerdefiniert.
FE-Länge	Geben Sie die Mindestanzahl an Maskenbits an, die übereinstimmen müssen. Bereich: 0-32.
LE-Länge	Geben Sie die maximale Anzahl von Maskenbits an, die übereinstimmen müssen. Bereich: 0-32.

Tabelle 3-2-7-9 Routing-Filterparameter

3.2.8 VRRP

Das Virtual Router Redundancy Protocol (VRRP) ist ein Computernetzwerkprotokoll, das die automatische Zuweisung verfügbarer Internetprotokoll (IP)-Router für teilnehmende Hosts ermöglicht. Dies erhöht die Verfügbarkeit und Zuverlässigkeit von Routing-Pfaden durch die automatische Auswahl von Standard-Gateways in einem IP-Subnetz.

Die Erhöhung der Anzahl der Exit-Gateways ist eine gängige Methode zur Verbesserung der Systemzuverlässigkeit. VRRP fügt eine Gruppe von Routern, die die Gateway-Funktion übernehmen, zu einer Backup-Gruppe hinzu, um einen virtuellen Router zu bilden. Der Wahlmechanismus von VRRP entscheidet, welcher Router die Weiterleitungsaufgabe übernimmt, und

Der Host im LAN muss lediglich das Standard-Gateway für den virtuellen Router konfigurieren.

In VRRP müssen Router Ausfälle des virtuellen Master-Routers erkennen können. Zu diesem Zweck sendet der virtuelle Master-Router Multicast-„Alive"-Ankündigungen an die virtuellen Backup-Router in derselben VRRP-Gruppe.

Der VRRP-Router mit der höchsten Nummer wird zum virtuellen Master-Router. Die VRRP-Router-Nummern reichen von 1 bis 255, wobei wir in der Regel 255 für die höchste Priorität und 100 für die Sicherung verwenden.

Wenn der aktuelle virtuelle Master-Router eine Ankündigung von einem Gruppenmitglied (Router-ID) mit einer höheren Priorität erhält, übernimmt dieses die Vorrangstellung und wird zum virtuellen Master-Router.

VRRP hat die folgenden Eigenschaften:

- Der virtuelle Router mit einer IP-Adresse wird als virtuelle IP-Adresse bezeichnet. Für den Host im LAN ist es lediglich erforderlich, die IP-Adresse des virtuellen Routers zu kennen und diese als Adresse des nächsten Hops der Standardroute festzulegen.
- Der Netzwerk-Host kommuniziert über diesen virtuellen Router mit dem externen Netzwerk.
- Ein Router wird aus der Gruppe der Router anhand seiner Priorität ausgewählt, um die Gateway-Funktion zu übernehmen. Andere Router werden als Backup-Router verwendet, um im Falle einer Störung die Aufgaben des Gateway-Routers zu übernehmen und so eine unterbrechungsfreie Kommunikation zwischen dem Host und dem externen Netzwerk zu gewährleisten.

Wenn sich die mit dem Uplink verbundene Schnittstelle im Status „Down" oder „Removed" befindet, senkt der Router aktiv seine Priorität, sodass die Priorität anderer Router in der Backup-Gruppe höher ist. Somit wird der Router mit der höchsten Priorität zum Gateway für die Übertragungsaufgabe.

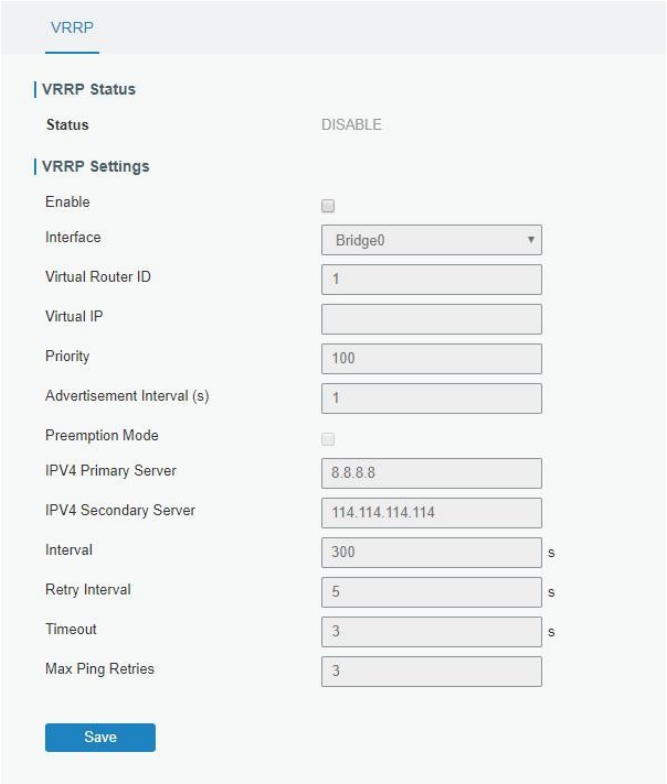


Abbildung 3-2-8-1

VRRP		
Element	**Beschreibung**	**Standard**
Aktivieren	VRRP aktivieren oder deaktivieren.	Deaktivieren
Schnittstelle	Wählen Sie die Schnittstelle des virtuellen Routers aus.	Keine

ID des virtuellen Routers	Benutzerdefinierte ID des virtuellen Routers. Bereich: 1-255.	Keine
Virtuelle IP	Legen Sie die IP-Adresse des virtuellen Routers fest.	Keine
Priorität	Der VRRP-Prioritätsbereich liegt zwischen 1 und 254 (eine höhere Zahl bedeutet eine höhere Priorität). Der Router mit der höheren Priorität wird mit größerer wahrscheinlich zum Gateway-Router.	100
Anzeigeintervall (s)	Zeitintervall für die Übertragung von Heartbeat-Paketen zwischen Router in der virtuellen IP-Gruppe. Bereich: 1-255.	1
Präemptionsmodus	Wenn der Router im Präventionsmodus arbeitet,sendet er, sobald er feststellt, dass seine eigene Priorität höher ist als die des aktuellen Gateway-Routers, ein VRRP-Benachrichtigungspaket, was zu einer Neuwahl des Gateway-Routers und schließlich zum Ersatz des ursprünglichen Gateway-Routers führt. Dementsprechend wird der ursprüngliche Gateway-Router zum Backup-Router.	Deaktivieren
IPV4-Primärserver	Der Router sendet ein ICMP-Paket an die IP-Adresse oder den Host , um festzustellen, ob die Internetverbindung noch verfügbar ist oder nicht.	8.8.8.8
Sekundärer IPV4-Server	Der Router versucht, den sekundären Servernamen anzupingen, wenn der primäre Sekundärserver nicht verfügbar ist.	223.5.5.5
Intervall	Zeitintervall (in Sekunden) zwischen zwei Pings.	300
Wiederholungsintervall	Legen Sie das Intervall für Ping-Wiederholungsversuche fest. Wenn ein Ping fehlschlägt, wiederholt der Router den Ping wiederholen.	5
Zeitlimit	Die maximale Zeit, die der Router auf eine Antwort auf eine Ping-Anfrage wartet. Wenn er innerhalb der in diesem Feld definierten Zeit keine Antwort erhält, wird die Ping-Anfrage als fehlgeschlagen betrachtet.	3
Maximale Anzahl von Ping-Wiederholungen	Die Anzahl der Wiederholungsversuche, die der Router beim Senden von Ping-Anfragen unternimmt, bis er die Verbindung als fehlgeschlagen betrachtet wird.	3

Tabelle 3-2-8-1 VRRP-Parameter

Beispiel für die zugehörige Konfiguration

VRRP-Anwendungsbeispiel

3.2.9 DDNS

Dynamic DNS (DDNS) ist eine Methode, die einen Nameserver im Domain Name System automatisch aktualisiert, wodurch Benutzer eine dynamische IP-Adresse mit einem statischen Domainnamen verknüpfen können.
DDNS dient als Client-Tool und muss mit dem DDNS-Server koordiniert werden. Vor Beginn der Konfiguration muss sich der Benutzer auf der Website eines geeigneten Domainnamenanbieters registrieren und einen Domainnamen beantragen.

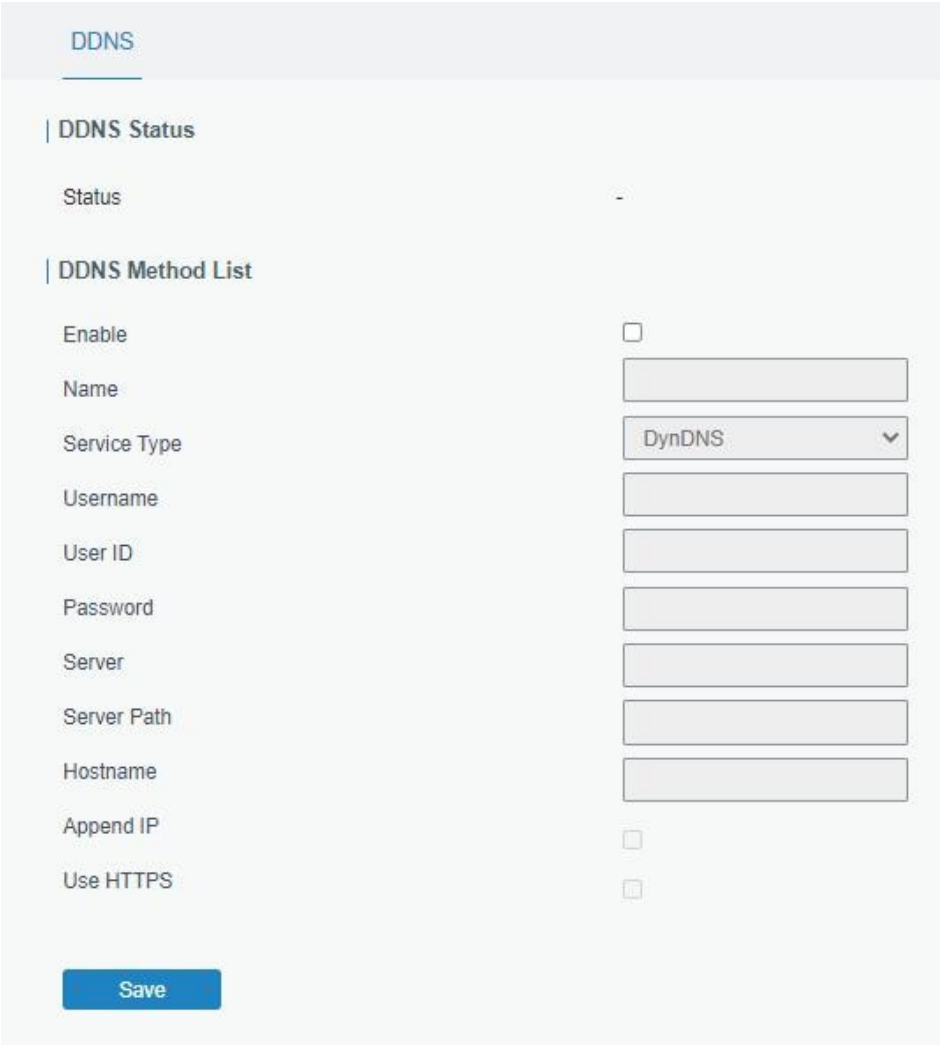


Abbildung 3-2-9-1

DDNS	
Element	**Beschreibung**
Aktivieren	DDNS aktivieren/deaktivieren.
Name	Geben Sie dem DDNS einen aussagekräftigen Namen.
Schnittstelle	Legen Sie die mit dem DDNS gebündelte Schnittstelle fest.
Diensttyp	Wählen Sie den DDNS-Dienstanbieter aus.
Benutzername	Geben Sie den Benutzernamen für die DDNS-Registrierung ein.
Benutzer-ID	Geben Sie die Benutzer-ID des benutzerdefinierten DDNS-Servers ein.
Passwort	Geben Sie das Passwort für die DDNS-Registrierung ein.
Server	Geben Sie den Namen des DDNS-Servers ein.
Serverpfad	Standardmäßig wird der Hostname an den Pfad angehängt.
Hostname	Geben Sie den Hostnamen für DDNS ein.
IP anhängen	Fügen Sie Ihre aktuelle IP-Adresse zum DDNS-Server-Update-Pfad hinzu.
Verwenden Sie HTTPS	Aktivieren Sie HTTPS für einige DDNS-Anbieter.

Tabelle 3-2-9-1 DDNS-Parameter

3.3 System

3.3.1 Allgemeine Einstellungen

3.3.1.1 Allgemein

Zu den allgemeinen Einstellungen gehören Systeminformationen und HTTPS-Zertifikate.

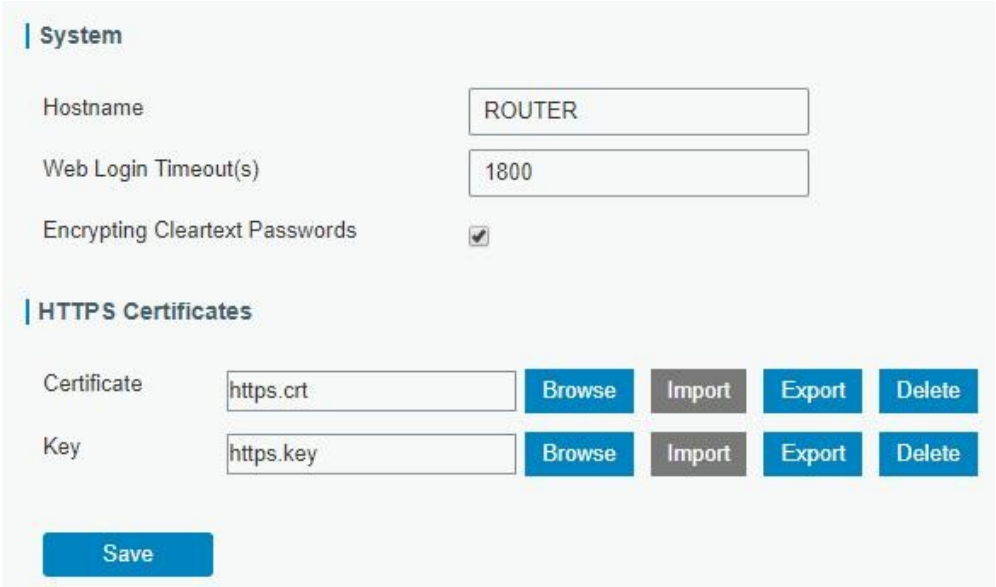


Abbildung 3-3-1-1

Allgemein		
Element	**Beschreibung**	**Standard**
System		
Hostname	Benutzerdefinierter Router-Name,muss mit einem Buchstaben beginnen.	ROUTER
Zeitlimit für Web-Anmeldung (s)	Bei Ablaufdes Zeitlimits müssen Sie sich erneut anmelden. Bereich: 100-3600.	1800
Verschlüsselung von Klartext Passwörter	Diese Funktion verschlüsselt alle Klartext-Passwörter in Verschlüsselungspasswörter.	Aktivieren
HTTPS-Zertifikate		
Zertifikat	Klicken Sie auf die Schaltfläche „Durchsuchen“, wählen Sie die Zertifikatsdatei auf dem PC aus und klicken Sie dann auf die Schaltfläche „Importieren“, um die Datei auf den Router hochzuladen. Durch Klicken auf die Schaltfläche „Exportieren“ wird die Datei auf den PC exportiert. Klicken Sie auf die Schaltfläche „Löschen“, um die Datei zu löschen.	--
Schlüssel	Klicken Sie auf die Schaltfläche „Durchsuchen“, wählen Sie die Schlüsseldatei auf dem PC aus und klicken Sie dann auf die Schaltfläche „Importieren“, um die Datei auf den Router hochzuladen. Durch Klicken auf die Schaltfläche „Exportieren“ wird die Datei auf den PC exportiert. Durch Klicken auf die Schaltfläche „Löschen“ wird die Datei gelöscht.	--

Tabelle 3-3-1-1 Allgemeine Einstellungsparameter

3.3.1.2 Systemzeit

In diesem Abschnitt wird erläutert, wie Sie die Systemzeit einschließlich Zeitzone und Zeitsynchronisationstyp einstellen.

Hinweis: Um sicherzustellen, dass der Router mit der richtigen Uhrzeit läuft, wird empfohlen, bei der Konfiguration des Routers die Systemzeit einzustellen

bei der Konfiguration des Routers die Systemzeit einzustellen.

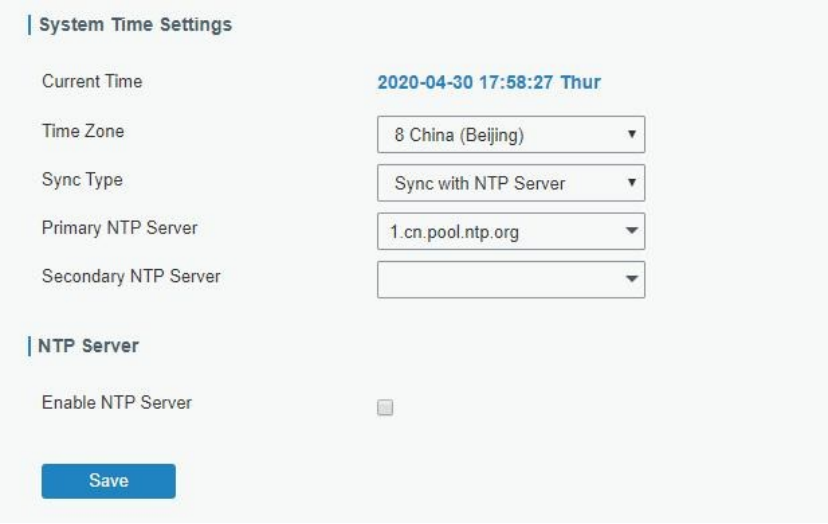


Abbildung 3-3-1-2

Systemzeit	
Element	**Beschreibung**
Aktuelle Uhrzeit	Zeigt die aktuelle Systemzeit an.
Zeitzone	Klicken Sie auf die Dropdown-Liste, um die Zeitzone auszuwählen, in der Sie sich befinden.
Synchronisierungstyp	Klicken Sie auf die Dropdown-Liste, um den Synchronisierungstyp auszuwählen. **Mit Browser synchronisieren:** Synchronisieren Sie die Zeit mit dem Browser. **Mit NTP-Server synchronisieren:** Zeit mit NTP-Server synchronisieren. **Manuell einrichten:** Konfigurieren Sie die Zeit manuell. **GPS-Zeitsynchronisierung:** Synchronisieren Sie die Zeit stündlich mit GPS. Dies ist nur bei der GPS-Version möglich. Stellen Sie sicher, dass GPS unter **„Service > GPS > GPS“** aktiviert ist. **Mit Mobilfunkbetreiber synchronisieren:** Synchronisieren Sie die Uhrzeit mit dem Mobilfunkbetreiber. Dies funktioniert nur, wenn das Gerät beim Mobilfunknetz registriert ist.
Mit Browser synchronisieren	Synchronisieren Sie die Zeit mit dem Browser.
Browser-Zeit	Zeigt die aktuelle Zeit des Browsers an.
Manuell einrichten	Konfigurieren Sie die Systemzeit manuell.
GPS-Zeit Synchronisierung	Synchronisieren Sie die Zeit mit GPS.
Primärer NTP-Server	Geben Sie die IP-Adresse oder den Domänennamen des primären NTP-Servers ein.
Sekundärer NTP-Server	Geben Sie die IP-Adresse oder den Domänennamen des sekundären NTP-Servers ein.
NTP-Server	
NTP-Server aktivieren	Der NTP-Client im Netzwerk kann eine Zeitsynchronisation mit dem Router durchführen , nachdem diese Option aktiviert wurde.

Tabelle 3-3-1-2 Systemzeitparameter

3.3.1.3 E-Mail

SMTP,kurz für Simple Mail Transfer Protocol, ist ein TCP/IP-Protokoll, das zum Senden und Empfangen von

. In diesem Abschnitt wird beschrieben, wie Sie E-Mail-Einstellungen konfigurieren und E-Mail-Gruppen für Alarme und Ereignisse hinzufügen.

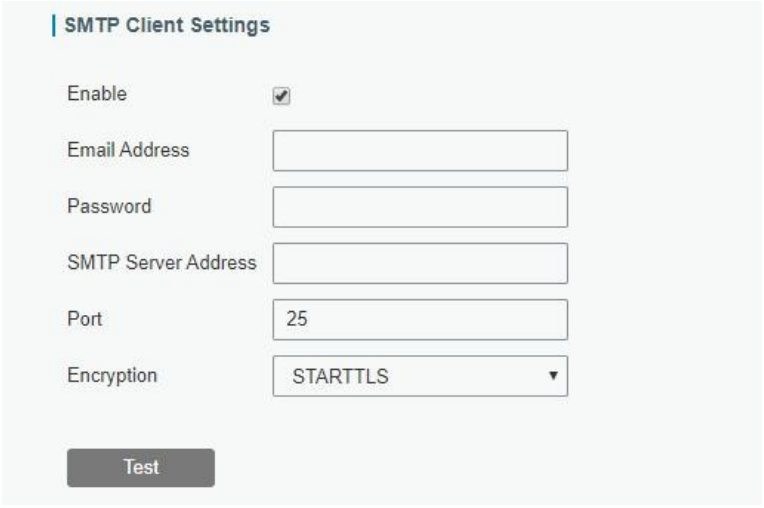


Abbildung 3-3-1-3

SMTP-Client-Einstellungen	
Element	**Beschreibung**
Aktivieren	Aktivieren oder deaktivieren Sie die SMTP-Client-Funktion.
E-Mail-Adresse	Geben Sie das E-Mail-Konto des Absenders ein.
Passwort	Geben Sie das E-Mail-Passwort des Absenders ein.
SMTP-Serveradresse	Geben Sie den Domainnamen des SMTP-Servers ein.
Port	Geben Sie den SMTP-Server-Port ein. Bereich: 1-65535.
Verschlüsselung	Auswahlmöglichkeiten: Keine, TLS/SSL, STARTTLS. **Keine:** Keine Verschlüsselung. Der Standardport ist 25. **STARTTLS:** STARTTLS ist eine Methode, um eine bestehende unsichere Verbindung mithilfe von SSL/TLS zu einer sicheren Verbindung zu machen. Der Standardport ist 587. **TLS/SSL:** Sowohl SSL als auch TLS bieten eine Möglichkeit, einen Kommunikationskanal zwischen zwei Computern (z. B. Ihrem Computer und unserem Server) zu verschlüsseln. TLS ist der Nachfolger von SSL, und die Begriffe SSL und TLS werden synonym verwendet, es sei denn, Sie beziehen sich auf eine bestimmte Version des Protokolls. Der Standardport ist 465.

Tabelle 3-3-1-3 SMTP-Einstellung

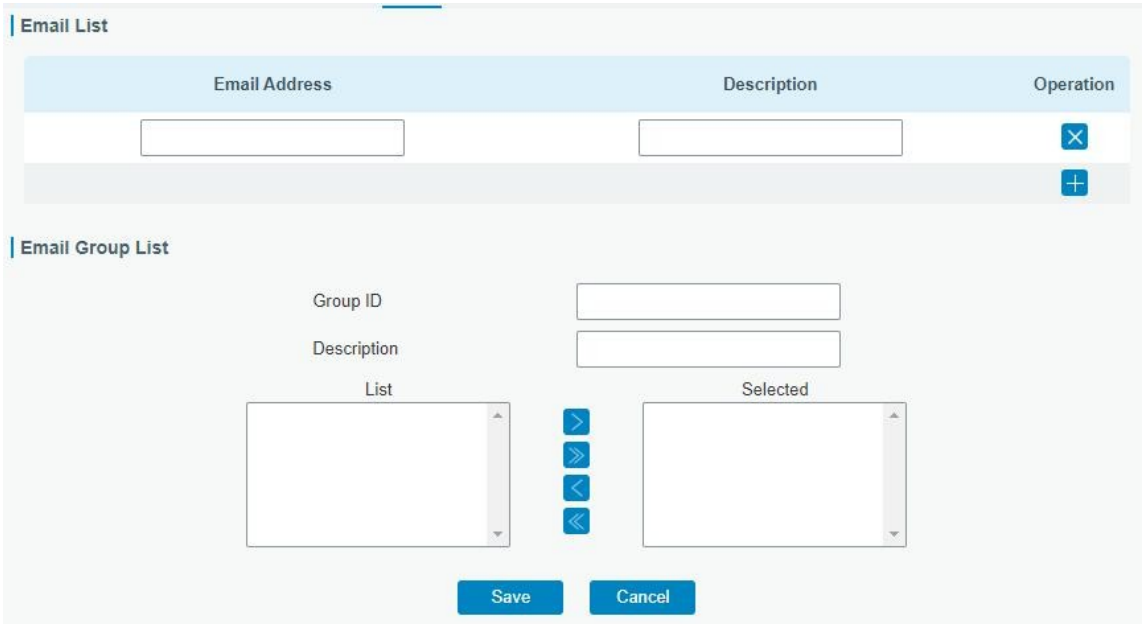


Abbildung 3-3-1-4

Element	Beschreibung
E-Mail-Liste	
E-Mail-Adresse	Geben Sie die E-Mail-Adresse ein.
Beschreibung	Die Beschreibung der E-Mail-Adresse.
E-Mail-Gruppenliste	
Gruppen-ID	Nummer für E-Mail-Gruppe festlegen. Bereich: 1-100.
Beschreibung	Die Beschreibung der E-Mail-Gruppe.
Liste	Zeigt die Liste der E-Mail-Adressen an.
Ausgewählt	Zeigt die ausgewählte E-Mail-Adresse an.

Tabelle 3-3-1-4 E-Mail-Einstellungen

Verwandte Themen

DI-Einstellungen

Ereigniseinstellungen

3.3.1.4 Speicher

Auf dieser Seite können Sie Informationen zur Micro-SD-Karte anzeigen.

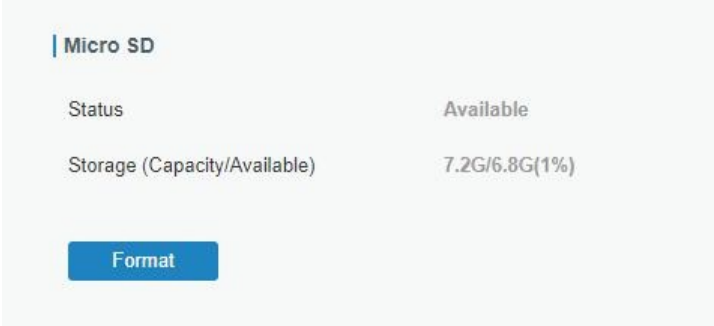


Abbildung 3-3-1-5

Speicher	
Element	**Beschreibung**
Status	Zeigt den Status der Micro-SD-Karte an, z. B. „Verfügbar“ oder „Nicht eingelegt“.
Speicher (Kapazität/Verfügbar)	Die Gesamtkapazität der Micro-SD-Karte.
Format	Formatieren Sie die Micro-SD-Karte.

Tabelle 3-3-1-5 Speicherinformationen

3.3.2 Telefon & SMS

3.3.2.1 Telefon

Die Telefoneinstellungen umfassen Anruf-/SMS-Auslöser, SMS-Steuerung und SMS-Alarm für Ereignisse.

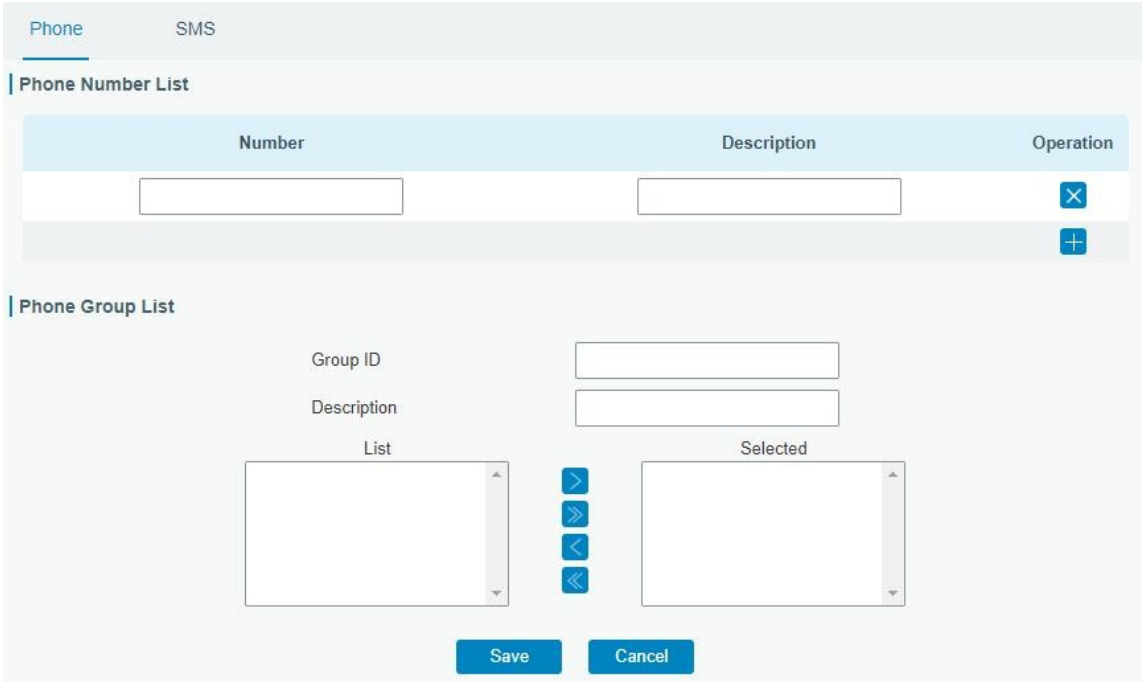


Abbildung 3-3-2-1

Telefon	
Element	**Beschreibung**
Telefonnummernliste	
Nummer	Geben Sie die Telefonnummer ein. Ziffern, „+“ und „-“ sind zulässig.
Beschreibung	Die Beschreibung der Telefonnummer.
Telefon-Gruppenliste	
Gruppen-ID	Nummer für die Telefongruppe festlegen. Bereich: 1-100.
Beschreibung	Die Beschreibung der Telefongruppe.
Liste	Zeigt die Telefonliste an.
Ausgewählt	Zeigt die ausgewählte Telefonnummer an.

Tabelle 3-3-2-1 Telefoneinstellungen

Verwandtes Thema

Verbindung bei Bedarf

3.3.2.2 SMS

Die SMS-Einstellungen umfassen die Fernsteuerung per SMS, das Senden von SMS sowie den Status des SMS-Empfangs und -Versands. Stellen Sie sicher, dass die Nummer der SMS-Zentrale auf der Seite **„Netzwerk > Schnittstelle > Mobilfunk"** eingegeben ist, bevor Sie die SMS-Funktionen verwenden.

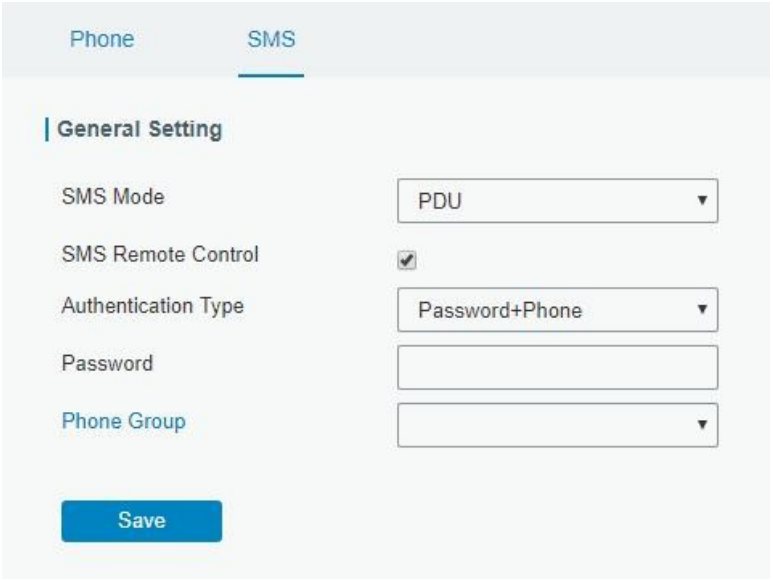


Abbildung 3-3-2-2

SMS-Einstellungen	
Element	**Beschreibung**
SMS-Modus	Wählen Sie den SMS-Modus aus: **Text:** Reiner Textmodus,der hauptsächlich in Europa und Amerika verwendet wird. Technisch gesehen kann er auch zum Versenden von Kurznachrichten in chinesischer Sprache verwendet werden. Wenn CLI-Befehle zur Steuerung des Routers gesendet werden sollen, wird die Auswahl des Textmodus empfohlen. **PDU:** Dies ist der Standard-Kodierungsmodus für Mobiltelefone, der dem SMS-Format aller Mobiltelefone entspricht allen SMS-Formaten von Mobiltelefonen entspricht und alle Zeichen verwenden kann.
SMS-Fernsteuerung Steuerung	Aktivieren/Deaktivieren der SMS-Fernsteuerung zum Senden von SMS zur Steuerung des Router.
Authentifizierungstyp	Sie können zwischen „Telefonnummer" und „Passwort + Telefonnummer" wählen. Telefonnummer: Nur die Telefonnummern in Telefongruppen unterstützen die Fernsteuerung. Passwort + Telefonnummer: Nur die Telefonnummern in Telefongruppen unterstützen die Fernsteuerung; außerdem sollte die Steuerungs-SMS im Format „Passwort+";"+Befehlsinhalt gesendet werden.
Passwort	Legen Sie ein Passwort für die Authentifizierung fest.
Telefongruppe	Wählen Sie die Telefongruppe aus, die für die Fernsteuerung verwendet werden soll. Der Benutzer kann klicken die Telefongruppe und die Telefonnummer einstellen.

Tabelle 3-3-2-2 Parameter für die SMS-Fernsteuerung

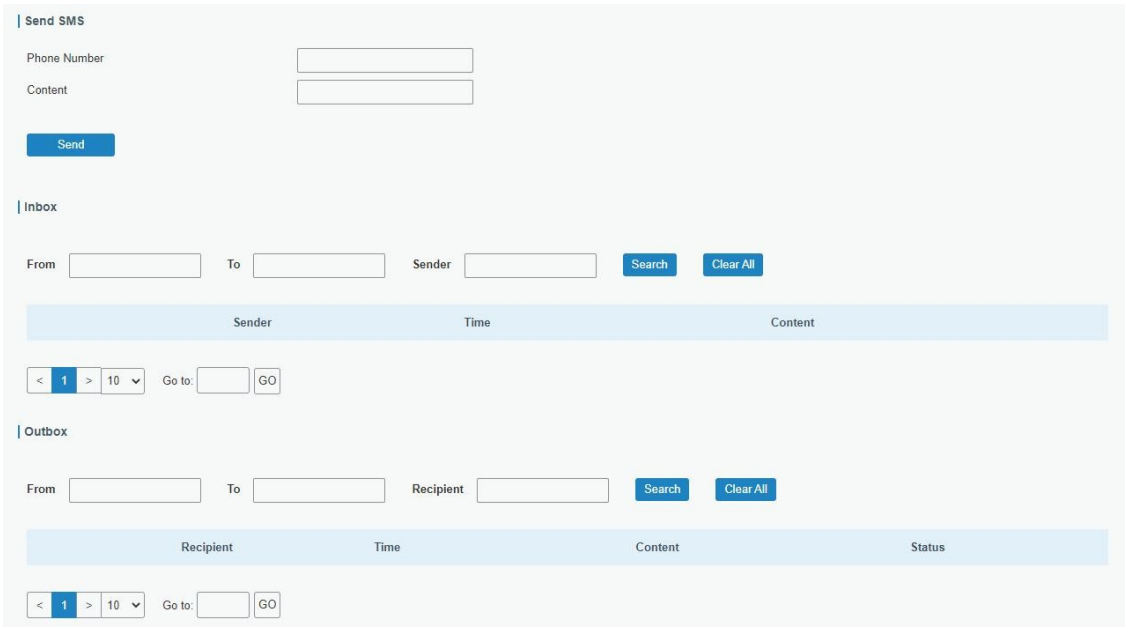


Abbildung 3-3-2-3

SMS	
Element	**Beschreibung**
SMS senden	
Telefonnummer	Geben Sie die Nummer ein, an die die SMS gesendet werden soll.
Inhalt	Inhalt der SMS.
Posteingang/Postausgang	
Absender	SMS-Absender von außerhalb.
Empfänger	SMS-Empfänger, an den UR35 sendet.
Von	Wählen Sie das Startdatum aus.
Bis	Wählen Sie das Enddatum aus.
Suchen	Nach SMS-Datensatz suchen.
Alle löschen	Löschen Sie alle SMS-Datensätze in der Web-GUI.

Tabelle 3-3-2-3 SMS-Einstellungen

3.3.3 Benutzerverwaltung

3.3.3.1 Konto

Hier können Sie den Benutzernamen und das Passwort des Administrators ändern.

Hinweis: Aus Sicherheitsgründen wird dringend empfohlen, diese zu ändern.

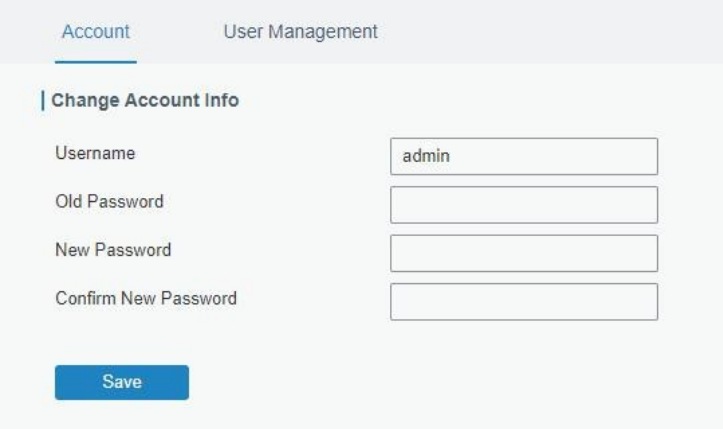


Abbildung 3-3-3-1

Konto	
Element	**Beschreibung**
Benutzername	Geben Sie einen neuen Benutzernamen ein. Sie können Zeichen wie a-z, 0-9, „_“ und „-“ verwenden. Das erste Zeichen darf keine Ziffer sein.
Altes Passwort	Geben Sie das alte Passwort ein.
Neues Passwort	Geben Sie ein neues Passwort ein. Sie können alle ASCII-Zeichen verwenden außer Leerzeichen verwenden.
Neues Passwort bestätigen	Geben Sie das neue Passwort erneut ein.

Tabelle 3-3-3-1 Kontoeinstellungen

3.3.3.2 Benutzerverwaltung

In diesem Abschnitt wird beschrieben, wie Sie allgemeine Benutzerkonten erstellen. Die allgemeinen Benutzerberechtigungen umfassen „Nur Lesen“ und „Lesen/Schreiben“.

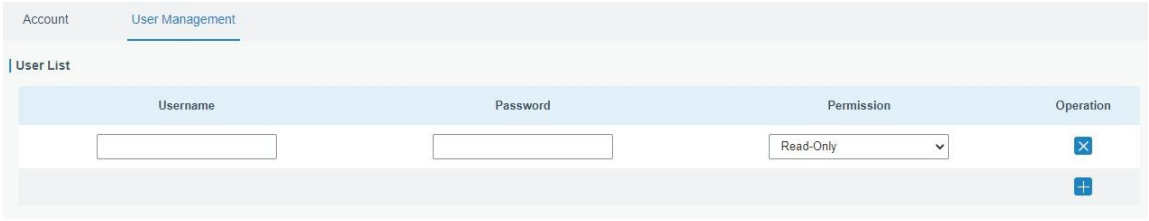


Abbildung 3-3-3-2

Benutzerverwaltung	
Element	**Beschreibung**
Benutzername	Geben Sie einen neuen Benutzernamen ein. Sie können Zeichen wie a-z, 0-9, „_“ und „-“ verwenden. Das erste Zeichen darf keine Ziffer sein.
Passwort	Legen Sie ein Passwort fest. Sie können alle ASCII-Zeichen außer Leerzeichen verwenden.
Berechtigung	Wählen Sie die Benutzerberechtigung aus „Nur Lesen“ und „Lesen/Schreiben“ aus. **Nur Lesen:** Benutzer können auf dieser Ebene nur die Konfiguration des Routers anzeigen. **Lesen/Schreiben:** Benutzer können in dieser Stufe die Konfiguration des Routers anzeigen und festlegen.

Tabelle 3-3-3-2 Benutzerverwaltung

3.3.4 AAA

Die AAA-Zugriffskontrolle wird für die Besucherkontrolle und die verfügbaren entsprechenden Dienste verwendet, sobald der Zugriff gewährt wurde. Sie verwendet dieselbe Methode, um drei unabhängige Sicherheitsfunktionen zu konfigurieren. Sie bietet Modularisierungsmethoden für folgende Dienste:

- Authentifizierung: Überprüft, ob der Benutzer zum Zugriff auf das Netzwerk berechtigt ist.
- Autorisierung: Autorisieren Sie die für den Benutzer verfügbaren zugehörigen Dienste.
- Abrechnung: Erfassen Sie die Nutzung von Netzwerkressourcen.

3.3.4.1 Radius

Radius verwendet UDP für den Transport und wird in der Regel in verschiedenen Netzwerkumgebungen mit höheren Anforderungen an Sicherheit und Berechtigungen für den Fernzugriff von Benutzern eingesetzt.

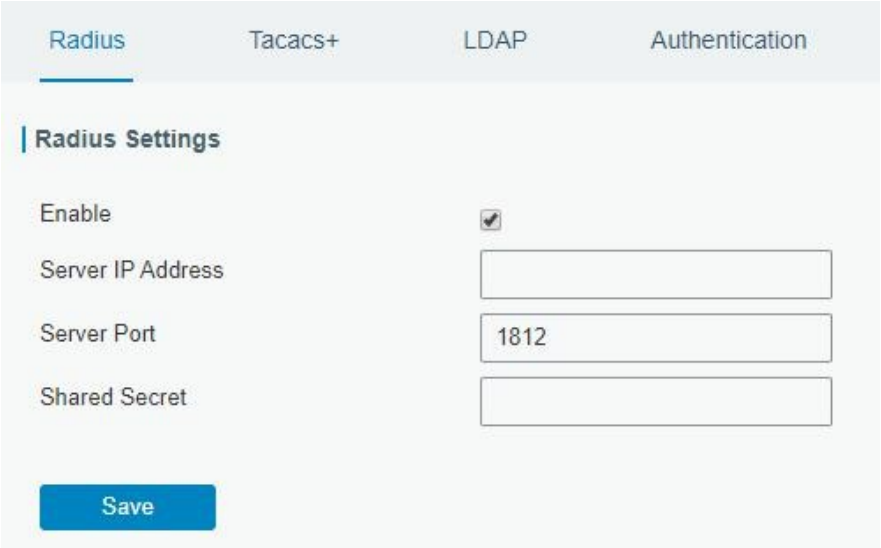


Abbildung 3-3-4-1

Radius	
Element	**Beschreibung**
Aktivieren	Aktivieren oder deaktivieren Sie Radius.
Server-IP-Adresse	Geben Sie die IP-Adresse/den Domänennamen des Radius-Servers ein.
Server-Port	Geben Sie den Port des Radius-Servers ein. Bereich: 1-65535.
Schlüssel	Geben Sie den Schlüssel ein, der mit dem des Radius-Servers übereinstimmt, um verbunden mit dem Radius-Server.

Tabelle 3-3-4-1 Radius-Parameter

3.3.4.2 TACACS

TACACS+ verwendet TCP für den Transport und wird hauptsächlich für die Authentifizierung, Autorisierung und Abrechnung von Zugangsbenutzern und Terminalbenutzern unter Verwendung von PPP und VPDN verwendet.

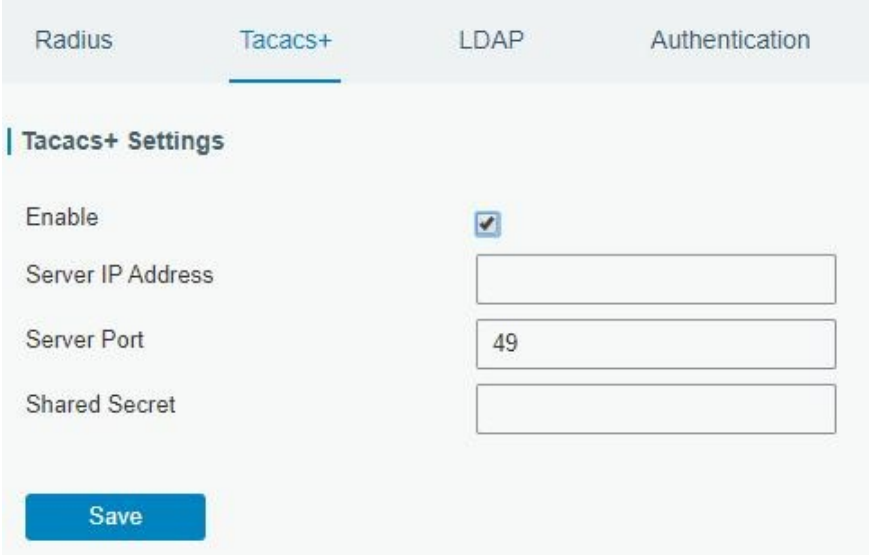


Abbildung 3-3-4-2

TACACS	
Element	**Beschreibung**
Aktivieren	Aktivieren oder deaktivieren Sie TACACS+.
Server-IP-Adresse	Geben Sie die IP-Adresse/den Domänennamen des TACACS+-Servers ein.
Server-Port	Geben Sie den Port des TACACS+-Servers ein. Bereich: 1-65535.
Schlüssel	Geben Sie den Schlüssel ein, der mit dem des TACACS+-Servers übereinstimmt, , um eine Verbindung mit dem TACACS+-Server herzustellen.

Tabelle 3-3-4-2 TACACS+-Parameter

3.3.4.3 LDAP

Eine häufige Verwendung von LDAP ist die Bereitstellung eines zentralen Speichers für Benutzernamen und Passwörter. Dadurch können viele verschiedene Anwendungen und Dienste eine Verbindung zum LDAP-Server herstellen, um Benutzer zu validieren.

LDAP basiert auf einer einfacheren Teilmenge der im X.500-Standard enthaltenen Standards. Aufgrund dieser Verwandtschaft wird LDAP manchmal auch als X.500-lite bezeichnet.

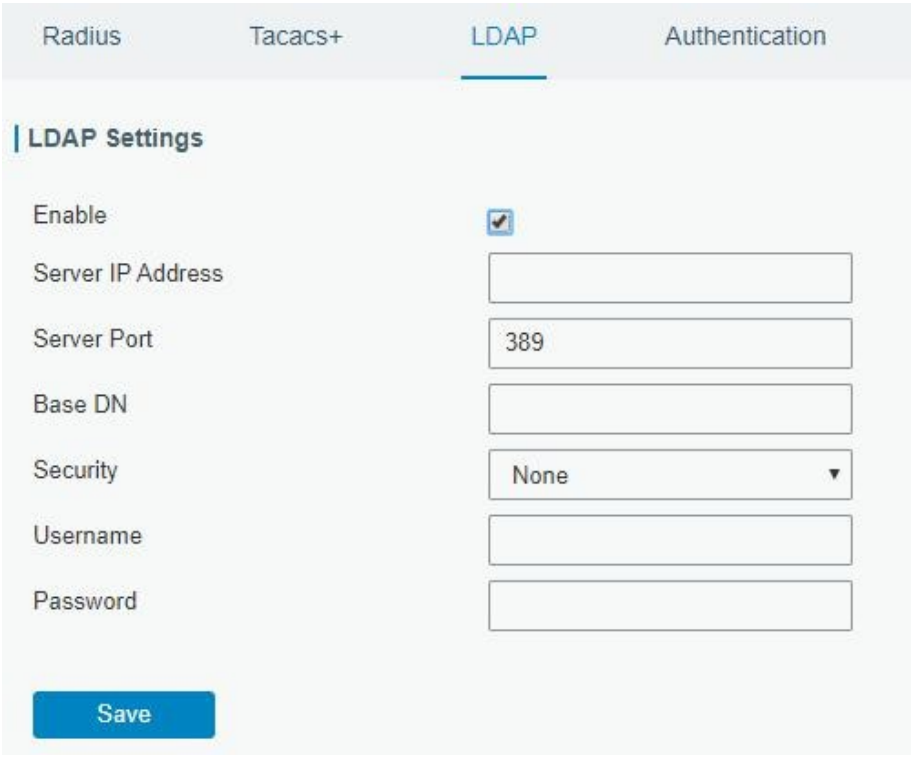


Abbildung 3-3-4-3

LDAP	
Element	**Beschreibung**
Aktivieren	LDAP aktivieren oder deaktivieren.
Server-IP-Adresse	Geben Sie die IP-Adresse/den Domänennamen des LDAP-Servers ein. Die maximale Anzahl beträgt 10.
Server-Port	Geben Sie den Port des LDAP-Servers ein. Bereich: 1-65535
Basis-DN	Die Spitze des LDAP-Verzeichnisbaums.
Sicherheit	Wählen Sie eine sichere Methode aus „Keine“, „StartTLS“ und „SSL“ aus.
Benutzername	Geben Sie den Benutzernamen für den Zugriff auf den Server ein.
Passwort	Geben Sie das Passwort für den Zugriff auf den Server ein.

Tabelle 3-3-5-3 LDAP-Parameter

3.3.4.4 Authentifizierung

AAA unterstützt die folgenden Authentifizierungsmethoden:

- Keine: Verwendet keine Authentifizierung, im Allgemeinen nicht empfohlen.
- Lokal: Verwendet die lokale Benutzernamendatenbank für die Authentifizierung.
  - ➢ Vorteile: Schnelligkeit, Kostensenkung.
  - ➢ Nachteile: Speicherkapazität durch Hardware begrenzt.
- Remote: Die Benutzerinformationen werden auf dem Authentifizierungsserver gespeichert. Radius, TACACS+ und LDAP werden für die Remote-Authentifizierung unterstützt.

Wenn Radius, TACACS+ und Local gleichzeitig konfiguriert sind, gilt folgende Prioritätsstufe: 1 > 2 > 3.

Abbildung 3-3-4-4

Authentifizierung	
Element	**Beschreibung**
Konsole	Wählen Sie die Authentifizierung für den Konsolenzugriff aus.
Web	Wählen Sie die Authentifizierung für den Webzugriff aus.
Telnet	Wählen Sie die Authentifizierung für den Telnet-Zugriff aus.
SSH	Wählen Sie die Authentifizierung für den SSH-Zugriff aus.

Tabelle 3-3-4-4 Authentifizierungsparameter

3.3.5 Geräteverwaltung

3.3.5.1 DeviceHub

Auf dieser Seite können Sie das Gerät mit dem Milesight DeviceHub verbinden, um den Router zentral und remote zu verwalten. Weitere Informationen finden Sie im ***DeviceHub-Benutzerhandbuch***.

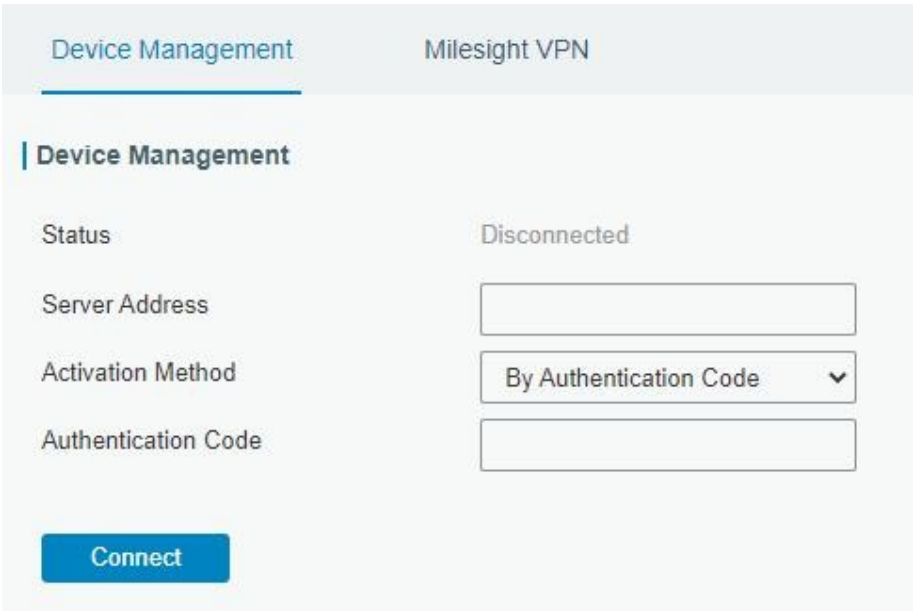


Abbildung 3-3-5-1

DeviceHub	
Element	**Beschreibung**
Status	Zeigen Sie den Verbindungsstatus zwischen dem Router und dem DeviceHub.
Getrennt	Klicken Sie auf diese Schaltfläche, um die Verbindung zwischen dem Router und dem DeviceHub zu trennen.
Serveradresse	IP-Adresse oder Domäne des Gerätemanagementservers.
Aktivierungsmethode	Wählen Sie die Aktivierungsmethode aus, um den Router mit dem DeviceHub-Server zu verbinden. Die Optionen sind „Per Authentifizierungscode“ und „Über den Kontonamen“.
Authentifizierungscode	Geben Sie den vom DeviceHub generierten Authentifizierungscode ein.
Kontoname	Geben Sie den registrierten DeviceHub-Account (E-Mail) und das Passwort ein.
Passwort	

Tabelle 3-3-5-1

3.3.5.2 Milesight VPN

Auf dieser Seite können Sie das Gerät mit dem Milesight VPN verbinden, um den Router und die angeschlossenen Geräte zentral und aus der Ferne zu verwalten. Weitere Informationen finden Sie im ***MilesightVPN-Benutzerhandbuch***.

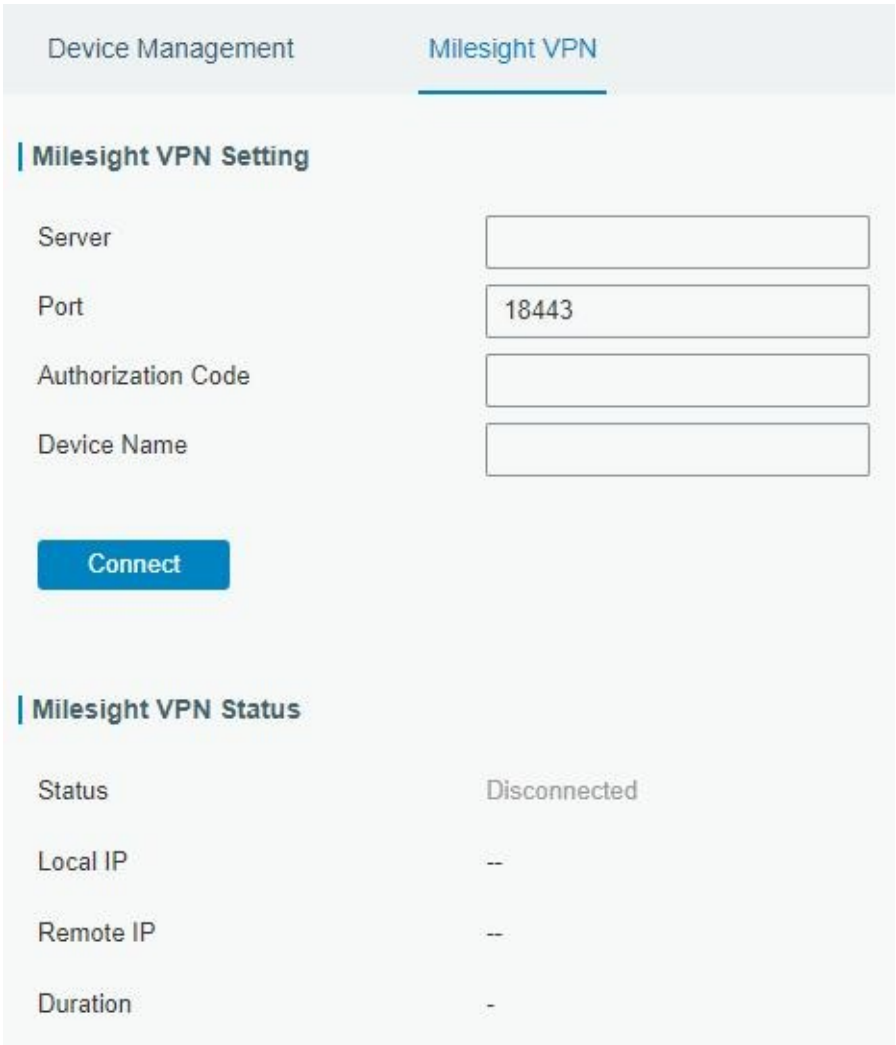


Abbildung 3-3-5-2

Milesight VPN	
Element	**Beschreibung**
Milesight VPN-Einstellungen	
Server	Geben Sie die IP-Adresse oder den Domänennamen von Milesight VPN ein.
Port	Geben Sie die HTTPS-Portnummer ein.
Autorisierungscode	Geben Sie den von Milesight VPN generierten Autorisierungscode ein.
Gerätename	Geben Sie den Namen des Geräts ein.
Milesight VPN-Status	
Status	Zeigen Sie die Verbindungsinformationen darüber an, ob der Router mit dem Milesight-VPN verbunden ist.
Lokale IP	Zeigt die virtuelle IP-Adresse des Routers an.
Remote-IP	Zeigt die virtuelle IP des Milesight-VPN an.
Dauer	Zeigt an, wie lange der Router bereits mit dem Milesight VPN verbunden ist.

Tabelle 3-3-5-2

3.3.6 Ereignisse

Die Ereignisfunktion kann bei bestimmten Systemereignissen Warnmeldungen per E-Mail versenden.

3.3.6.1 Ereignisse

Auf dieser Seite können Sie Alarmmeldungen anzeigen.

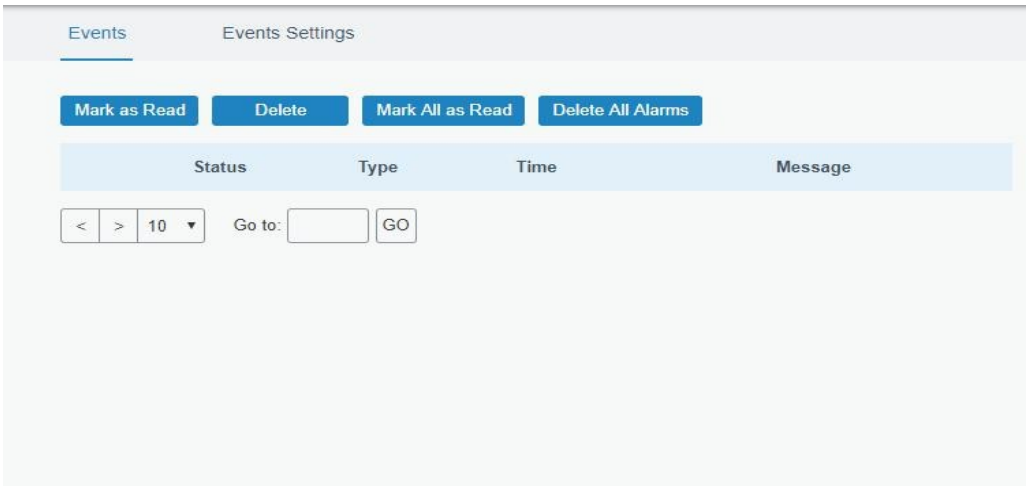


Abbildung 3-3-6-1

Ereignisse	
Element	**Beschreibung**
Als gelesen markieren	Markieren Sie den ausgewählten Ereignisalarm als gelesen.
Löschen	Löschen Sie den ausgewählten Ereignisalarm.
Alle als gelesen markieren	Markieren Sie alle Ereignisalarme als gelesen.
Alle Alarme löschen	Löschen Sie alle Ereignisalarme.
Status	Zeigt den Lesestatus der Ereignisalarme an, z. B. „Gelesen“ und „Ungelesen“.

Typ	Zeigen Sie den Ereignistyp an, der alarmiert werden soll.
Zeit	Zeigen Sie die Alarmzeit an.
Meldung	Zeigen Sie den Inhalt des Alarms an.

Tabelle 3-3-6-1 Ereignisparameter

3.3.6.2 Ereigniseinstellungen

In diesem Abschnitt können Sie festlegen, welche Ereignisse aufgezeichnet werden sollen und ob Sie bei Änderungen E-Mail- und SMS-Benachrichtigungen erhalten möchten.

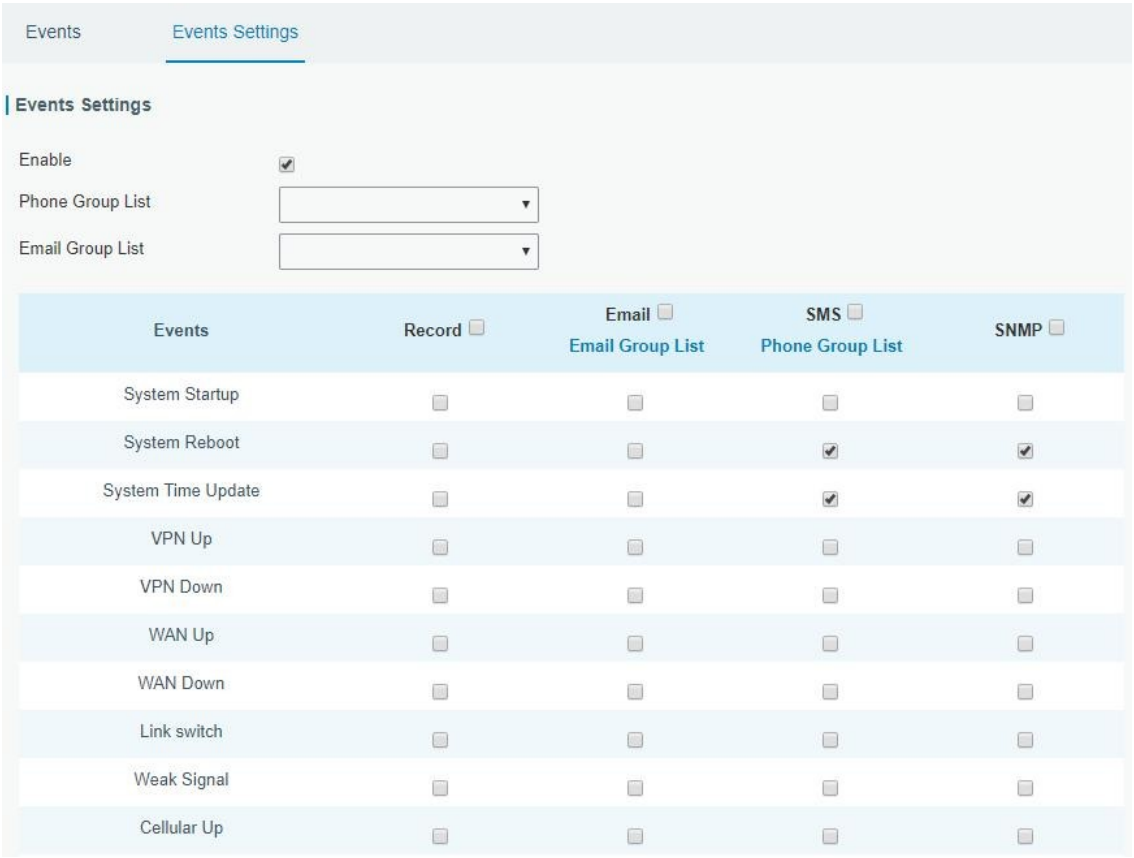


Abbildung 3-3-6-2

Abbildung 3-3-6-3

Ereigniseinstellungen	
Element	**Beschreibung**
Aktivieren	Aktivieren Sie diese Option, um die „Ereigniseinstellungen“ zu aktivieren.
Telefon-Gruppenliste	Wählen Sie die Telefongruppe aus, die SMS-Alarme empfangen soll.
E-Mail-Gruppenliste	Wählen Sie eine E-Mail-Gruppe aus, die den Alarm erhalten soll.
Aufzeichnen	Der relevante Inhalt des Ereignisalarms wird auf der Seite „Ereignis“ aufgezeichnet, wenn diese Option aktiviert ist.
E-Mail	Der relevante Inhalt des Ereignisalarms wird per E-Mail versendet , wenn diese Option aktiviert ist.
E-Mail-Einstellungen	Klicken Sie auf „E-Mail“, um zur Seite „E-Mail“ weitergeleitet zu werden und E-Mail-Gruppenliste konfigurieren.
SMS	Der relevante Inhalt des Ereignisalarms wird per SMS versendet , wenn diese Option aktiviert ist.
SMS-Einstellungen	Klicken Sie darauf, um zur Seite „Telefon“ weitergeleitet zu werden, auf der Sie die Telefon-Gruppenliste konfigurieren können.
VPN aktiv	VPN ist verbunden.
VPN-Verbindung unterbrochen	VPN ist getrennt.
WAN aktiv	Ethernet-Kabel ist mit dem WAN-Port verbunden.
WAN ausgefallen	Das Ethernet-Kabel ist vom WAN-Port getrennt.
Verbindung umschalten	Wechseln Sie zu einer anderen Schnittstelle für den Internetzugang.
Schwaches Signal	Der Signalpegel des Mobilfunknetzes ist niedrig (RSSI < 11 oder ≥ 99).
Mobilfunk aktiv	Das Mobilfunknetz ist verbunden.
Mobilfunknetz ausgefallen	Das Mobilfunknetz ist getrennt.
Mobilfunkdatenstatistik Löschen	Setzen Sie die Datennutzung der Haupt-SIM-Karte auf Null zurück.
Der Mobilfunkdatenverkehr ist fast aufgebraucht	Die Haupt-SIM-Karte erreicht das Datenvolumenlimit.
Mobilfunkdatenverkehr Überlauf	Die Haupt-SIM-Karte hat das Datenvolumen überschritten.
WLAN aktiv (AP)	Das WLAN (AP) ist aktiviert.
WLAN aus (AP)	Das WLAN (AP) funktioniert nicht mehr.
WLAN aktiv (Client)	Das WLAN (Client) ist aktiviert.
WLAN ausgefallen (Client)	Das WLAN (Client) funktioniert nicht mehr.

Tabelle 3-3-6-2 Ereignisparameter

Verwandte Themen

E-Mail-Einstellungen

3.4 Dienst

3.4.1 E/A

3.4.1.1 DI

In diesem Abschnitt wird erläutert, wie Sie Überwachungsbedingungen für digitale Eingänge konfigurieren und bestimmte Aktionen ausführen können

auszuführen, sobald die Bedingung erfüllt ist.

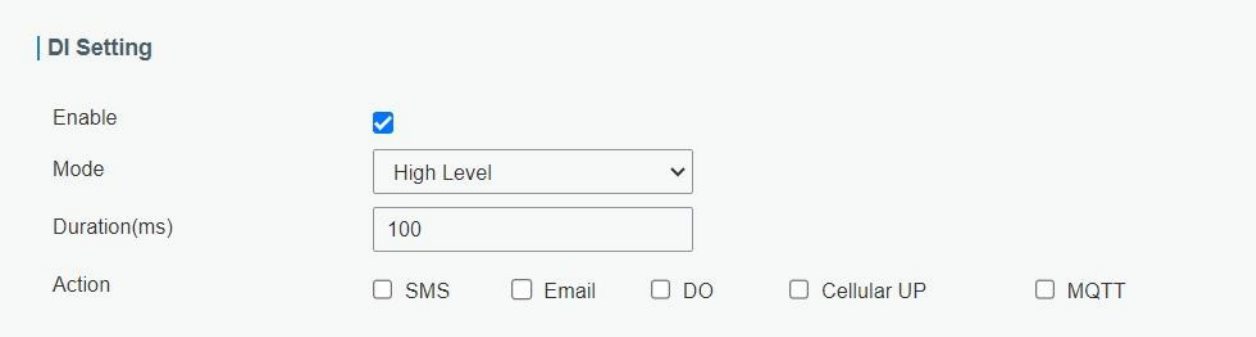


Abbildung 3-4-1-1

DI	
Element	**Beschreibung**
Aktivieren	DI aktivieren oder deaktivieren.
Modus	Die Optionen sind „High Level“, „Low Level“ und „Counter“.
Dauer (ms)	Legen Sie die Dauer des hohen/niedrigen Pegels im digitalen Eingang fest. Bereich: 1-10000.
Bedingung	Wählen Sie die Bedingung aus, die den Zähler auslöst. **Niedrig->Hoch:** Der Zählerwert erhöht sich um 1, wenn sich der Status des digitalen Eingangs von niedrig auf hoch ändert. **Hoch->Niedrig:** Der Zählerwert erhöht sich um 1, wenn sich der Status des digitalen Eingangs von einem hohen Pegel zu einem niedrigen Pegel ändert.
Zähler	Das System ergreift entsprechende Maßnahmen, wenn der Zählerwert den voreingestellten Wert erreicht und setzt den Zählerwert dann auf 0 zurück. Bereich: 1-100.
Aktion	Wählen Sie die entsprechenden Aktionen aus, die das System ausführen soll, wenn der digitale Eingangsmodus die voreingestellte Bedingung oder Dauer erfüllt. **SMS:** Aktivieren Sie diese Option, um SMS-Alarme zu versenden. **E-Mail:** Aktivieren Sie diese Option, um E-Mail-Alarme zu versenden. **DO:** Steuern Sie den DO-Status gemäß den Einstellungen auf **der Seite „Service > I/O > DO“**. **Mobilfunk UP:** Lösen Sie aus, dass der Router von offline auf die Registrierung im Mobilfunknetz umschaltet. **MQTT**: Aktivieren Sie diese Option, um Nachrichten an den MQTT-Broker zu senden. Die MQTT-Verbindung wird eingerichtet. auf der Seite **„Service > MQTT“**.

Tabelle 3-4-1-1 DI-Parameter

Verwandte Themen

DO-Einstellung

E-Mail-Einstellung

Verbindung bei Bedarf

3.4.1.2 DO

In diesem Abschnitt wird beschrieben, wie Sie den digitalen Ausgabemodus konfigurieren.

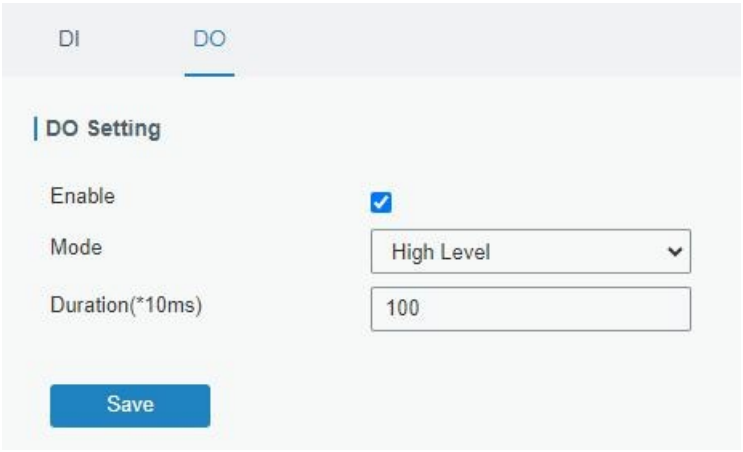


Abbildung 3-4-1-2

DO	
Element	**Beschreibung**
Aktivieren	DO aktivieren oder deaktivieren.
Modus	Wählen Sie den Arbeitsmodus von DO aus. **High Level:** DO wird ausgelöst, um ein High-Level-Signal zu senden. **Low Level:** DO wird ausgelöst, um ein Low-Level-Signal zu senden. **Pulse:** DO wird ausgelöst, um Impulse zu senden. **Benutzerdefiniert:** DO über SMS auf der Telefongruppe auslösen.
Anfangsstatus	Wählen Sie den Anfangszustand von DO, wenn der Modus „Benutzerdefiniert" oder „Impuls" ist. Impuls eingestellt ist. Dies ist auch der Anfangszustand beim Neustart des Routers.
Dauer (*10 ms)	Wenn der Modus „High Level" oder „Low Level" ist, legen Sie die Dauer des High/Low-Pegel am digitalen Ausgang ein. Bereich: 1-10000.
Dauer von High Level (*10 ms)	Stellen Sie die Dauer des hohen Pegels des Impulses ein. Bereich: 1-10000.
Dauer des niedrigen Pegels (*10 ms)	Stellen Sie die Dauer des niedrigen Pegels des Impulses ein. Bereich: 1-10000.
Anzahl der Impulse	Stellen Sie die Anzahl der Impulse ein. Bereich: 1-100.
Telefongruppe	Wählen Sie die Telefongruppe aus, die für die E/A-Konfiguration verwendet werden soll. Der Benutzer kann auf die Telefongruppe klicken und die Telefonnummer festlegen.

Tabelle 3-4-1-2 DO-Einstellungen

Verwandte Themen

DI-Einstellung

3.4.2 Serielle Schnittstelle

In diesem Abschnitt wird erläutert, wie Sie die Parameter der seriellen Schnittstelle konfigurieren, um die Kommunikation mit seriellen Terminals herzustellen, und wie Sie den Arbeitsmodus konfigurieren, um die Kommunikation mit dem entfernten Rechenzentrum herzustellen, sodass eine bidirektionale Kommunikation zwischen seriellen Terminals und dem entfernten Rechenzentrum möglich ist.

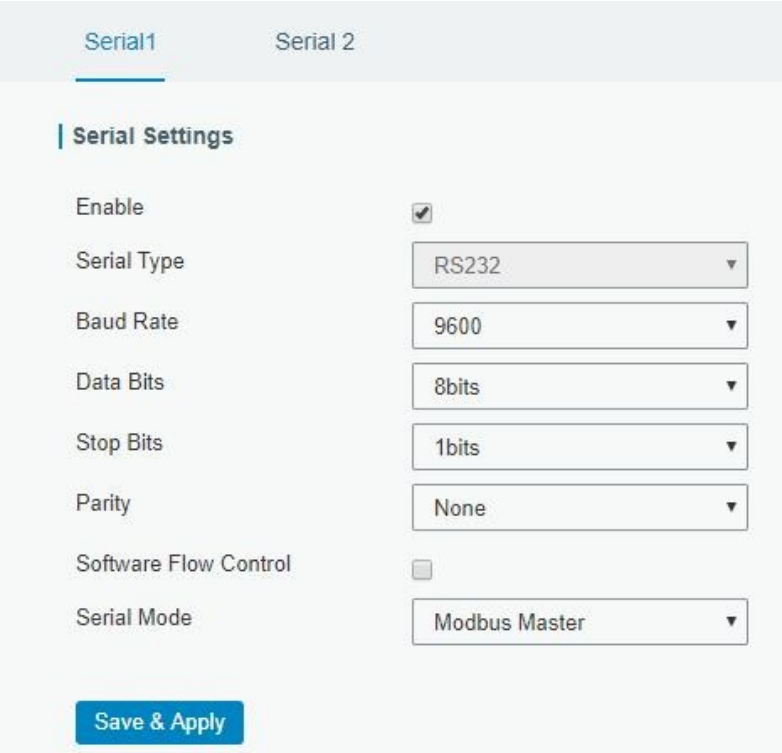


Abbildung 3-4-2-1

Serielle Einstellungen	
Element	**Beschreibung**
Aktivieren	Aktivieren oder deaktivieren Sie die serielle Schnittstellenfunktion.
Serieller Typ	Wählen Sie den seriellen Typ als RS232 oder RS485 aus.
Baudrate	Der Bereich liegt zwischen 300 und 230400. Entspricht der Baudrate des angeschlossenen Endgerät.
Datenbits	Die Optionen sind 8 und 7. Gleiches gilt für die Datenbits des angeschlossenen Endgeräts Gerät.
Stopbits	Die Optionen sind 1 und 2. Gleiches gilt für die Stoppbits des angeschlossenen Endgeräts Gerät.
Parität	Die Optionen sind „Keine“, „Ungerade“ und „Gerade“. Gleich wie bei der Parität des angeschlossenen Terminalgeräts.
Software-Ablauf Steuerung	Aktivieren oder deaktivieren Sie die Software-Flusskontrolle.
Serieller Modus	Wählen Sie den Arbeitsmodus der seriellen Schnittstelle aus. **DTU-Modus:** Die serielle Schnittstelle kann eine Verbindung mit dem Remote-Server/Client herstellen. **GPS:** Gehen Sie zu **„Service“ > „GPS“ > „GPS Serial Forwarding“**, um die grundlegenden Parameter für die Übertragung von GPS-Daten an die serielle Schnittstelle zu konfigurieren. **Modbus-Client:** Gehen Sie zu **„Service“ > „Modbus-Client“**, um die grundlegenden Parameter und Kanäle zu konfigurieren. **Modbus-Server:** Gehen Sie zu **„Service“ > „Modbus-Server“**, um grundlegende Parameter.

Tabelle 3-4-2-1 Serielle Parameter

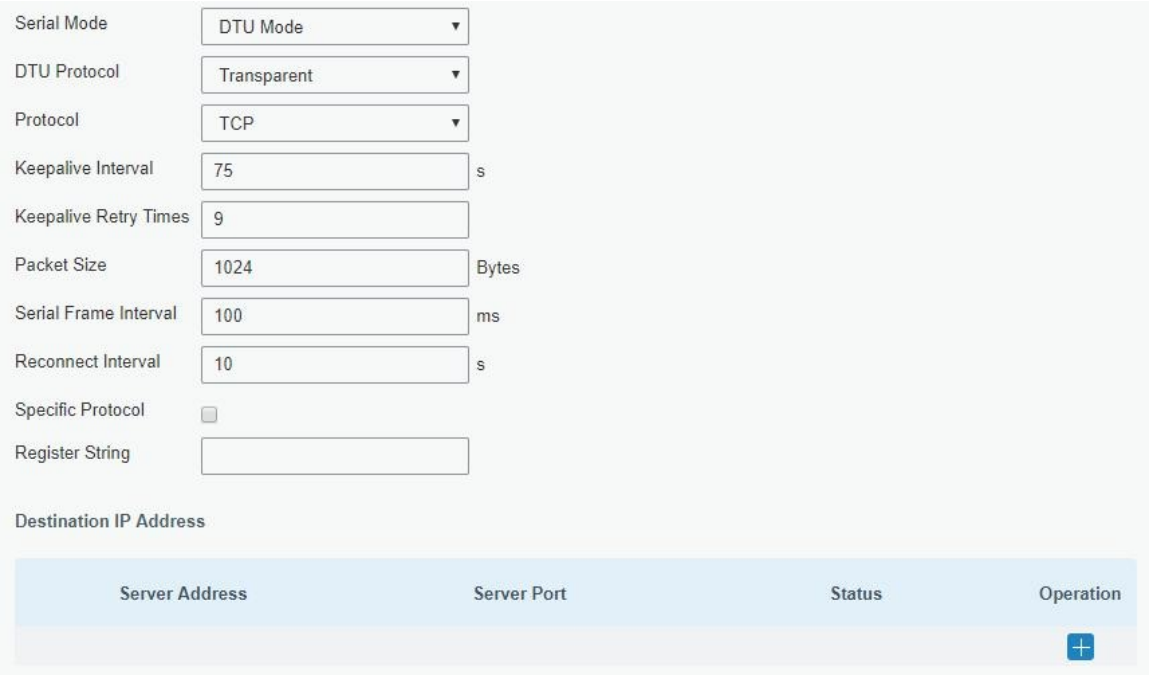


Abbildung 3-4-2-2

DTU-Modus		
Element	**Beschreibung**	**Standard**
DTU-Protokoll	Wählen Sie aus den folgenden Protokollen aus: **Transparent:** Der Router wird als TCP/UDP-Client verwendet und überträgt Daten transparent an den Server. **TCP-Server:** Der Router wird als TCP-Server verwendet, um auf Abfragedaten zu warten. **UDP-Server:** Der Router wird als UDP-Server verwendet, um auf Abfragedaten zu warten. **Modbus:** Der Router wird als Modbus-Gateway verwendet, das die Konvertierung zwischen Modbus RTU und Modbus TCP ermöglicht. **MQTT:** Der Router wird als MQTT-Client verwendet, um Daten weiterzuleiten an MQTT-Broker oder Weiterleitung der Downlink-Daten an die serielle Schnittstelle.	--
TCP/UDP-Server		
Listening-Port	Legen Sie den Listening-Port des Routers fest. Bereich: 1-65535.	502
Keepalive-Intervall	Nachdem die TCP-Verbindung hergestellt wurde, sendet der Client regelmäßig ein Heartbeat-Paket , um die Verbindung aufrechtzuerhalten. Der Intervallbereich liegt zwischen 1 und 3600 Sekunden.	75
Keepalive-Wiederholungsversuche	Wenn der TCP-Heartbeat zeitlich abgelaufen ist, sendet der Router den Heartbeat erneut. Nachdem die voreingestellte Anzahl an Wiederholungsversuchen erreicht ist, wird die TCP-Verbindung wiederhergestellt. Der Bereich für die Wiederholungsversuche liegt zwischen 1 und 16.	9
Paketgröße	Legen Sie die Größe des seriellen Datenrahmens fest. Das Paket wird gesendet, wenn die voreingestellte Rahmengröße erreicht ist. Der Größenbereich liegt zwischen 1 und 1024 Byte.	1024
Serielles Rahmenintervall	Das Intervall, in dem der Router die im Pufferbereich gespeicherten realen seriellen Daten an das öffentliche Netzwerk sendet. Der Bereich liegt zwischen 10 und 65535 ms. **Hinweis:** Die Daten werden an das öffentliche Netzwerk gesendet, wenn die tatsächliche serielle Datengröße die voreingestellte Paketgröße erreicht, auch wenn sie innerhalb des seriellen Rahmenintervall liegt.	100

Tabelle 3-4-2-2 DTU-Parameter

Element	Beschreibung	Standard
Transparentes		
Protokoll	Wählen Sie das TCP- oder UDP-Protokoll aus.	TCP
Keepalive-Intervall (s)	Nachdem der TCP-Client mit dem TCP-Server verbunden ist, sendet der Client regelmäßig ein Heartbeat-Paket über TCP, um die Verbindung aufrechtzuerhalten. Der Intervallbereich liegt zwischen 1 und 3600 s.	75
Keepalive-Wiederholungsversuche	Wenn der TCP-Heartbeat-Zeitüberschreitung erreicht ist, sendet der Router den Heartbeat erneut. Nachdem die voreingestellte Anzahl an Wiederholungsversuchen erreicht ist, stellt der Router die Verbindung zum TCP-Server wieder her. Der Bereich liegt zwischen 1 und 16.	9
Paketgröße	Legen Sie die Größe des seriellen Datenrahmens fest. Das Paket wird gesendet, wenn die voreingestellte Rahmengröße erreicht ist. Der Bereich liegt zwischen 1 und 1024 Byte.	1024
Serielles Rahmenintervall	Das Intervall, in dem der Router die im Pufferbereich gespeicherten realen seriellen Daten an das öffentliche Netzwerk sendet. Der Bereich liegt zwischen 10 und 65535 ms. **Hinweis:** Die Daten werden an das öffentliche Netzwerk gesendet, wenn die Größe der tatsächlichen seriellen Daten die voreingestellte Paketgröße erreicht, auch wenn sie innerhalb des seriellen Rahmenintervalls liegt.	100
Wiederverbinden Intervall	Nach einem Verbindungsfehler stellt der Router die Verbindung zum Server im voreingestellten Intervall erneut mit dem Server. Der Bereich liegt zwischen 10 und 60 Sekunden.	10
Spezifisches Protokoll	Durch ein bestimmtes Protokoll kann der Router eine Verbindung zur TCP2COM-Software verbinden.	--
Heartbeat Intervall	Über ein bestimmtes Protokoll sendet der Router regelmäßig Heartbeat-Pakete an den Server, um die Verbindung aufrechtzuerhalten. Der Intervallbereich liegt zwischen 1 und 3600 Sekunden.	30
ID	Definieren Sie eine eindeutige ID für jeden Router. Nicht länger als 63 Zeichen ohne Leerzeichen.	--
Registrierungszeichenfolge	Definieren Sie eine Registrierungszeichenfolge für die Verbindung mit dem Server.	Null
Serveradresse	Geben Sie die TCP- oder UDP-Serveradresse (IP/Domänenname) ein.	Null
Server-Port	Geben Sie den TCP- oder UDP-Serverport ein. Bereich: 1-65535.	Null
Status	Zeigt den Verbindungsstatus zwischen dem Router und dem Server an.	--
Modbus		
Lokaler Port	Legen Sie den Listening-Port des Routers fest. Bereich: 1-65535.	502
Maximale TCP Clients	Geben Sie die maximale Anzahl von TCP-Clients an, die eine Verbindung zum Router, der als TCP-Server fungiert, eine Verbindung herstellen dürfen.	32
Verbindungszeitlimit	Wenn der TCP-Server innerhalb der Verbindungszeitüberschreitung keine Daten vom Slave-Gerät empfängt innerhalb der Verbindungszeitüberschreitung keine Daten vom Slave-Gerät empfängt, wird die TCP-Verbindung unterbrochen.	60
Leseintervall	Legen Sie das Intervall für das Lesen von Remote-Kanälen fest. Wenn ein Lesezyklus endet, beginnt der neue Lesezyklus, bis dieses Intervall abgelaufen ist. Wenn es auf 0 gesetzt ist, startet das Gerät den neuen Lesezyklus neu, nachdem alle Kanäle gelesen wurden.	100
Antwortzeitlimit	Legen Sie die maximale Antwortzeit fest, die der Router auf die Antwort auf den Befehl wartet. Wenn das Gerät nach Ablauf der maximalen Antwortzeit keine Antwort erhält, wird davon ausgegangen, dass der Befehl fehlgeschlagen ist.	3000
Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl von Wiederholungsversuchen fest, nachdem das Lesen fehlgeschlagen ist.	3

MQTT		
Paketgröße	Legen Sie die Größe des seriellen Datenrahmens fest. Das Paket wird gesendet, wenn die voreingestellte Rahmengröße erreicht ist. Der Bereich liegt zwischen 1 und 1024 Byte.	1024
Serielles Rahmenintervall	Das Intervall, in dem der Router die im Pufferbereich gespeicherten echten seriellen Daten an das öffentliche Netzwerk sendet. Der Bereich liegt zwischen 10 und 65535 ms. **Hinweis:** Die Daten werden an das öffentliche Netzwerk gesendet, wenn die tatsächliche serielle Datenmenge die voreingestellte Paketgröße erreicht, auch wenn sie innerhalb des seriellen Rahmenintervalls liegen.	100
MQTT Verbindung	Wählen Sie die MQTT-Verbindung zum Senden von Daten aus der seriellen Schnittstelle aus. Diese wird auf der Seite Seite **„Service > MQTT“ eingerichtet.**	Null
Typ	Wählen Sie für diese transparente Verbindung „Uplink“ oder „Downlink“. Jeder Typ unterstützt maximal 10 Verbindungen hinzugefügt werden.	Null
Thema	Themenname, der für die Veröffentlichung von Daten der seriellen Schnittstelle verwendet wird.	Null
Beibehalten	Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als beibehaltene Nachricht festzulegen.	Null
QoS	QoS0, QoS1 oder QoS2 sind optional.	Null

Tabelle 3-4-2-3 DTU-Parameter

Beispiel für die zugehörige Konfiguration

DTU-Anwendungsbeispiel

3.4.3 Modbus-Server (Slave)

In diesem Abschnitt wird beschrieben, wie Sie den E/A-Status über Modbus TCP, Modbus RTU und Modbus RTU über TCP abrufen können.

3.4.3.1 Modbus TCP

Sie können die Adresse der DI- und DO-Ports so definieren, dass der Status von DI abgefragt und der Status von DO über das Modbus-TCP-Protokoll gesteuert werden kann.

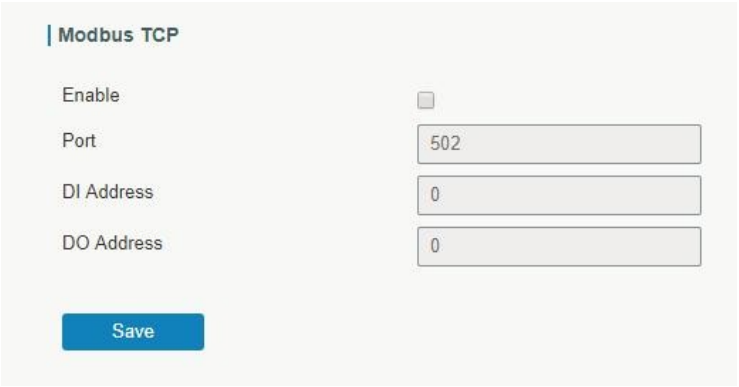


Abbildung 3-4-3-1

Modbus TCP		
Element	**Beschreibung**	**Standard**
Aktivieren	Modbus TCP aktivieren/deaktivieren.	Deaktivieren
Port	Legen Sie den Listening-Port des Routers fest. Bereich: 1-65535.	502
DI-Adresse	Legen Sie die Adresse von DI fest, Bereich: 0-255.	0

DO-Adresse	Definieren Sie die Adresse von DO, Bereich: 0, 2-255.	0

Tabelle 3-4-3-1 Modbus-TCP-Parameter

3.4.3.2 Modbus RTU

Sie können die Adresse der DI- und DO-Ports definieren, um den Status von DI abzufragen und den Status von DO über das Modbus-RTU-Protokoll zu steuern.

Abbildung 3-4-3-2

Modbus RTU		
Element	**Beschreibung**	**Standard**
Aktivieren	Modbus RTU aktivieren/deaktivieren.	Deaktivieren
Serielle Schnittstelle	Wählen Sie die entsprechende serielle Schnittstelle aus.	Seriell
Server-ID	Die Server-ID wird zur Unterscheidung verschiedener Server verwendet. Geräte auf derselben Verbindung.	1
DI-Adresse	Definieren Sie die Adresse von DI, Bereich: 0-255.	0
DO-Adresse	Definieren Sie die Adresse von DO, Bereich: 0, 2-255.	0

Tabelle 3-4-3-2 Modbus-RTU-Parameter

3.4.3.3 Modbus RTU über TCP

Sie können die Adresse der DI- und DO-Ports so definieren, dass der Status von DI abgefragt und der Status von DO über Modbus RTU über TCP gesteuert werden kann.

Abbildung 3-4-3-3

Modbus RTU über TCP

Element	Beschreibung	Standard
Aktivieren	Modbus RTU über TCP-Funktion aktivieren/deaktivieren.	Deaktivieren
Server-ID	Die Server-ID dient zur Unterscheidung verschiedener Geräte auf derselben Verbindung.	1
Geräte-ID	Geräte-ID festlegen. Der Server ruft die Geräte-ID vom Server, um die Identität zu identifizieren, damit der Server mehrere Geräte verwalten kann.	--
Wiederverbindung Intervall	Das Wiederverbindungsintervall, wenn das Gerät und der Server keine Verbindung herstellen können oder die Verbindung unterbrochen wird.	10
DI-Adresse	Definieren Sie die Adresse von DI, Bereich: 0-255.	0
DO-Adresse	Definieren Sie die Adresse von DO, Bereich: 0, 2-255.	0
Serverliste		
IP	Geben Sie die IP-Adresse des Servers ein.	
Port	Geben Sie den Port des Servers ein. Bereich: 0-65535.	
Status	Zeigt den Verbindungsstatus zwischen dem Router und dem Server an.	

Tabelle 3-4-3-3 Modbus RTU über TCP-Parameter

3.4.4 Modbus-Client (Master)

Der UR35-Router kann als Modbus-Client eingerichtet werden, um den Remote-Modbus-Server abzufragen und entsprechend der Antwort einen Alarm zu senden.

3.4.4.1 Modbus-Client

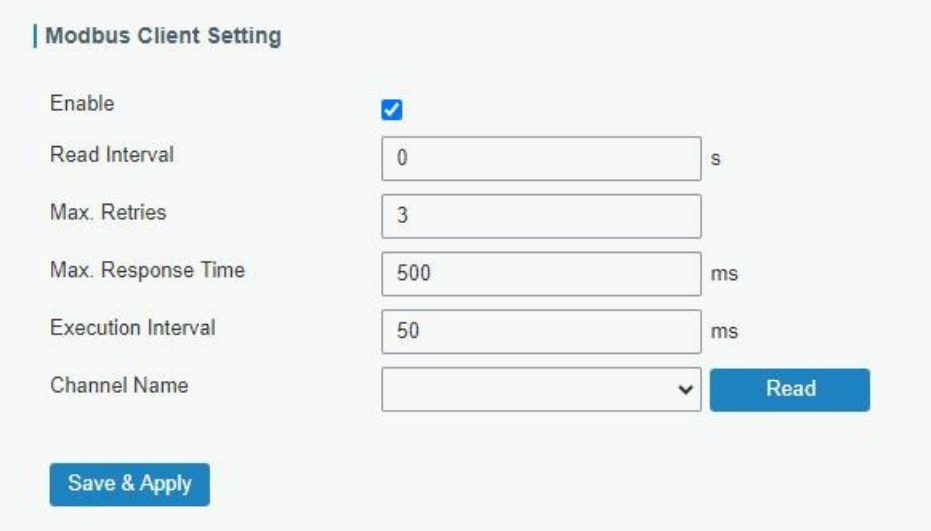


Abbildung 3-4-4-1

Modbus-Client		
Element	**Beschreibung**	**Standard**
Aktivieren	Modbus-Client aktivieren/deaktivieren.	--
Leseintervall	Legen Sie das Intervall für das Lesen von Remote-Kanälen fest. Wenn der Lesezyklus endet, werden die Befehle, die nicht gesendet wurden, verworfen und der neue Lesezyklus beginnt. Wenn der Wert auf 0 gesetzt ist, Gerät den neuen Lesezyklus neu, nachdem alle Kanäle	0

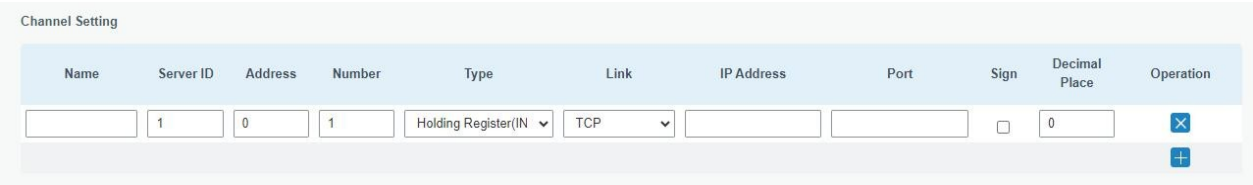
	gelesen wurden. Bereich: 0-600.	
Max. Wiederholungsversuche	Legen Sie die maximale Anzahl der Wiederholungsversuche nach einem Lesefehler fest, Bereich: 0-5.	3
Max. Antwortzeit/ms	Legen Sie die maximale Antwortzeit fest, die der Router auf die Antwort auf den Befehl wartet. Wenn das Gerät nach Ablauf der maximalen Antwortzeit keine Antwort erhält, wird davon ausgegangen , dass der Befehl abgelaufen ist. Bereich: 10-1000.	500
Ausführungsintervall Intervall/ms	Das Ausführungsintervall zwischen den einzelnen Befehlen. Bereich: 10–1000.	50
Kanal Name	Wählen Sie einen lesbaren Kanal aus der Kanalliste aus.	--

Tabelle 3-4-4-1

3.4.4.2 Kanal

Auf dieser Seite können Sie Kanäle hinzufügen und Alarmeinstellungen konfigurieren, um den Router mit dem Remote-Modbus-Server zu verbinden, die Adresse auf dieser Seite abzufragen und Alarme vom Router unter verschiedenen Bedingungen zu empfangen.

Abbildung 3-4-4-2



Kanaleinstellung	
Element	**Beschreibung**
Name	Legen Sie den Namen fest, um den Remote-Kanal zu identifizieren. Er darf nicht leer sein.
Server-ID	Legen Sie die Modbus-Server-ID fest.
Adresse	Die Startadresse für das Lesen von Modbus.
Nummer	Die Lesemenge ab der Startadresse.
Typ	Datentyp des Lesebefehls, Optionen sind Spule, Diskret, Halteregister (INT16), Eingangsregister (INT16), Halteregister (INT32) und Halteregister (Float).
Verbindung	Wählen Sie die serielle Schnittstelle oder die TCP-Verbindung aus. **Serielle Schnittstelle:** Der Router kommuniziert mit Geräten über das Modbus-RTU-Protokoll. **TCP:** Der Router kommuniziert mit Geräten über das Modbus-TCP-Protokoll.
IP-Adresse	Wenn die Verbindung TCP ist, geben Sie die IP-Adresse des entfernten Modbus-TCP-Geräts ein.
Port	Wenn es sich um eine TCP-Verbindung handelt, geben Sie den Port des entfernten Modbus-TCP-Geräts ein.
Zeichen	Wenn es sich um ein Halte- oder Eingangsregister handelt, aktivieren oder deaktivieren Sie diese Option, um anzugeben, ob dieser Kanal vorzeichenbehaftet ist.
Dezimalstelle	Wenn der Typ ein Halte- oder Eingangsregister ist, geben Sie einen Punkt in der Lesung in die Position des Kanals. Beispiel: Der gelesene Kanalwert beträgt 1234 und die Dezimalstelle ist gleich 2, dann ist der tatsächliche Wert 12,34.

Tabelle 3-4-4-2

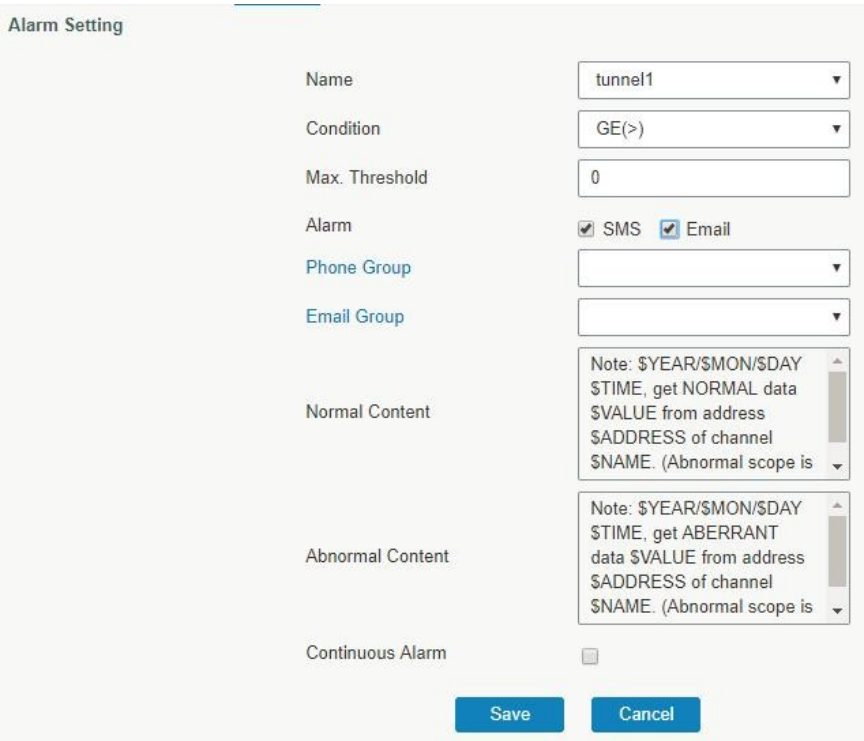


Abbildung 3-4-4-3

Alarmeinstellung	
Element	**Beschreibung**
Name	Legen Sie denselben Namen wie den Kanalnamen fest, um den Remote-Kanal zu identifizieren.
Bedingung	Die Bedingung, die den Alarm auslöst.
Min Schwellenwert	Legen Sie den Mindestwert fest, bei dem die Warnmeldung ausgelöst wird. Wenn der tatsächliche Wert unter Bei Überschreiten dieses Wertes wird der Alarm ausgelöst.
Max. Schwellenwert	Legen Sie den Maximalwert fest, bei dem der Alarm ausgelöst wird. Wenn der tatsächliche Wert diesen Wert überschreitet diesem Wert liegt, wird der Alarm ausgelöst.
Alarm	Wählen Sie die Alarmmethode als SMS oder E-Mail.
SMS	Der voreingestellte Alarmtext wird an die angegebene Telefonnummer gesendet.
Telefon Gruppe	Wählen Sie die Telefongruppe aus, die die Alarm-SMS erhalten soll.
E-Mail-Gruppe	Wählen Sie die E-Mail-Gruppe aus, die die Alarm-E-Mail erhalten soll.
Normaler Inhalt	Wenn der tatsächliche Wert nach Überschreiten des Schwellenwerts wieder auf den Normalwert zurückkehrt Schwellenwert wieder auf den Normalwert zurückkehrt, hebt der Router automatisch den Alarm wegen einer Anomalie auf und sendet den voreingestellten normalen Inhalt an die angegebene Telefongruppe.
Anormaler Inhalt	Wenn der tatsächliche Wert den voreingestellten Schwellenwert überschreitet, löst der Router automatisch den Alarm aus und sendet den voreingestellten abnormalen Inhalt an die angegebene Telefongruppe.
Kontinuierlich Alarm	Sobald diese Funktion aktiviert ist, wird derselbe Alarm kontinuierlich gemeldet. Andernfalls wird derselbe Alarm nur einmal gemeldet.

Tabelle 3-4-4-3

Abbildung 3-4-4-4

TCP-Weiterleitung	
Element	**Beschreibung**
Name	Der Name des Kanals des Modbus-Clients.
IP	Die IP-Adresse des Servers, an den die Pakete weitergeleitet werden.
Port	Der Port des Servers, an den die Pakete weitergeleitet werden.

Tabelle 3-4-4-4

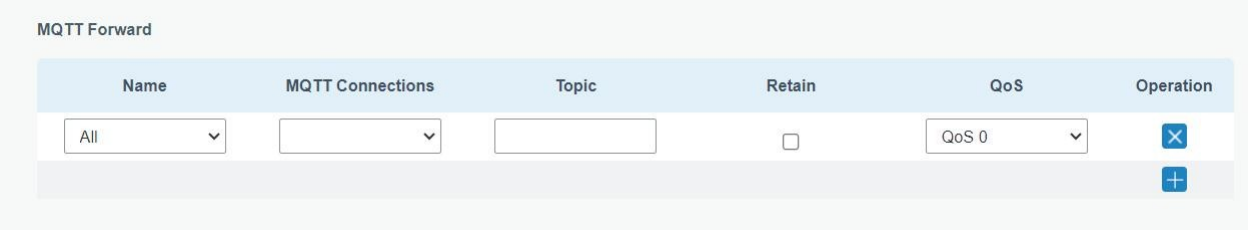


Abbildung 3-4-4-5

MQTT-Weiterleitung	
Element	**Beschreibung**
Name	Der Name des Kanals des Modbus-Clients.
MQTT Verbindungen	Wählen Sie die MQTT-Verbindung aus, um Modbus-Kanaldaten zu senden. Diese ist auf der Seite **„Service > MQTT“**.
Thema	Themenname, der für die Veröffentlichung von Modbus-Kanaldaten verwendet wird.
Beibehalten	Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als Retain-Nachricht festzulegen.
QoS	QoS0, QoS1 oder QoS2 sind optional.

Tabelle 3-4-4-5

3.4.5 GPS (gilt nur für GPS-Version)

Wenn Sie GPS-Daten empfangen möchten, sollten Sie die GPS-Funktion auf dieser Seite aktivieren.

Abbildung 3-4-5-1

3.4.5.1 GPS-IP-Weiterleitung

GPS-IP-Weiterleitung bedeutet, dass GPS-Daten über das Internet weitergeleitet werden können.

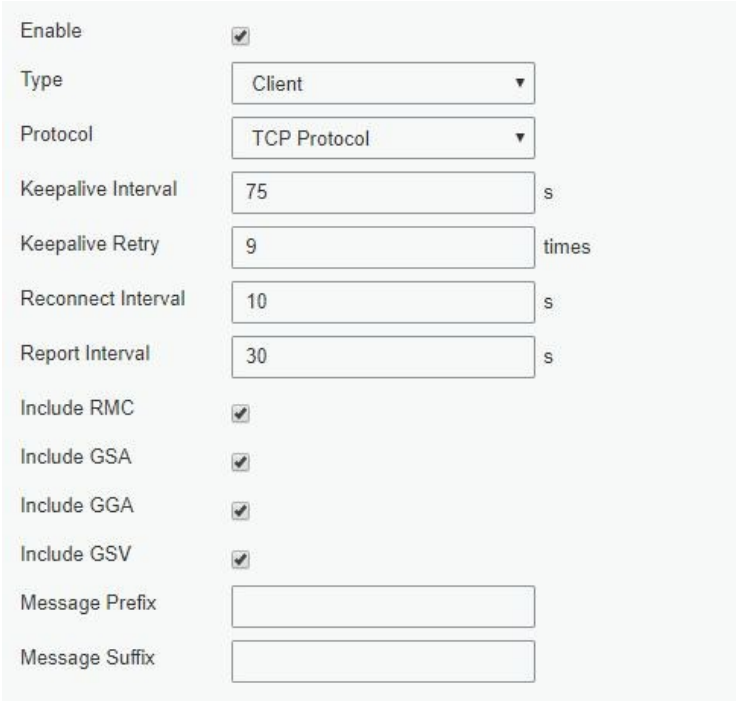


Abbildung 3-4-5-2

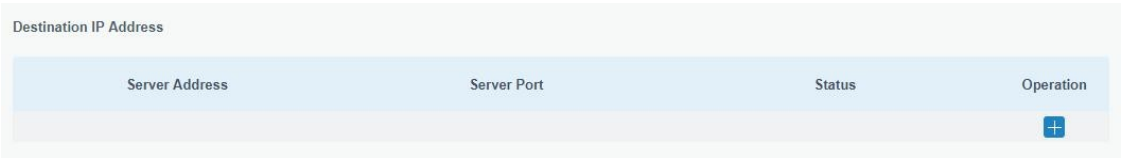


Abbildung 3-4-5-3

GPS-IP-Weiterleitung		
Element	**Beschreibung**	**Standard**
Aktiv	Leiten Sie die GPS-Daten an den Client oder Server weiter.	Deaktivieren
Typ	Wählen Sie den Verbindungstyp des Routers als Client oder Server aus.	Client
Protokoll	Wählen Sie das Protokoll für die Datenübertragung als TCP oder UDP.	TCP
Keepalive-Intervall	Nach der Verbindung mit dem Server/Client sendet der Router einen Heartbeat. Senden Sie regelmäßig ein Paket an den Server/Client, um die Verbindung aufrechtzuerhalten. Der Intervallbereich liegt zwischen 1 und 3600 Sekunden.	75
Keepalive-Wiederholungsversuch	Wenn der TCP-Heartbeat-Zeitüberschreitung erreicht ist, sendet der Router den Heartbeat erneut. Nach Erreichen der voreingestellten Wiederholungszeiten stellt der Router die Verbindung zum TCP-Server wieder her. Der Bereich liegt zwischen 1 und 16.	9
Lokaler Port	Legen Sie den Listening-Port des Routers fest. Bereich: 1-65535.	
Wiederverbinden Intervall	Nach einem Verbindungsfehler stellt der Router die Verbindung zum Server im voreingestellten Intervall erneut mit dem Server. Der Bereich liegt zwischen 10 und 60 Sekunden.	10
Meldeintervall	Der Router sendet GPS-Daten in voreingestellten Intervallen an den Server/Client. Der Bereich liegt zwischen 1 und 60 Sekunden.	30
RMC einschließen	RMC umfasst Daten zu Uhrzeit, Datum, Position, Kurs und Geschwindigkeit.	--
GSA einschließen	GSA umfasst den Betriebsmodus des GPS-Empfängers,die verwendeten Satelliten in der	--

	Positionsbestimmung verwendeten Satelliten und die DOP-Werte.	
GGA einschließen	GGA umfasst Zeit-, Positions- und Fix-Typ-Daten.	--
GSV einbeziehen	GSV enthält die Anzahl, Höhe und Azimut der GPS-Satelliten und SNR-Werte.	--
Nachricht Präfix	Fügen Sie den GPS-Daten ein Präfix hinzu.	Null
Nachricht Suffix	Fügen Sie den GPS-Daten ein Suffix hinzu.	Null
Ziel-IP-Adresse		
Server Adresse	Geben Sie die Serveradresse ein, um GPS-Daten zu empfangen (IP/Domänenname).	--
Server-Port	Geben Sie den Port für den Empfang von GPS-Daten ein. Bereich: 1-65535.	--
Status	Zeigt den Verbindungsstatus zwischen dem Router und dem Server an.	--

Tabelle 3-4-5-1 GPS-IP-Weiterleitungsparameter

3.4.5.2 GPS-Serienweiterleitung

GPS-IP-Weiterleitung bedeutet, dass GPS-Daten an den seriellen Anschluss weitergeleitet werden können.

Abbildung 3-4-5-4

GPS-Serienweiterleitung		
Element	**Beschreibung**	**Standard**
Aktiv	Leitet die GPS-Daten an den voreingestellten seriellen Anschluss weiter.	Deaktivieren
Serieller Typ	Wählen Sie den seriellen Anschluss aus, der die GPS-Daten empfangen soll. Stellen Sie sicher, dass der serieller Anschluss unter **„Service > Serieller Anschluss“** aktiviert ist.	--
Meldeintervall	Der Router leitet die GPS-Daten an die serielle Schnittstelle weiter, und zwar Voreingestelltes Intervall. Der Bereich liegt zwischen 1 und 60 Sekunden.	30
RMC einbeziehen	RMC umfasst Daten zu Uhrzeit, Datum, Position, Kurs und Geschwindigkeit.	--
GSA einschließen	GSA umfasst den Betriebsmodus des GPS-Empfängers, die verwendeten Satelliten für die Positionsbestimmung verwendeten Satelliten und DOP-Werte.	--
GGA einschließen	GGA umfasst Zeit-, Positions- und Fix-Typ-Daten.	--

GSV einbeziehen	GSV umfasst die Anzahl, Höhe und Azimut der GPS-Satelliten und SNR-Werte.	--

Tabelle 3-4-5-2 GPS-Serienweiterleitungsparameter

3.4.5.3 GPS MQTT-Weiterleitung

GPS-MQTT-Weiterleitung bedeutet, dass GPS-Rohdaten automatisch an den MQTT-Broker weitergeleitet werden können.

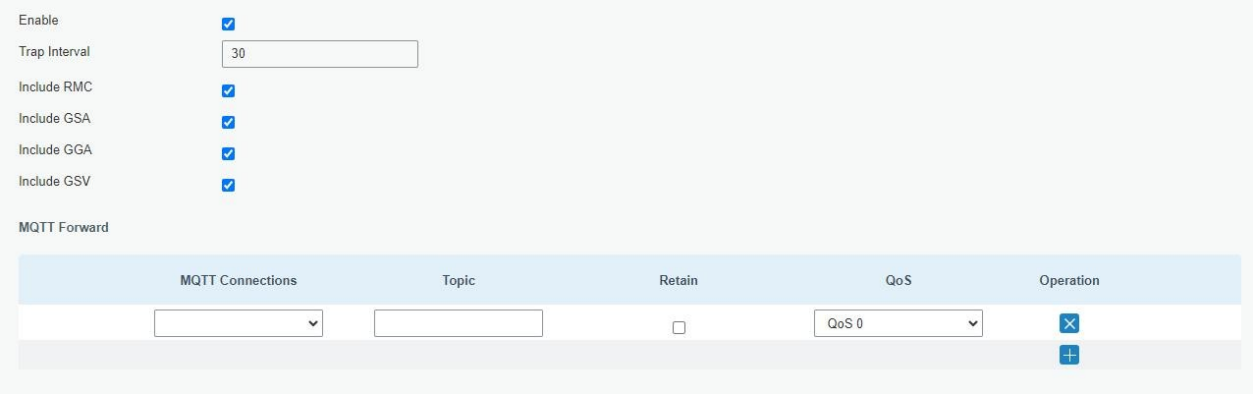


Abbildung 3-4-5-5

GPS-MQTT-Weiterleitung		
Element	**Beschreibung**	**Standard**
Aktivieren	Leitet die GPS-Daten automatisch an den MTT-Broker weiter.	Deaktivieren
Trap-Intervall	Das Intervall, in dem die GPS-Daten ermittelt und an den MQTT-Broker zu lokalisieren und weiterzuleiten. Der Bereich liegt zwischen 1 und 60 Sekunden.	30
RMC einschließen	RMC umfasst Daten zu Uhrzeit, Datum, Position, Kurs und Geschwindigkeit.	--
GSA einschließen	GSA umfasst den Betriebsmodus des GPS-Empfängers,die verwendeten Satelliten für die Positionsbestimmung und die DOP-Werte.	--
GGA	GGA umfasst Zeit-, Positions- und Fix-Typ-Daten.	--
GSV einbeziehen	GSV umfasst die Anzahl, Höhe und Azimut der GPS-Satelliten und SNR-Werte.	--
MQTT-Weiterleitung		
MQTT Verbindungen	Wählen Sie die MQTT-Verbindung zum Senden von GPS-Daten aus. Diese ist unter **„Service“ > MQTT** eingerichtet.	
Thema	Themenname für die Veröffentlichung von GPS-Rohdaten.	
Beibehalten	Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als gespeicherte Nachricht festzulegen.	
QoS	QoS0, QoS1 oder QoS2 sind optional.	

Tabelle 3-4-5-3 GPS-MQTT-Weiterleitungsparameter

3.4.6 MQTT

UR35 unterstützt die Arbeit als MQTT-Client, um Daten und Router-Informationen auf zwei Arten an den MQTT-Broker weiterzuleiten:

1. Benutzer senden Anfragen an den Router, um die Routerinformationen abzufragen.
2. Der Router veröffentlicht die Daten automatisch.

Abbildung 3-4-6-1

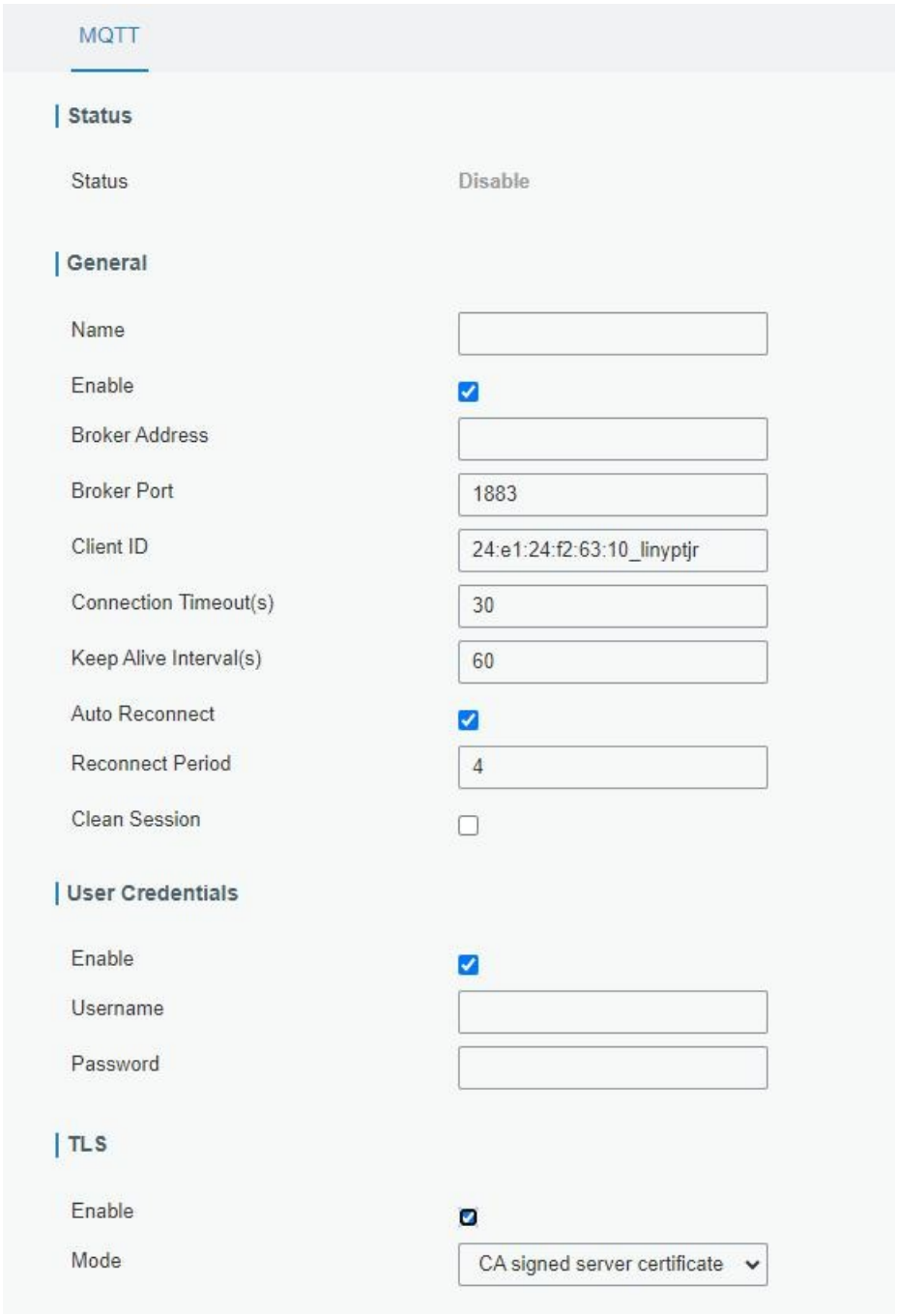


Abbildung 3-4-6-2

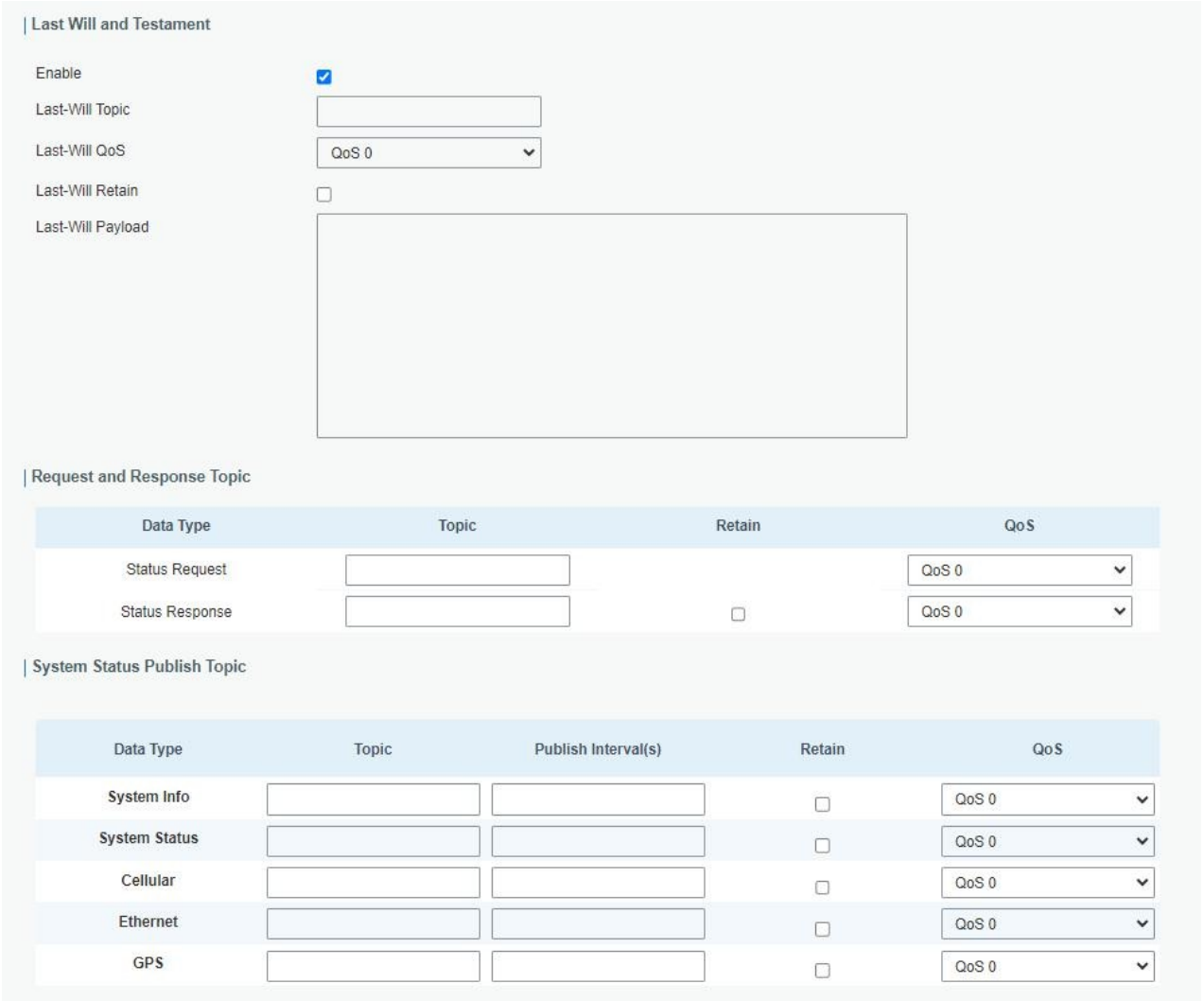


Abbildung 3-4-6-3

MQTT-Einstellungen	
Element	**Beschreibung**
Status	Zeige den Verbindungsstatus zwischen Router und MQTT-Broker an.
Allgemein	
Name	Passen Sie einen eindeutigen Verbindungsnamen an. Nach dem Speichern kann dieser nicht mehr geändert werden. Speichern
Aktivieren	Aktivieren oder deaktivieren Sie diese MQTT-Verbindung.
Broker-Adresse	MQTT-Broker-Adresse zum Empfangen von Daten.
Broker-Port	MQTT-Broker-Port zum Empfangen von Daten.
Client-ID	Die Client-ID ist die eindeutige Identität des Clients gegenüber dem Server. Sie muss eindeutig sein. wenn alle Clients mit demselben Server verbunden sind, und es ist der Schlüssel zur Verarbeitung von Nachrichten mit QoS 1 und 2.
Verbindung Zeitüberschreitung/s	Wenn der Client nach Ablauf des Verbindungszeitlimits keine Antwort erhält, Verbindung als unterbrochen betrachtet. Der Bereich: 1-65535.
Keep Alive Intervall/s	Nachdem der Client mit dem Server verbunden ist, sendet der Client regelmäßig Heartbeat-Pakete Paket an den Server, um die Verbindung aufrechtzuerhalten. Bereich: 1-65535.
Auto	Wenn die Verbindung unterbrochen wird, versuchen Sie, die Verbindung zum Server automatisch wiederherzustellen.

Wiederverbinden	
Wiederverbinden Zeitraum	Wenn die Verbindung unterbrochen wird, wird der Zeitraum für die erneute Verbindung mit dem Server .
Sitzung bereinigen	Wenn diese Option aktiviert ist, erstellt die Verbindung eine temporäre Sitzung, und alle Informationen gehen verloren, wenn die Verbindung des Clients zum Broker unterbrochen wird. Wenn diese Option deaktiviert ist, erstellt die Verbindung eine dauerhafte Sitzung, die bestehen bleibt und speichert Offline-Nachrichten, bis die Sitzung nach Ablauf der Zeit abgemeldet wird.
Benutzeranmeldedaten	
Aktivieren	Benutzeranmeldedaten aktivieren.
Benutzername	Der Benutzername, der für die Verbindung mit dem MQTT-Broker verwendet wird.
Passwort	Das Passwort, das für die Verbindung mit dem MQTT-Broker verwendet wird.
TLS	
Aktivieren	Aktivieren Sie die TLS-Verschlüsselung in der MQTT-Kommunikation.
Modus	Wählen Sie zwischen selbstsignierten Zertifikaten und CA-signierten Serverzertifikaten. **CA-signiertes Serverzertifikat:** Überprüfen Sie das Zertifikat mit dem Zertifikat, das von der Zertifizierungsstelle (CA) ausgestellt und auf dem Gerät vorinstalliert ist. **Selbstsignierte Zertifikate:** Laden Sie die benutzerdefinierten CA-Zertifikate, Client-Zertifikate und den geheimen Schlüssel zur Überprüfung hoch.
Letzter Wille und Testament	
Aktivieren	Die Last-Will-Nachricht wird automatisch gesendet, wenn die Verbindung zum MQTT-Client abnormal getrennt wird. Sie wird in der Regel verwendet, um Geräte-Statusinformationen zu senden oder andere Geräte oder Proxy-Server über den Offline-Status des Geräts zu informieren .
Last-Will-Thema	Passen Sie das Thema an, um Last-Will-Nachrichten zu empfangen.
Last-Will-QoS	QoS0, QoS1 oder QoS2 sind optional.
Last-Will-Beibehaltung	Aktivieren Sie diese Option, um die Last-Will-Nachricht als Retain-Nachricht festzulegen.
Letzter Wille Nutzlast	Passen Sie den Inhalt der Last-Will-Nachricht an.
Anfrage- und Antwortthema	
Thema	Der Router unterstützt das Senden von Anfragen zur Abfrage von Router-Informationen. **Statusabfrage:** Benutzer können Anfragen an dieses Thema senden, um Router-Informationen abzufragen. Anfrageformat: *{* *"id":"1",* *"status":"systeminfo", „sn":* "64E1213132456", „need_response":1 //1 bedeutet, dass eine Antwort erforderlich ist *}* Die ID ist ein Zufallswert, und der Status kann auf fünf Arten festgelegt werden: systeminfo, systemstatus, cellular, ethernet, gps. **Statusantwort:** Benutzer können dieses Thema abonnieren, um die Antworten zu erhalten.
Beibehalten	Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als gespeicherte Nachricht festzulegen.
QoS	QoS0, QoS1 oder QoS2 sind optional.
Systemstatus-Veröffentlichungsthema	

Datentyp	Datentyp, der automatisch an den MQTT-Broker gesendet wird. Beachten Sie, dass es sich bei den GPS-Daten auf dieser Seite keine Rohdaten, sondern dekodierte Standortdaten sind.
Thema	Themenname des für die Veröffentlichung verwendeten Datentyps.
Veröffentlichungsintervall (s)	Das Intervall, in dem Daten automatisch an den MQTT-Broker veröffentlicht werden.
Beibehalten	Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als gespeicherte Nachricht festzulegen.
QoS	QoS0, QoS1 oder QoS2 sind optional.

Tabelle 3-4-6-1 MQTT-Parameter

3.4.7 SNMP

SNMP wird häufig im Netzwerkmanagement für die Netzwerküberwachung verwendet. SNMP stellt Verwaltungsdaten mit Variablenform im verwalteten System bereit. Das System ist in einer Verwaltungsinformationsbasis (MIB) organisiert, die den Systemstatus und die Konfiguration beschreibt. Diese Variablen können von Verwaltungsanwendungen aus ferngesteuert abgefragt werden.

Die Konfiguration von SNMP im Netzwerk, NMS und einem Verwaltungsprogramm von SNMP sollte auf dem Manager eingerichtet werden.

Die folgenden Konfigurationsschritte sind erforderlich, um eine Abfrage von NMS durchzuführen:

1. Aktivieren Sie die SNMP-Einstellung.
2. Laden Sie die MIB-Datei herunter und laden Sie sie in NMS.
3. Konfigurieren Sie die MIB-Ansicht.
4. Konfigurieren Sie VCAM.

Beispiel für eine entsprechende Konfiguration

SNMP-Anwendungsbeispiel

3.4.7.1 SNMP

UR35 unterstützt die Versionen SNMPv1, SNMPv2c und SNMPv3. SNMPv1 und SNMPv2c verwenden die Authentifizierung über einen Community-Namen. SNMPv3 verwendet die Authentifizierung durch Verschlüsselung mit Benutzername und Passwort.

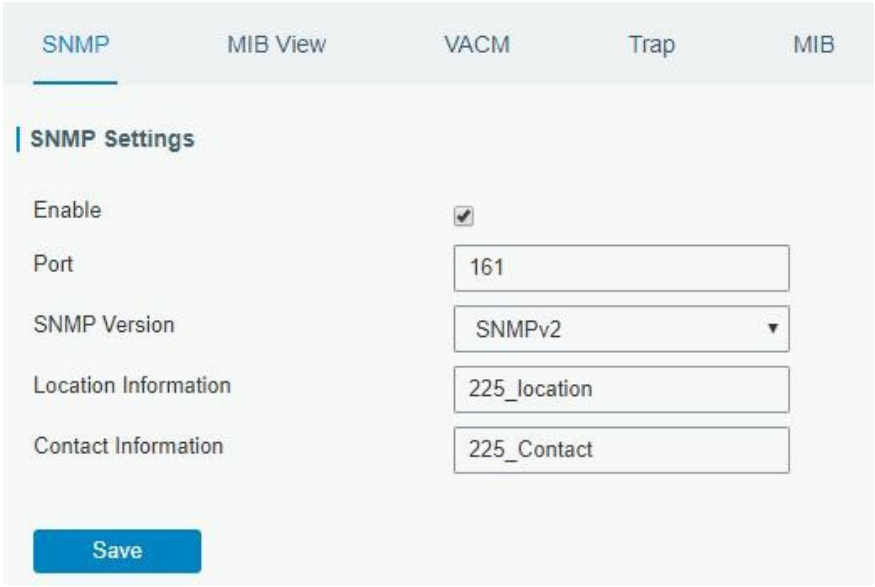


Abbildung 3-4-7-1

SNMP-Einstellungen	
Element	**Beschreibung**
Aktivieren	Aktivieren oder deaktivieren Sie die SNMP-Funktion.
Port	SNMP-Empfangsport festlegen. Bereich: 1-65535. Der Standardport ist 161.
SNMP-Version	Wählen Sie die SNMP-Version aus; unterstützt SNMP v1/v2c/v3.
Standortinformationen	Geben Sie die Standortinformationen ein.
Kontakt	Geben Sie die Kontaktinformationen ein.

Tabelle 3-4-7-1 SNMP-Parameter

3.4.7.2 MIB-Ansicht

In diesem Abschnitt wird erläutert, wie Sie die MIB-Ansicht für die Objekte konfigurieren.

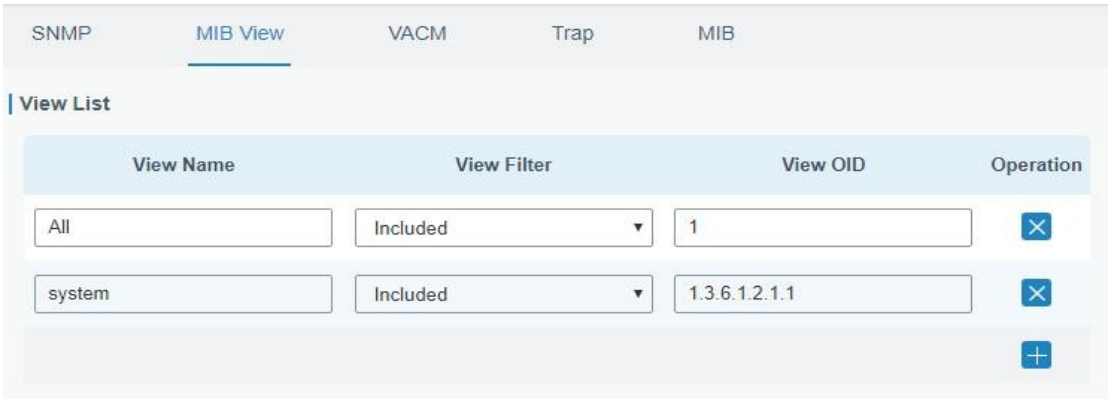


Abbildung 3-4-7-2

MIB-Ansicht	
Element	**Beschreibung**
Ansichtsname	Legen Sie den Namen der MIB-Ansicht fest.
Ansichtsfilter	Wählen Sie zwischen „Enthalten" und „Ausgeschlossen".

Ansicht-OID	Geben Sie die OID-Nummer ein.
Enthalten	Sie können alle Knoten innerhalb des angegebenen MIB-Knotens abfragen.
Ausgeschlossen	Sie können alle Knoten außer dem angegebenen MIB-Knoten abfragen.

Tabelle 3-4-7-2 MIB-Ansichtsparameter

3.4.7.3 VACM

In diesem Abschnitt wird beschrieben, wie Sie VCAM-Parameter konfigurieren.

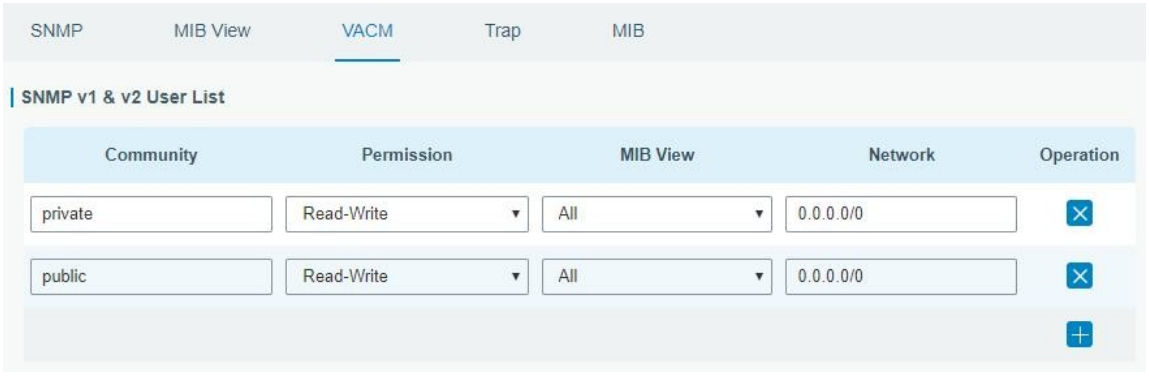


Abbildung 3-4-7-3

VACM	
Element	**Beschreibung**
SNMP v1 & v2 Benutzerliste	
Community	Legen Sie den Community-Namen fest.
Berechtigung	Wählen Sie zwischen „Nur Lesen" und „Lesen/Schreiben".
MIB-Ansicht	Wählen Sie eine MIB-Ansicht aus der MIB-Ansichtsliste aus, um Berechtigungen festzulegen.
Netzwerk	Die IP-Adresse und die Bits des externen Netzwerks, das auf die MIB-Ansicht zugreift.
Lesen/Schreiben	Die Berechtigung für den angegebenen MIB-Knoten ist Lesen und Schreiben.
Nur Lesen	Die Berechtigung für den angegebenen MIB-Knoten ist schreibgeschützt.
SNMP v3-Benutzergruppe	
Gruppenname	Legen Sie den Namen der SNMPv3-Gruppe fest.
Sicherheitsstufe	Wählen Sie zwischen „NoAuth/NoPriv", „Auth/NoPriv" und „Auth/Priv".
Schreibgeschützte Ansicht	Wählen Sie eine MIB-Ansicht aus der MIB-Ansichtsliste aus, um die Berechtigung als „Nur Lesen" festzulegen.
Lese-/Schreibansicht	Wählen Sie eine MIB-Ansicht aus der MIB-Ansichtsliste aus, um die Berechtigung auf „Lesen-Schreiben" zu setzen.
Inform-Ansicht	Wählen Sie eine MIB-Ansicht aus der MIB-Ansichtsliste aus, um die Berechtigung auf „Informieren" festzulegen.
SNMP v3-Benutzerliste	
Benutzername	Legen Sie den Namen des SNMPv3-Benutzers fest.
Gruppenname	Wählen Sie eine Benutzergruppe aus, die konfiguriert werden soll.
Authentifizierung	Wählen Sie zwischen „MD5", „SHA" und „Keine" aus.
Authentifizierung Passwort	Das Passwort muss eingegeben werden, wenn die Authentifizierung „MD5" oder „SHA" ist.
Verschlüsselung	Wählen Sie zwischen „AES", „DES" und „Keine".
Verschlüsselung Passwort	Das Passwort muss eingegeben werden, wenn die Verschlüsselung „AES" oder „DES" ist.

Tabelle 3-4-7-3 VACM-Parameter

3.4.7.4 Trap

In diesem Abschnitt wird erläutert, wie Sie die Netzwerküberwachung durch SNMP-Traps aktivieren können.

Abbildung 3-4-7-4

SNMP-Trap	
Element	**Beschreibung**
Aktivieren	Aktivieren oder deaktivieren Sie die SNMP-Trap-Funktion.
SNMP-Version	Wählen Sie die SNMP-Version aus; unterstützt SNMP v1/v2c/v3.
Serveradresse	Geben Sie die IP-Adresse oder den Domänennamen des NMS ein.
Port	Geben Sie den UDP-Port ein. Der Portbereich liegt zwischen 1 und 65535. Der Standardport ist 162.
Name	Geben Sie den Gruppennamen ein, wenn Sie SNMP v1/v2c verwenden; geben Sie den Benutzernamen ein, wenn Sie SNMP v3.
Auth/Priv-Modus	Wählen Sie zwischen „NoAuth & No Priv", „Auth & NoPriv" und „Auth & Priv".

Tabelle 3-4-7-4 Trap-Parameter

3.4.7.5 MIB

In diesem Abschnitt wird beschrieben, wie Sie MIB-Dateien herunterladen können. Die letzte MIB-Datei „LTE-ROUTER-MIB.txt" ist für den UR35-Router bestimmt.

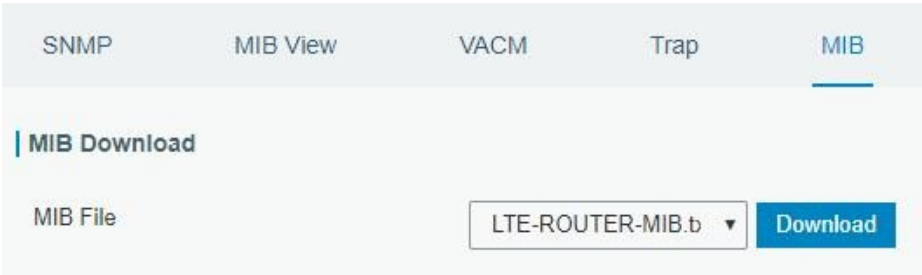


Abbildung 3-4-7-5

MIB	
Element	**Beschreibung**
MIB-Datei	Wählen Sie die gewünschte MIB-Datei aus.

Herunterladen	Klicken Sie auf die Schaltfläche „Herunterladen“, um die MIB-Datei auf den PC herunterzuladen.

Tabelle 3-4-7-5 MIB-Download

3.4.8 TR069

Der Technical Report 069 (TR-069) ist eine technische Spezifikation des Broadband Forum, die ein Anwendungsschichtprotokoll für die Fernverwaltung und Bereitstellung von Kundenendgeräten (CPE) definiert, die mit einem Internetprotokoll (IP)-Netzwerk verbunden sind.

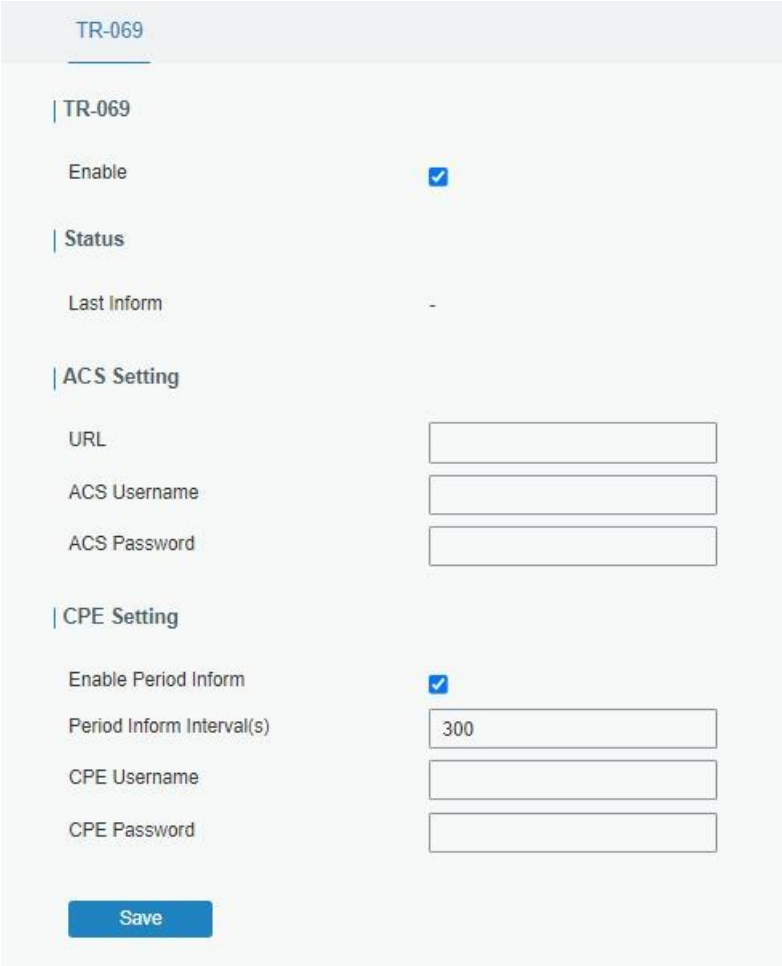


Abbildung 3-4-8-1

TR-069	
Element	**Beschreibung**
Aktivieren	Aktivieren oder deaktivieren Sie die TR069-Funktion.
Letzte Benachrichtigung	Das letzte Mal, als der Router TR069 ACS informiert hat.
ACS-Einstellung	
URL	Die URL des TR069-Autokonfigurationsservers (ACS).
ACS-Benutzername	Der Benutzername, den ACS zur Authentifizierung des CPE verwendet, wenn es eine Verbindungsanfrage initiiert.
ACS-Passwort	Das von ACS verwendete Passwort zur Authentifizierung des CPE, wenn es eine Verbindungsanforderung.
CPE-Einstellung	
Aktivierungszeitraum	Aktivieren oder deaktivieren Sie die regelmäßige Benachrichtigung.

Informationszeitraum	
Periodische Benachrichtigung Intervall (s)	Das Intervall, in dem Informationen an ACS gemeldet werden sollen. Dieses sollte kürzer sein als das Timeout des Peer-ACS.
CPE-Benutzername	Der Benutzername, den CPE zur Authentifizierung des ACS verwendet, wenn es eine Verbindungsanforderung initiiert.
CPE-Passwort	Das Passwort, das von CPE zur Authentifizierung des ACS verwendet wird, wenn es eine Verbindungsanforderung initiiert.

Tabelle 3-4-8-1 TR069-Parameter

3.5 Wartung

In diesem Abschnitt werden die Systemwartungstools und die Verwaltung beschrieben.

3.5.1 Tools

Zu den Tools zur Fehlerbehebung gehören Ping, Traceroute, Paketanalysator und qxdmlog.

3.5.1.1 Ping

Das Ping-Tool wurde entwickelt, um externe Netzwerke anzupingen.

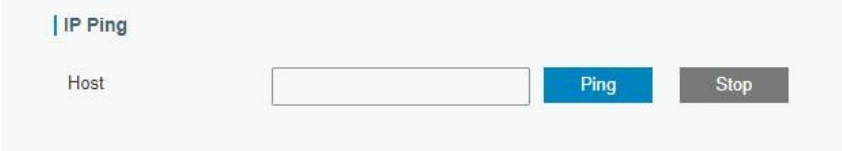


Abbildung 3-5-1-1

PING	
Element	**Beschreibung**
Host	Ping-Befehl für das externe Netzwerk vom Router aus.

Tabelle 3-5-1-1 IP-Ping-Parameter

3.5.1.2 Traceroute

Das Traceroute-Tool wird zur Fehlerbehebung bei Netzwerk-Routing-Fehlern verwendet.

Abbildung 3-5-1-2

Traceroute	
Element	**Beschreibung**
Host	Adresse des zu ermittelnden Zielhosts.

Tabelle 3-5-1-2 Traceroute-Parameter

3.5.1.3 Paketanalysator

Der Paketanalysator wird zum Erfassen der Pakete verschiedener Schnittstellen verwendet.

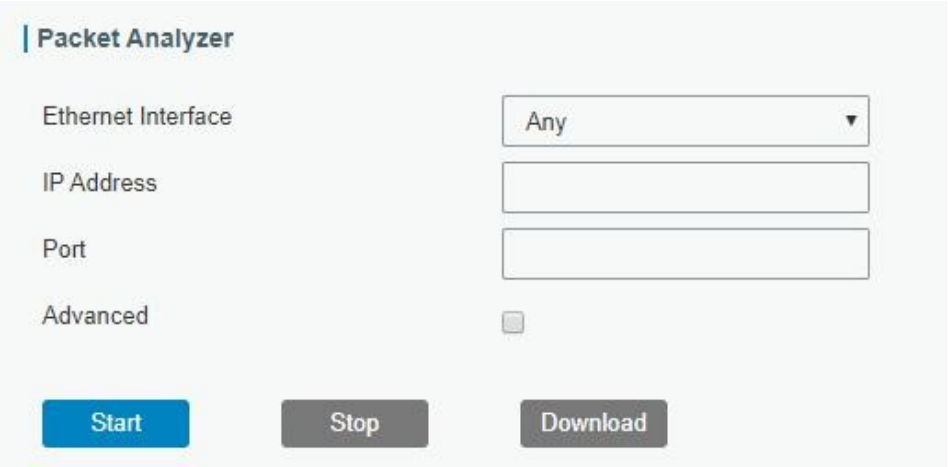


Abbildung 3-5-1-3

Paketanalysator	
Element	**Beschreibung**
Ethernet-Schnittstelle	Wählen Sie die Schnittstelle aus, über die Pakete erfasst werden sollen.
IP-Adresse	Legen Sie die IP-Adresse fest, die der Router erfassen soll.
Port	Legen Sie den Port fest, den der Router erfassen soll.
Erweitert	Legen Sie die Regeln für den Sniffer fest. Das Format lautet tcpdump.

Tabelle 3-5-1-3 Parameter des Paketanalysators

3.5.1.4 Qxdmlog

In diesem Abschnitt können Sie Diagnoseprotokolle über das QXDM-Tool erfassen.

Abbildung 3-5-1-4

3.5.2 Debugger

3.5.2.1 Mobilfunk-Debugger

In diesem Abschnitt wird erläutert, wie Sie AT-Befehle an den Router senden und Mobilfunk-Debug-Informationen überprüfen können.

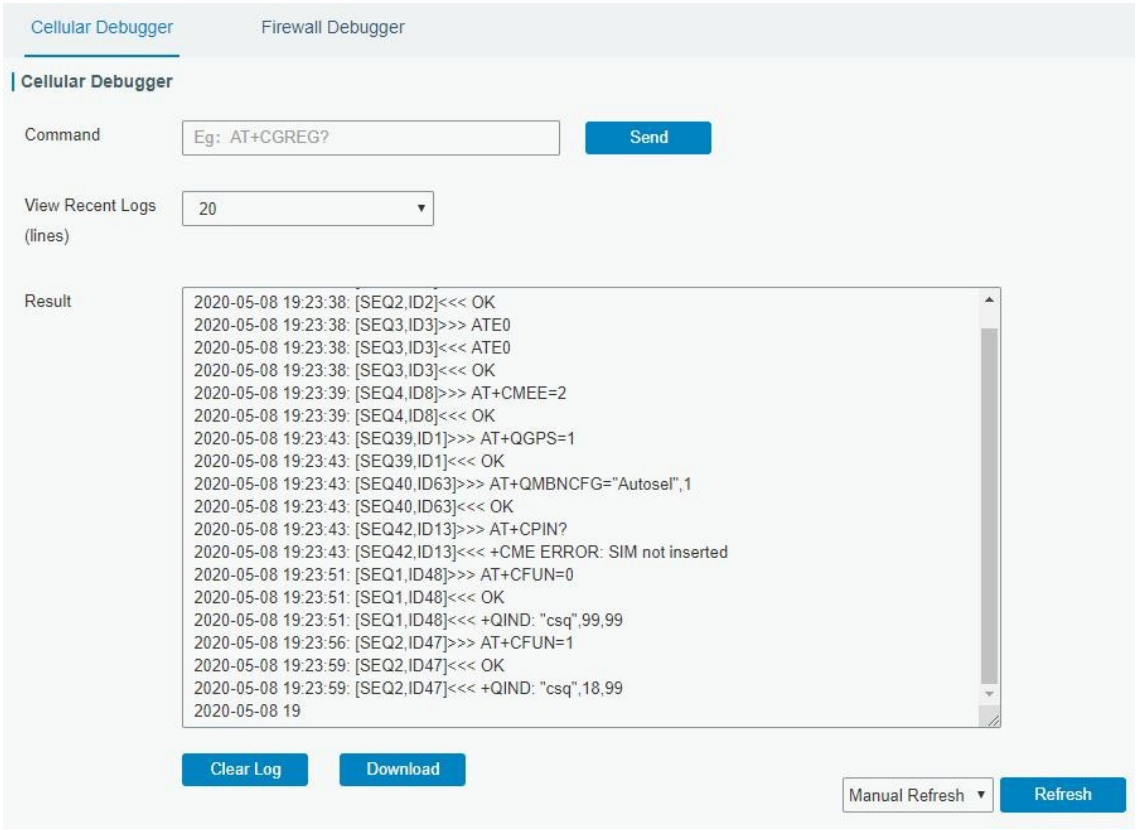


Abbildung 3-5-2-1

Mobilfunk-Debugger	
Element	**Beschreibung**
Befehl	Geben Sie den AT-Befehl ein, den Sie an das Mobilfunkmodem senden möchten.
Aktuelle Protokolle anzeigen (Zeilen)	Zeigen Sie die angegebenen Zeilen des Ergebnisses an.
Ergebnis	Zeigen Sie das Antwort-Ergebnis vom Mobilfunkmodem an.

Tabelle 3-5-2-1 Parameter des Mobilfunk-Debuggers

3.5.2.2 Firewall-Debugger

In diesem Abschnitt wird erläutert, wie Sie Befehle an den Router senden und Firewall-Informationen überprüfen können.

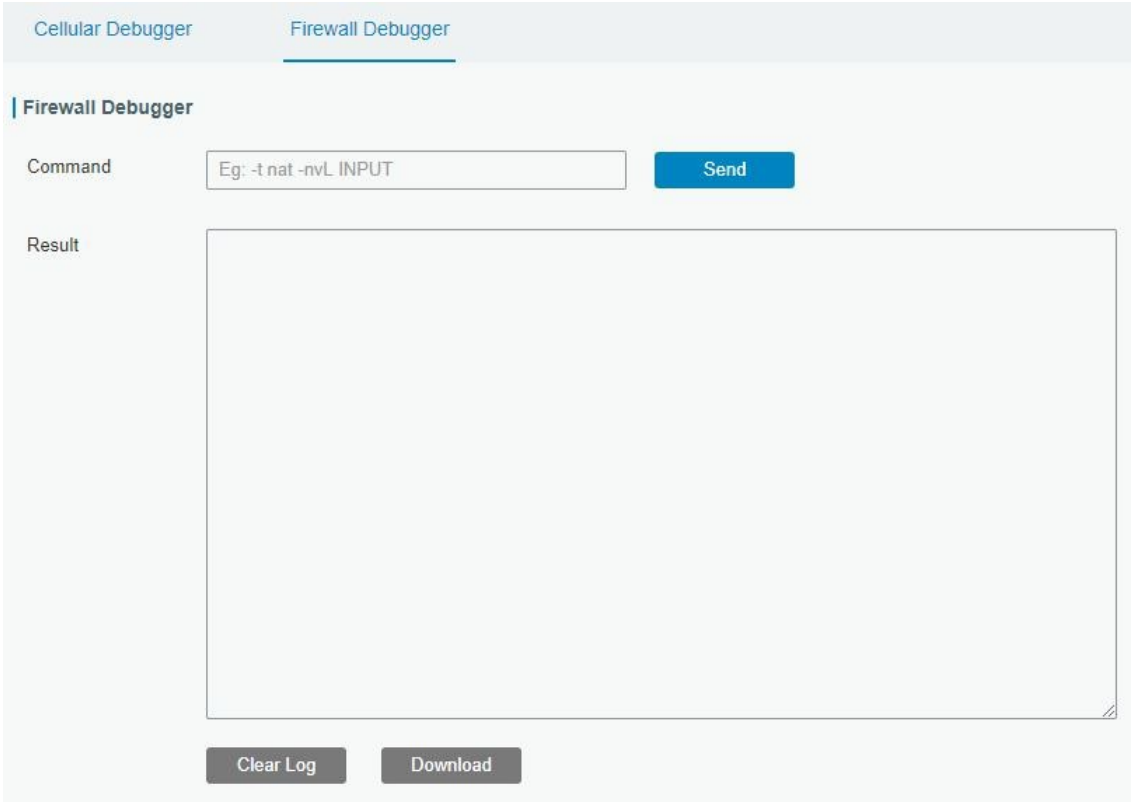


Abbildung 3-5-2-2

Firewall-Debugger	
Element	**Beschreibung**
Befehl	Geben Sie den AT-Befehl ein, den Sie an das Firewall-Modul senden möchten.
Ergebnis	Zeigen Sie das Antwort-Ergebnis vom Firewall-Modul an.

Tabelle 3-5-2-2 Firewall-Debugger-Parameter

3.5.3 Protokoll

Das Systemprotokoll enthält eine Aufzeichnung von Informations-, Fehler- und Warnereignissen, die Aufschluss über die Systemprozesse geben. Durch Überprüfen der im Protokoll enthaltenen Daten kann ein Administrator oder Benutzer, der Fehler im System behebt, die Ursache eines Problems identifizieren oder feststellen, ob die Systemprozesse erfolgreich geladen werden. Ein Remote-Protokollserver ist möglich, und der Router lädt alle Systemprotokolle auf einen Remote-Protokollserver wie Syslog Watcher hoch.

3.5.3.1 Systemprotokoll

In diesem Abschnitt wird beschrieben, wie Sie das aktuelle Protokoll im Web anzeigen können.

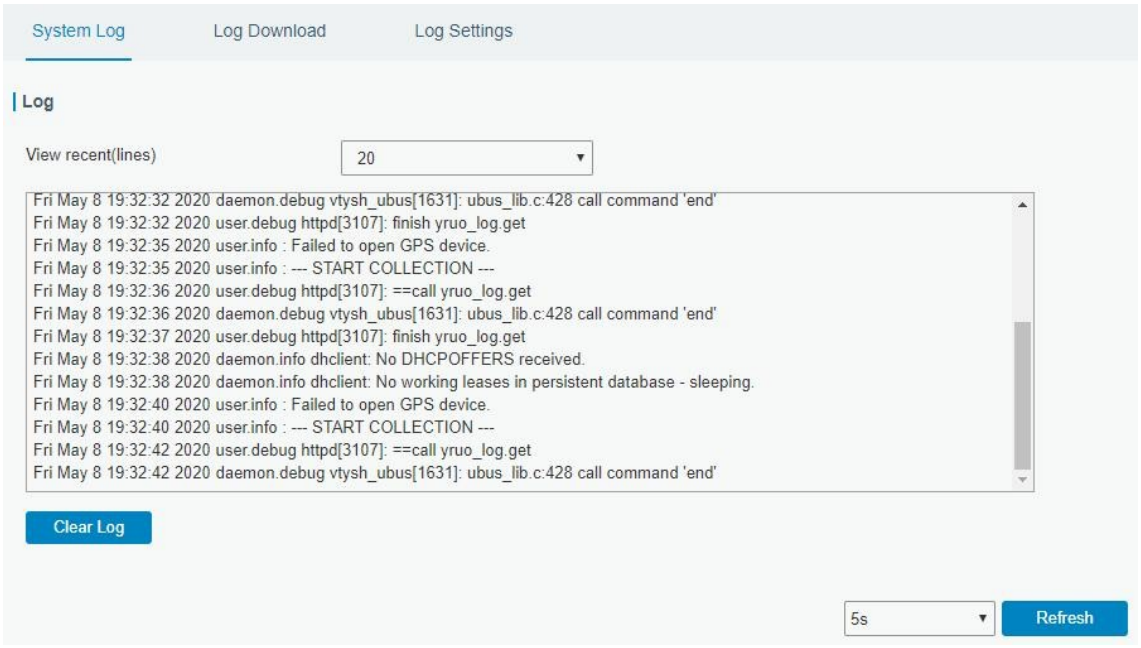


Abbildung 3-5-3-1

Systemprotokoll	
Element	**Beschreibung**
Aktuelle (Zeilen) anzeigen	Zeigt die angegebenen Zeilen des Systemprotokolls an.
Protokoll löschen	Löschen Sie das aktuelle Systemprotokoll.

Tabelle 3-5-3-1 Parameter für das Systemprotokoll

3.5.3.2 Protokoll herunterladen

In diesem Abschnitt wird beschrieben, wie Sie Protokolldateien herunterladen können.

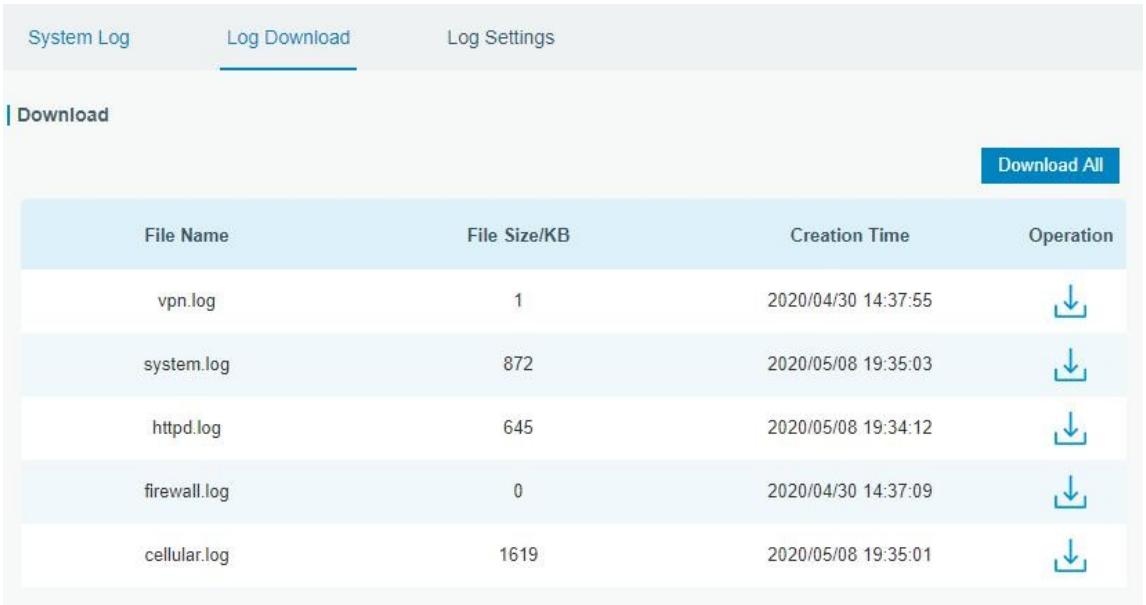


Abbildung 3-5-3-2

Protokoll-Download	
Element	**Beschreibung**
Alle herunterladen	Alle Protokolldateien herunterladen.

Dateiname	Zeigt den Namen der Protokolldateien an.
Dateigröße/KB	Größe der Protokolldateien anzeigen.
Erstellungszeit	Zeigt die Erstellungszeit der Protokolldateien an.
Vorgang	Klicken Sie hier, um alle Protokolldateien herunterzuladen.

Tabelle 3-5-3-2 Systemprotokollparameter

3.5.3.3 Protokolleinstellungen

In diesem Abschnitt wird erläutert, wie Sie den Remote-Protokollserver und die lokalen Protokolleinstellungen aktivieren.

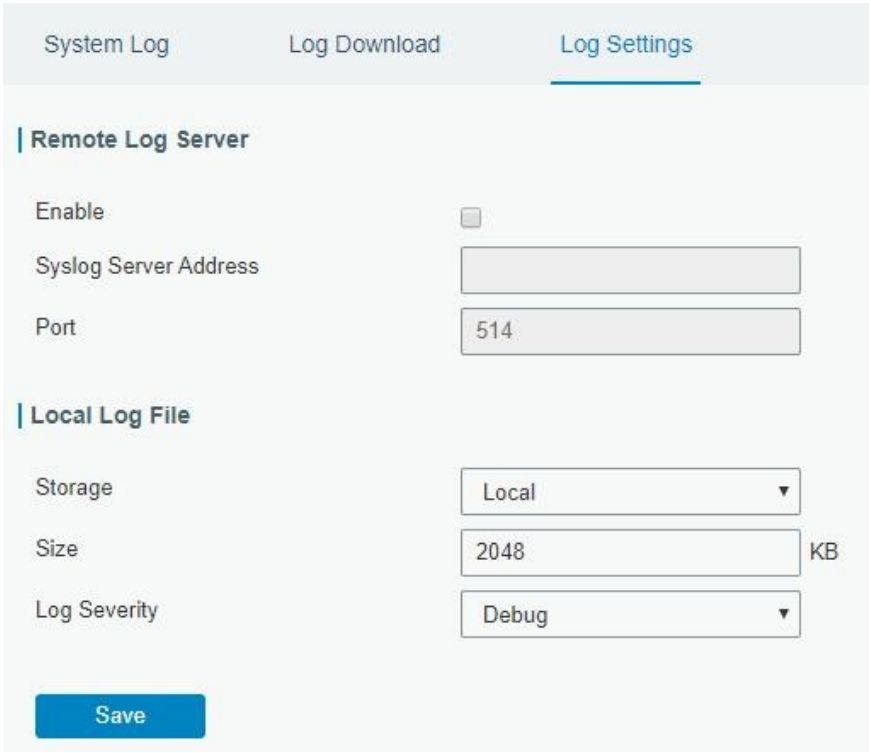


Abbildung 3-5-3-3

Protokolleinstellungen	
Element	**Beschreibung**
Remote-Protokollserver	
Aktivieren	Wenn „Remote-Protokollserver“ aktiviert ist, sendet der Router alle Systemprotokolle an den Remote-Server.
Syslog-Serveradresse	Geben Sie die Adresse des Remote-Systemprotokoll-Servers ein (IP/Domänenname).
Port	Geben Sie den Port des Remote-Systemprotokoll-Servers ein.
Lokale Protokolldatei	
Speicher	Der Benutzer kann die Protokolldatei im Speicher oder auf einer TF-Karte speichern.
Größe	Legen Sie die Größe der zu speichernden Protokolldatei fest.
Protokollschweregrad	Die Liste der Schweregrade entspricht dem Syslog-Protokoll.

Tabelle 3-5-3-3 Protokolleinstellungsparameter

3.5.4 Aktualisierung

In diesem Abschnitt wird beschrieben, wie Sie die Router-Firmware über das Internet aktualisieren können. In der Regel ist ein Firmware-Upgrade nicht erforderlich.

Hinweis: Während der Firmware-Aktualisierung sind keine Vorgänge auf der Webseite zulässig, da dies zu einer Unterbrechung der Aktualisierung oder sogar zu einem Ausfall des Geräts führen kann.

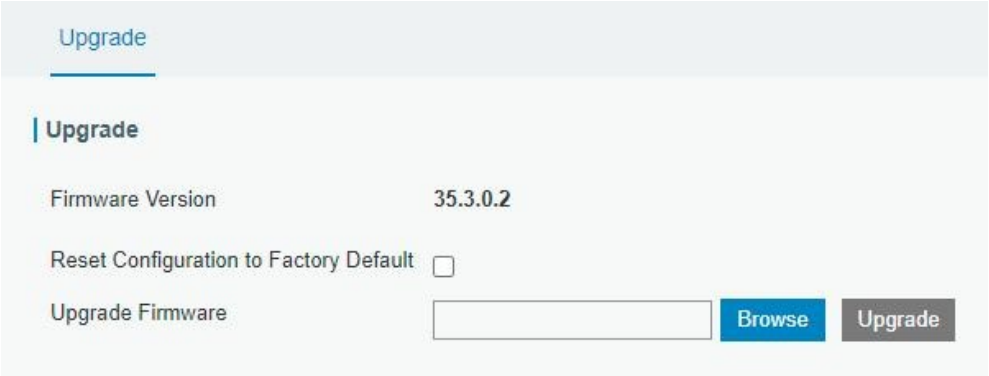


Abbildung 3-5-4-1

Aktualisierung	
Element	**Beschreibung**
Firmware-Version	Zeigt die aktuelle Firmware-Version an.
Konfiguration zurücksetzen auf Werkseinstellungen zurücksetzen	Wenn diese Option aktiviert ist, wird der Router nach dem Upgrade auf die Werkseinstellungen zurückgesetzt.
Firmware aktualisieren	Klicken Sie auf die Schaltfläche „Durchsuchen“, um die neue Firmware-Datei auszuwählen, und klicken Sie auf „Aktualisieren“, um die Firmware zu aktualisieren.

Tabelle 3-5-4-1 Upgrade-Parameter

Beispiel für die zugehörige Konfiguration

Firmware-Upgrade

3.5.5 Sichern und Wiederherstellen

In diesem Abschnitt wird erläutert, wie Sie eine vollständige Sicherung der Systemkonfigurationen in einer Datei erstellen, die Konfigurationsdatei auf dem Router wiederherstellen und die Werkseinstellungen zurücksetzen.

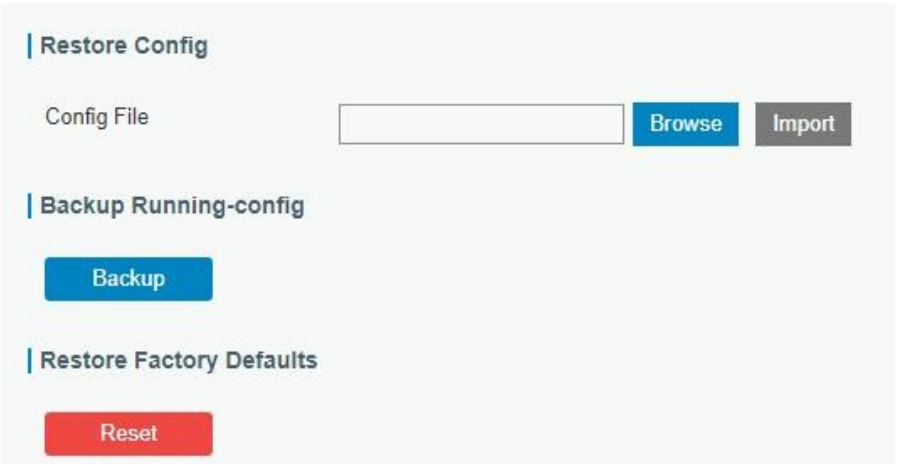


Abbildung 3-5-5-1

Sichern und Wiederherstellen

Element	Beschreibung
Konfigurationsdatei	Klicken Sie auf die Schaltfläche „Durchsuchen“, um die Konfigurationsdatei auszuwählen, und klicken Sie dann auf „Importieren“, um die Konfigurationsdatei auf den Router hochzuladen.
Sicherung	Klicken Sie auf „Sichern“, um die aktuelle Konfigurationsdatei auf den PC zu exportieren.
Zurücksetzen	Klicken Sie auf die Schaltfläche „Zurücksetzen“, um die Werkseinstellungen wiederherzustellen. Der Router wird nach Abschluss des Zurücksetzens neu gestartet.

Tabelle 3-5-5-1 Parameter für Sicherung und Wiederherstellung

Beispiel für die entsprechende Konfiguration

Werkseinstellungen wiederherstellen

3.5.6 Neustart

Auf dieser Seite können Sie den Router sofort oder regelmäßig neu starten. Wir empfehlen dringend, vor dem Neustart des Routers auf die Schaltflächen „Speichern“ und „Übernehmen“ zu klicken, um den Verlust der neuen Konfiguration zu vermeiden.

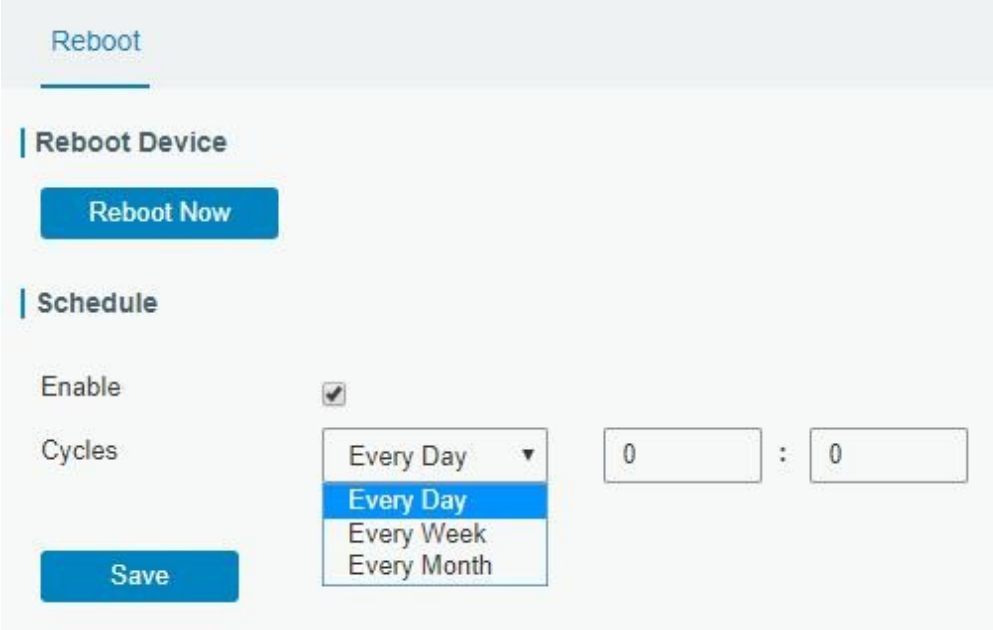


Abbildung 3-5-6-1

Neustart	
Artikel	**Beschreibung**
Jetzt neu starten	Den Router sofort neu starten.
Zeitplan	
Aktivieren	Starten Sie den Router in festgelegten Intervallen neu.
Zyklen	Wählen Sie das Datum und die Uhrzeit für die Ausführung des Zeitplans aus.

Tabelle 3-5-2-1 Zeitplanparameter

3.6 APP

3.6.1 Python

Python ist eine objektorientierte Programmiersprache, die aufgrund ihrer klaren Syntax und Lesbarkeit an Beliebtheit gewonnen hat.

Als interpretierte Sprache verfolgt Python eine Designphilosophie, die Wert auf die Lesbarkeit des Codes legt, insbesondere durch die Verwendung von Einrückungen zur Abgrenzung von Codeblöcken anstelle von geschweiften Klammern oder Schlüsselwörtern, sowie eine Syntax, die es Programmierern ermöglicht, Konzepte in weniger Codezeilen auszudrücken als in anderen Sprachen wie C++ oder Java. Die Sprache bietet Konstrukte und soll das Schreiben klarer Programme sowohl im kleinen als auch im großen Maßstab ermöglichen.

Benutzer können Python verwenden, um schnell einen Prototyp des Programms zu erstellen, der die endgültige Schnittstelle des Programms darstellen kann, diesen mit einer geeigneteren Sprache umschreiben und dann die erweiterte Klassenbibliothek kapseln, die Python aufrufen kann.

In diesem Abschnitt wird beschrieben, wie Sie den relevanten Betriebsstatus wie App-Manager, SDK-Version, erweiterter Speicher usw. anzeigen können. Außerdem können Sie hier die App-Manager-Konfiguration ändern und das Python-App-Paket importieren.

3.6.1.1 Python

Für die Python-App muss eine Micro-SD-Karte installiert sein.

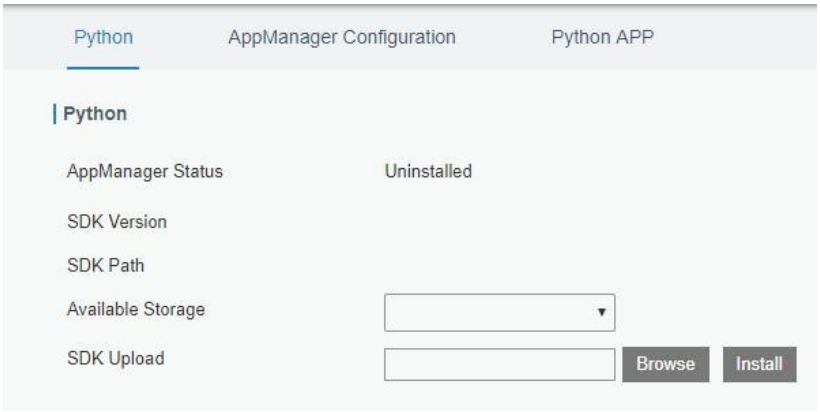


Abbildung 3-6-1-1

Python	
Element	**Beschreibung**
AppManager-Status	Zeigt den Ausführungsstatus von AppManager an, z. B. „Deinstalliert“, „Wird ausgeführt“ oder „Beendet“.
SDK-Version	Zeigt die Version des installierten SDK an.
SDK-Pfad	Zeigen Sie den SDK-Installationspfad an.
Verfügbarer Speicher	Wählen Sie verfügbaren Speicherplatz wie Micro SD, um das SDK zu installieren.
SDK hochladen	Laden Sie das SDK für Python hoch und installieren Sie es.
Deinstallieren	Deinstallieren Sie das SDK.
Anzeigen	Anwendungsstatus anzeigen, der von AppManager verwaltet wird.

Tabelle 3-6-1-1 Python-Parameter

3.6.1.2 App Manager-Konfiguration

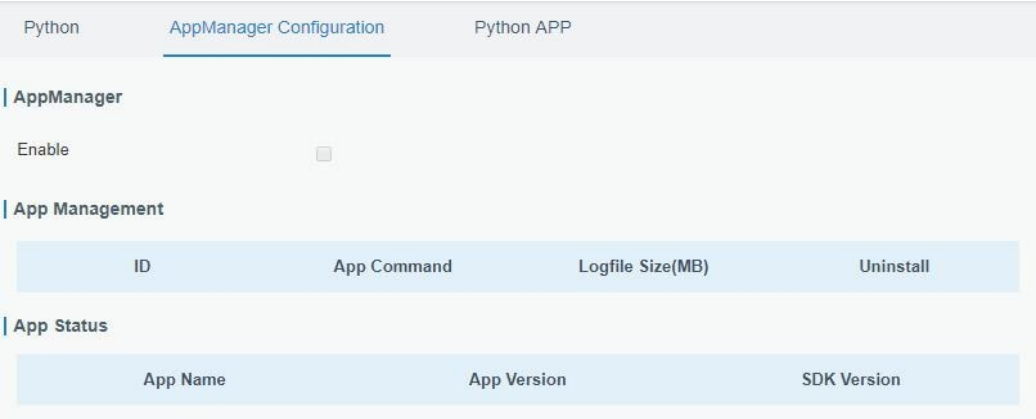


Abbildung 3-6-1-2

AppManager-Konfiguration	
Element	**Beschreibung**
Aktivieren	Nach der Aktivierung in Python AppManager kann der Benutzer auf die Schaltfläche „Anzeigen“ auf der „Python“-Webseite auf die Schaltfläche „Anzeigen“, um den vom AppManager verwalteten Anwendungsstatus anzuzeigen.
App-Verwaltung	
ID	Zeigt die ID der importierten App an.
App-Befehl	Zeigt den Namen der importierten App an.
Logdateigröße (MB)	Benutzerdefinierte Logdateigröße. Bereich: 1-50.
Deinstallieren	App deinstallieren.
App-Status	
App-Name	Zeigt den Namen der importierten App an.
App-Version	Zeigt die Version der importierten App an.
SDK-Version	Zeigt die SDK-Version an, auf der die importierte App basiert.

Tabelle 3-6-1-2 APP-Manager-Parameter

3.6.1.3 Python-App

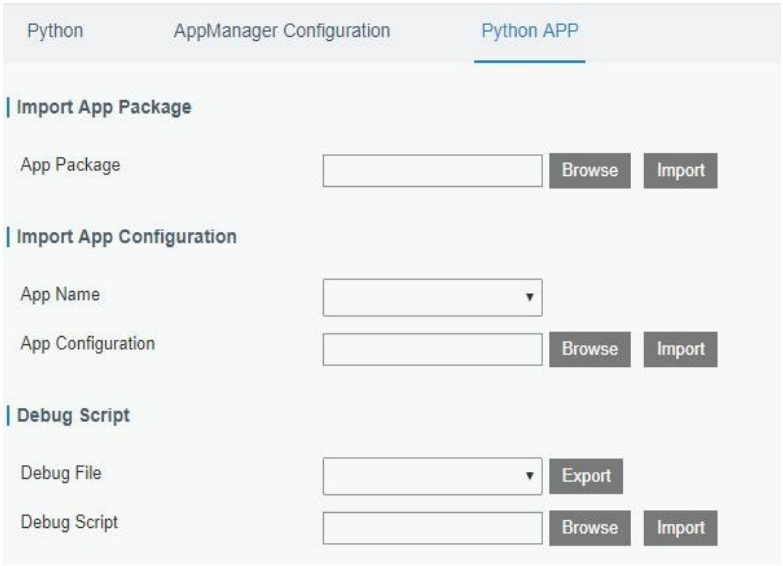


Abbildung 3-6-1-3

Python-App

Element	Beschreibung
App-Paket	Wählen Sie das App-Paket aus und importieren Sie es.
App-Name	Wählen Sie die App aus, um die Konfiguration zu importieren.
App-Konfiguration	Wählen Sie die Konfigurationsdatei aus und importieren Sie sie.
Debug-Datei	Skriptdatei exportieren.
Skript debuggen	Wählen Sie das zu debuggende Python-Skript aus und importieren Sie es.

Tabelle 3-6-1-3 APP-Parameter

Kapitel 4 Anwendungsbeispiele

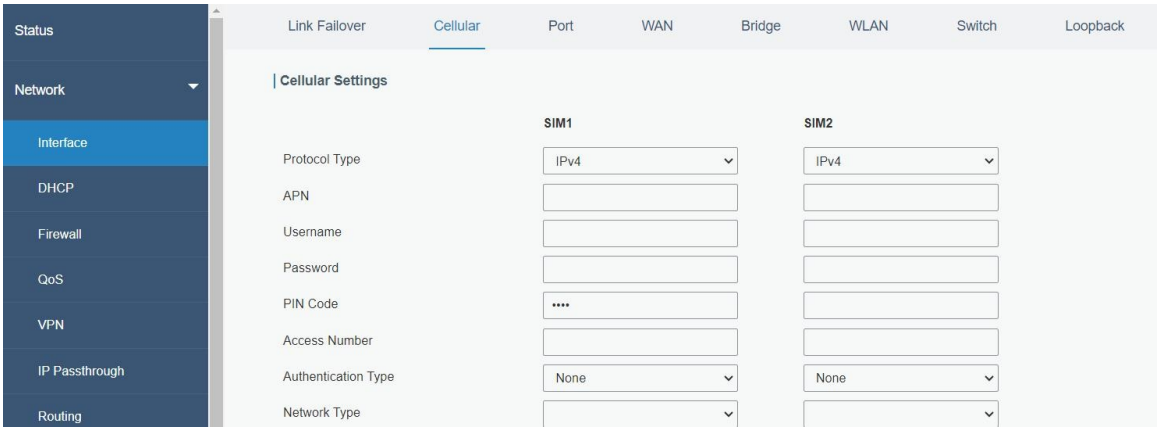
4.1 Netzwerkverbindung

4.1.1 Mobilfunkverbindung

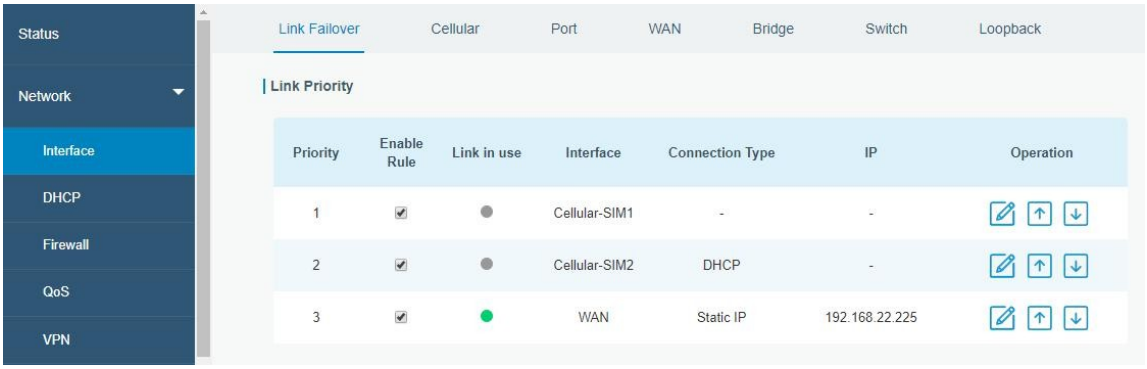
Die UR35-Router verfügen über zwei Mobilfunk-Schnittstellen mit den Bezeichnungen SIM1 und SIM2. Es ist jeweils nur eine Mobilfunk-Schnittstelle aktiv. Wir zeigen Ihnen anhand eines Beispiels, wie Sie eine SIM-Karte in den SIM1-Steckplatz des UR35 einlegen und den Router so konfigurieren, dass Sie über Mobilfunk Zugang zum Internet erhalten.

Konfigurationsschritte

1. Stellen Sie sicher, dass die SIM-Karte vor dem Einschalten richtig eingelegt ist und alle Mobilfunkantennen an den richtigen Anschlüssen angeschlossen sind.
2. Gehen Sie zu **Netzwerk > Schnittstelle > Mobilfunk > Mobilfunkeinstellungen**, um die Mobilfunkdaten zu konfigurieren, und klicken Sie dann auf **Speichern** und **Anwenden**.

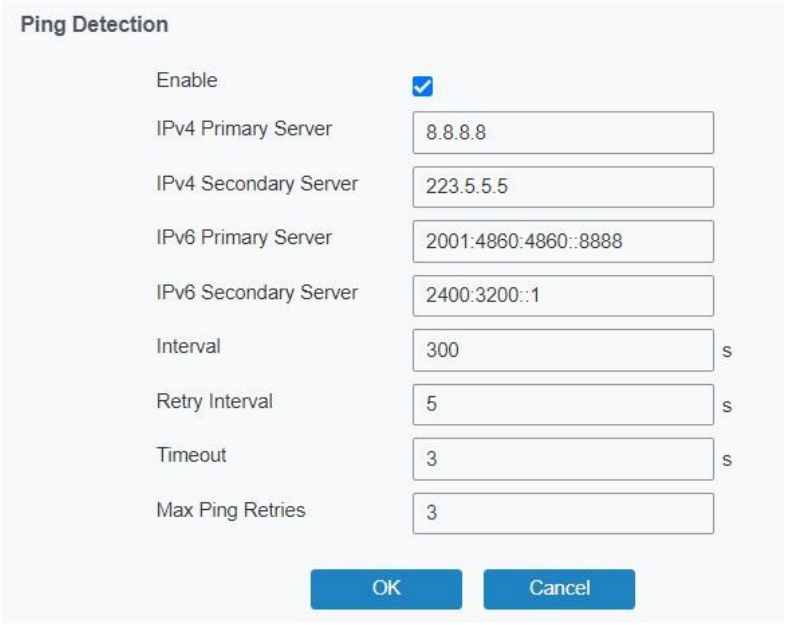


3. Gehen Sie zu **Netzwerk > Schnittstelle > Link-Failover**, um die entsprechende SIM zu aktivieren, und ziehen Sie die Schaltflächen, um die Link-Priorität zu ändern.

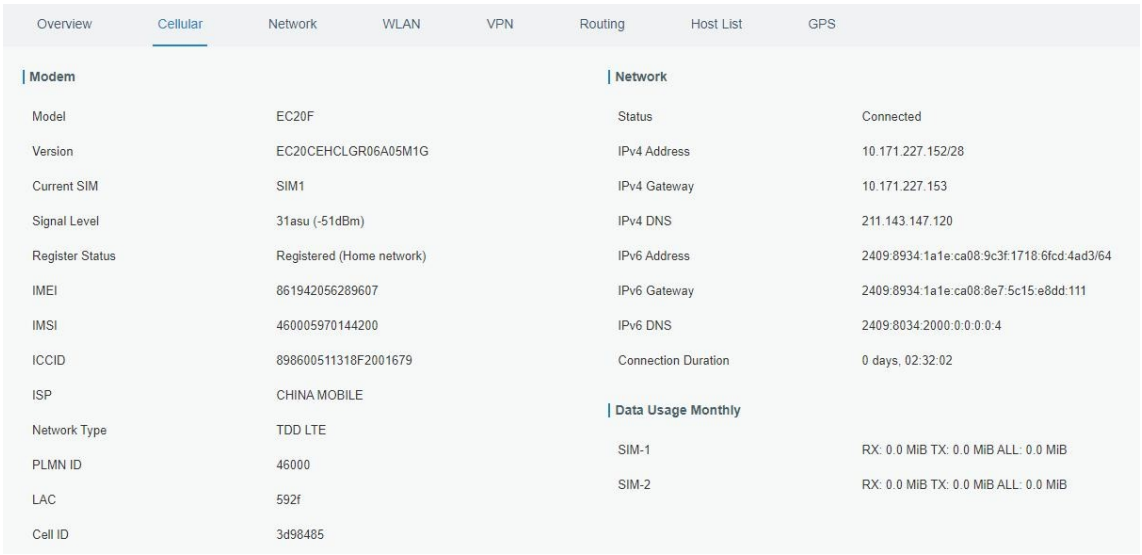


4. Klicken Sie auf „ “, um die ICMP-Ping-Erkennungsinformationen zu konfigurieren. Wenn die Ping-Prüfung aktiviert ist, sendet der Router ICMP-Pakete an den Erkennungsserver, um zu überprüfen, ob diese Verbindung gültig ist. Wenn keine Antwort erfolgt und die maximale Anzahl an Wiederholungsversuchen überschritten wird, wechselt er zur Verbindung mit niedrigerer Priorität.

Hinweis: Wenn Sie eine private SIM-Karte verwenden, ändern Sie bitte die Adresse des privaten Servers oder deaktivieren Sie die Ping-Prüfung.



5. Gehen Sie zu **„Status" > „Mobilfunk"**, um den Status der Mobilfunkverbindung anzuzeigen. Wenn „Verbunden" angezeigt wird, hat SIM1 erfolgreich eine Verbindung hergestellt.



Verwandtes Thema

Mobilfunk-Einstellungen

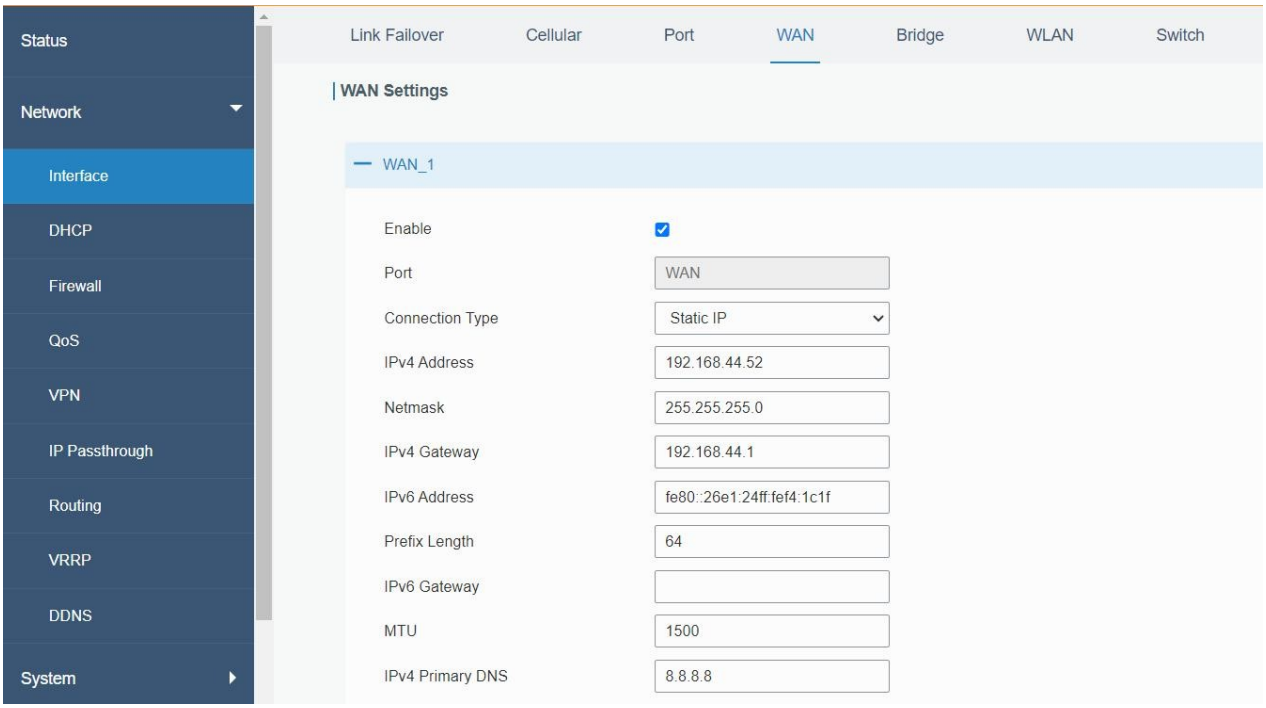
Mobilfunkstatus

4.1.2 Ethernet-WAN-Verbindung

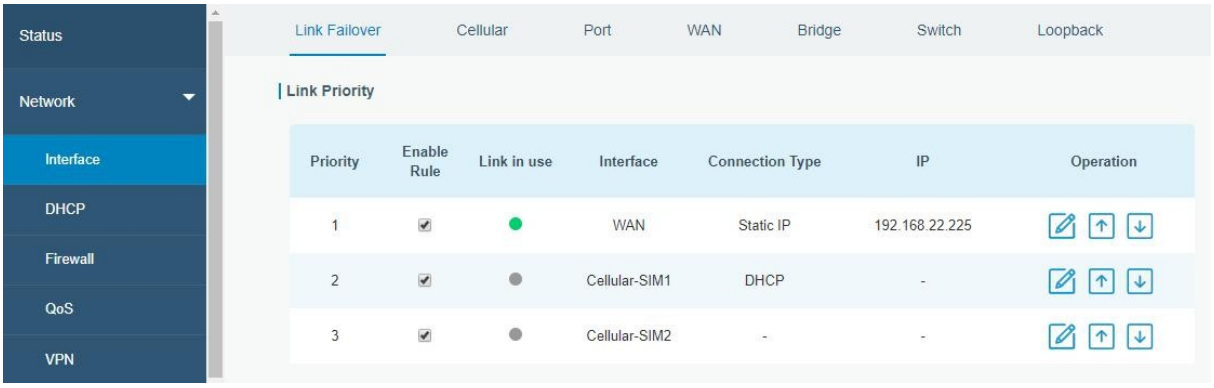
UR35 unterstützt den Internetzugang über den WAN-Port.

Konfigurationsschritte

1. Gehen Sie zu **Netzwerk > Schnittstelle > WAN**, um den Verbindungstyp auszuwählen und die WAN-Parameter zu konfigurieren, und speichern Sie anschließend alle Einstellungen. Die folgenden Beispiele für den statischen IP-Typ, den DHCP-Client-Typ und den PPPoE-Typ sind zu Ihrer Information aufgeführt.



2. Gehen Sie zu **Netzwerk > Schnittstelle > Link-Failover,** um WAN zu aktivieren, und ziehen Sie die Schaltflächen, um die Link-Priorität zu ändern.



Verwandtes

Thema WAN-Einstellung

WAN-Status

4.2 Beispiel für eine WLAN-Anwendung

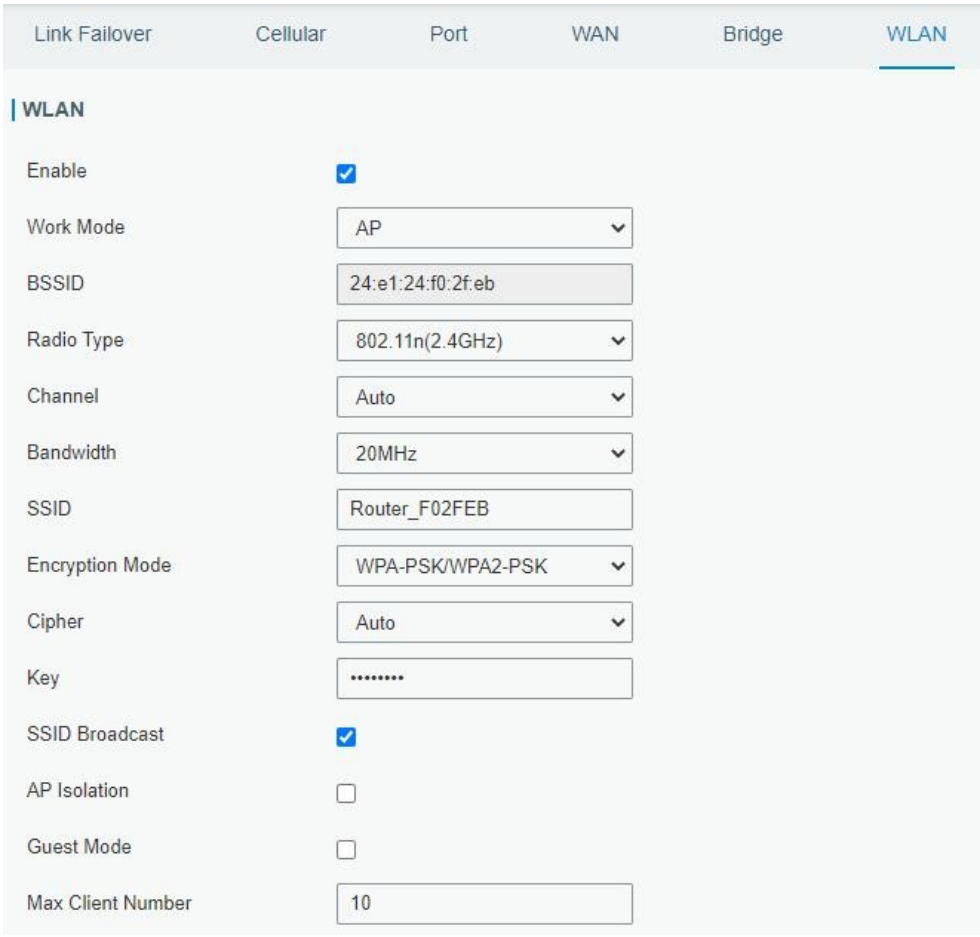
4.2.1 AP-Modus

Der UR35 unterstützt die Funktion als Zugangspunkt (AP), um anderen Geräten Netzwerkzugang zu gewähren.

Konfigurationsschritte

1. Gehen Sie zu **Netzwerk > Schnittstelle > WLAN,** um den Arbeitsmodus als AP auszuwählen und die erforderlichen WLAN-Parameter zu definieren

und speichern Sie anschließend alle Einstellungen.



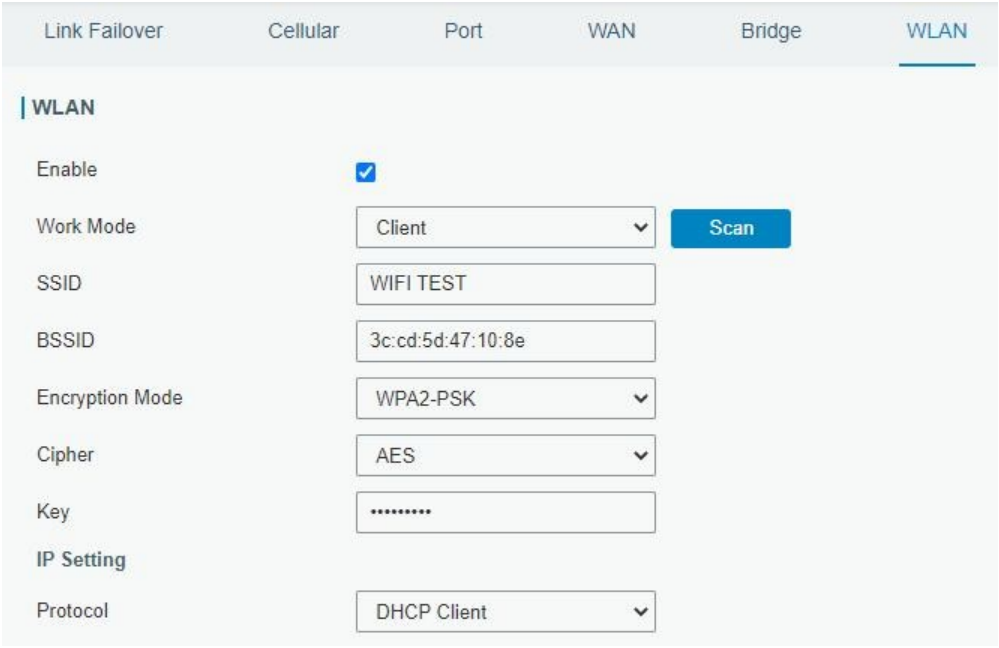
2. Verwenden Sie ein Smartphone, um eine Verbindung zum Zugangspunkt des UR35 herzustellen. Gehen Sie zu **Status > WLAN**, um die AP-Einstellungen und Informationen zum verbundenen Client/Benutzer zu überprüfen.

4.2.2 Client-Modus

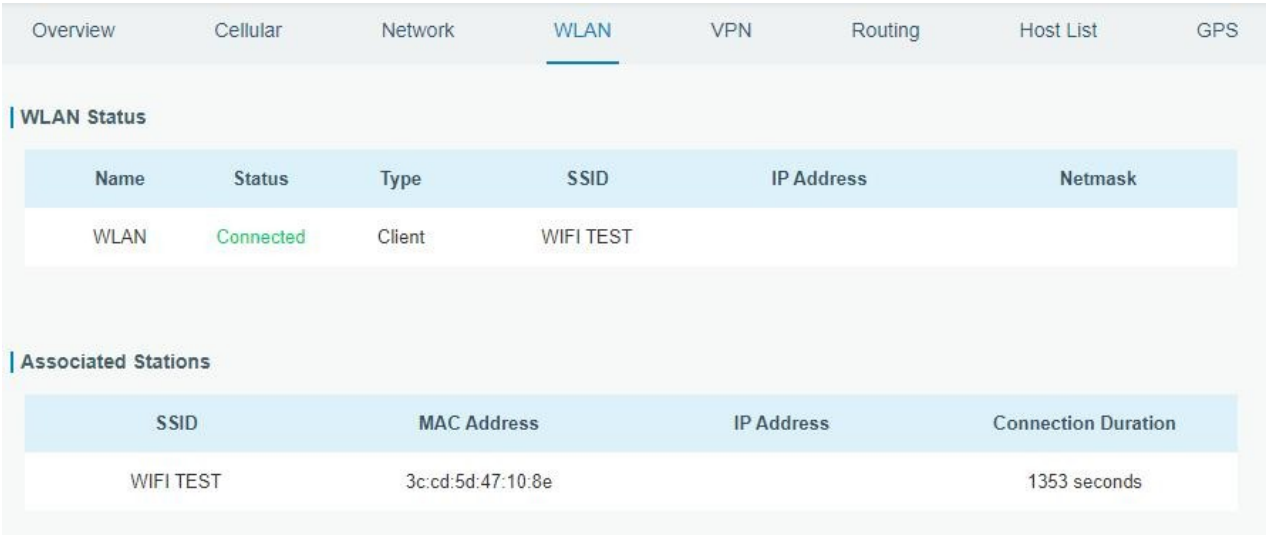
Der UR35 unterstützt die Verwendung als WLAN-Client, um eine Verbindung zu einem Zugangspunkt herzustellen und Internetzugang zu erhalten.

Konfigurationsschritte

1. Gehen Sie zu **Netzwerk > Schnittstelle > WLAN**, klicken Sie auf **„Scannen“**, um nach Zugangspunkten zu suchen, klicken Sie auf **„Mit Netzwerk verbinden“** und speichern Sie dann die Einstellungen. Bei einigen Zugangspunkten muss das WLAN-Passwort eingegeben werden.



2. Gehen Sie zu **Status > WLAN**, um den Verbindungsstatus des Clients zu überprüfen.



Verwandtes

Thema WLAN-

Einstellungen

WLAN-Status

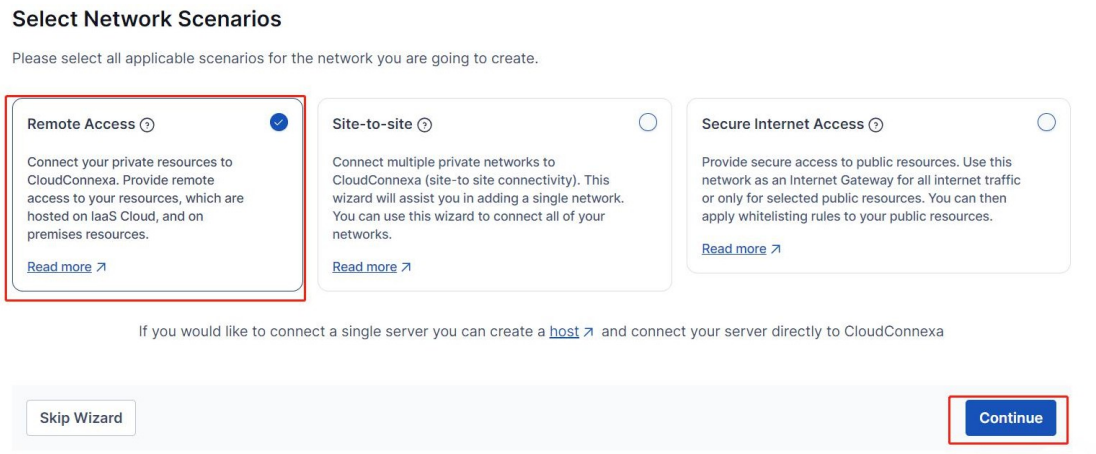
4.3 Beispiel für eine OpenVPN-Client-Anwendung

UR35-Router können als OpenVPN-Clients oder OpenVPN-Server fungieren. Wir zeigen Ihnen anhand eines Beispiels, wie Sie einen OpenVPN-Client für die Verbindung mit OpenVPN cloudConnexa konfigurieren.

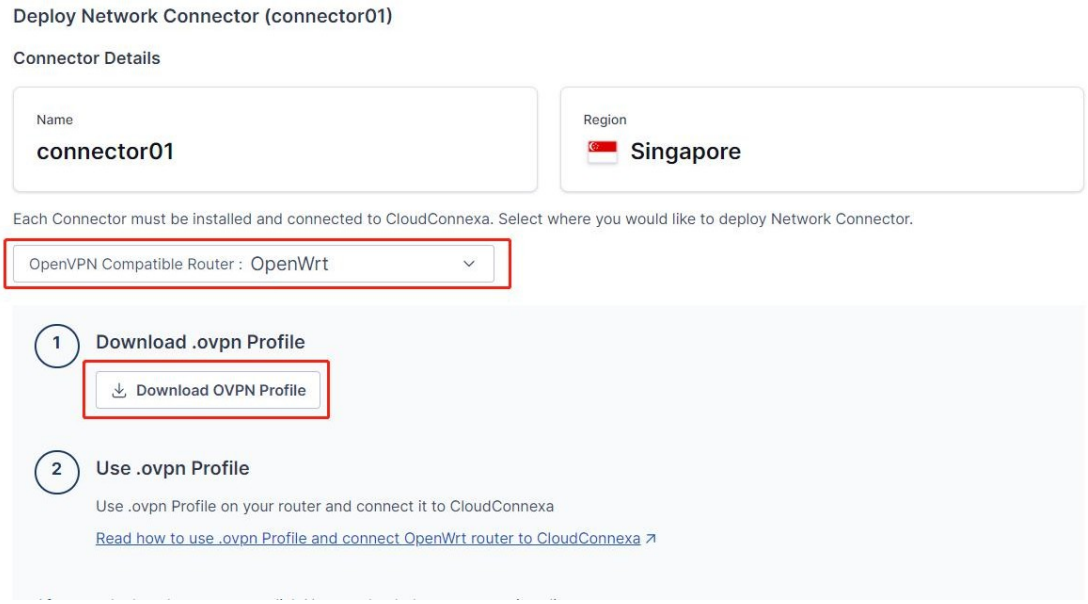
Konfigurationsschritte

1. Stellen Sie sicher, dass der UR35 Zugang zum Internet hat.
2. Melden Sie sich bei Ihrem cloudConnexa-Konto an, wählen Sie den Abschnitt „Netzwerk“ und wählen Sie den gewünschten Dienst entsprechend

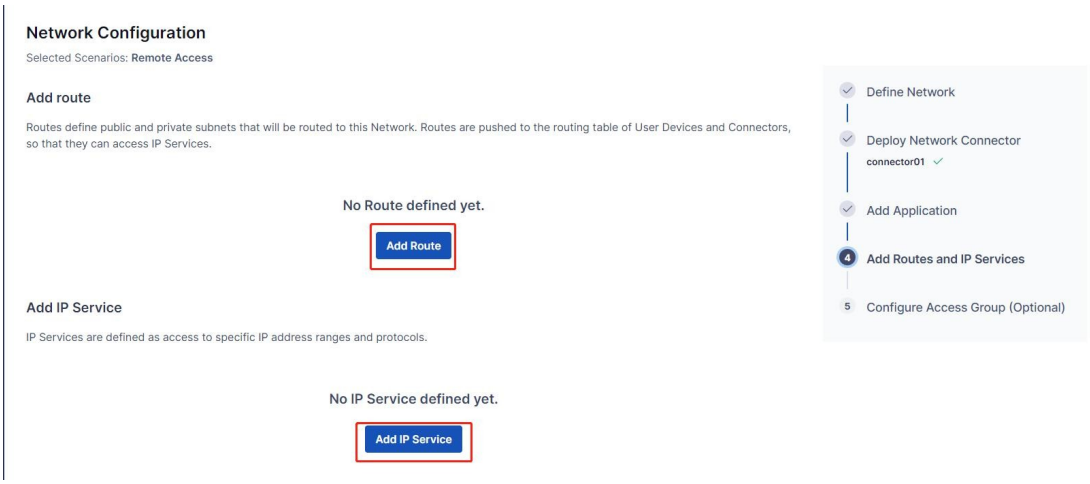
Ihren Anforderungen und folgen Sie den Anweisungen des Assistenten, um mit den Einstellungen fortzufahren.



3. Wählen Sie als Anbietertyp „OpenWrt“ aus und laden Sie die OVPN-Datei herunter.

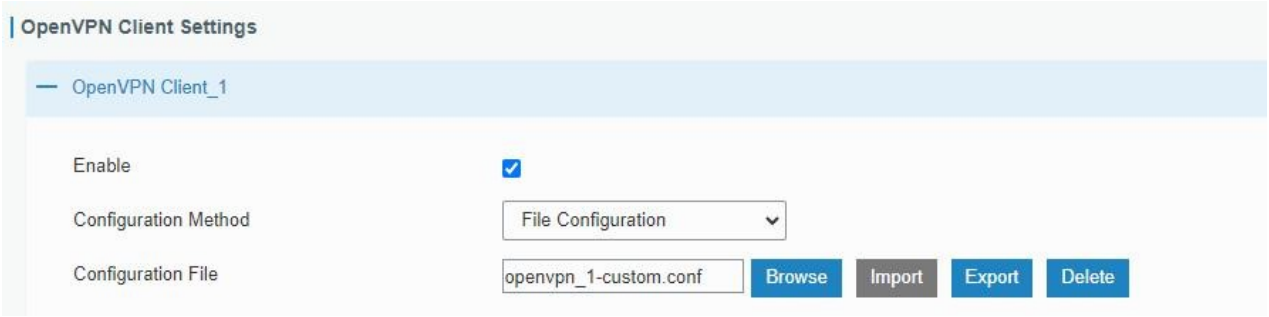


4. Wenn Sie auf die Endgeräte im Subnetz zugreifen müssen, müssen Sie die Route und den IP-Dienst als LAN-Subnetz des Routers hinzufügen.

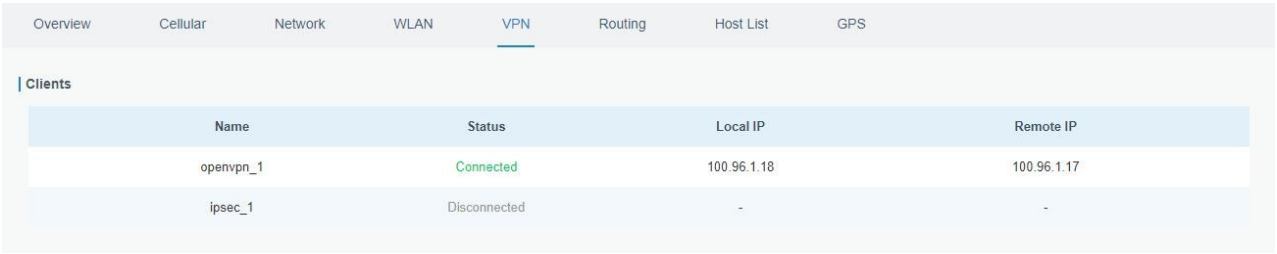


5. Gehen Sie zu **„Netzwerk > VPN > OpenVPN-Client“**, wählen Sie als Konfigurationsmethode „Dateikonfiguration“ und

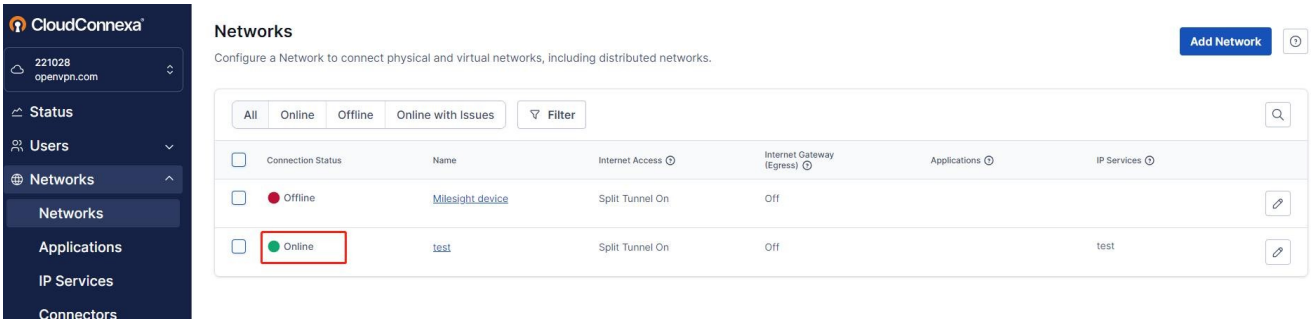
importe die OVPN-Datei.



6. Gehen Sie zur Seite **„Status > VPN“**, um zu überprüfen, ob der Client verbunden ist.



Sie können den Verbindungsstatus auch auf CloudConnexa überprüfen.



Verwandtes

Thema OpenVPN-

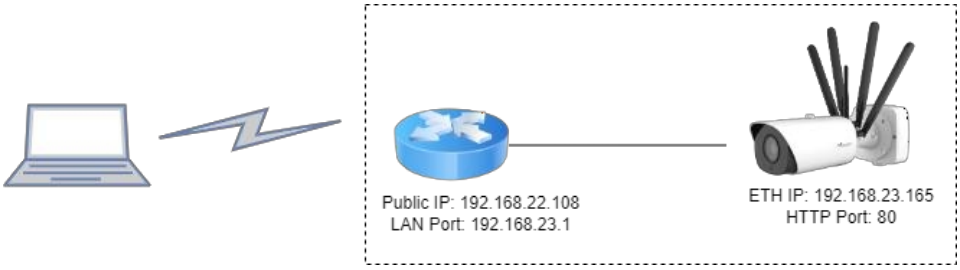
Client VPN-

Status

4.4 Beispiel für eine NAT-Anwendung

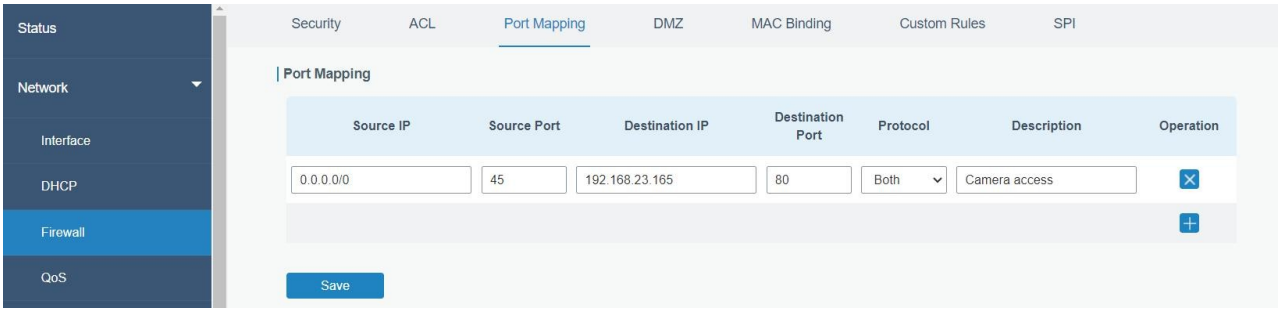
Beispiel

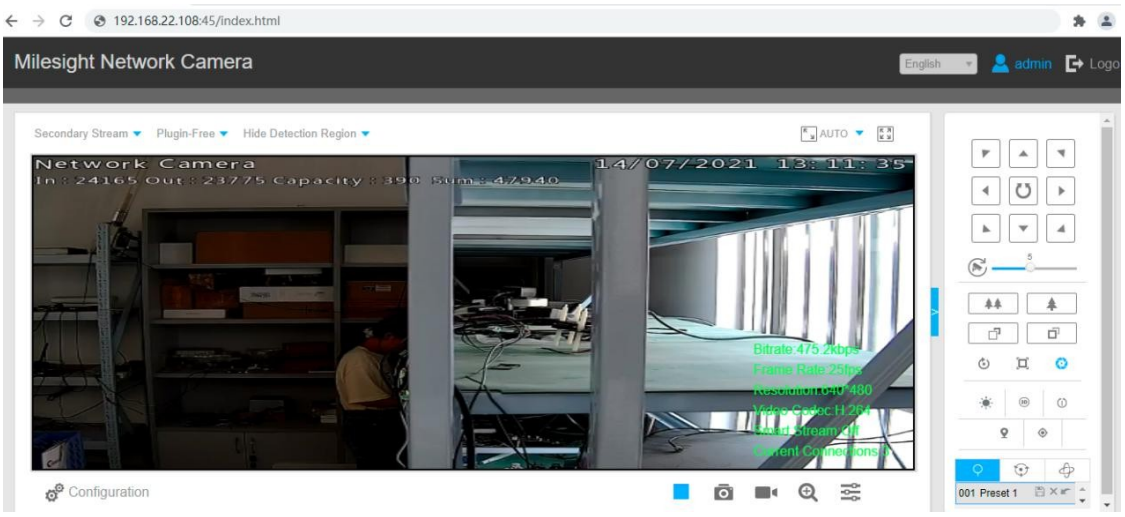
Ein UR35-Router kann über Mobilfunk auf das Internet zugreifen und erhält eine öffentliche IP-Adresse. Der LAN-Port ist mit einer IP-Kamera verbunden, deren IP-Adresse 192.168.23.165 lautet und deren HTTP-Port 80 ist. Auf diese IP-Kamera kann über die folgenden Port-Mapping-Einstellungen mit der öffentlichen IP-Adresse zugegriffen werden.



Konfigurationsschritte

Gehen Sie zu **„Firewall > Portzuordnung“** und konfigurieren Sie die Portzuordnungsparameter wie unten angegeben. Die Quell-IP-Adresse 0.0.0.0/0 bedeutet, dass alle externen Adressen Zugriff haben. Danach können Benutzer die öffentliche IP-Adresse: externen Port verwenden, um auf die IP-Kamera zuzugreifen.





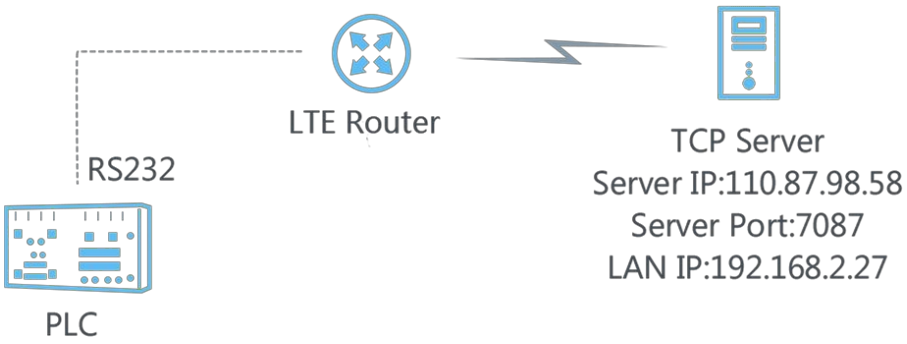
Verwandtes Thema

Portzuordnung

4.5 DTU-Anwendungsbeispiel

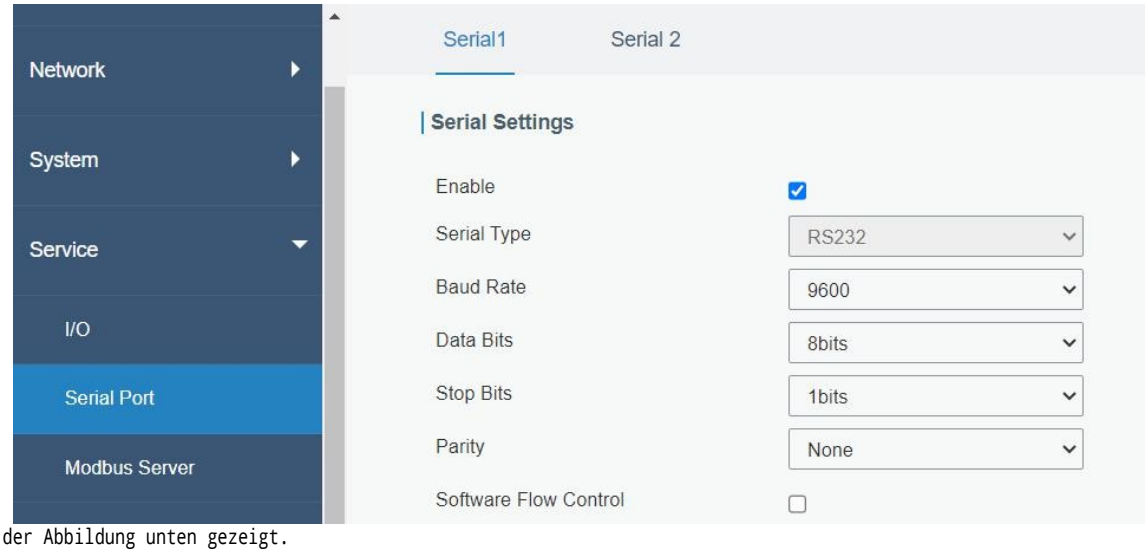
Beispiel

Eine SPS ist über RS232 mit dem UR35 verbunden und muss die Daten transparent an einen Remote-TCP-Server weiterleiten.



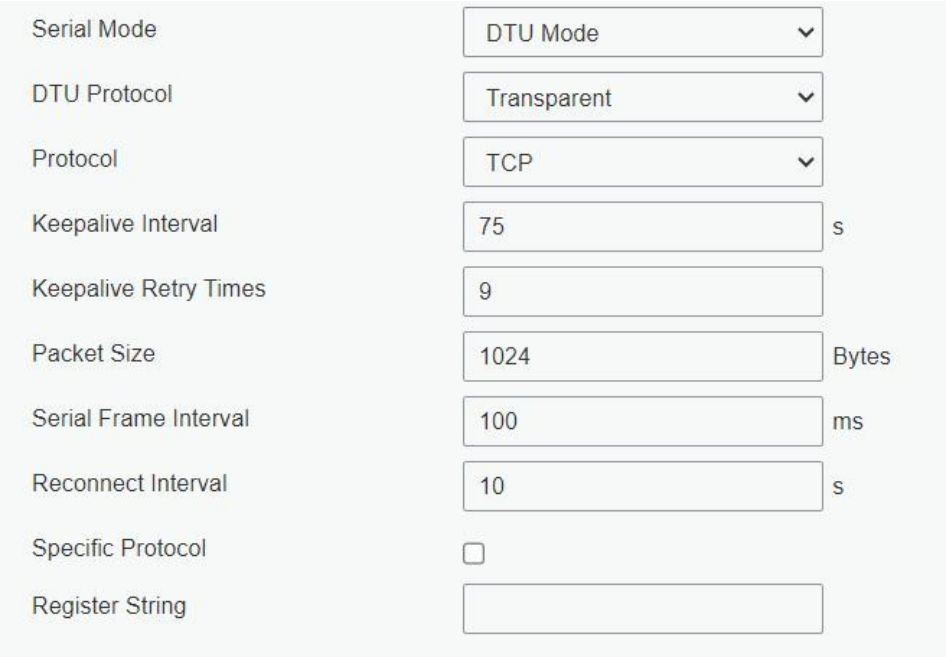
Konfigurationsschritte

1. Gehen Sie zu **„Service" > „Serial Port" > „Serial1"**, aktivieren Sie „Serial 1" und konfigurieren Sie die Parameter für die serielle Schnittstelle. Die Parameter für die serielle Schnittstelle müssen mit denen der SPS übereinstimmen, wie in

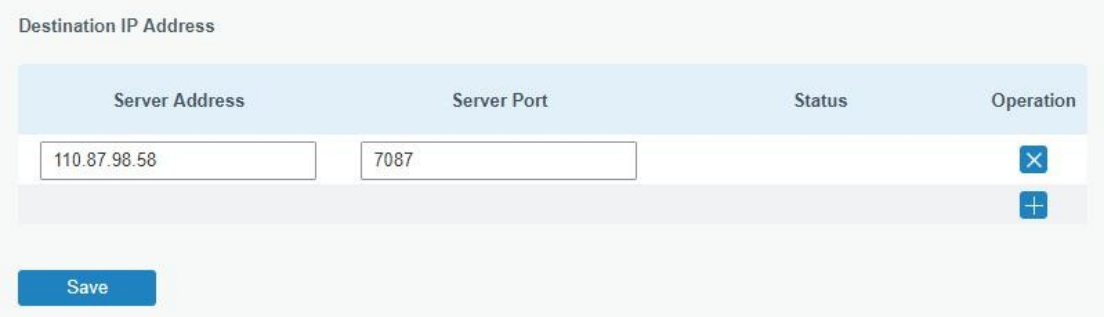


der Abbildung unten gezeigt.

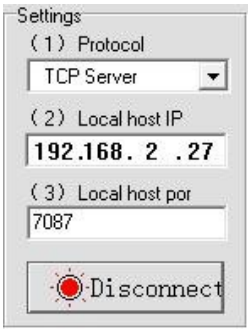
2. Konfigurieren Sie den seriellen Modus als DTU-Modus, das DTU-Protokoll als „Transparent" und das Protokoll als TCP.



3. Konfigurieren Sie die IP-Adresse und den Port des TCP-Servers.



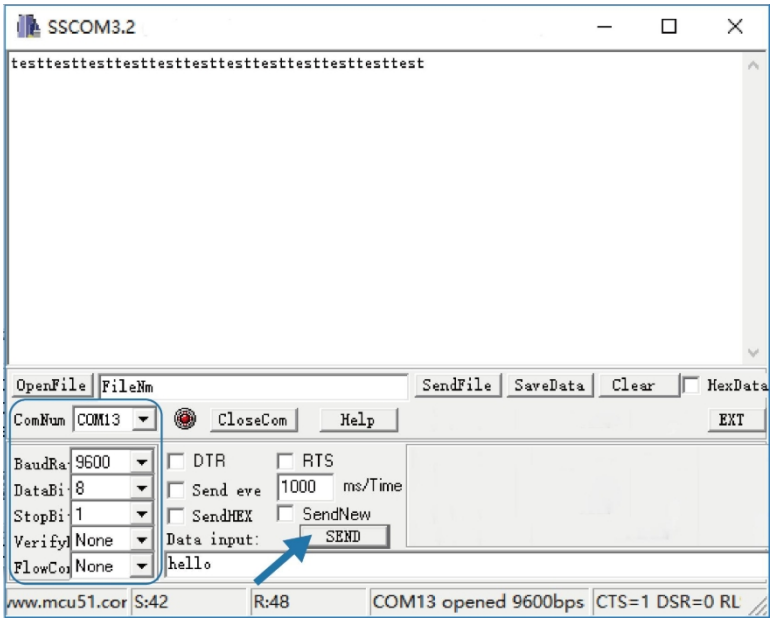
4. Starten Sie den TCP-Server auf dem PC. Nehmen Sie als Beispiel die Testsoftware **Netassist**. Stellen Sie sicher, dass die Portzuordnung bereits vorgenommen wurde.



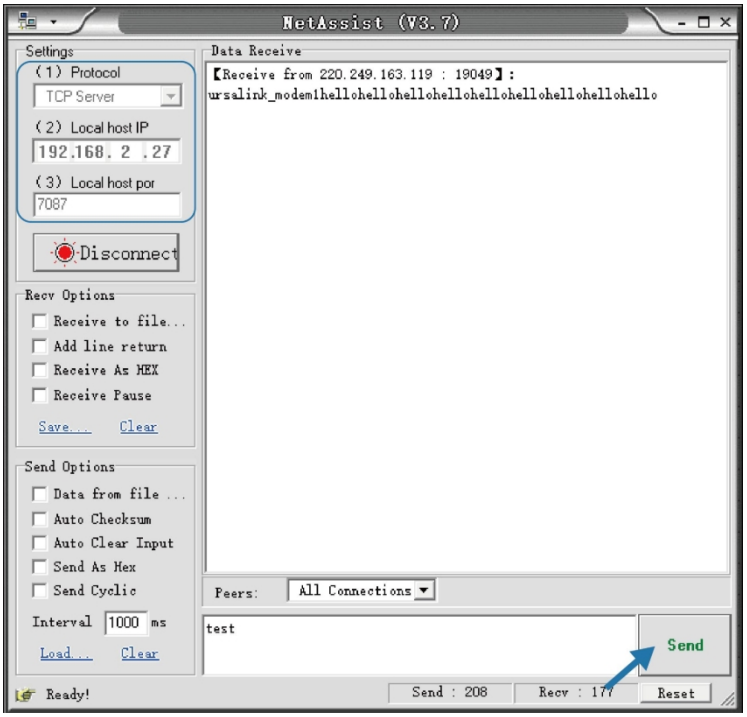
5. Verbinden Sie das UR35 über RS232 mit dem PC für die SPS-Simulation. Starten Sie dann die **sscom**-Software auf dem PC, um die Kommunikation über die serielle Schnittstelle zu testen.

6. Nachdem die Verbindung zwischen dem UR35 und dem TCP-Server hergestellt wurde, können Sie Daten zwischen sscom und Netassit senden.

PC-Seite



TCP-Serverseite



7. Nachdem der Test der seriellen Kommunikation abgeschlossen ist, können Sie die SPS zum Testen an den RS232-Anschluss des UR35 anschließen.

Verwandtes Thema

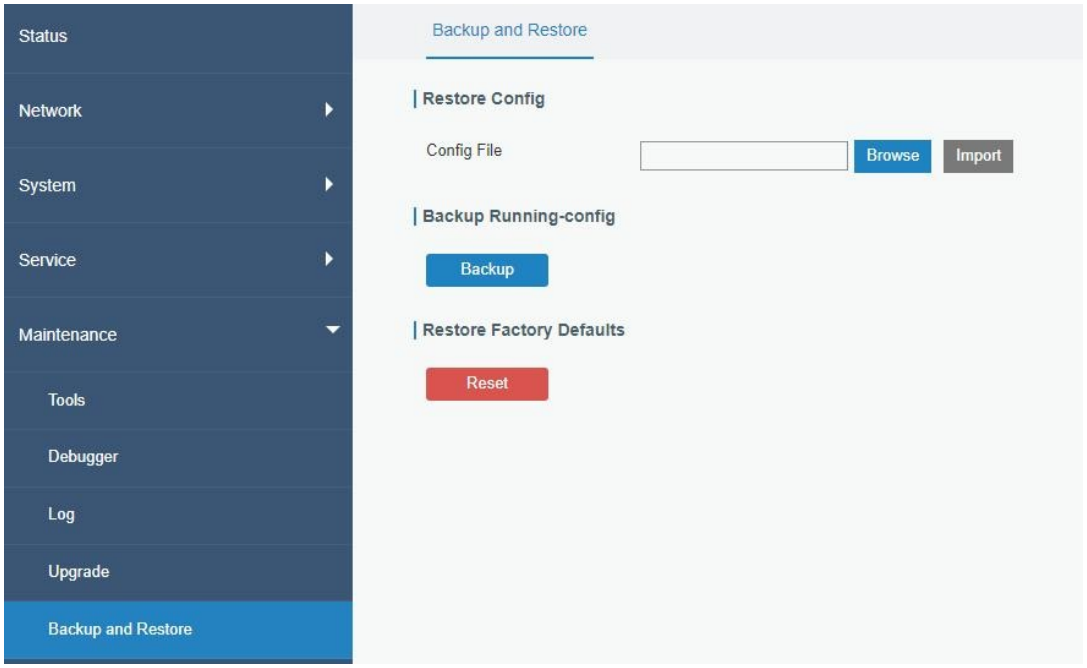
Serieller Port

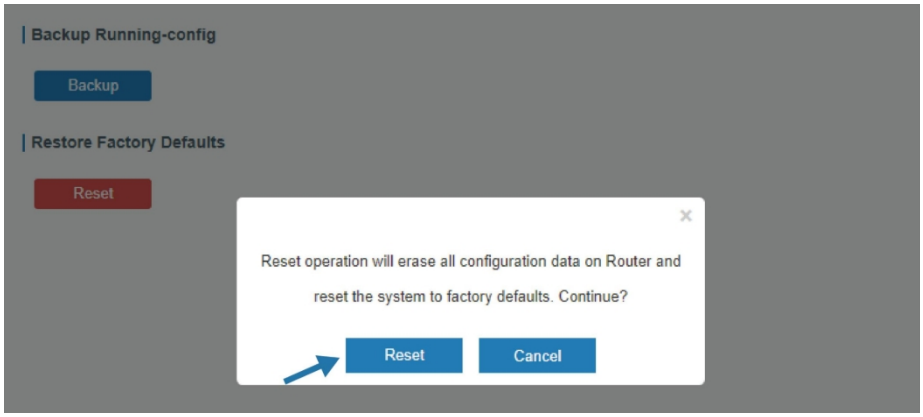
4.6 Werkseinstellungen wiederherstellen

Methode 1:

Melden Sie sich bei der Weboberfläche an, gehen Sie zu **„Wartung > Sichern und Wiederherstellen“** und klicken Sie auf die Schaltfläche **„Zurücksetzen“**.

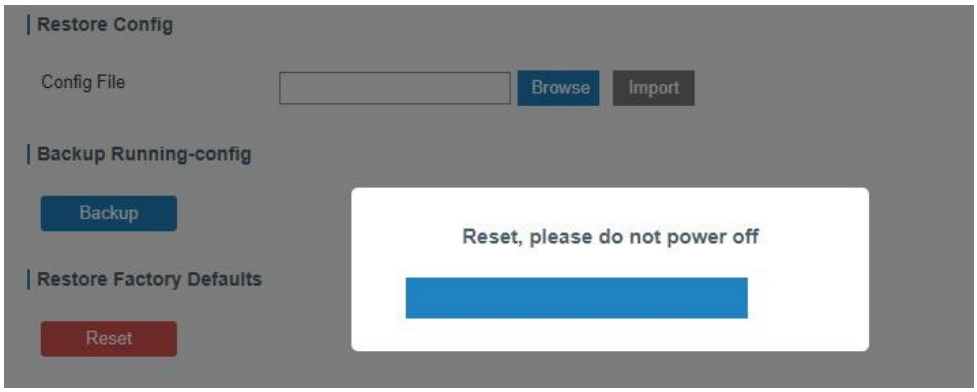
Sie werden gefragt, ob Sie das Gerät auf die Werkseinstellungen zurücksetzen möchten. Klicken Sie dann auf die Schaltfläche





„Zurücksetzen“.

Der Router wird dann neu gestartet und sofort auf die Werkseinstellungen zurückgesetzt.



Warten Sie, bis die SYSTEM-LED langsam blinkt und die Anmeldeseite erneut angezeigt wird. Dies bedeutet, dass der Router erfolgreich auf die Werkseinstellungen zurückgesetzt wurde.

Verwandtes Thema

Werkseinstellungen wiederherstellen

Methode 2:

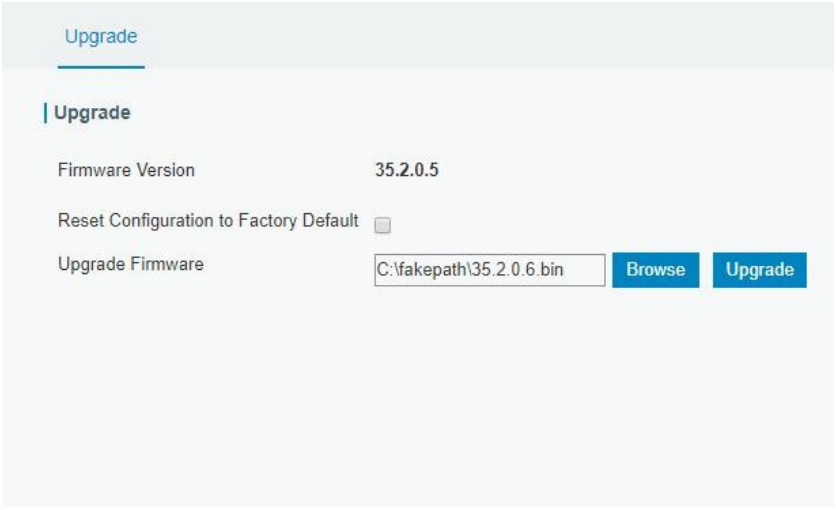
Suchen Sie die Reset-Taste am Router und halten Sie sie länger als 5 Sekunden gedrückt, bis die LED blinkt.

4.7 Firmware-Upgrade

Es wird empfohlen, dass Sie sich vor dem Aktualisieren der Router-Firmware zunächst an den technischen Support von Milesight wenden. Nachdem Sie die Firmware-Datei erhalten haben, führen Sie bitte die folgenden Schritte aus, um die Aktualisierung abzuschließen.

1. Gehen Sie zu **„Wartung" > „Upgrade"**, klicken Sie auf **„Durchsuchen"** und wählen Sie die richtige Firmware-Datei auf dem PC aus.
2. Klicken Sie auf „**Upgrade**" und der Router überprüft, ob die Firmware-Datei korrekt ist. Wenn dies der Fall ist, wird die Firmware in den Router importiert und der Router beginnt mit dem Upgrade.

Hinweis: Es wird empfohlen, vor dem Upgrade das Kontrollkästchen „Konfiguration auf Werkseinstellungen zurücksetzen" zu aktivieren.



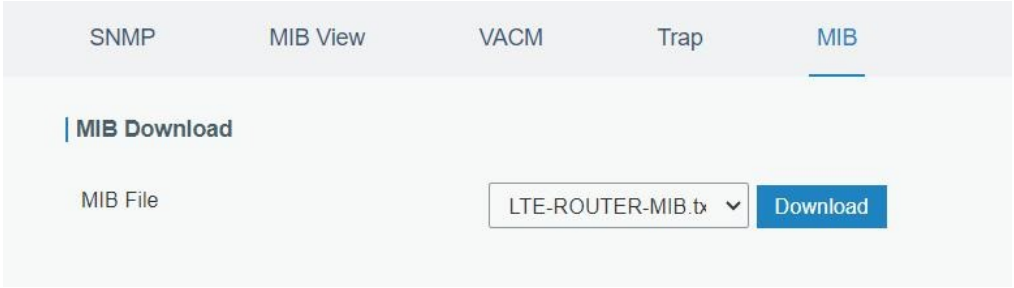
Verwandtes Thema

Upgrade

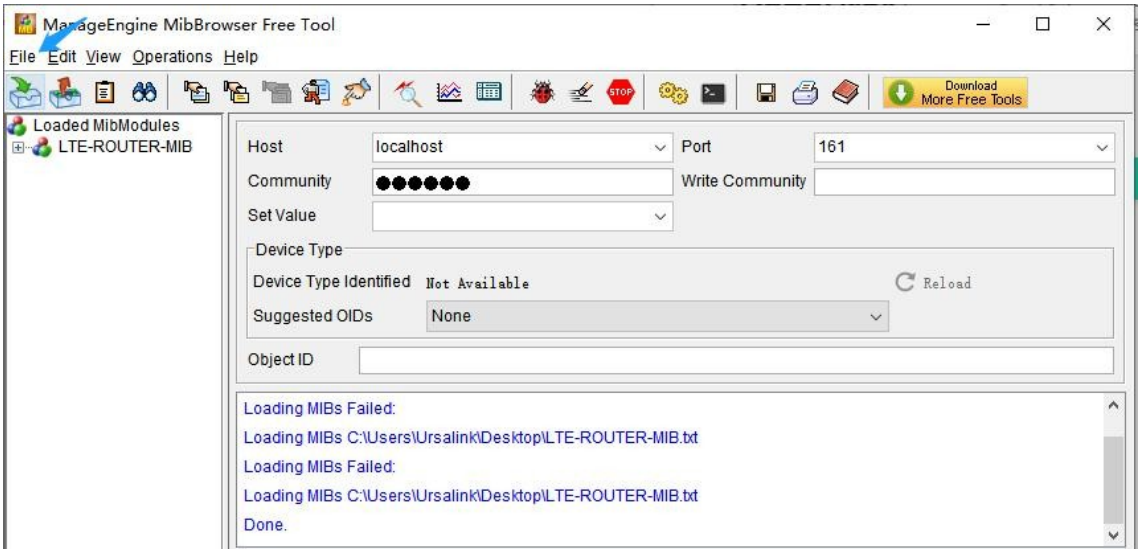
4.8 SNMP-Anwendungsbeispiel

Bevor Sie die SNMP-Parameter konfigurieren, laden Sie bitte zunächst die entsprechende MIB-Datei aus der WEB-GUI des UR35 herunter und laden Sie sie dann in eine beliebige Software oder ein Tool hoch, das das Standard-SNMP-Protokoll unterstützt. Hier verwenden wir das kostenlose Tool ManageEngine MibBrowser als Beispiel, um auf den Router zuzugreifen und Mobilfunkdaten abzufragen.

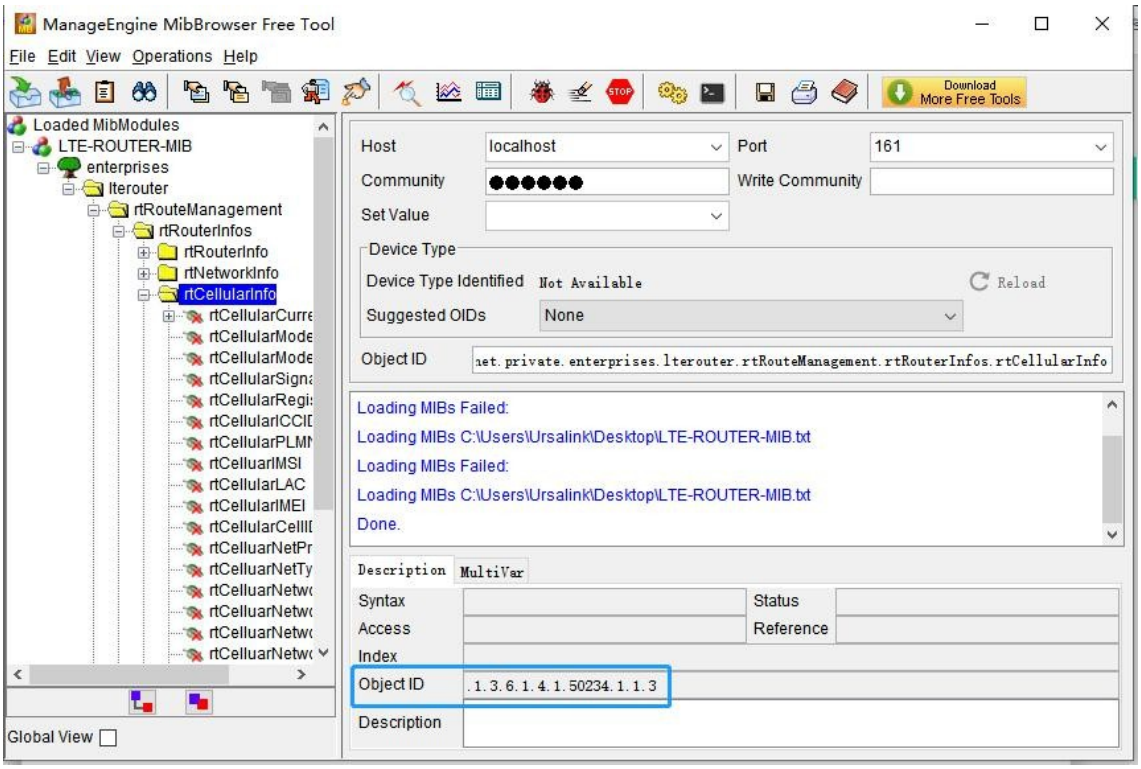
1. Gehen Sie zu **„Service > SNMP > MIB"** und laden Sie die MIB-Datei **„LTE-ROUTER-MIB.txt"** auf Ihren PC herunter.



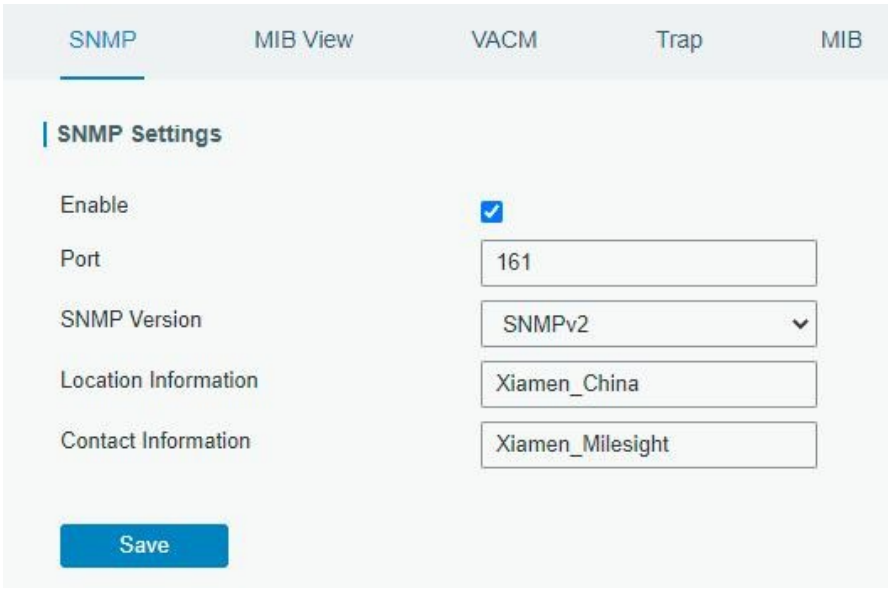
2. Starten Sie das kostenlose Tool ManageEngine MibBrowser auf dem PC. Klicken Sie in der Menüleiste auf **„Datei > MIB laden“**. Wählen Sie dann die Datei **„LTE-ROUTER-MIB.txt“** vom PC aus und laden Sie sie in die Software hoch.



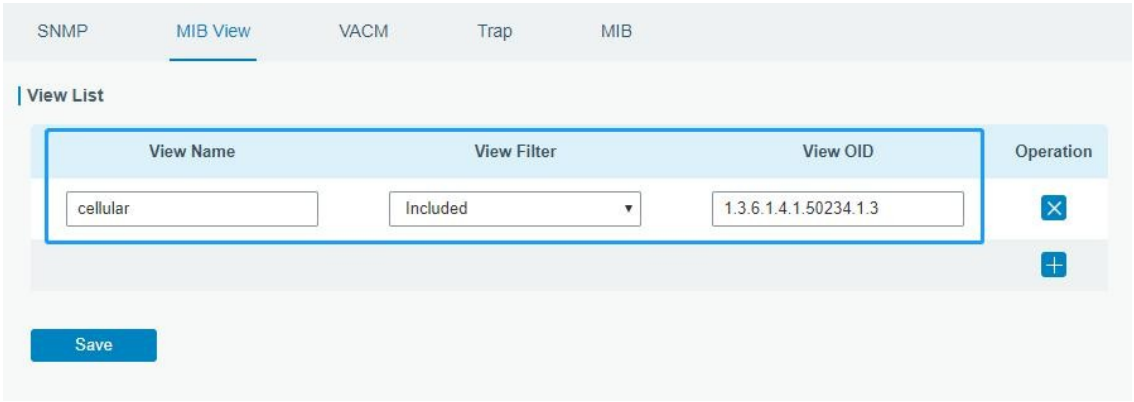
Klicken Sie auf die Schaltfläche „+“ neben LTE-ROUTER-MIB im Menü **„Loaded MibModules“** und suchen Sie **„usCellularinfo“**. Dann sehen Sie, dass die OID der Mobilfunkdaten „.1.3.6.1.4.1.50234“ lautet, die in den MIB-Ansichtseinstellungen eingegeben wird.



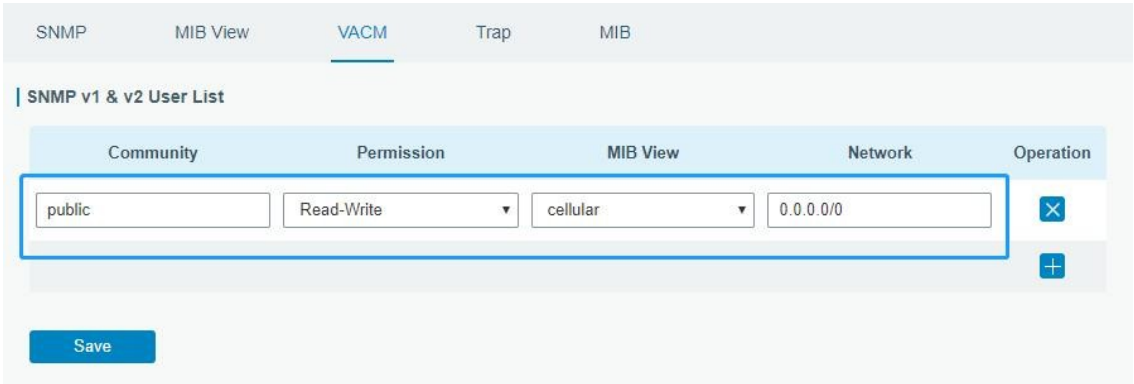
3. Gehen Sie zu **„Service > SNMP > SNMP“**, um die SNMP-Funktion zu aktivieren.



4. Klicken Sie auf „ + “ , um eine neue MIB-Ansicht hinzuzufügen und die Ansicht für den Zugriff von außen zu definieren. Klicken Sie anschließend auf die Schaltfläche „Save“.



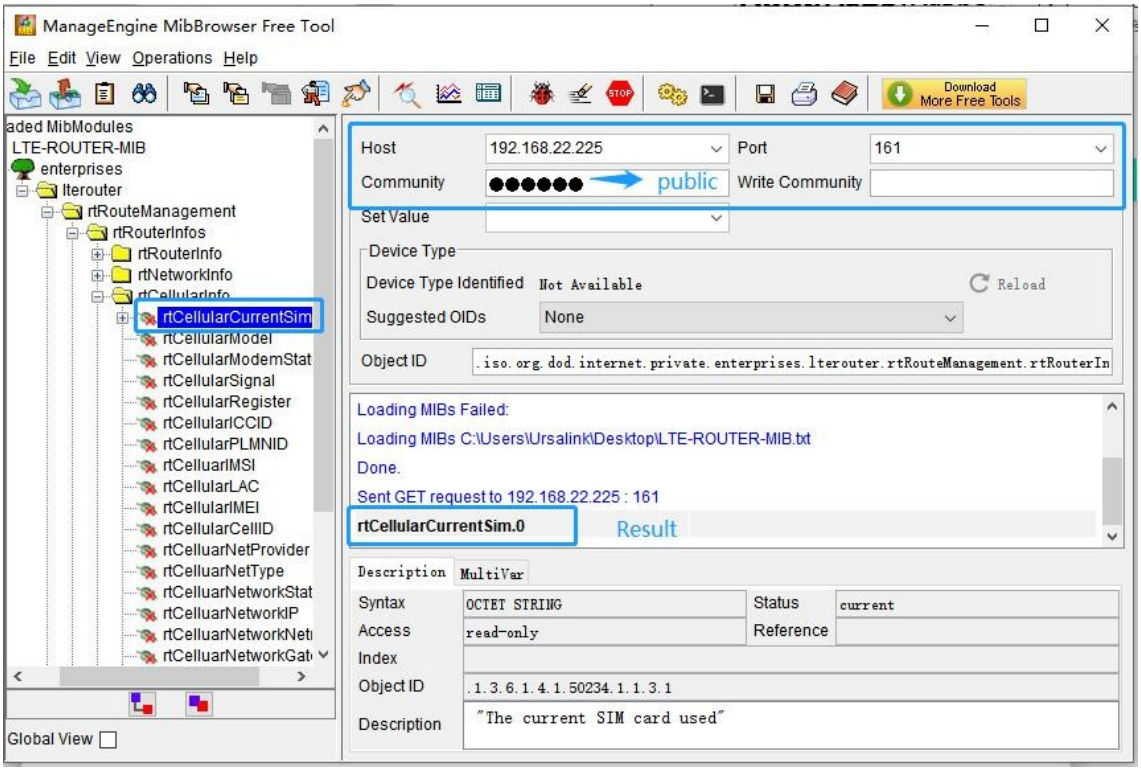
5. Klicken Sie auf „ + “ , um eine neue VACM-Einstellung hinzuzufügen, mit der Sie die Zugriffsberechtigung für die angegebene Ansicht aus dem angegebenen externen Netzwerk definieren können, und speichern Sie anschließend alle Einstellungen.



6. Gehen Sie zu „MibBrowser“, geben Sie die Host-IP-Adresse, den Port und die Community ein. Klicken Sie mit der rechten Maustaste auf **„usCellular CurrentSim“**

und klicken Sie dann auf **„FET“**. Daraufhin werden die aktuellen SIM-Informationen im Ergebnisfeld angezeigt. Auf die gleiche Weise können Sie weitere

Mobilfunkinformationen auf die gleiche Weise abrufen.



Verwandtes Thema

SNMP

4.9 VRRP-Anwendungsbeispiel

Anwendungsbeispiel

Ein Webserver benötigt über den UR35-Router einen Internetzugang. Um Datenverluste aufgrund eines Routerausfalls zu vermeiden, können zwei UR35-Router als VRRP-Backup-Gruppe eingesetzt werden, um die Netzwerkzuverlässigkeit zu verbessern.

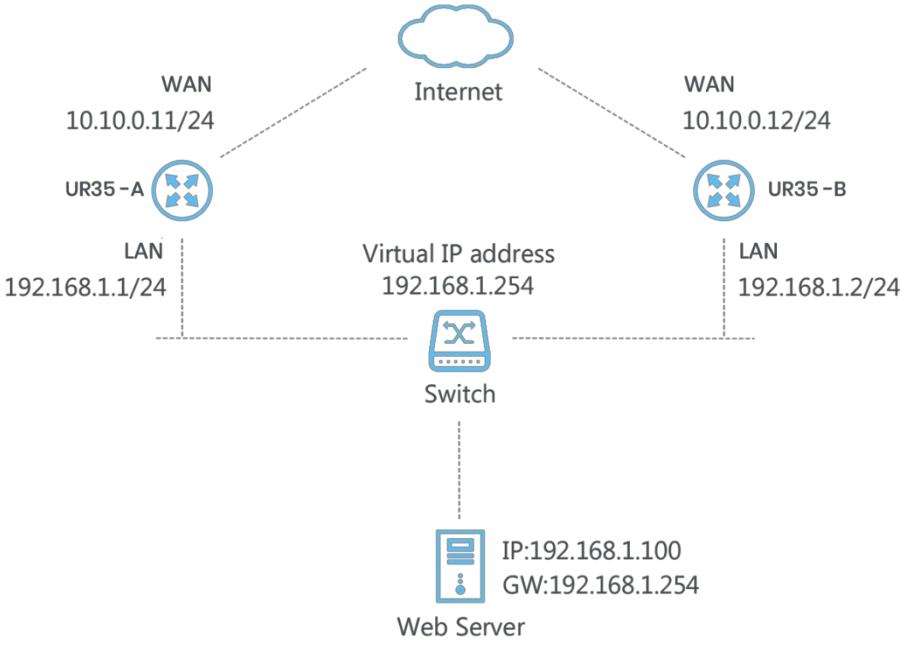
VRRP-Gruppe:

Die WAN-Ports des UR35-Routers A und des Routers B sind über ein kabelgebundenes Netzwerk mit dem Internet verbunden. Die LAN-Ports der beiden Router sind mit einem Switch verbunden.

Die virtuelle IP-Adresse lautet 192.168.1.254/24.

Router	Virtuelle Router-ID (gleich für A und B)	Port mit Switch verbunden	LAN IP-Adresse	Priorität	Präemptionsmodus
A	1	LAN2	192.168.1.1	110	Aktivieren
B	1	LAN2	192.168.1.2	100	Deaktivieren

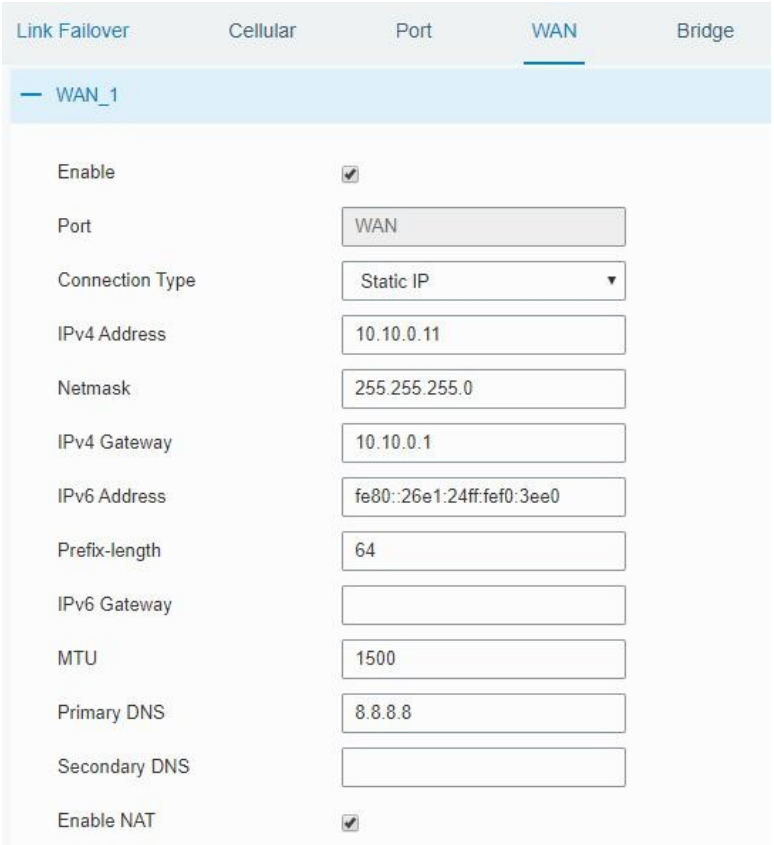
Siehe die folgende Topologie.



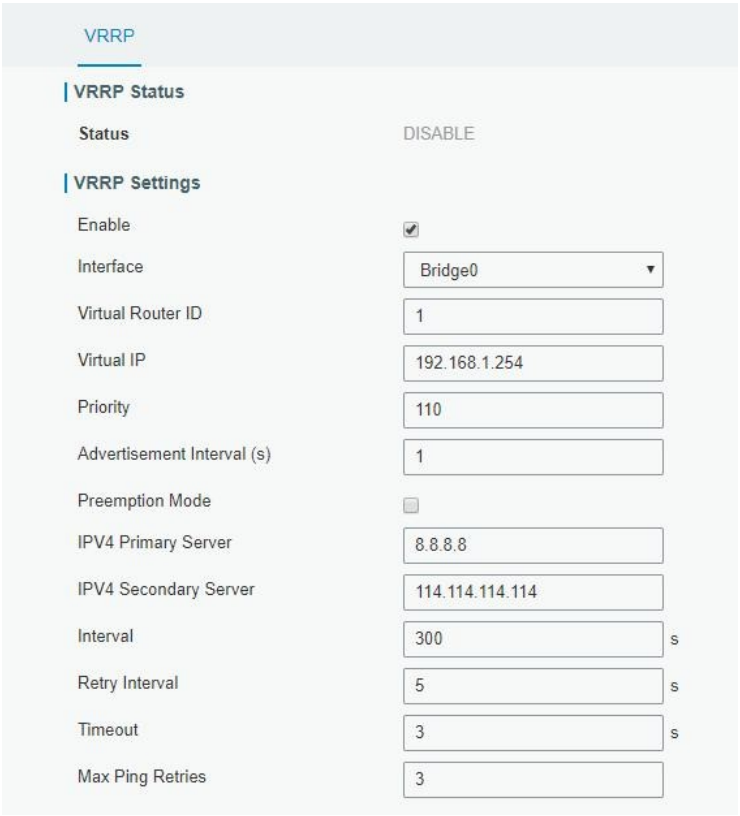
Konfigurationsschritte

Konfiguration von Router A

1. Gehen Sie zu **Netzwerk > Schnittstelle > WAN** und konfigurieren Sie die kabelgebundene WAN-Verbindung wie unten beschrieben.

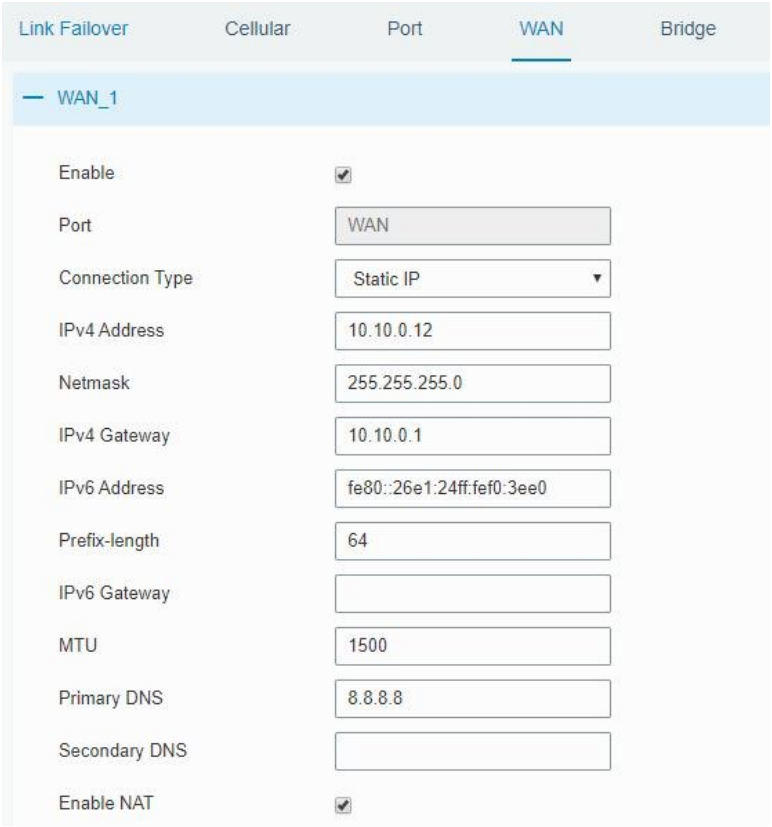


2. Gehen Sie zu **Netzwerk > VRRP > VRRP** und konfigurieren Sie die VRRP-Parameter wie unten beschrieben.

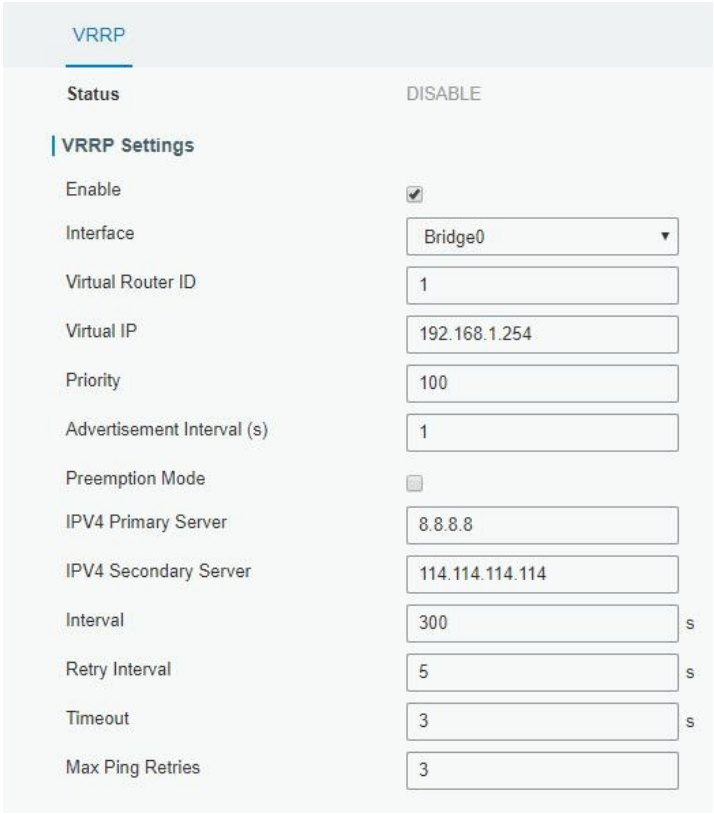


Konfiguration von Router B

1. Gehen Sie zu **Netzwerk > Schnittstelle > WAN** und konfigurieren Sie die kabelgebundene WAN-Verbindung wie unten beschrieben.



2. Gehen Sie zu **Netzwerk > VRRP > VRRP** und konfigurieren Sie die VRRP-Parameter wie unten beschrieben.



Wenn Sie alle Konfigurationen abgeschlossen haben, klicken Sie oben rechts auf die Schaltfläche **„Übernehmen"**, damit die Änderungen wirksam werden.

Ergebnis: Normalerweise ist A der Master-Router, der als Standard-Gateway verwendet wird. Wenn die Stromversorgung von Router A ausfällt oder Router A einen Ausfall erleidet, wird Router B zum Master-Router und als Standard-Gateway verwendet. Wenn der Preemption-Modus aktiviert ist, wird Router A zum Master und Router B wird wieder zum Backup herabgestuft, sobald Router A wieder auf das Internet zugreifen kann.

Verwandte Themen

VRRP-Einstellung

4.10 QoS-Anwendungsbeispiel

Beispiel

Konfigurieren Sie den UR35-Router so, dass er die lokale Präferenz auf verschiedene FTP-Download-Kanäle verteilt. Die gesamte Download-Bandbreite beträgt 75000 kbps.

Hinweis: Die „Gesamt-Downloadbandbreite" sollte geringer sein als die tatsächliche maximale Bandbreite der WAN- oder Mobilfunk-Schnittstelle.

FTP-Server-IP und -Port	Prozent	Maximale Bandbreite (kbps)	Minimale Bandbreite (kbps)
110.21.24.98:21	40	30000	25000
110.32.91.44:21	60	45000	40000

Konfigurationsschritte

1. Gehen Sie zu **Netzwerk > QoS > QoS (Download),** um QoS zu aktivieren und die gesamte Download-Bandbreite festzulegen.

2. Klicken Sie auf „ “, um Dienstklassen einzurichten.

Hinweis: Die Prozentsätze müssen zusammen 100 % ergeben.

3. Klicken Sie auf „ “, um Regeln für Dienstkategorien festzulegen.

Hinweis:

IP/Port: null bezieht sich auf jede IP-Adresse/jeden Port.

Klicken Sie auf die Schaltfläche **„Speichern** und **Anwenden“**.

Verwandtes Thema

QoS-Einstellung

[ENDE]