Milesight

Vorwort

Vielen Dank, dass Sie sich für den industriellen Mobilfunkrouter UR32L von Milesight entschieden haben. Der industrielle Mobilfunkrouter UR32L bietet eine stabile Netzwerkverbindung mit umfassenden Funktionen wie automatischem Failover/Failback, erweitertem Betriebstemperaturbereich, zwei SIM-Karten, Hardware-Watchdog, VPN, Fast Ethernet und vielem mehr.

In diesem Handbuch wird beschrieben, wie Sie den industriellen Mobilfunkrouter UR32L konfigurieren und bedienen. Hier finden Sie detaillierte Informationen zu den Funktionen und zur Konfiguration des Routers.

Leser

Diese Anleitung richtet sich in erster Linie an folgende Benutzer:

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

Verwandte Dokumente

Dokument	Beschreibung
UR32L-Datenblatt	Datenblatt für den industriellen Mobilfunkrouter UR32L.
UR32L Schnellstartanleitung	Schnellinstallationsanleitung für den industriellen Mobilfunkrouter UR32L.

Konformitätserklärung

Der UR32L 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 Tel.: 86-592-5085280
Fax: 86-592-5023065
Adresse: Gebäude C09, Software Park III, Xiamen 361024, China

Revisionsverlauf

Datum	Dokumentversion	Beschreibung
23. März 2021	V 1.0	Erstversion
17. September 2021	V 1.1	1. Unterstützung für Mobilfunk- und Ping-Erkennung IPv6 2. WAN-Verbindungstyp hinzufügen: DHCPv6-Client, DS-Lite 3. DHCPv6-Serverfunktion hinzufügen 4. Funktion für statisches IPv6-Routing hinzufügen 5. Expertenoption in IPsec-Einstellungen hinzufügen 6. Unterstützung für das Löschen von SMS-Eingangs- und Ausgangsmappen

Inhalt

Kapitel 1 Produktvorstellung

1.1 Übersicht

Der UR32L ist ein industrieller Mobilfunkrouter mit integrierten intelligenten Softwarefunktionen, der für vielfältige M2M/IoT-Anwendungen entwickelt wurde. Der UR32L 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 UR32L eine Netzwerkverbindung mit Wire-Speed bei geringem Stromverbrauch und extrem kompakter Bauweise, um eine äußerst sichere und zuverlässige Verbindung zum Funknetzwerk zu gewährleisten.

Der UR32L 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 UR32L-Schnellstartanleitung.

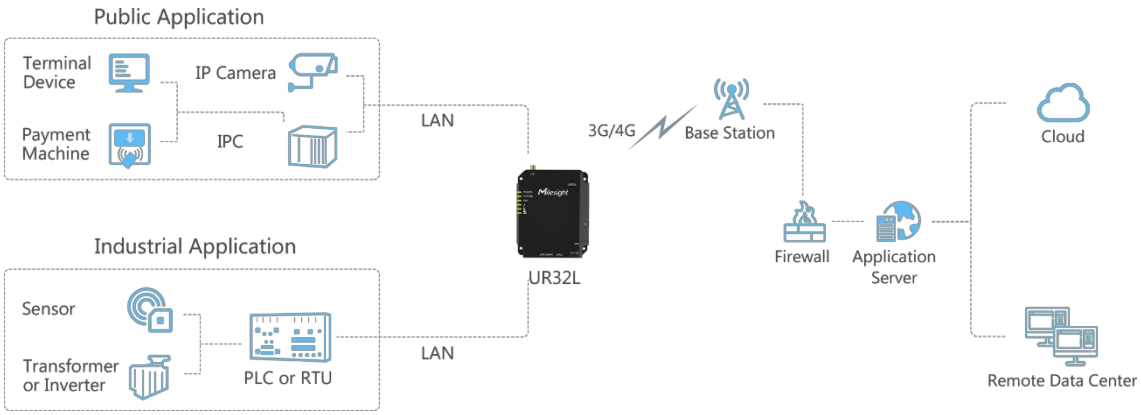


Abbildung 1-1

1.2 Vorteile

Vorteile

- Integrierte industrielle leistungsstarke NXP-CPU, großer Speicher
- Schnelle Ethernets für schnelle Datenübertragung
- 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
- Integrierter Hardware-Watchdog, der verschiedene Fehler automatisch 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 Ebenen von Benutzerberechtigungen

Einfache Wartung

- Milesight DeviceHub ermöglicht 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.
- Web-GUI und CLI ermöglichen dem Administrator eine einfache Verwaltung und schnelle Konfiguration einer großen Anzahl von Geräten
- Effiziente Verwaltung der Remote-Router auf der bestehenden Plattform über den Industriestandard SNMP

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 zur Unterstützung weiterer Anwendungen
- Unterstützt umfangreiche Protokolle wie SNMPModbus-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
Speiche	128 MB Flash, 128 MB DDR3 RAM
Mobilfunk-Schnittstellen	
Anschlüsse	1 × 50 Ω SMA (Mittelstift: SMA-Buchse)
SIM-Steckplätze	1 (Mini-SIM-2FF)
Ethernet	
Anschlüsse	2 × 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)

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 usw.
VPN-Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE
Zugriffsauthentifizierung	CHAP/PAP/MS-CHAP/MS-CHAPV2
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
Zuverlässigke	VRRP, WAN-Failover
Stromversorgung und Verbrauch	
Anschluss	2-polig mit 5,08-mm-Anschlussblock
Eingangsspannung	9–48 VDC
Leistungsaufnahme	Typisch 1,8 W, max. 2,2 W (im Nicht-PoE-
Modus) Ausgangsleistung	2 × 802.3 af/at PoE-Ausgang
Physikalische Eigenschaften	
Schutzart	IP30
Wohnraum	Metall
Abmessungen	108 x 90 x 26 mm (4,25 x 3,54 x 1,02 Zoll)
Befestigung	Tisch-, Wand- oder DIN-Schienenmontage
Sonstiges	
Reset-Taste	1 × RESET
LED-Anzeigen	1 × POWER, 1 × SYSTEM, 1 × SIM, 3 × Signalstärke
Integrie	Watchdog, Timer
Umgebung	
Betriebstemperatur	-40 °C bis +70 °C (-40 °F bis +158 °F) Reduzierte Mobilfunkleistung 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)

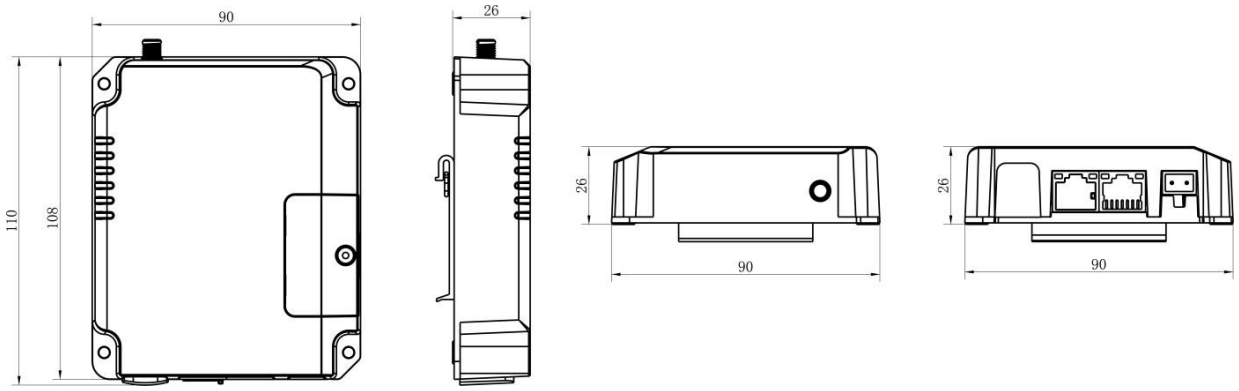


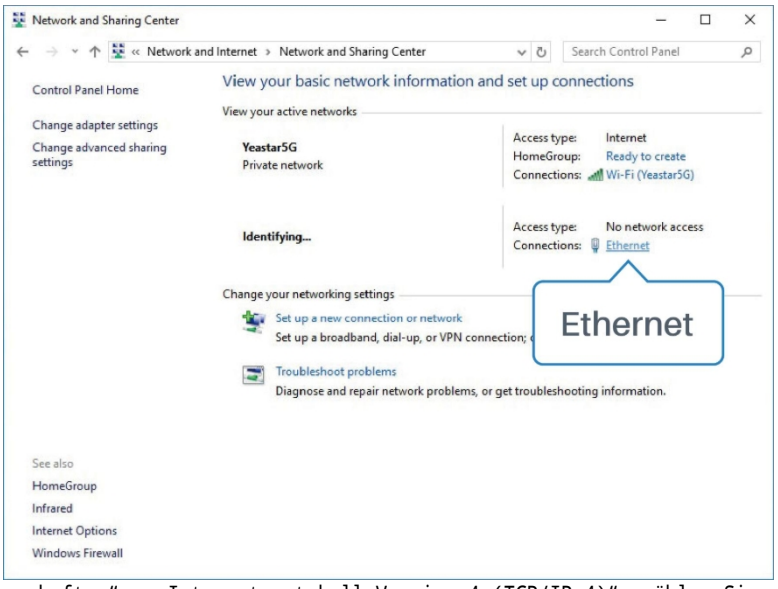
Abbildung 1-2

Kapitel 2 Zugriff auf die Web-GUI

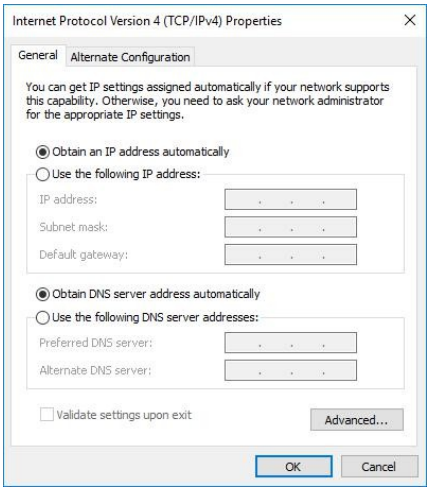
In diesem Kapitel wird erläutert, wie Sie auf die Web-GUI des UR32L-Routers zugreifen können. Schließen Sie den PC direkt an den LAN-Anschluss des UR32L-Routers an. Die folgenden Schritte basieren auf dem Betriebssystem Windows 10 und dienen als Referenz.

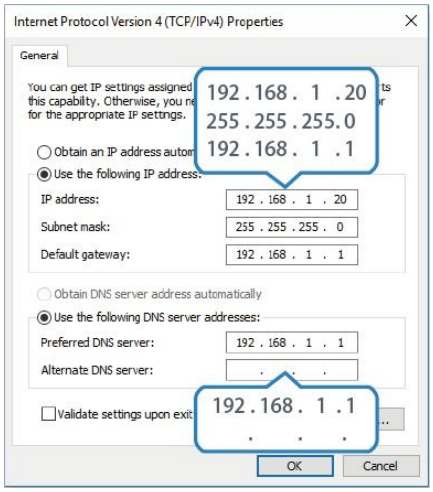
Benutzername: admin
Passwort: password IP-
Adresse: 192.168.1.1

1. Gehen Sie zu „Systemsteuerung“ → „Netzwerk und Internet“ → „Netzwerk- und Freigabecenter“ und klicken Sie dann auf „Ethernet“ (kann auch einen anderen Namen haben).



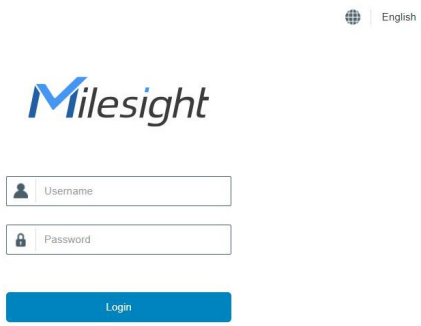
2. Gehen Sie zu „Eigenschaften“ → „Internetprotokoll Version 4 (TCP/IPv4)“, wählen Sie „IP-Adresse automatisch beziehen“ oder „Folgende IP-Adresse verwenden“ und weisen Sie dann manuell eine statische IP-Adresse innerhalb desselben Subnetzes des Geräts zu.





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.

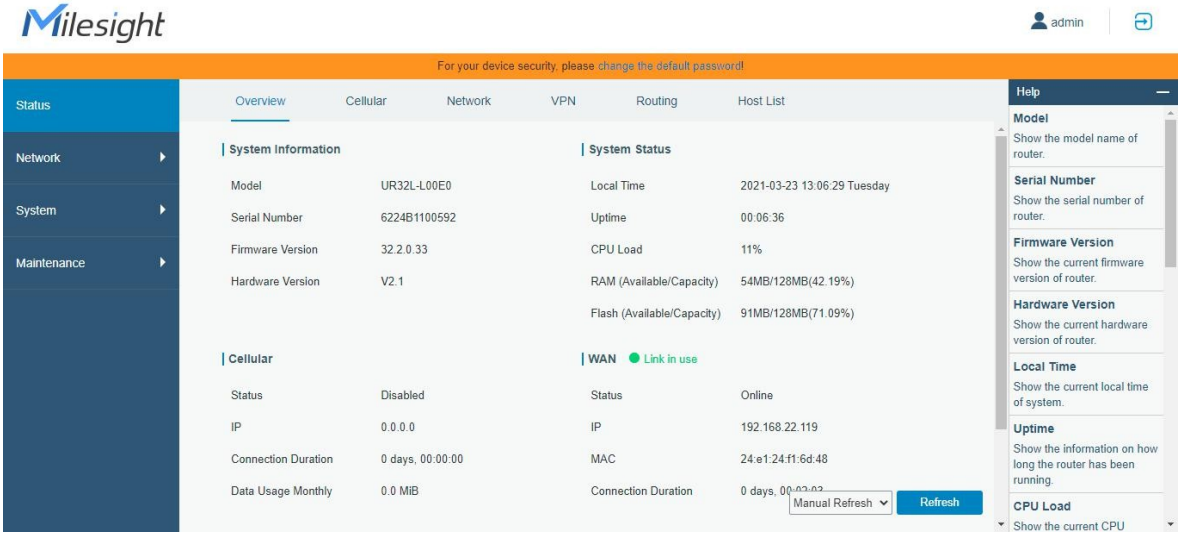
4. Geben Sie den Benutzernamen und das Passwort ein und klicken Sie auf „Anmelden“.



Wenn Sie den Benutzernamen oder das Passwort mehr als fünf Mal 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.

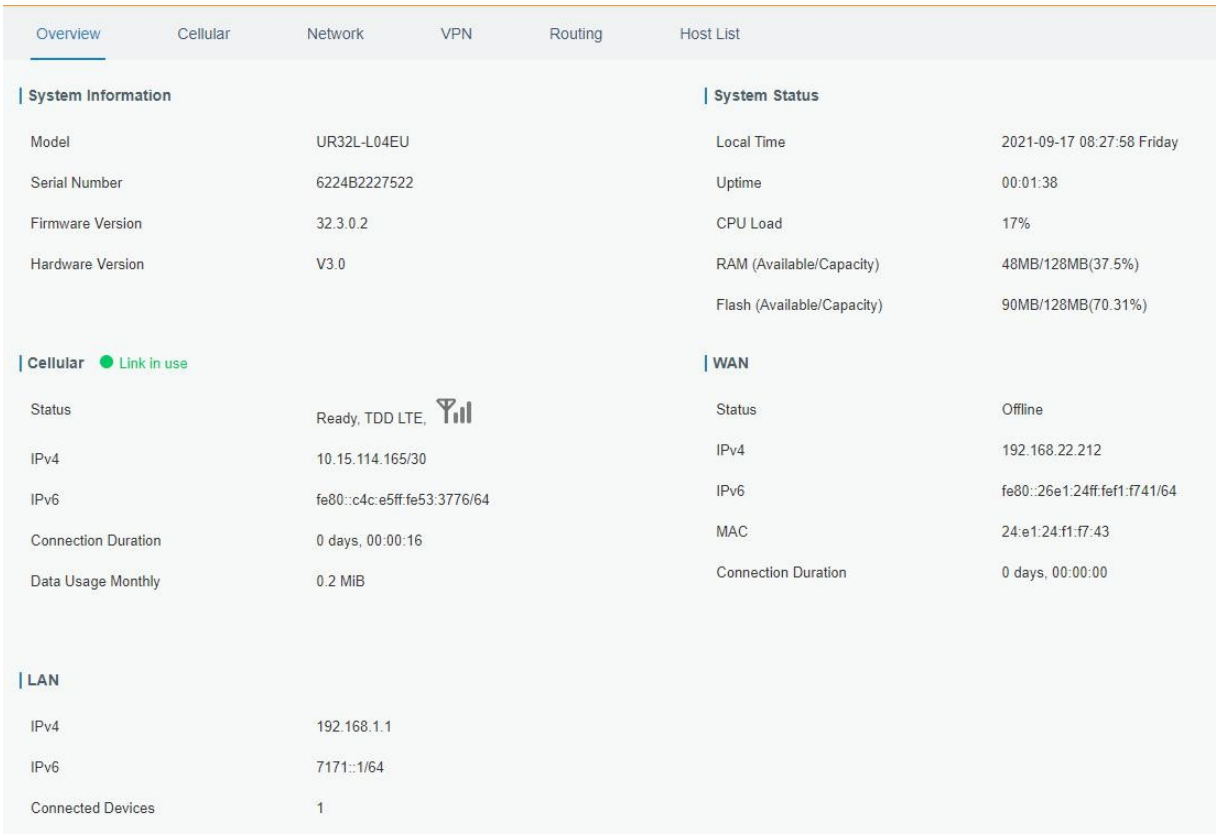


Abbildung 3-1-1-1

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	Zeigt an, wie lange der Router bereits läuft. in Betrieb ist.
CPU-Auslastung	Zeigt die aktuelle CPU-Auslastung des Routers an.
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.

Tabelle 3-1-1-2 Systemstatus

Mobilfunk	
Element	Beschreibung
Status	Zeigt den Echtzeitstatus der aktuellen SIM-Karte an.
IPv4/IPv6	Zeigt 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

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 3-1-1-5 LAN-Status

3.1.2 Mobilfunk

Auf dieser Seite können Sie den Mobilfunknetzstatus des Routers anzeigen.

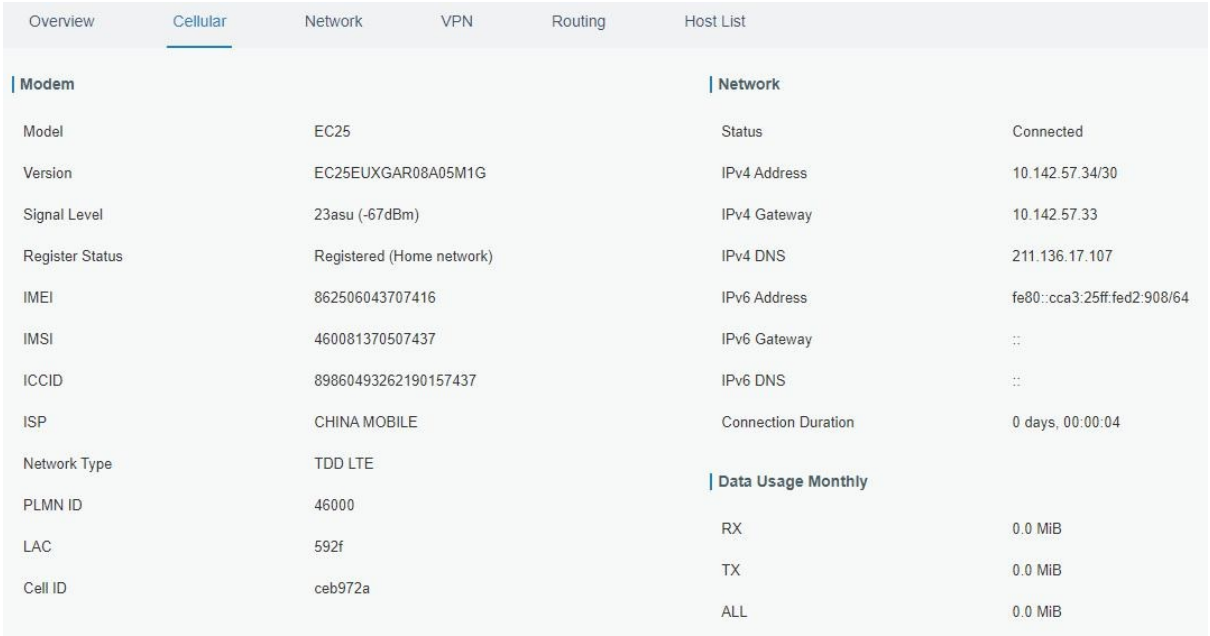


Abbildung 3-1-2-1

Modem-Informationen	
Element	Beschreibung
Status	Zeigt den entsprechenden Erkennungsstatus des Moduls und der SIM-Karte an.
Version	Zeigt die Firmware-Version des Mobilfunkmoduls an.
Signalpegel	Zeigt den Mobilfunksignalpegel an.
Registrierungsstatus	Zeigt den Registrierungsstatus der SIM-Karte an.
IMEI	Zeigt die IMEI des Moduls an.
IMSI	Zeigt die IMSI der SIM-Karte an.
ICCID	Zeigt 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	Zeigt die Cell-ID des Standorts der SIM-Karte 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	Zeigen Sie die IPv4/IPv6-DNS des Mobilfunknetzes an.
Verbindungsdauer	Zeigen Sie Informationen darüber an, wie lange das Mobilfunknetz verbunden war verbunden ist.

Tabelle 3-1-2-2 Netzwerkstatus

Datenverbrauch monatlich	
Element	Beschreibung
RX	Zeigt die monatliche Statistik zur RX-Datennutzung der SIM-Karte an.
TX	Zeigt die monatliche TX-Datenverbrauchsstatistik der SIM-Karte an.
ALL	Zeigt die monatliche Gesamtstatistik zum Datenverbrauch der SIM-Karte 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.

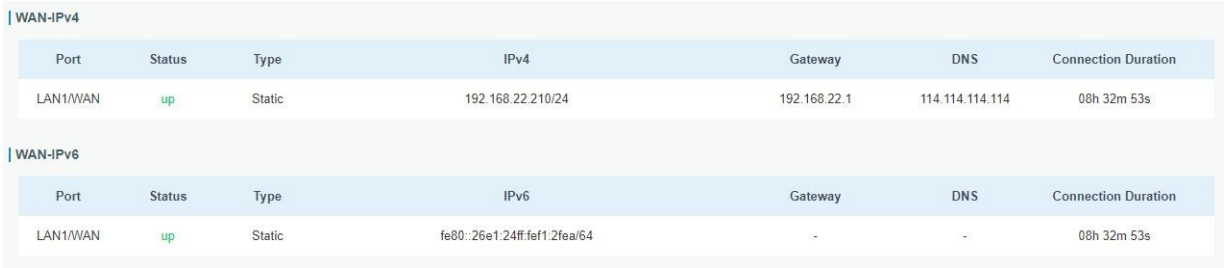


Abbildung 3-1-3-1

WAN-Status

Element	Beschreibung
Port	Zeigt den Namen des WAN-Ports an.
Status	Zeigt den Status des WAN-Ports an. „up“ bezieht sich auf oder einen Status, bei dem 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	Zeigen Sie die IPv4-Adresse mit Netzmaske oder die IPv6-Adresse mit Präfixlänge des WAN-Port.
Gateway	Zeigt das Gateway des WAN-Ports an.
DNS	Zeigt das DNS des WAN-Ports an.
Verbindungsdauer	Zeigt an, wie lange das Ethernet-Kabel , wenn die WAN-Funktion aktiviert ist. Sobald die WAN-Funktion deaktiviert oder die Ethernet-Verbindung getrennt wird, wird die Dauer nicht mehr angezeigt.

Tabelle 3-1-3-1 WAN-Status

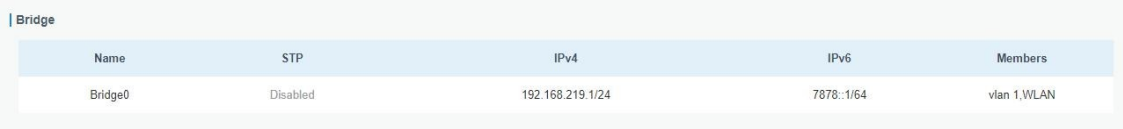


Abbildung 3-1-3-2

Brücke	
Element	Beschreibung
Name	Zeigen Sie 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	Zeigt die Mitglieder der Bridge-Schnittstelle an.

Tabelle 3-1-3-2 Bridge-Status

3.1.4 VPN

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

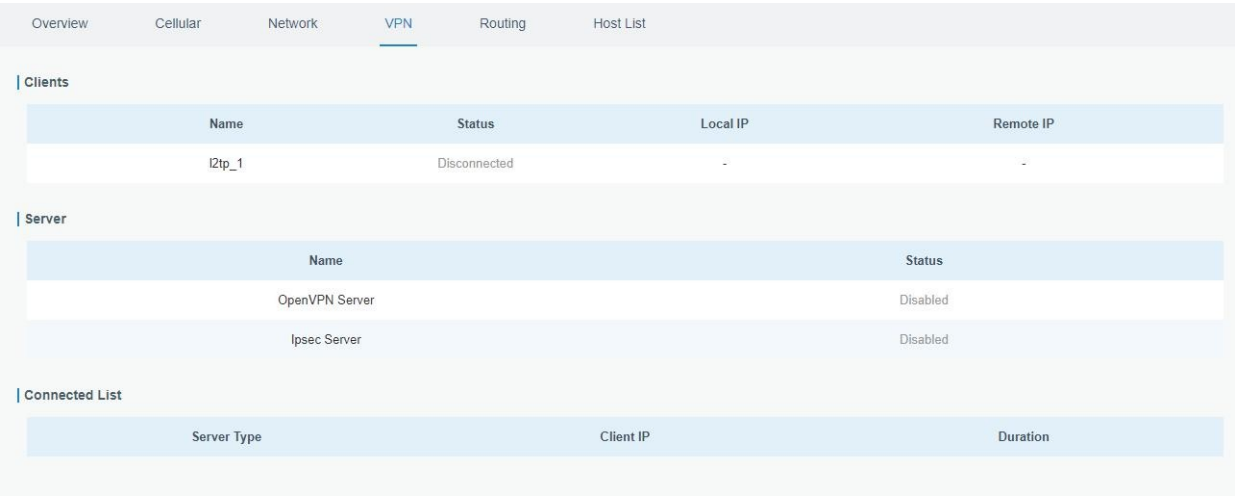


Abbildung 3-1-4-1

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	Zeigt die tatsächliche 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	Zeigen Sie die IP-Adresse des Clients an, der sich mit dem Server verbunden hat.
Dauer	Zeigen Sie 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 wird die Dauer nicht mehr gezählt.

Tabelle 3-1-4-1 VPN-Status

3.1.5 Routing

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

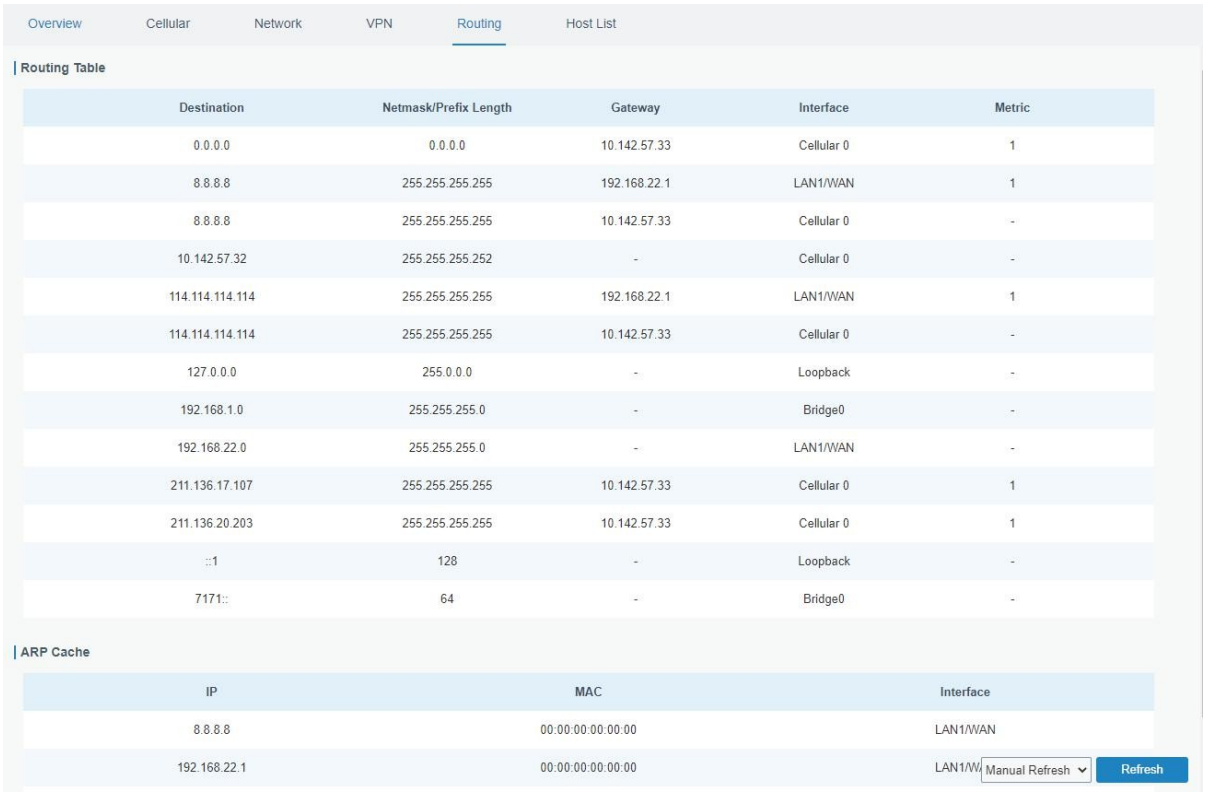


Abbildung 3-1-5-1

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

Tabelle 3-1-5-1 Routing-Informationen

3.1.6 Host-Liste

Auf dieser Seite können Sie die Host-Informationen einsehen.

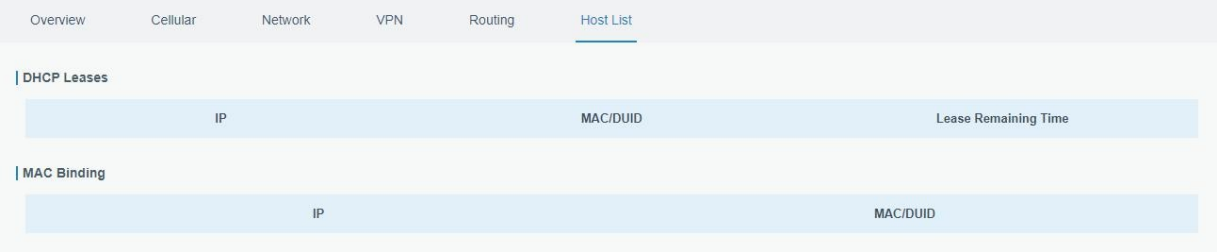


Abbildung 3-1-6-1

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	Zeigt die verbleibende Lease-Zeit des DHCP-Clients an.
MAC-Bindung	
IP & MAC	Zeigt die IP-Adresse und MAC-Adresse an, die in der Liste „Statische IP“ des DHCP-Dienst.

Tabelle 3-1-6-1 Beschreibung der Hostliste

3.2 Netzwerk

3.2.1 Schnittstelle

3.2.1.1 Link-Failover

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 UR32L einen zweiten Link aus, bei dem IPv6 als primärer IPv6-Link fungiert, und umgekehrt.

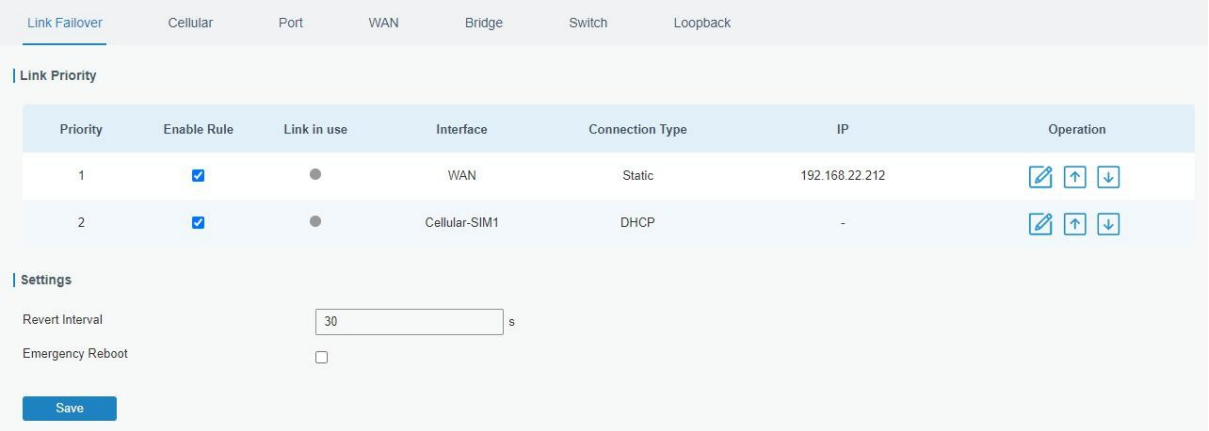


Abbildung 3-2-1-1

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, wählt der Router diese Schnittstelle für seine Switching-Regel aus. Wenn die Mobilfunk-Schnittstelle hier nicht aktiviert ist, wird auch 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	
Rückstellintervall	Geben Sie die Anzahl der Sekunden an, die gewartet werden soll, bevor zur Link mit höherer Priorität zu wechseln. 0 bedeutet, dass die Funktion deaktiviert ist.
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 Link-Ausfallsicherung

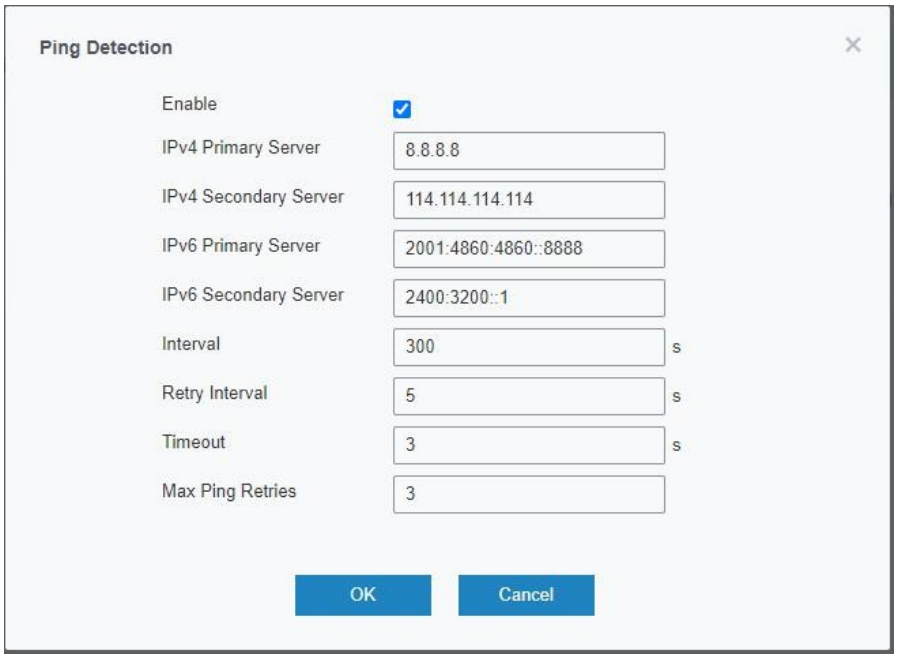


Abbildung 3-2-1-2

Ping-Erkennung	
Element	Beschreibung
Aktivieren	Wenn diese Option aktiviert ist, überprüft der Router regelmäßig den Verbindungsstatus des Links.
IPv4/IPv6 Primär	Der Router sendet ein ICMP-Paket an die IPv4/IPv6-Adresse

Server	oder den Hostnamen, um festzustellen, ob die Internetverbindung noch verfügbar ist oder nicht.
IPv4/IPv6 Sekundär Server	Der Router versucht, den sekundären Servernamen anzupingen, wenn Primärserver nicht verfügbar ist.
Intervall	Zeitintervall (in Sekunden) zwischen zwei Pings.
Wiederholungsintervall	Legen Sie das Intervall für Ping-Wiederholungen fest. Wenn ein Ping fehlschlägt, sendet der Router in jedem Wiederholungsintervall erneut einen Ping senden.
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 des Routers, der Ping-Anfragen sendet, bis feststellt, dass die Verbindung fehlgeschlagen ist.

Tabelle 3-2-1-2 Ping-Erkennungsparameter

3.2.1.2 Mobilfunk

In diesem Abschnitt wird erläutert, wie die entsprechenden Parameter für das Mobilfunknetz eingestellt werden.

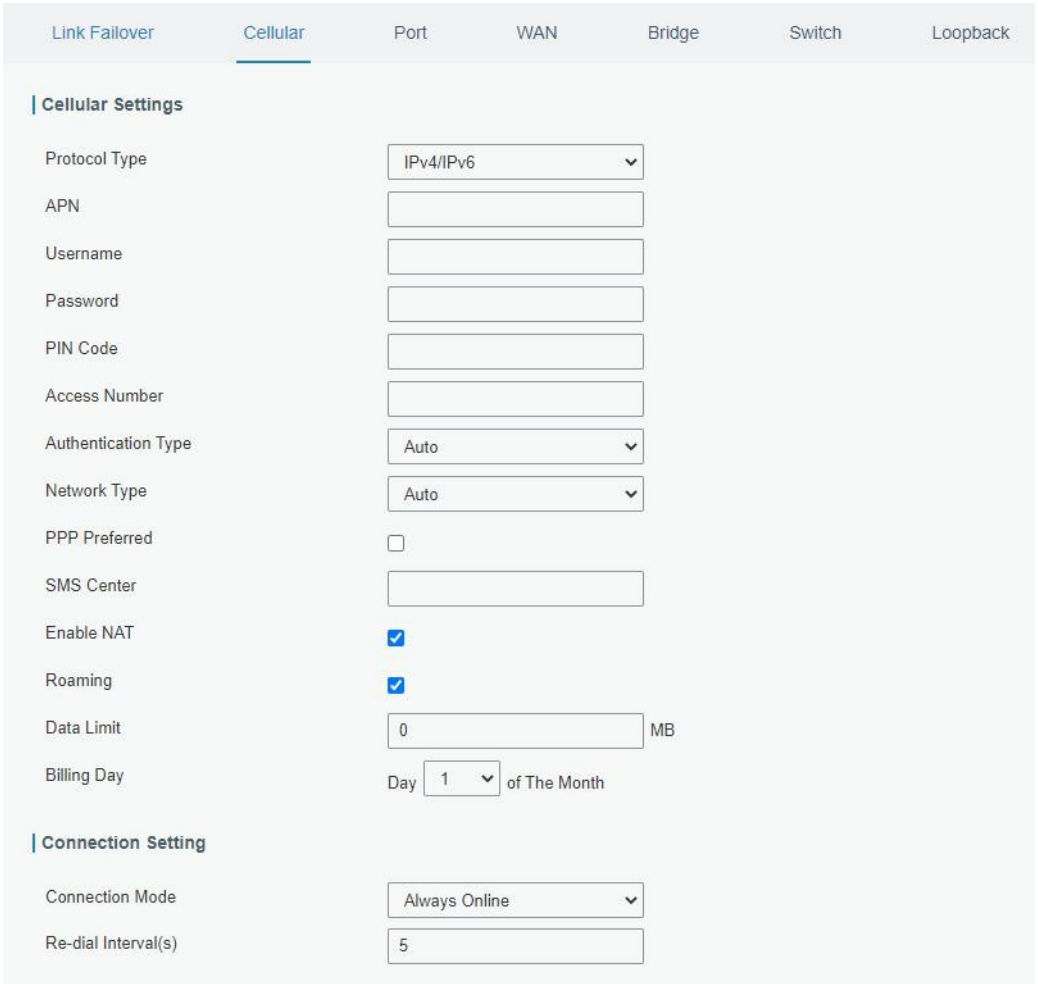


Abbildung 3-2-1-3

Mobilfunk-Einstellungen	
Element	Beschreibung
Protokoll	Wählen Sie zwischen „IPv4“, „IPv6“ und „IPv4/IPv6“.
APN	Geben Sie den Zugangspunktnamen für die Mobilfunk-Einwahlverbindung ein, der vom lokalen Internetdienstanbieter bereitgestellt wird.
Benutzername	Geben Sie den Benutzernamen für die vom lokalen ISP bereitgestellte Mobilfunk-Einwahlverbindung ein Internetdienstanbieters bereitgestellt wird.
Passwort	Geben Sie das Passwort für die Mobilfunk-Einwahlverbindung ein, das Ihnen von Ihrem lokalen Internetdienstanbieters.
PIN-Code	Geben Sie einen 4- bis 8-stelligen PIN-Code ein, um die SIM-Karte zu entsperren.
Zugangsnummer	Geben Sie die Nummer der Einwahlzentrale für die vom lokalen Internetdienstanbieter bereitgestellte Mobilfunk-Einwahlverbindung ein vom lokalen ISP bereitgestellt wird.
Authentifizierungstyp	Wählen Sie zwischen „Auto“, „PAP“, „CHAP“, „MS-CHAP“ und „MS-CHAPv2“.
Netzwerktyp	Wählen Sie zwischen „Auto“, „Nur 4G“, „Nur 3G“ und „Nur 2G“. Auto: Automatische Verbindung zum Netzwerk mit dem stärksten Signal. Nur 4G: Verbindung nur zum 4G-Netzwerk. Und so weiter.
PPP bevorzugt	Die PPP-Einwahlmethode wird bevorzugt.
SMS-Zentrum	Geben Sie die Nummer des lokalen SMS-Centers ein, um SMS-Nachrichten zu speichern, weiterzuleiten, zu konvertieren und Zustellung von SMS-Nachrichten.
NAT aktivieren	Aktivieren oder deaktivieren Sie die NAT-Funktion.
Roaming	Roaming aktivieren oder deaktivieren.
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 das Datenvolumen auf 0 zurück.

Tabelle 3-2-1-3 Mobilfunkparameter

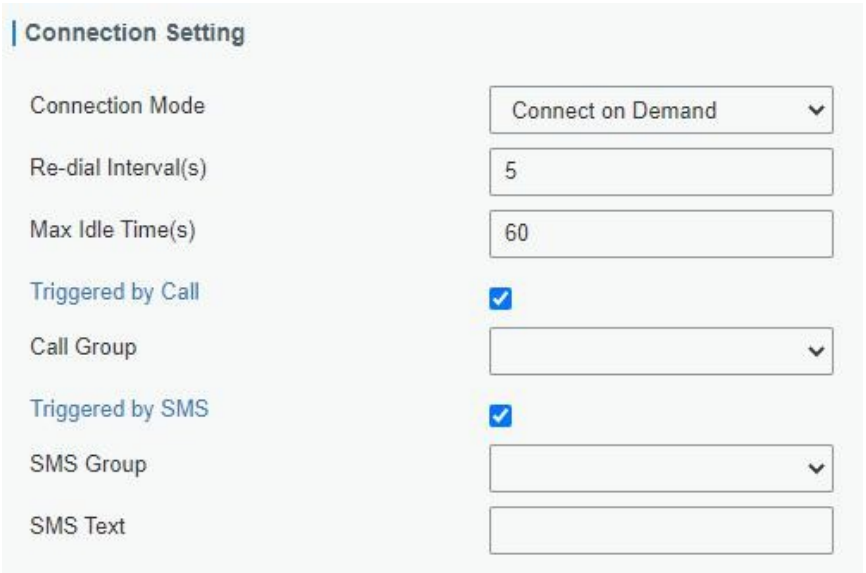


Abbildung 3-2-1-4

Verbindungseinstellungen	
Element	Beschreibung
Verbindungsmodus	Wählen Sie zwischen „Immer online“ und „Bei Bedarf verbinden“.
Wählintervall(e)	Stellen Sie das Intervall ein, nach dem die Verbindung zum ISP wiederhergestellt werden soll, wenn sie unterbrochen wurde. Der Standardwert beträgt 5 Sekunden.
Maximale Leerlaufzeiten	Legen Sie die maximale Dauer fest, die der Router im Leerlaufzustand verbleiben soll, wenn die aktuelle Verbindung inaktiv ist. Bereich: 10–3600
Durch Anruf ausgelöst	Der Router wechselt automatisch vom Offline-Modus in den Mobilfunkmodus , 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 die Telefongruppe einzurichten.
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 die Auslösung aus. Gehen Sie zu „System > Telefon & SMS > SMS“, um eine SMS-Gruppe einzurichten.
SMS-Text	Geben Sie den SMS-Inhalt für den Auslöser ein.

Tabelle 3-2-1-4 Mobilfunkparameter

Verwandte Themen
Mobilfunknetzverbindung
Telefongruppe

3.2.1.3 Anschluss

In diesem Abschnitt wird beschrieben, wie Sie die Ethernet-Port-Parameter konfigurieren. Der Mobilfunkrouter UR32L unterstützt 2 Fast-Ethernet-Ports.

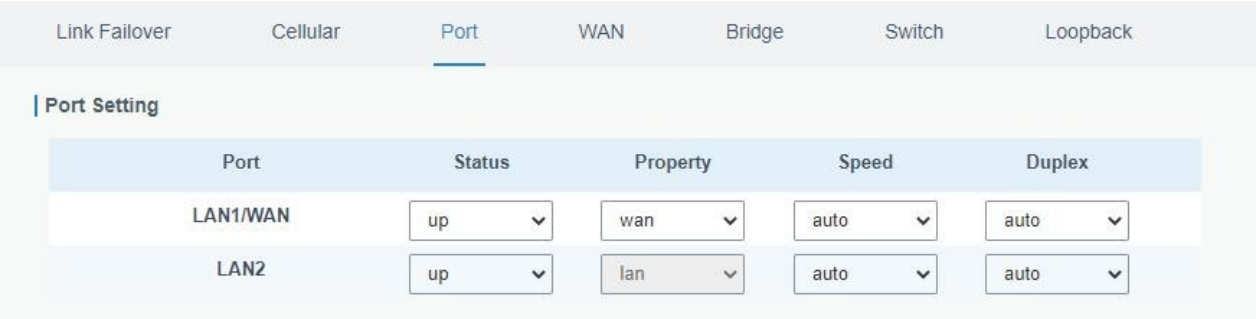


Abbildung 3-2-1-5

Port-Einstellung	
Element	Beschreibung
Port	Benutzer können die Ethernet-Ports entsprechend ihren Anforderungen definieren.
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	Stellen Sie die Geschwindigkeit des Ethernet-Ports ein. Die Optionen sind „Auto“, „100 Mbit/s“ 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

3.2.1.4 WAN

Der WAN-Port kann über ein Ethernet-Kabel mit dem Internet verbunden werden. Er unterstützt 5 Verbindungstypen.

- Statische IP: Konfigurieren Sie die IP-Adresse, die Netzmaske und das Gateway für die Ethernet-WAN-Schnittstelle.
- DHCP-Client: Konfigurieren Sie die Ethernet-WAN-Schnittstelle als DHCP-Client, um die IP-Adresse automatisch zu beziehen.
- 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: Verwenden Sie IPv4-in-IPv6-Tunneling, um IPv4-Pakete des Endgeräts über einen Tunnel im IPv6-Zugangsnetzwerk an den ISP zu senden.

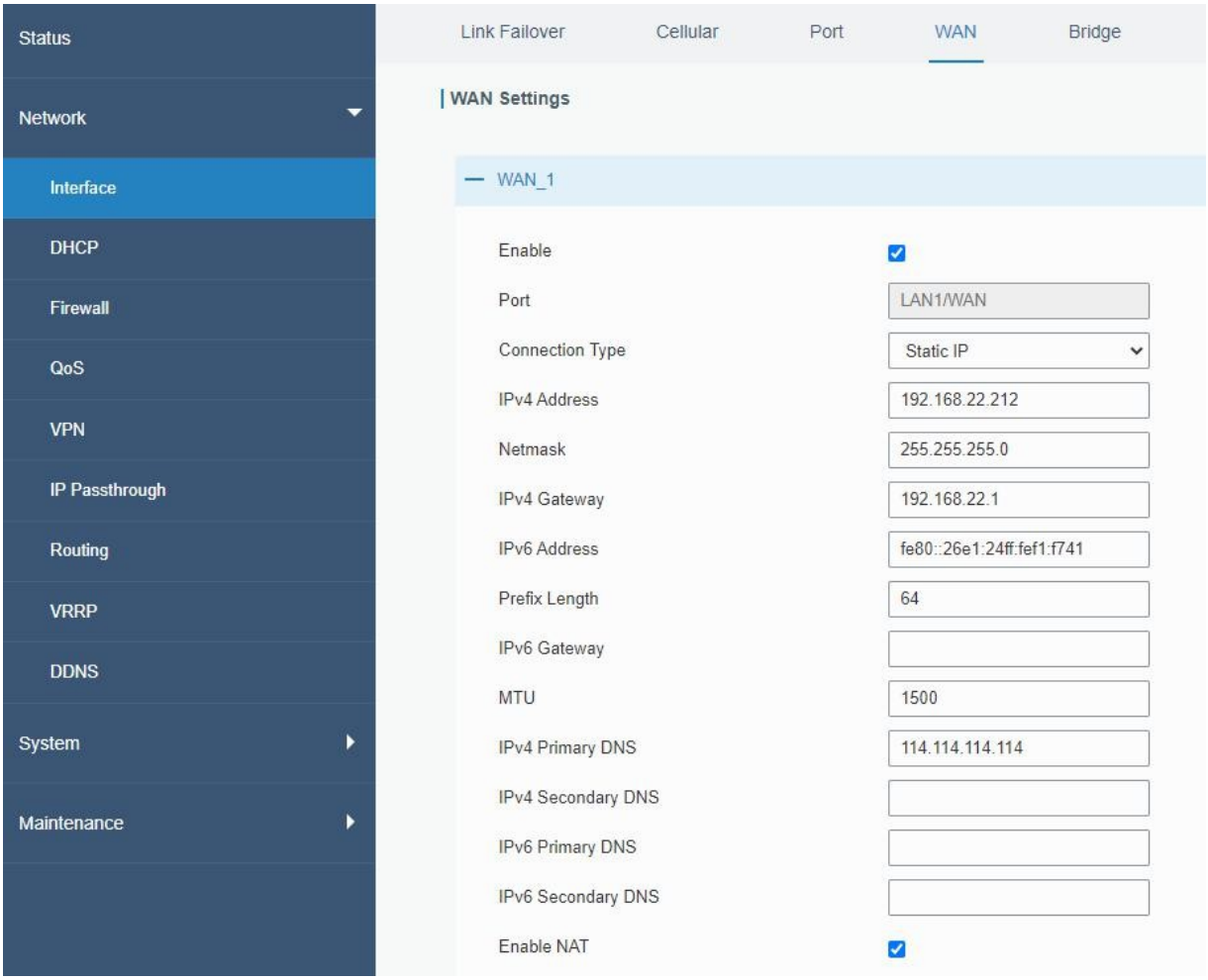


Abbildung 3-2-1-6

WAN-Einstellung		
Element	Beschreibung	Standard
Aktivieren	WAN-Funktion aktivieren.	Aktivieren

Port	Der Port, der derzeit als WAN-Port festgelegt ist.	WAN
Verbindungstyp	Wählen Sie zwischen „Statische IP“, „DHCP-Client“, „DHCPv6 Client“, „Dual-Stack Lite“ und „PPPoE“.	Statische IP
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 3-2-1-6 WAN-Parameter

1. Statische IP-Konfiguration

Wenn das externe Netzwerk eine feste IP für die WAN-Schnittstelle zuweist, kann der Benutzer den Modus „Statische IP“ auswählen.

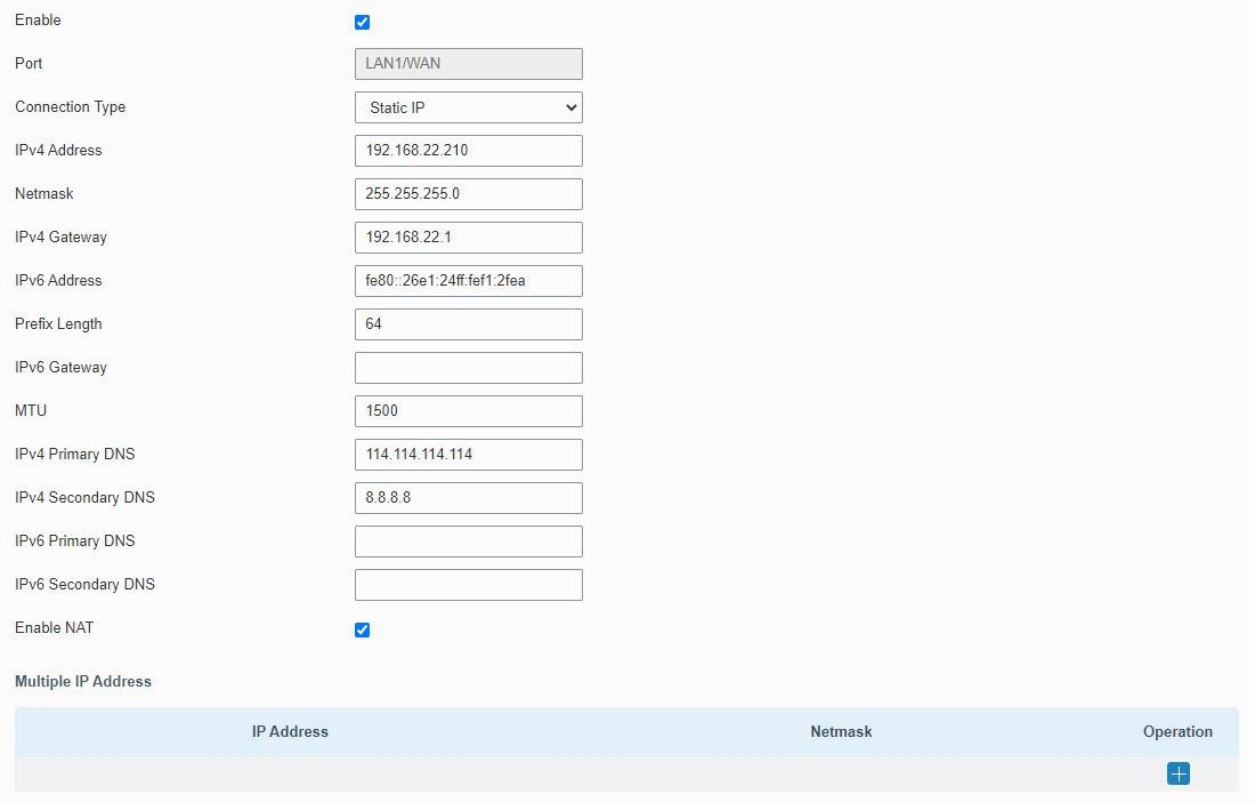


Abbildung 3-2-1-7

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 3-2-1-7 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, kann der Benutzer den Modus „DHCP-Client“ auswählen, um die IP-Adresse automatisch zu beziehen.

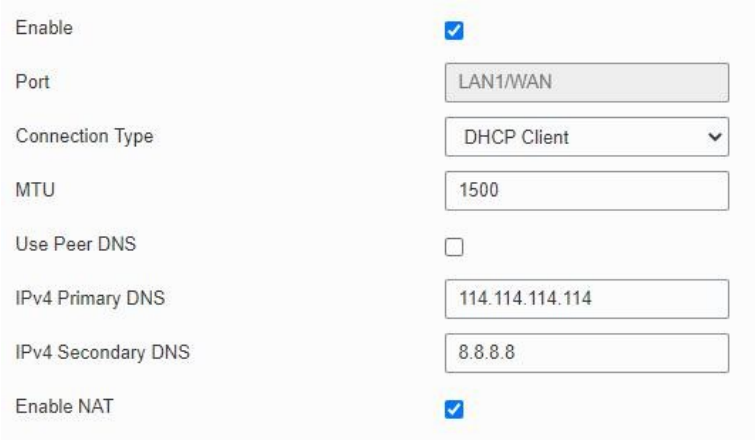


Abbildung 3-2-1-8

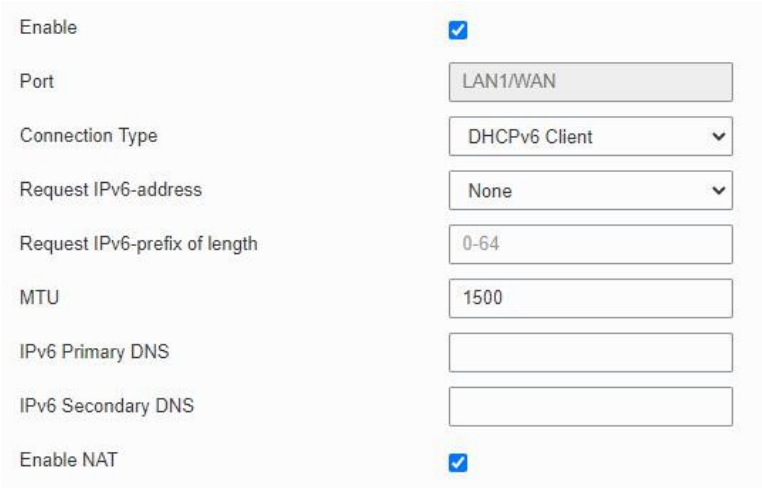


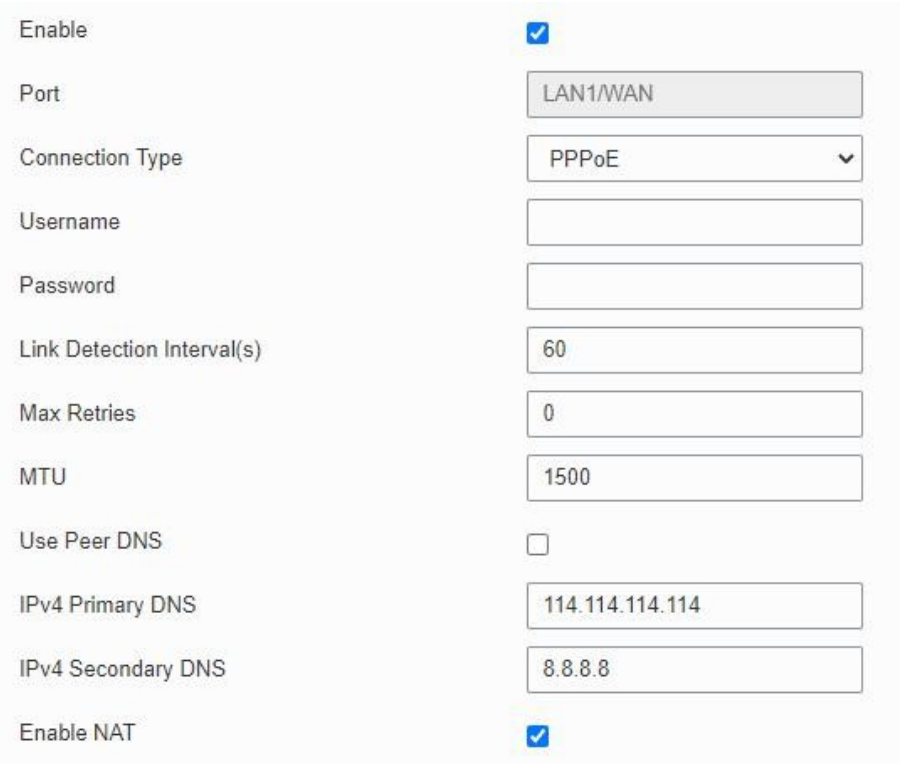
Abbildung 3-2-1-9

DHCP-Client	
Element	Beschreibung
Peer-DNS verwenden	Peer-DNS während des PPP-Wählvorgangs 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 Spezifische Adresse ist relevant für die Präfixlänge der von Ihnen festgelegten IPv6-Adresse.
Anfordern der Präfixlänge von IPv6	Legen Sie die Präfixlänge der IPv6-Adresse fest, die der Router vom DHCP-Server erhalten soll.

Tabelle 3-2-1-8 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 3-2-1-10

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 3-2-1-9 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.

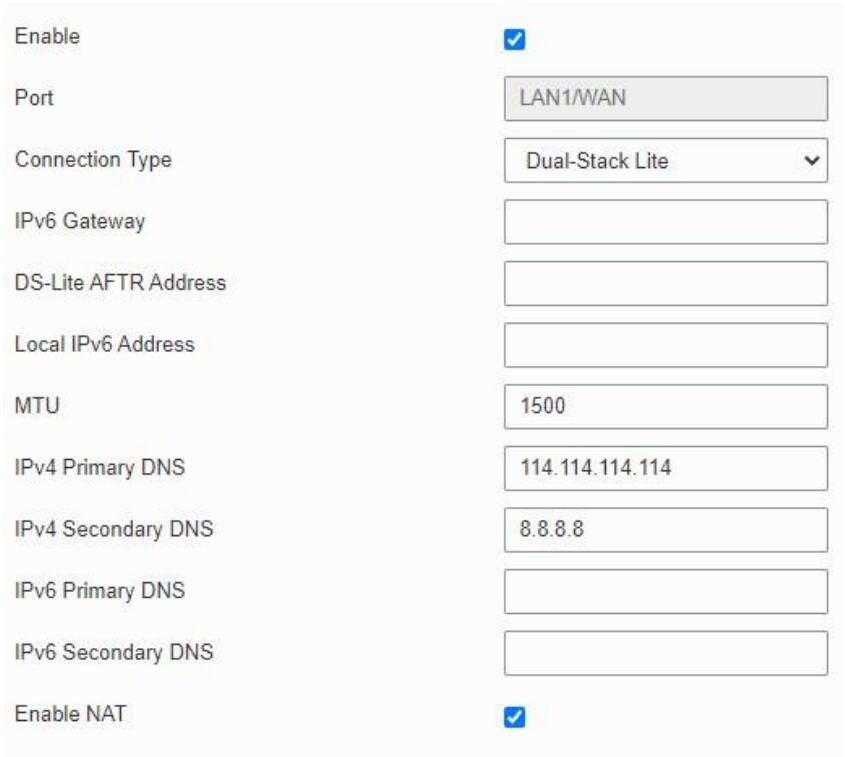


Abbildung 3-2-1-11

Dual-Stack Lite	
Element	Beschreibung
IPv6-Gateway	Stellen Sie das Gateway für die IPv6-Adresse des WAN-Ports ein.
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 3-2-1-10 Dual-Stack Lite-Parameter

Beispiel für die zugehörige Konfiguration

Ethernet-WAN-Verbindung

3.2.1.5 Bridge

Die Bridge-Einstellung wird zur Verwaltung von LAN-Geräten verwendet, die an die LAN-Ports des UR32L angeschlossen sind, sodass jedes dieser Geräte auf das Internet zugreifen kann.

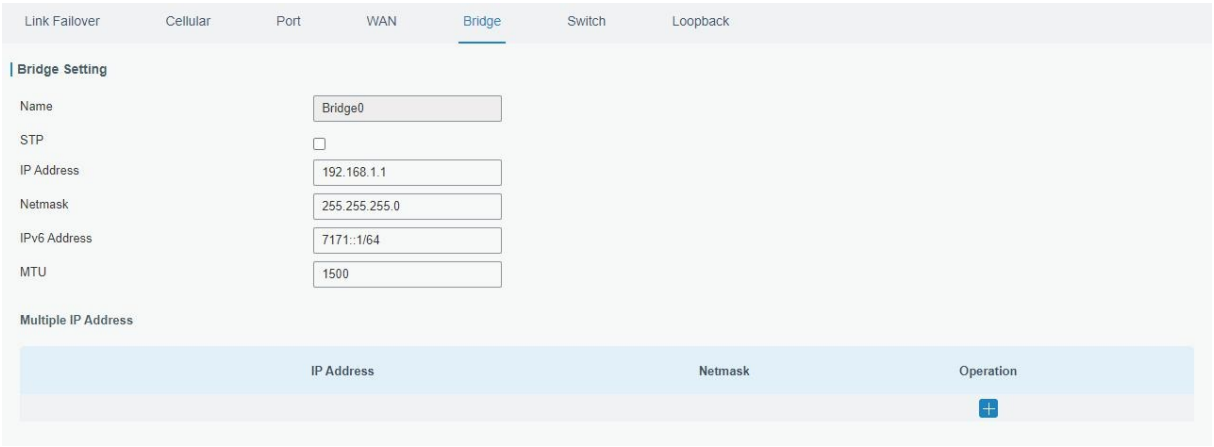


Abbildung 3-2-1-12

Bridge		
Element	Beschreibung	Standard
Name	Zeigt den Namen der Bridge 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 3-2-1-11 Brückeneinstellungen

3.2.1.6 Switch

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

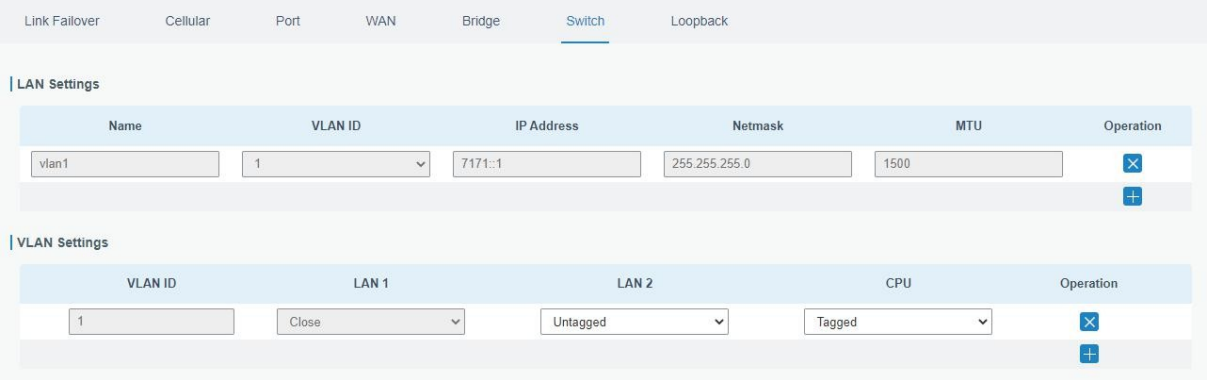


Abbildung 3-2-1-13

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	Legen Sie die IP-Adresse des LAN-Ports fest.
Netzmaske	Legen Sie die Netzmaske des LAN-Ports fest.
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	Binden Sie das VLAN an die entsprechenden Ports und wählen Sie den Status aus „Getaggt“, „Nicht getaggt“ und „Schließen“ für Ethernet-Frames auf der Trunk-Verbindung aus.
CPU	Steuerung der Kommunikation zwischen VLAN und anderen Netzwerken.

Tabelle 3-2-1-12 VLAN-Trunk-Parameter

3.2.1.7 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.

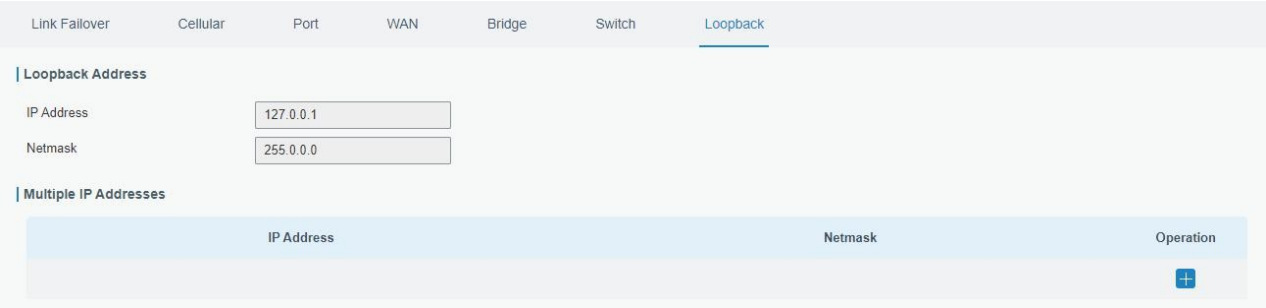


Abbildung 3-2-1-14

Loopback		
Element	Beschreibung	Standard
IP-Adresse	Unveränderlich	127.0.0.1

Netzmaske	Unveränderlich	255.0.0.0
Mehrere IP-Adressen Adressen	Abgesehen von der oben genannten IP-Adresse kann der Benutzer andere IP-Adressen konfigurieren.	Null

Tabelle 3-2-1-13 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 UR32L kann als DHCP-Server oder DHCPv6-Server eingerichtet werden, um IP-Adressen zu vergeben, 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 UR32L unterstützt nur Stateful DHCPv6, wenn er als DHCPv6-Server arbeitet.

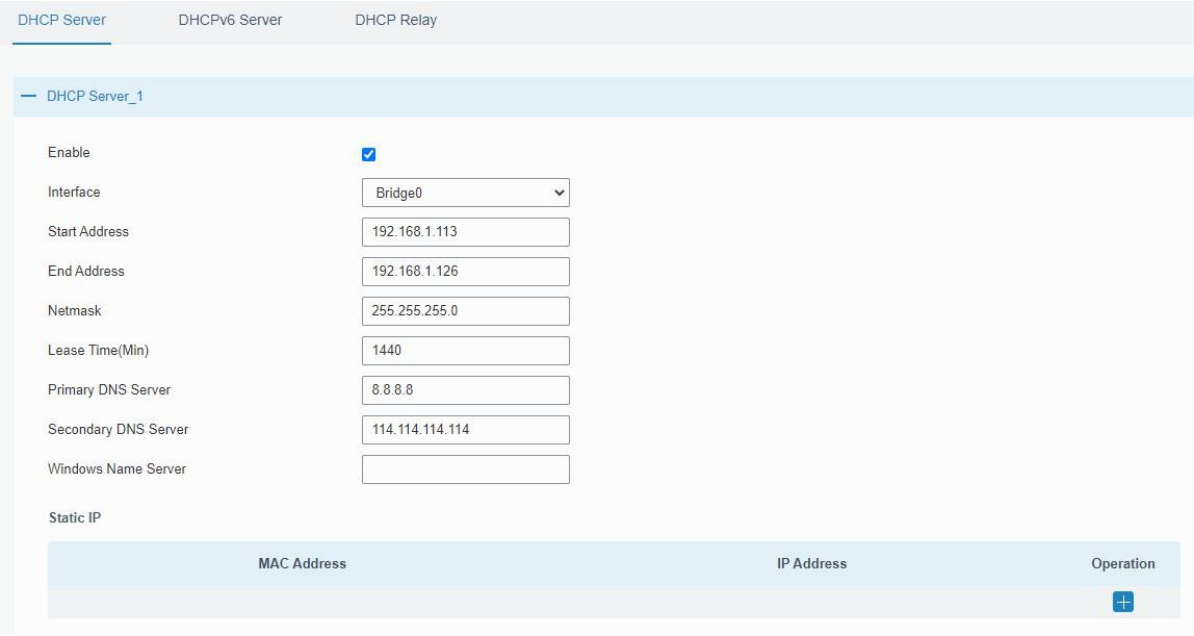


Abbildung 3-2-2-1

Abbildung 3-2-2-2

DHCP-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.	192.168.1.100
Endadresse	Definieren Sie das Ende des Pools von IP-Adressen, die an DHCP-Clients vermietet werden.	192.168.1.199
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 IP-Adresse verwenden kann. Vom DHCP-Server bezogene Adresse. 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

UR32L 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.

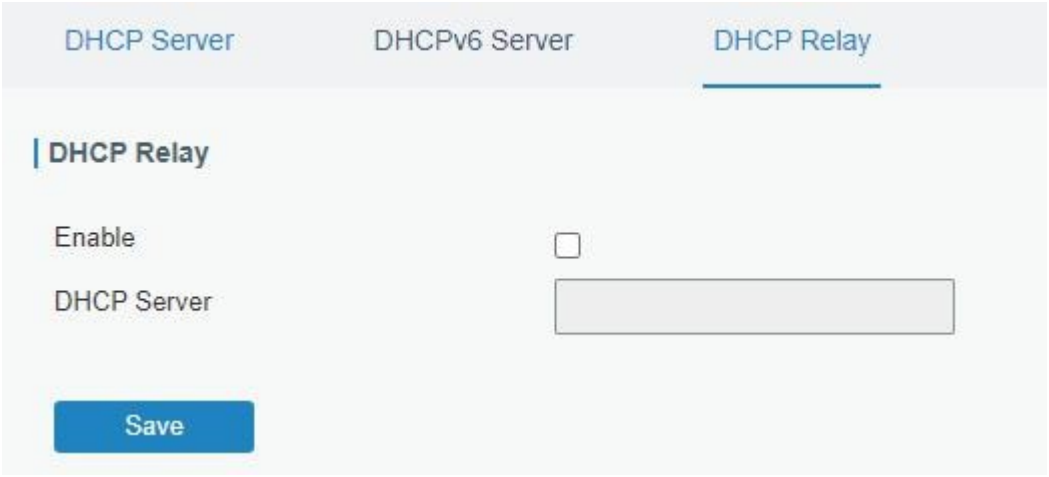


Abbildung 3-2-2-3

DHCP-Relay	
Element	Beschreibung
Aktivieren	DHCP-Relay aktivieren oder deaktivieren.
DHCP-Server	DHCP-Server einrichten, bis zu 10 Server können 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

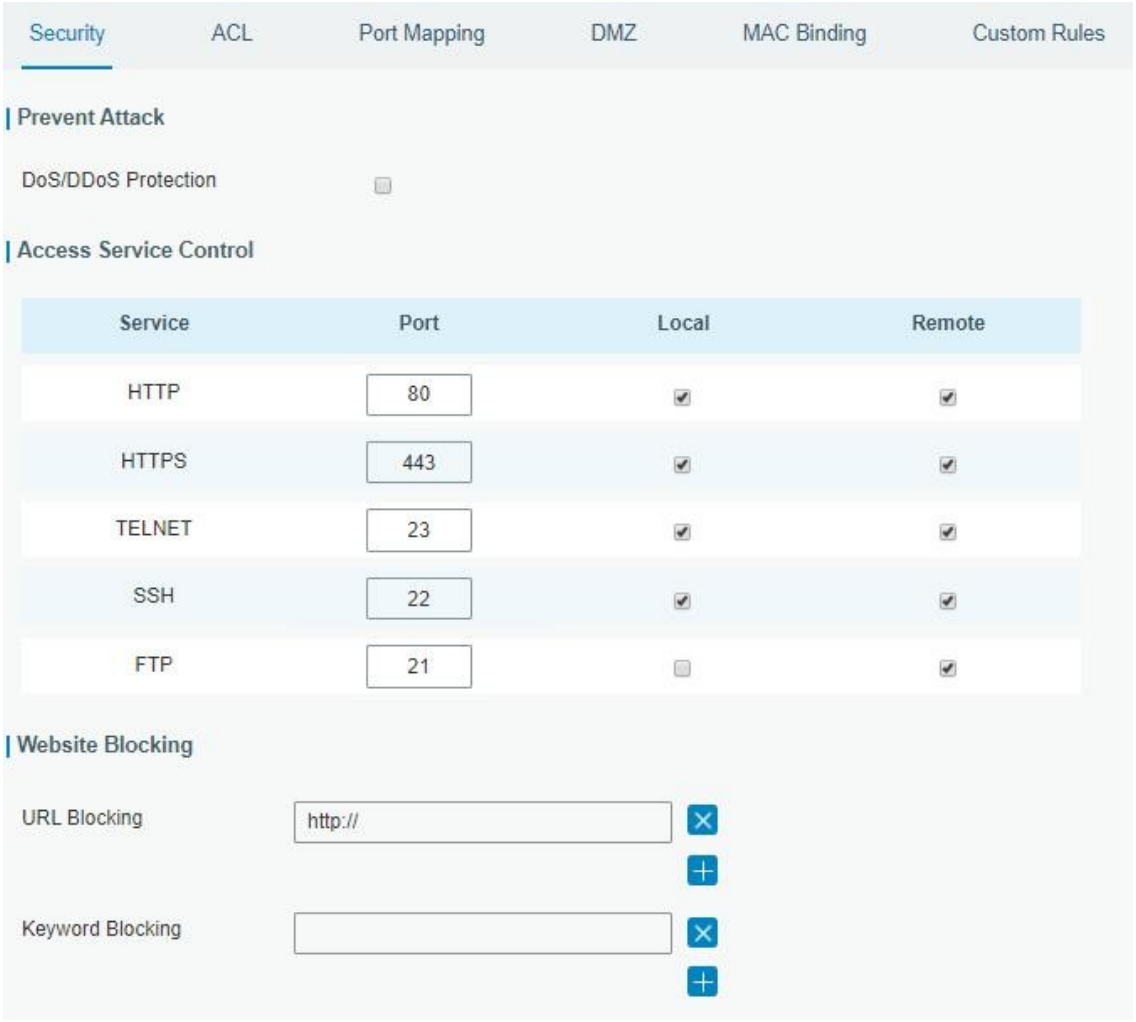


Abbildung 3-2-3-1

Element	Beschreibung	Standard
Angriffe verhindern		
DoS/DDoS-Schutz	Aktivieren/Deaktivieren Sie den Schutz vor DoS/DDoS-Angriffen.	Deaktivieren
Zugriff auf Dienststeuerung		
Port	Portnummer der Dienste festlegen. 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 über HTTPS anmelden, um nach Aktivierung der Option über das Web darauf zuzugreifen und es zu steuern.	443
TELNET	Benutzer können sich lokal und remote beim Gerät anmelden über Telnet, nachdem die Option aktiviert wurde.	23
SSH	Benutzer können sich lokal und remote beim Gerät anmelden.	22

	über SSH, nachdem die Option aktiviert wurde.	
FTP	Benutzer können sich lokal und remote über FTP anmelden, nachdem die Option aktiviert wurde.	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 ACL definierten Regeln für die Datenpaketzuordnung können auch von anderen Funktionen verwendet werden, die eine Unterscheidung des Datenflusses erfordern.

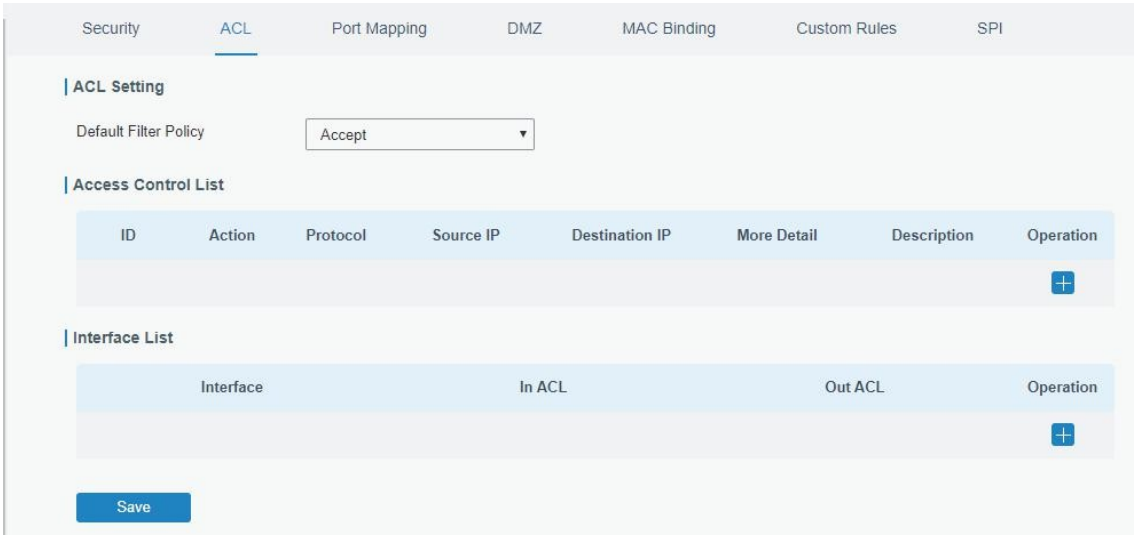


Abbildung 3-2-3-2

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	Platzhaltermaske der Quellnetzwerkadresse.
Ziel-IP	Zielnetzwerkadresse (0.0.0.0 bedeutet alle).
Ziel-Platzhalter 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. einen bestimmten Port, einen Portbereich usw.
Quellport	Legen Sie die Quellportnummer fest. Bereich: 1-65535.
Start-Quellport	Legen Sie die Startnummer des Quellports fest. Bereich: 1-65535.
Endpunkt des Quellports	Legen Sie die Nummer des Endquellports fest. 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	Endziel-Portnummer festlegen. 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

Beispiel für eine zugehörige Konfiguration

Beispiel für eine Zugriffskontrollanwendung

3.2.3.3 Portzuordnung

Port-Mapping ist eine Anwendung der Netzwerkadressübersetzung (NAT), die eine Kommunikationsanfrage von der Kombination aus Adresse und Portnummer zu einer anderen umleitet, während die Pakete ein Netzwerk-Gateway wie einen Router oder eine Firewall durchlaufen.

Klicken Sie auf „ + “, um neue Port-Mapping-Regeln hinzuzufügen.

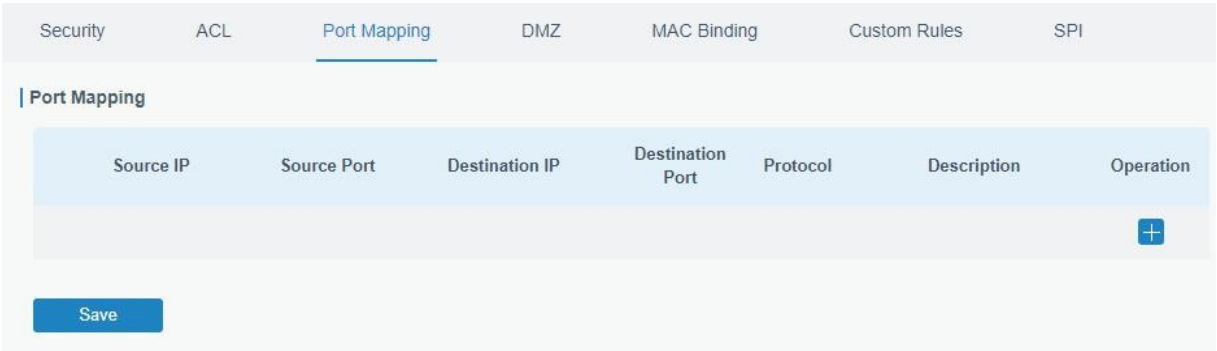


Abbildung 3-2-3-3

Portzuordnung	
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

NAT-Anwendungsbeispiel

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.

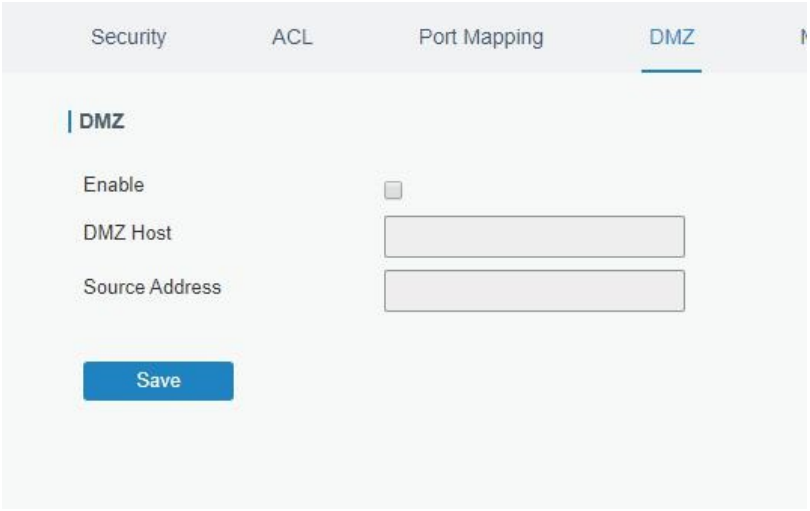


Abbildung 3-2-3-4

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 „beliebige 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.

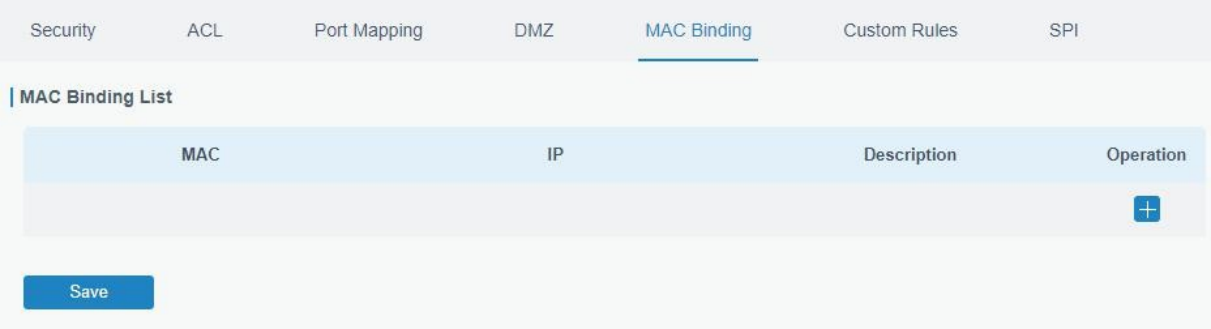


Abbildung 3-2-3-5

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.

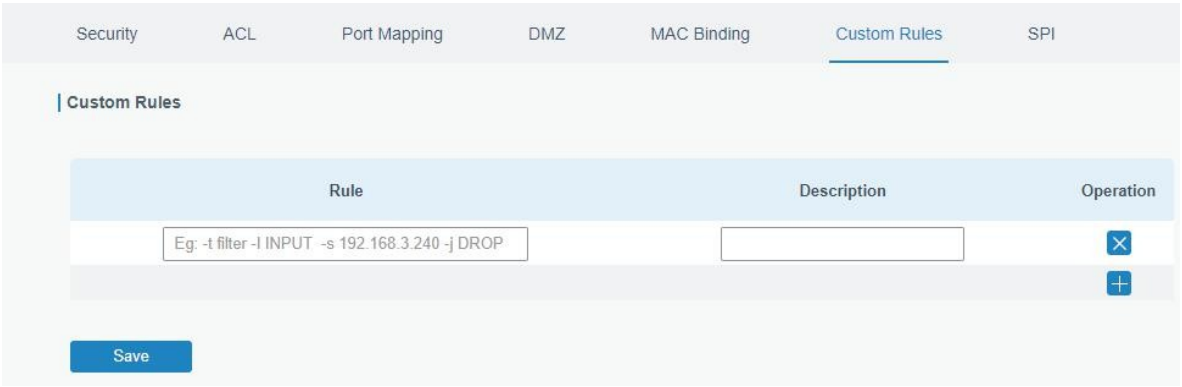


Abbildung 3-2-3-6

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

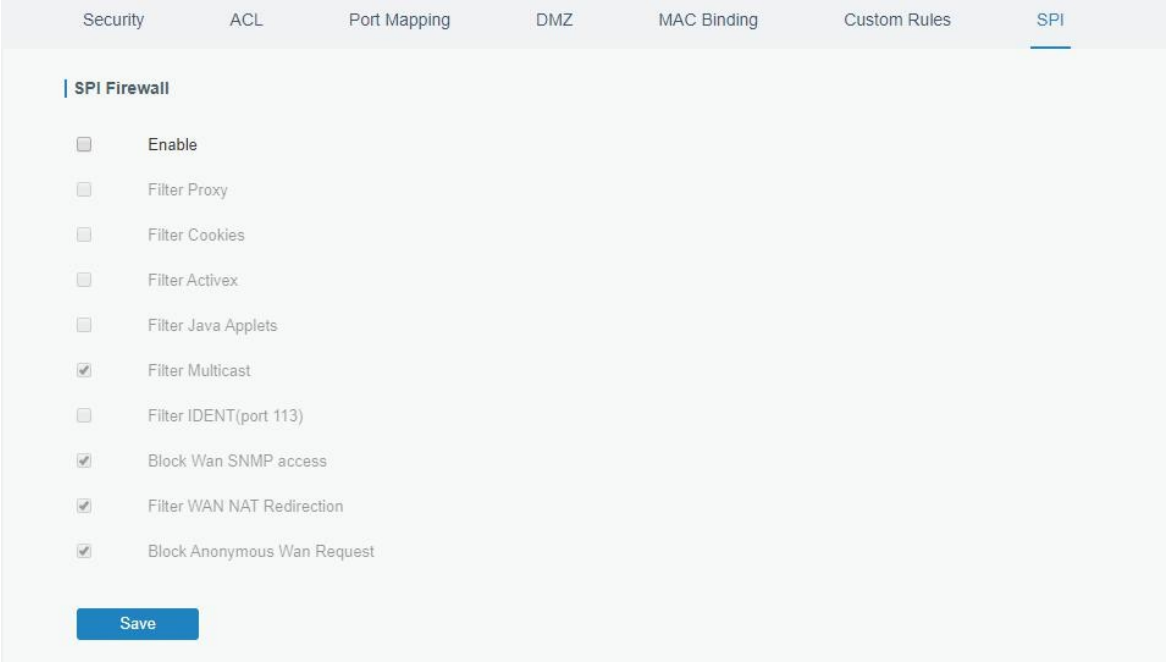


Abbildung 3-2-3-7

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 verfälscht das Cookie. Versucht, die Verwendung von Cookies zu verhindern.
Filter ActiveX	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.
WAN-SNMP-Zugriff blockieren	Blockieren Sie SNMP-Anfragen aus dem WAN.
Filter 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 Port-Umleitung 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.

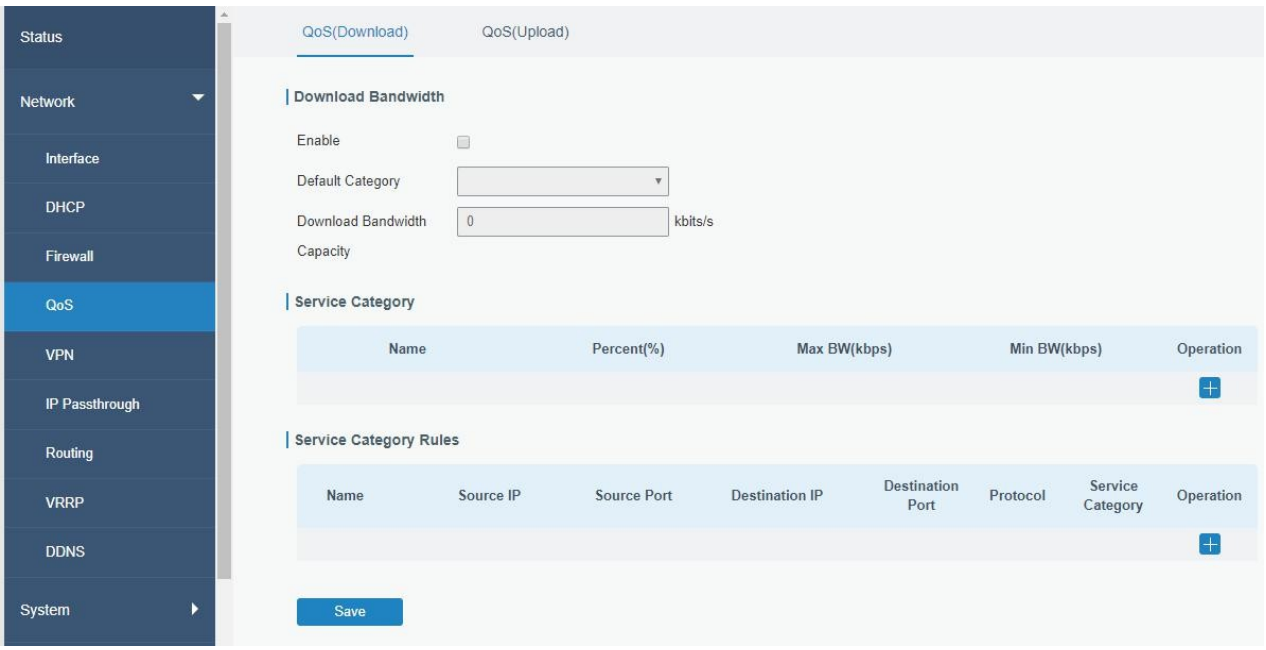


Abbildung 3-2-4-1

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 verbrauchen darf. Der Wert sollte geringer 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” liegen.
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 (leeren Feld bedeutet

	beliebig).
Zielport	Zielport der Flusssteuerung. Bereich: 0-65535 (leer lassen 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 UR32L 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.

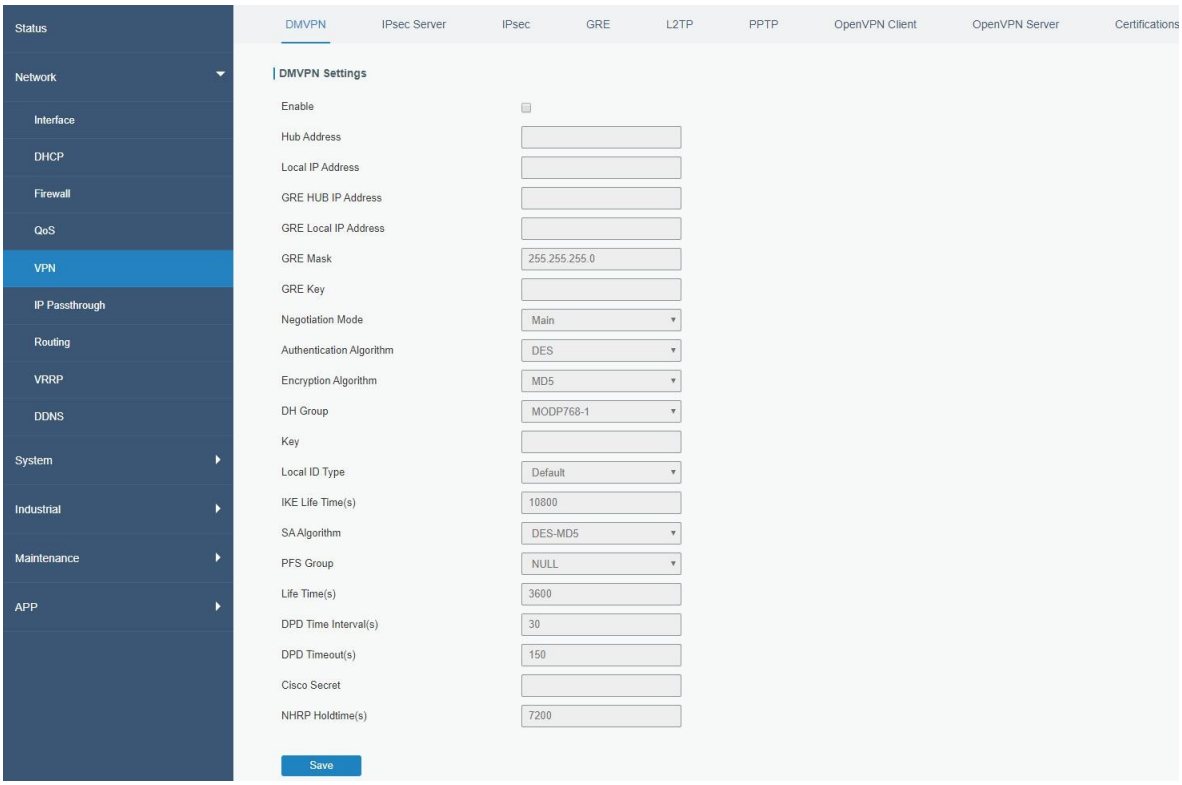


Abbildung 3-2-5-1

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 der 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.

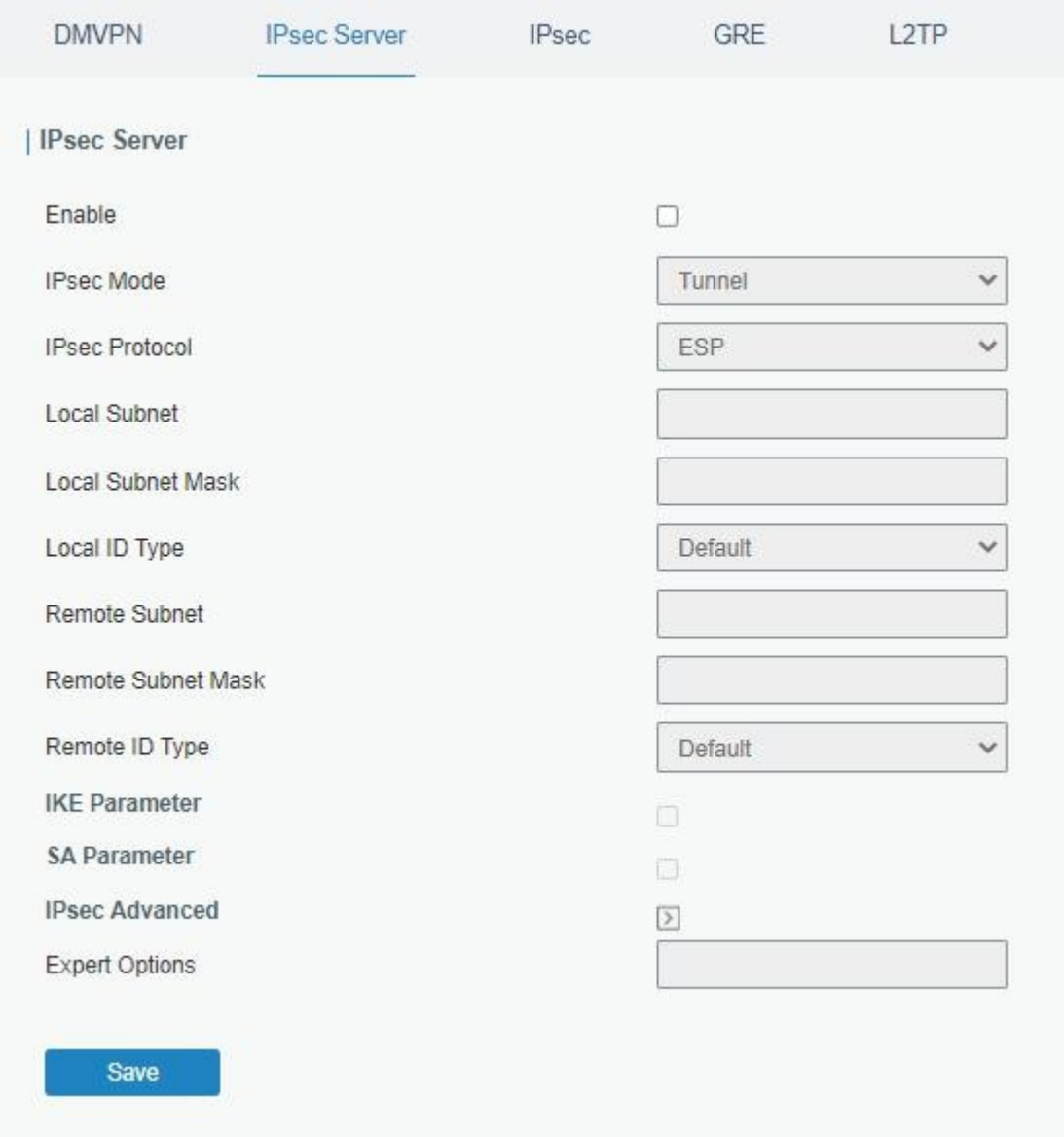


Abbildung 3-2-5-2

IPsec-Server	
Element	Beschreibung
Aktivieren	IPsec-Tunnel aktivieren. Es sind maximal 3 Tunnel zulässig.
IPsec-Modus	Wählen Sie zwischen „Tunnel“ und „Transport“.
IPsec-Protokoll	Wählen Sie zwischen „ESP“ und „AH“.
Lokales Subnetz	Geben Sie die IP-Adresse des lokalen Subnetzes ein, das durch IPsec geschützt ist.
Lokale Subnetz-Netzmaske	Geben Sie die lokale Netzmaske ein, die durch IPsec geschützt wird.
Lokaler ID-Typ	Wählen Sie zwischen „Standard“, „ID“, „FQDN“ und „Benutzer-FQDN“.
Remote-Subnetz	Geben Sie die IP-Adresse des Remote-Subnetzes ein, das durch IPsec geschützt wird.
Remote-Subnetzmaske	Geben Sie die Remote-Netzmaske ein, die durch IPsec geschützt wird.
Remote-ID-Typ	Wählen Sie zwischen „Standard“, „ID“, „FQDN“ und „Benutzer-FQDN“.

Tabelle 3-2-5-2 IPsec-Parameter

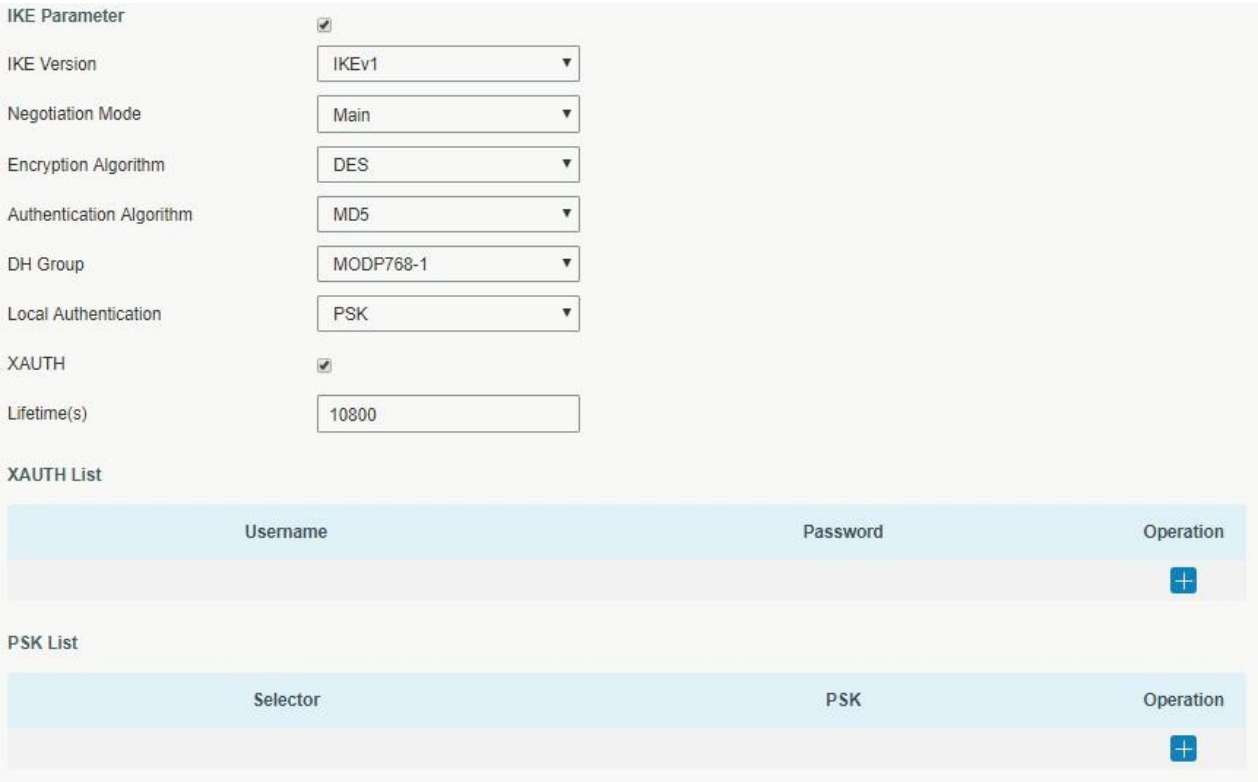


Abbildung 3-2-5-3

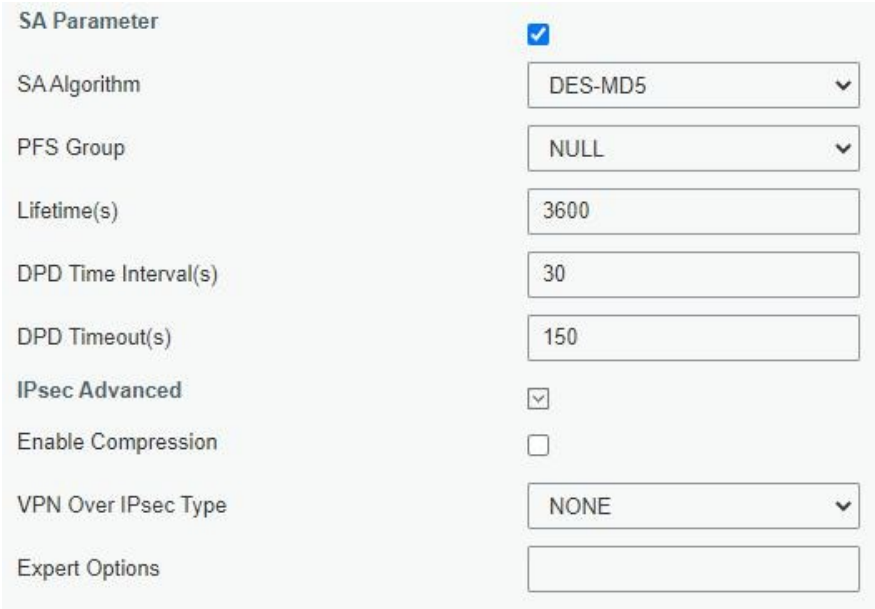


Abbildung 3-2-5-4

IKE-Parameter	
Element	Beschreibung
IKE-Version	Wählen Sie zwischen „IKEv1" und „IKEv2".
Verhandlungsmodus	Wählen Sie zwischen „Main" und „Aggressive".
Verschlüsselungsalgorithmus	Wählen Sie zwischen „DES", „3DES", „AES128", „AES192" und „AES256".
Authentifizierungsalgorithmus	Wählen Sie zwischen „MD5" und „SHA1".
DH-Gruppe	Wählen Sie zwischen „MODP768_1", „MODP1024_2" und „MODP1536_5".
Lokale Authentifizierung	Wählen Sie zwischen „PSK" und „CA".

XAUTH	Geben Sie den XAUTH-Benutzernamen und das Passwort ein, nachdem XAUTH aktiviert wurde.
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 Passwort ein, das für die xauth-Authentifizierung verwendet wird.
PSK-Liste	
Selektor	Geben Sie die entsprechende Identifikationsnummer für die PSK-Authentifizierung ein.
PSK	Geben Sie den vorab geteilten Schlüssel ein.
SA-Parameter	
SA-Algorithmus	Wählen Sie aus „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)	Legen Sie das DPD-Intervall fest, um zu erkennen, ob die Gegenstelle ausgefallen ist.
DPD-Zeitüberschreitung(en)	DPD-Zeitlimit festlegen. Bereich: 10-3600.
IPsec erweitert	
Komprimierung aktivieren	Der Kopf des IP-Pakets wird nach der Aktivierung komprimiert.
VPN über IPsec-Typ	Wählen Sie zwischen „NONE”, „GRE” und „L2TP”, um die VPN-über-IPsec-Funktion zu aktivieren. .
Benutzer kann in diesem Feld einige andere Initialisierungszeichenfolgen eingeben und die Zeichenfolgen mit „;“ trennen. Wenn	Der Benutzer kann in diesem Feld einige andere Initialisierungszeichenfolgen eingeben und die Zeichenfolgen mit „;“ trennen. Wenn beispielsweise weitere lokale oder entfernte Subnetze hinzugefügt werden müssen, können Benutzer hier Inhalte hinzufügen.

Tabelle 3-2-5-3 IPsec-Serverparameter

3.2.5.3 IPSec

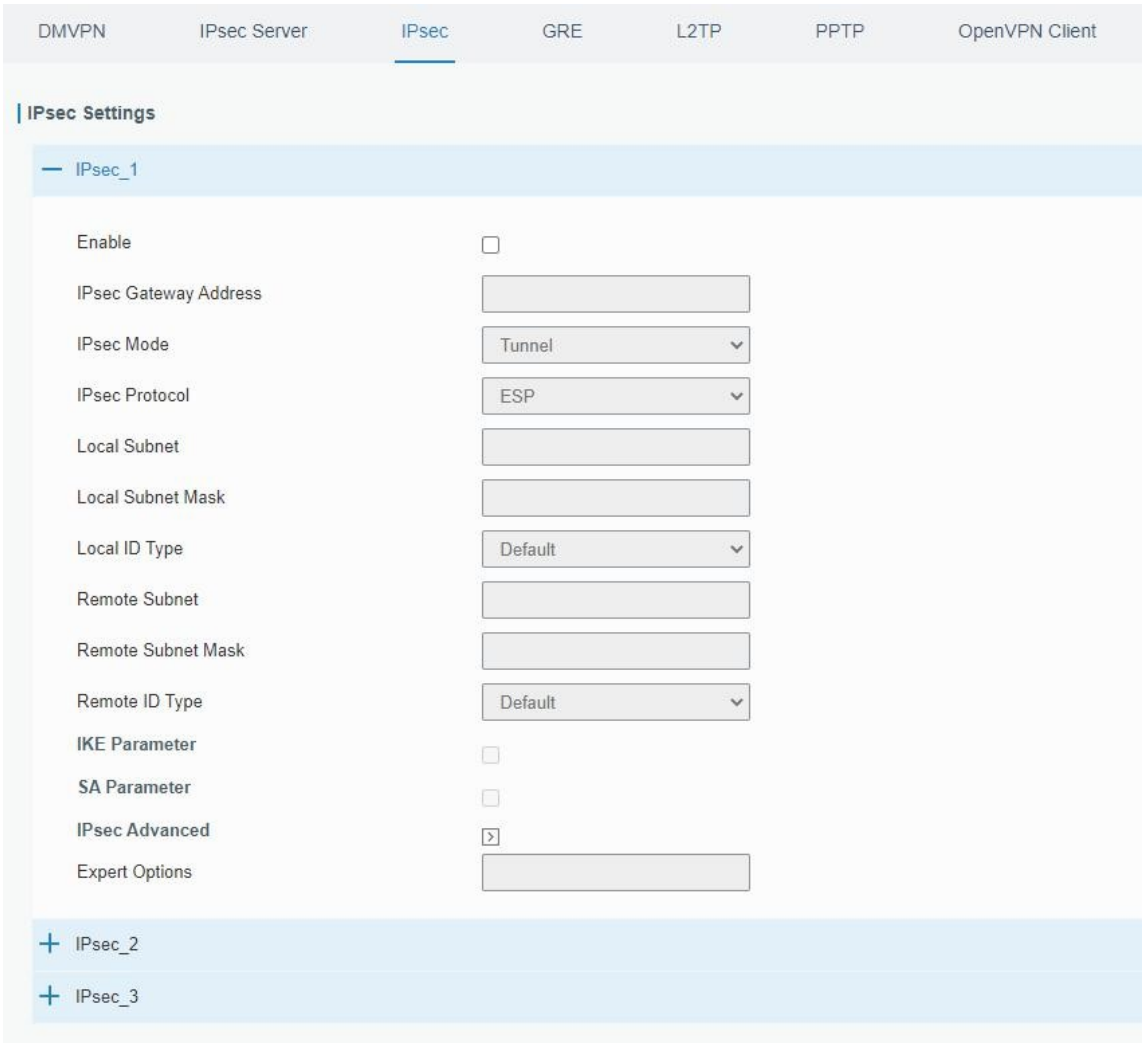


Abbildung 3-2-5-5

IPsec	
Element	Beschreibung
Aktivieren	IPsec-Tunnel aktivieren. Es sind maximal 3 Tunnel zulässig.
IPsec-Gateway-Adresse	Geben Sie die IP-Adresse oder den Domänennamen des Remote-IPsec-Servers ein. .
IPsec-Modus	Wählen Sie zwischen „Tunnel“ und „Transport“.
IPsec-Protokoll	Wählen Sie zwischen „ESP“ und „AH“.
Lokales Subnetz	Geben Sie die IP-Adresse des lokalen Subnetzes ein, das durch IPsec geschützt wird.
Lokale Subnetz-Netzmaske	Geben Sie die lokale Netzmaske ein, die durch IPsec geschützt wird.
Lokaler ID-Typ	Wählen Sie zwischen „Standard“, „ID“, „FQDN“ und „Benutzer-FQDN“.
Remote-Subnetz	Geben Sie die IP-Adresse des Remote-Subnetzes ein, das durch IPsec geschützt wird.
Remote-Subnetzmaske	Geben Sie die Remote-Netzmaske ein, die durch IPsec geschützt wird.
Remote-ID-Typ	Wählen Sie zwischen „Standard“, „ID“, „FQDN“ und „Benutzer-FQDN“.

Tabelle 3-2-5-4 IPsec-Parameter

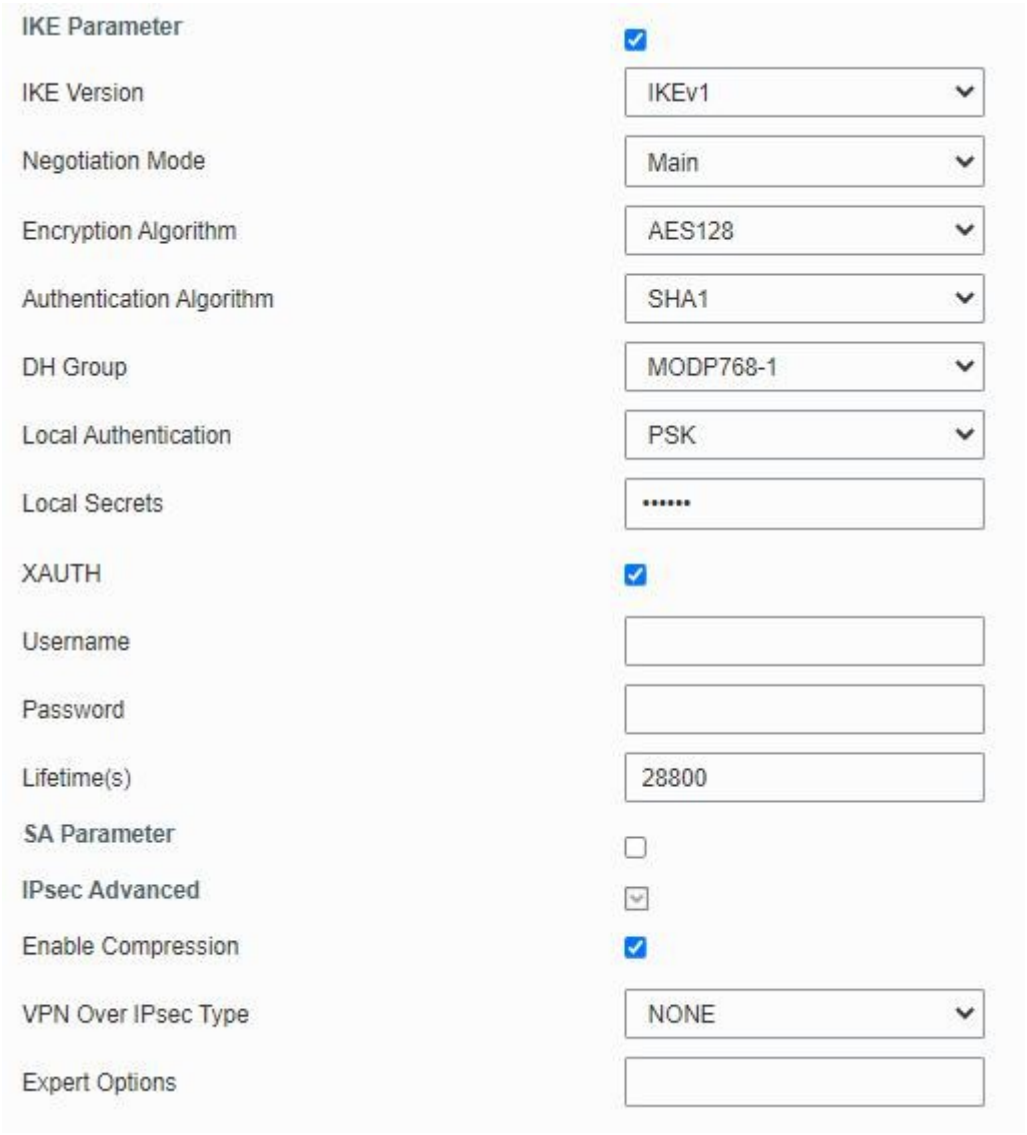


Abbildung 3-2-5-6

IKE-Parameter	
Element	Beschreibung
IKE-Version	Wählen Sie zwischen „IKEv1" und „IKEv2".
Verhandlungsmodus	Wählen Sie zwischen „Main" und „Aggressive".
Verschlüsselungsalgorithmus	Wählen Sie zwischen „DES", „3DES", „AES128", „AES192" und „AES256".
Authentifizierungsalgorithmus	Wählen Sie zwischen „MD5" und „SHA1"
DH-Gruppe	Wählen Sie zwischen „MODP768_1", „MODP1024_2" und „MODP1536_5".
Lokale Authentifizierung	Wählen Sie zwischen „PSK" und „CA".
Lokale Geheimnisse	Geben Sie den vorab geteilten Schlüssel ein.
XAUTH	Geben Sie den XAUTH-Benutzernamen und das Passwort ein, nachdem XAUTH aktiviert wurde.
Lebensdauer (s)	Legen Sie die Lebensdauer in der IKE-Verhandlung fest. Bereich: 60-86400.
SA-Parameter	
SA-Algorithmus	Wählen Sie aus „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(en)	Legen Sie die DPD-Intervallzeit fest, um zu erkennen, ob die Gegenstelle ausgefallen ist.
DPD-Zeitüberschreitung(en)	Legen Sie das DPD-Zeitlimit fest. Bereich: 10-3600.
IPsec erweitert	
Komprimierung aktivieren	Der Kopf des IP-Pakets wird nach der Aktivierung komprimiert.
VPN über IPsec-Typ	Wählen Sie zwischen „NONE”, „GRE” und „L2TP”, um die VPN-über-IPsec-Funktion zu aktivieren. .
Expertenoption	Der Benutzer kann in diesem Feld einige andere Initialisierungszeichenfolgen eingeben und die Zeichenfolgen mit „;“ trennen. Wenn beispielsweise weitere lokale oder Remote-Subnetze hinzugefügt werden müssen Subnetze hinzugefügt werden müssen, können Benutzer hier Inhalte hinzufügen.

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.

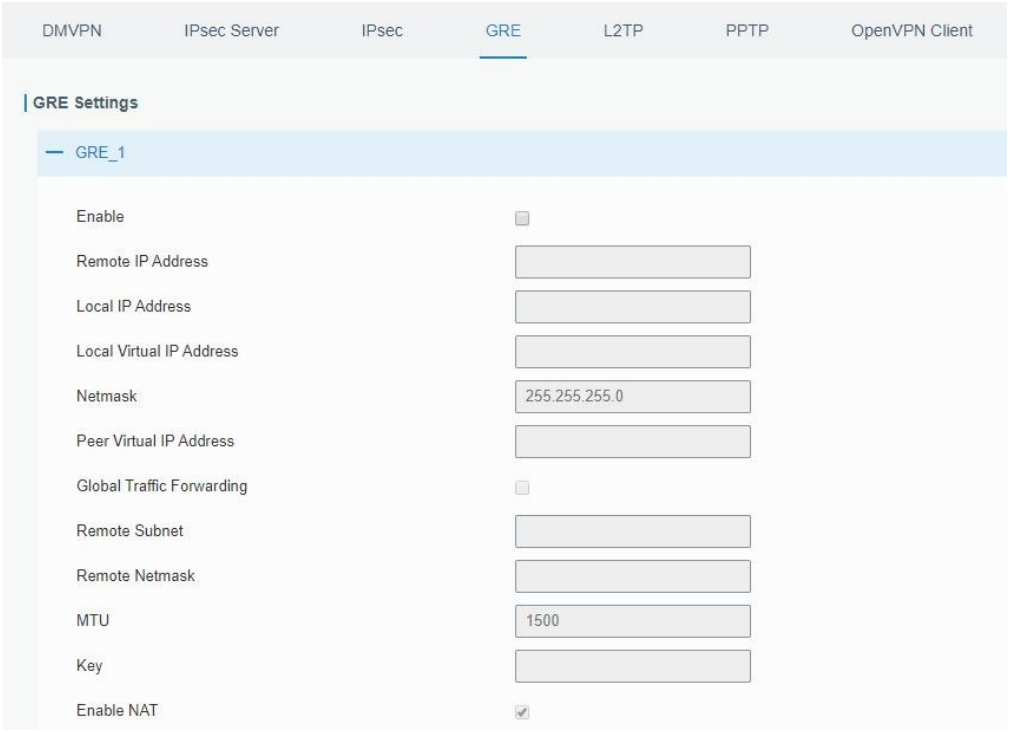


Abbildung 3-2-5-7

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.

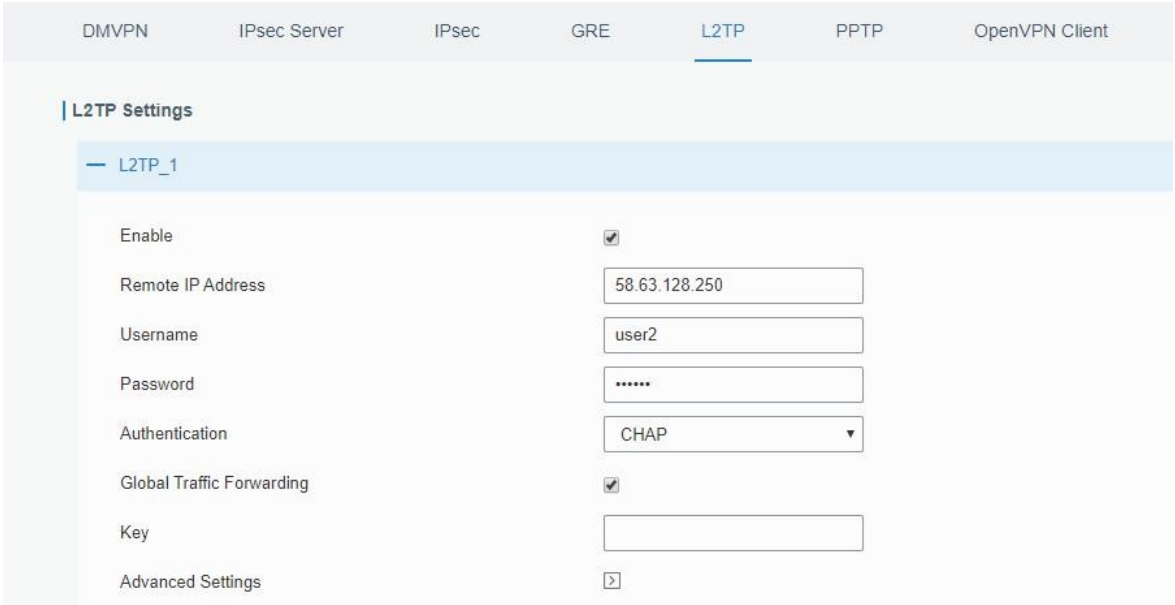


Abbildung 3-2-5-8

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.

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-Netzmaske ein, die L2TP schützt.
Schlüssel	Geben Sie das Passwort für den L2TP-Tunnel ein.

Tabelle 3-2-5-7 L2TP-Parameter

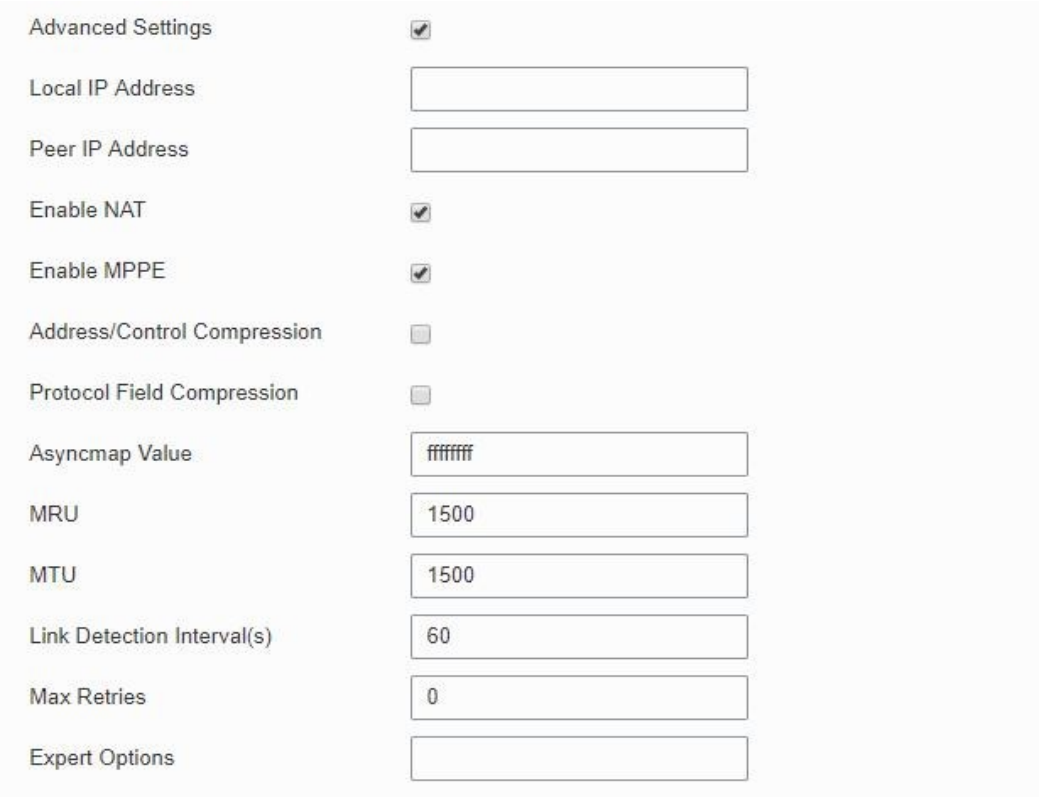


Abbildung 3-2-5-9

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 des PPP-Protokolls. 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.
Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl von Wiederholungsversuchen fest, um den L2TP-Verbindungsfehler zu erkennen Verbindungsfehler zu erkennen. Bereich: 0-10.
Expertenoptionen	Der Benutzer kann in diesem Feld einige andere PPP-Initialisierungszeichenfolgen eingeben Feld eingeben und die Zeichenfolgen durch Leerzeichen trennen.

Tabelle 3-2-5-8 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.

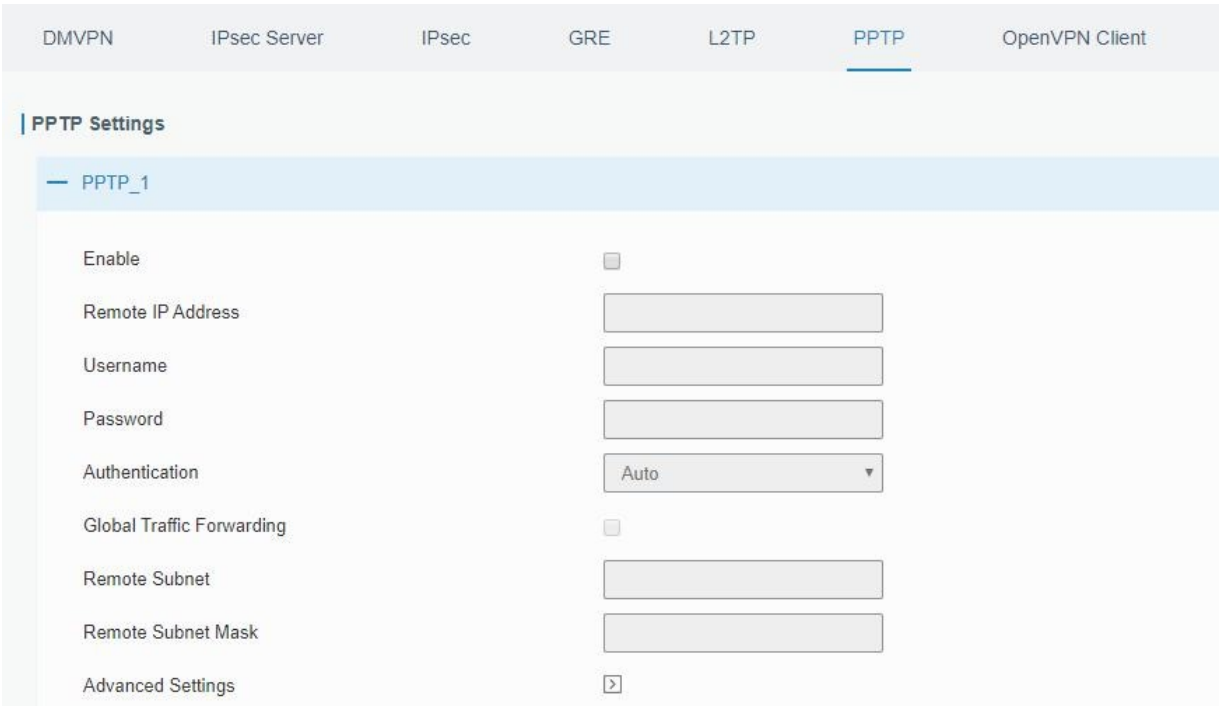


Abbildung 3-2-5-10

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 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	Der gesamte Datenverkehr wird über den PPTP-Tunnel gesendet, sobald

Weiterleitung	aktiviert.
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

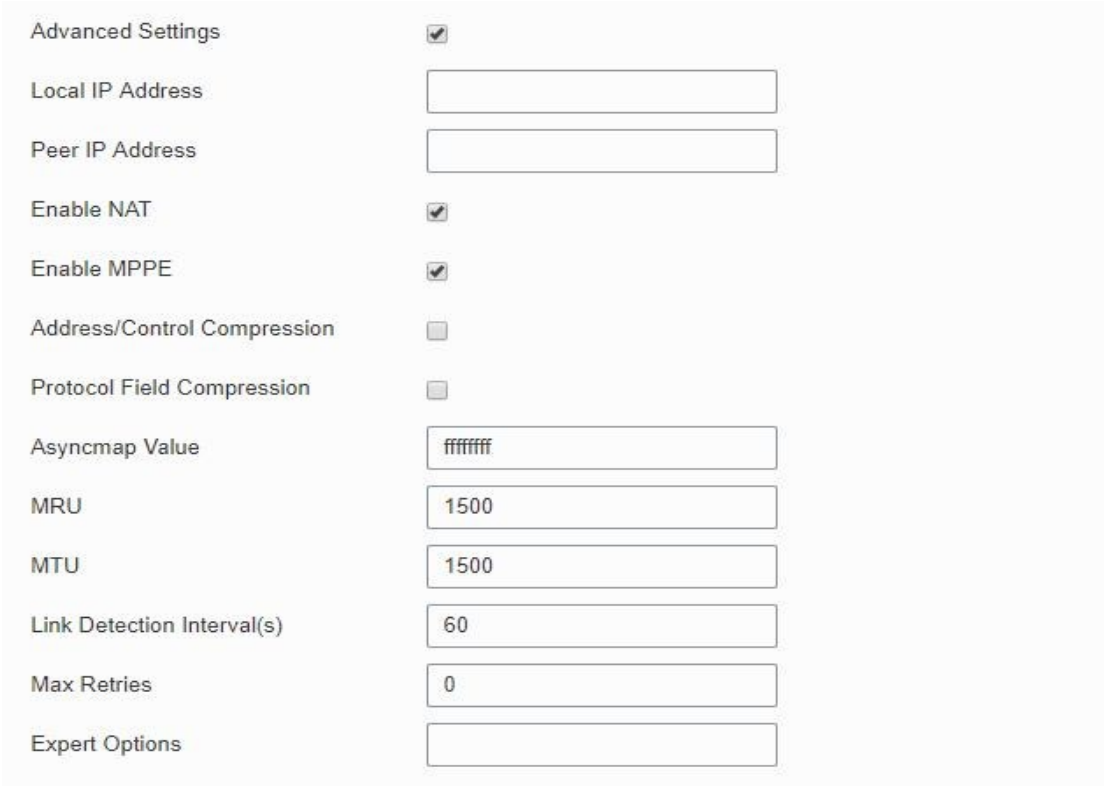


Abbildung 3-2-5-11

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 PPP-Protokoll-Initialisierungszeichenfolgen. Der Benutzer kann Der Standardwert. 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 einige andere PPP-Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Leerzeichen trennen.

Tabelle 3-2-5-10 PPTP-Parameter

Beispiel für eine entsprechende Konfiguration

PPTP-Anwendungsbeispiel

3.2.5.7 OpenVPN-Client

OpenVPN ist ein Open-Source-Produkt für virtuelle private Netzwerke (VPN), das ein vereinfachtes Sicherheitsframework, ein modulares Netzwerkdesign und plattformübergreifende Portabilität bietet.

Zu den Vorteilen von OpenVPN gehören:

- Sicherheitsvorkehrungen, die sowohl gegen aktive als auch passive Angriffe wirken.
- Kompatibilität mit allen gängigen Betriebssystemen.
- Hohe Geschwindigkeit (in der Regel 1,4 Megabyte pro Sekunde).
- Möglichkeit, mehrere Server so zu konfigurieren, dass sie zahlreiche Verbindungen gleichzeitig verarbeiten können.
- Alle Verschlüsselungs- und Authentifizierungsfunktionen der OpenSSL-Bibliothek.
- Erweitertes Bandbreitenmanagement.
- Eine Vielzahl von Tunneling-Optionen.
- Kompatibilität mit Smartcards, die die Windows Crypt-Anwendungsprogrammierschnittstelle (API) unterstützen.

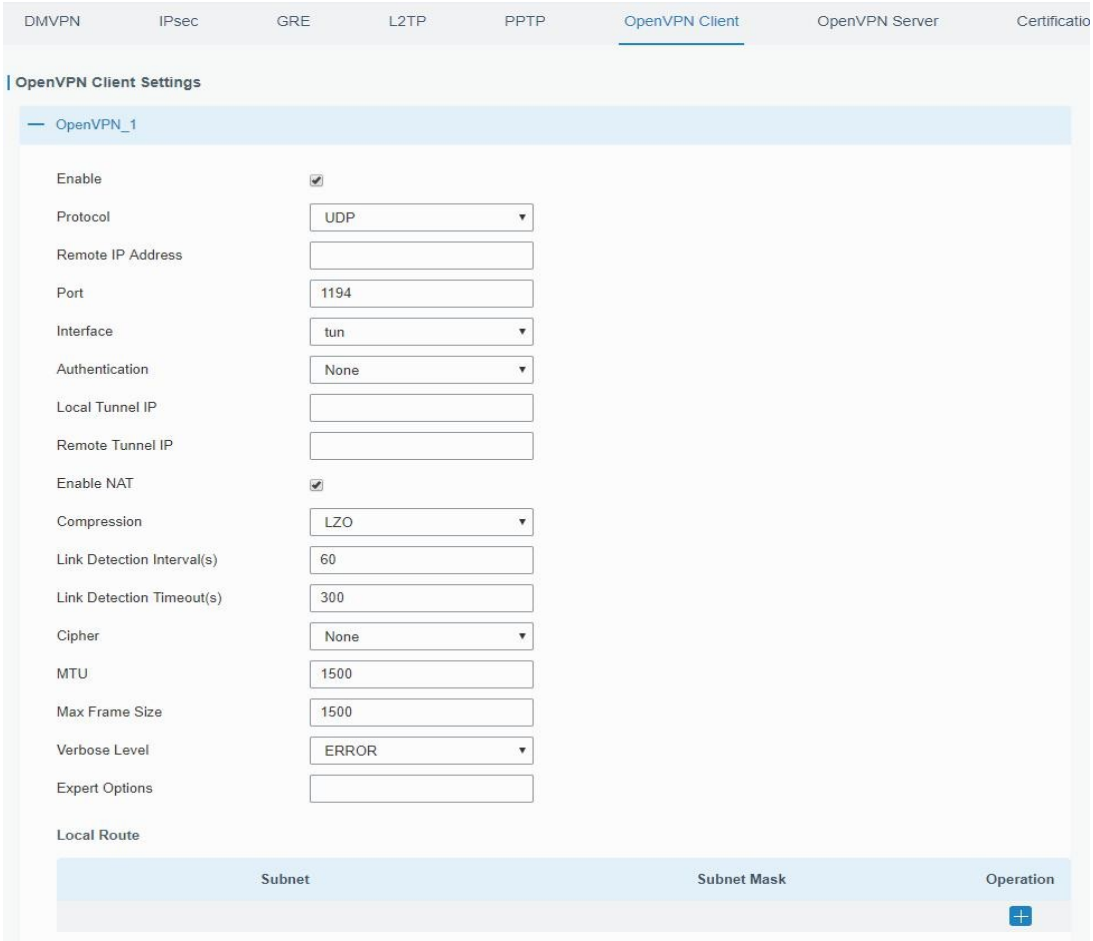


Abbildung 3-2-5-12

OpenVPN-Client	
Element	Beschreibung
Aktivieren	OpenVPN-Client aktivieren. Es sind maximal 3 Tunnel zulässig.
Protokoll	Wählen Sie zwischen „UDP" und „TCP".
Remote-IP-Adresse	Geben Sie die IP-Adresse oder den Domänennamen des Remote-OpenVPN-Servers ein.
Port	Geben Sie die Portnummer des Remote-OpenVPN-Servers ein. Bereich: 1–65535
Schnittstelle	Wählen Sie zwischen „tun" und „tap".
Authentifizierung	Wählen Sie zwischen „Keine", „Vorab geteilt", „Benutzername/Passwort", „X.509-Zertifikat" und „X.509-Zertifikat+Benutzer".
Lokale Tunnel-IP	Legen Sie die lokale Tunneladresse fest.
Remote-Tunnel-IP	Geben Sie die Remote-Tunneladresse ein.
Globale Datenweiterleitung	Der gesamte Datenverkehr wird über den OpenVPN-Tunnel gesendet, wenn diese Funktion aktiviert ist.
TLS-Authentifizierung aktivieren	Aktivieren Sie diese Option, um die TLS-Authentifizierung zu aktivieren.
Benutzername	Geben Sie den vom OpenVPN-Server bereitgestellten Benutzernamen ein.
Passwort	Geben Sie das vom OpenVPN-Server bereitgestellte Passwort ein.
NAT aktivieren	NAT-Traversal-Funktion aktivieren.
Komprimierung	Wählen Sie LZO, um Daten zu komprimieren.
Link-Erkennungsintervall (s)	Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Bereich: 10–1800
Zeitlimit für Verbindungserkennung (s)	Legen Sie das Zeitlimit für die Verbindungserkennung fest. OpenVPN wird nach Ablauf des Zeitlimits wiederhergestellt. Zeitüberschreitung wiederhergestellt. Bereich: 60–3600.
Verschlüsselung	Wählen Sie zwischen „NONE", „BF-CBC", „DE-CBC", „DES-EDE3-CBC", „AES-128-CBC", „AES-192-CBC" und „AES-256-CBC".
MTU	Geben Sie die maximale Übertragungseinheit ein. Bereich: 128–1500.
Maximale Frame-Größe	Legen Sie die maximale Rahmengröße fest. Bereich: 128–1500.
Ausführlichkeitsstufe	Wählen Sie zwischen „ERROR", „WARING", „NOTICE" und „DEBUG".
Expertenoptionen	Der Benutzer kann in diesem Feld einige andere PPP-Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Leerzeichen trennen.
Lokale Route	
Subnetz	Legen Sie die IP-Adresse der lokalen Route fest.
Subnetzmaske	Legen Sie die Netzmaske der lokalen Route fest.

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

3.2.5.8 OpenVPN-Server

Der UR32L unterstützt den OpenVPN-Server, um sichere Punkt-zu-Punkt- oder Standort-zu-Standort-Verbindungen in gerouteten oder gebrückten Konfigurationen und Fernzugriffsfunktionen zu erstellen.

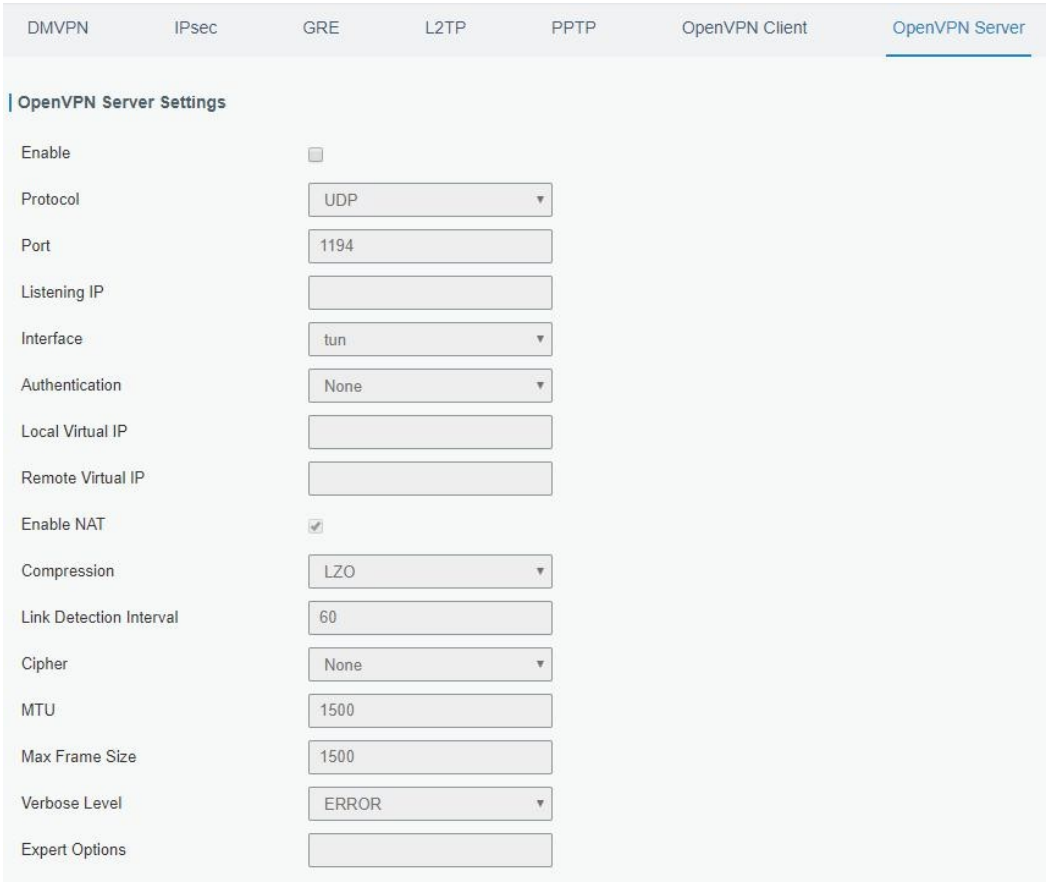


Abbildung 3-2-5-13

Abbildung 3-2-5-14

OpenVPN-Server	
Artikel	Beschreibung
Aktivieren	OpenVPN-Server aktivieren/deaktivieren.
Protokoll	Wählen Sie zwischen TCP und UDP.
Port	Geben Sie die Nummer des Listening-Ports ein. Bereich: 1-65535.
IP-Adresse	Geben Sie die WAN-IP-Adresse oder die LAN-IP-Adresse ein. Wenn Sie das Feld leer lassen, werden alle aktiven WAN-IP- und LAN-IP-Adressen.
Schnittstelle	Wählen Sie zwischen „tun" und „tap".
Authentifizierung	Wählen Sie zwischen „Keine", „Vorab geteilt", „Benutzername/Passwort", „X.509-Zertifikat" und „X.509-Zertifikat + Benutzer".
Lokale virtuelle IP	Die lokale Tunneladresse des OpenVPN-Tunnels.
Virtuelle Remote-IP	Die Remote-Tunneladresse des OpenVPN-Tunnels.

Client-Subnetz	Lokale Subnetz-IP-Adresse des OpenVPN-Clients.
Client-Netzmaske	Lokale Netzmaske des OpenVPN-Clients.
Neuverhandlung Intervall(e)	Intervall für die Neuverhandlung festlegen. Bereich: 0-86400.
Maximale Anzahl Clients	Maximale Anzahl von OpenVPN-Clients. Bereich: 1-128.
CRL aktivieren	CRL aktivieren
Client-zu-Client aktivieren	Zugriff zwischen verschiedenen OpenVPN-Clients zulassen.
Dup-Client aktivieren	Erlauben Sie mehreren Benutzern, dieselbe Zertifizierung zu verwenden.
NAT aktivieren	Aktivieren Sie diese Option, um die NAT-Traversal-Funktion zu aktivieren.
Komprimierung	Wählen Sie „LZO“, um Daten zu komprimieren.
Link-Erkennungsintervall	Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Bereich: 10-1800.
Verschlüsselung	Wählen Sie zwischen „KEINE“, „BF-CBC“, „DES-CBC“, „DES-EDE3-CBC“, „AES-128-CBC“, „AES-192-CBC“ und „AES-256-CBC“.
MTU	Geben Sie die maximale Übertragungseinheit ein. Bereich: 64-1500.
Maximale Frame-Größe	Legen Sie die maximale Rahmengröße fest. Bereich: 64-1500.
Ausführlichkeitsstufe	Wählen Sie zwischen „ERROR“, „WARING“, „NOTICE“ und „DEBUG“.
Expertenoptionen	Der Benutzer kann in diesem Feld einige andere PPP-Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Leerzeichen trennen.
Lokale Route	
Subnetz	Die tatsächliche lokale IP-Adresse des OpenVPN-Clients.
Netzmaske	Die tatsächliche lokale Netzmaske des OpenVPN-Clients.
Konto	
Benutzername und Passwort	Legen Sie Benutzername und Passwort für den OpenVPN-Client fest.

Tabelle 3-2-5-12 OpenVPN-Serverparameter

3.2.5.9 Zertifikate

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

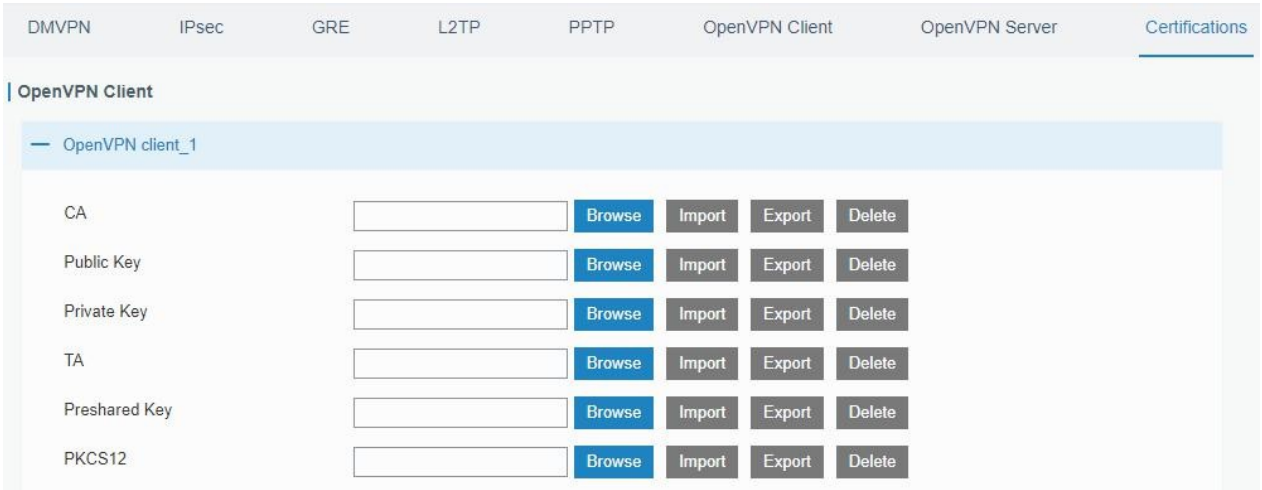


Abbildung 3-2-5-15

OpenVPN-Client	
Element	Beschreibung
CA	CA-Zertifikatsdatei importieren/exportieren.
Öffentlicher Schlüssel	Öffentliche Schlüsseldatei importieren/exportieren.
Privater Schlüssel	Importieren/Exportieren der Datei mit dem privaten Schlüssel.
TA	TA-Schlüsseldatei importieren/exportieren.
Vorab geteilter Schlüssel	Importieren/Exportieren einer statischen Schlüsseldatei.
PKCS12	PKCS12-Zertifikatsdatei importieren/exportieren.

Tabelle 3-2-5-13 OpenVPN-Client-Zertifizierungsparameter

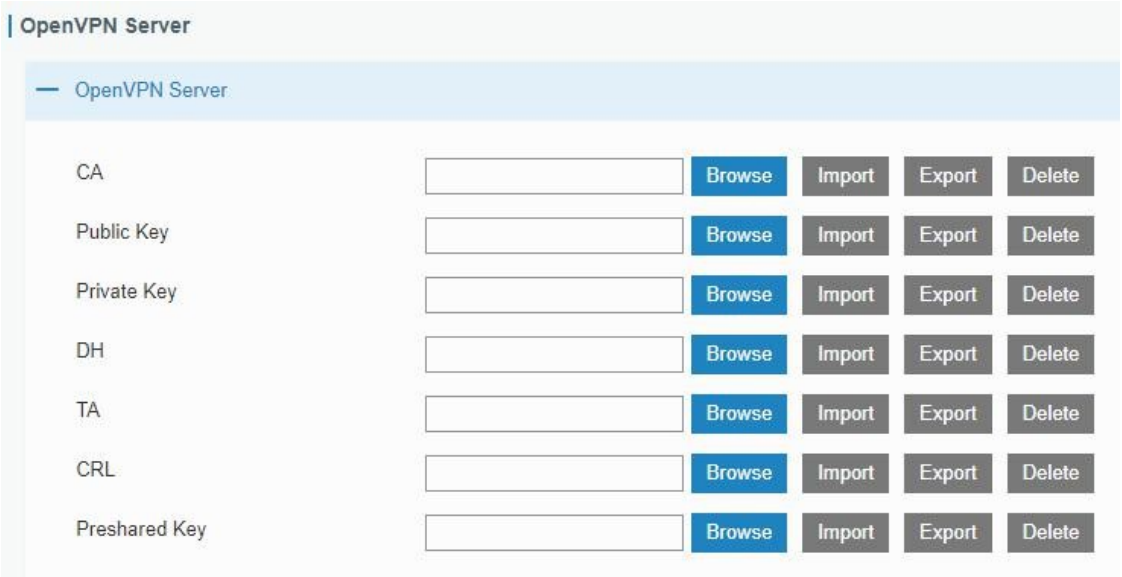


Abbildung 3-2-5-16

OpenVPN-Server	
Element	Beschreibung
CA	CA-Zertifikatsdatei importieren/exportieren.
Öffentlicher Schlüssel	Öffentliche Schlüsseldatei importieren/exportieren.
Privater Schlüssel	Importieren/Exportieren der privaten Schlüsseldatei.
DH	DH-Schlüsseldatei importieren/exportieren.
TA	Importieren/Exportieren einer TA-Schlüsseldatei.
CRL	CRL importieren/exportieren.
Vorab vereinbarter Schlüssel	Importieren/Exportieren einer statischen Schlüsseldatei.

Tabelle 3-2-5-14 OpenVPN-Serverparameter

Abbildung 3-2-5-17

IPsec	
Element	Beschreibung
CA	CA-Zertifikat importieren/exportieren.
Client-Schlüssel	Client-Schlüssel importieren/exportieren.
Serverschlüssel	Importieren/Exportieren Sie den Serverschlüssel.
Privater Schlüssel	Privaten Schlüssel importieren/exportieren.
CRL	Importieren/Exportieren der Zertifikatswiederherstellungsliste.

Tabelle 3-2-5-15 IPsec-Parameter

Abbildung 3-2-5-18

IPsec-Server	
Element	Beschreibung
CA	CA-Zertifikat importieren/exportieren.
Lokales Zertifikat	Lokale Zertifikatsdatei importieren/exportieren.
Privater Schlüssel	Privaten Schlüssel importieren/exportieren.
CRL	Importieren/Exportieren der Zertifikatswiederherstellungsliste.

Tabelle 3-2-5-16 IPsec-Serverparameter

3.2.6 IP-Passthrough

Im IP-Passthrough-Modus wird die vom Internetanbieter zugewiesene IP-Adresse an ein einzelnes LAN-Clientgerät weitergegeben, das mit dem Router verbunden ist.

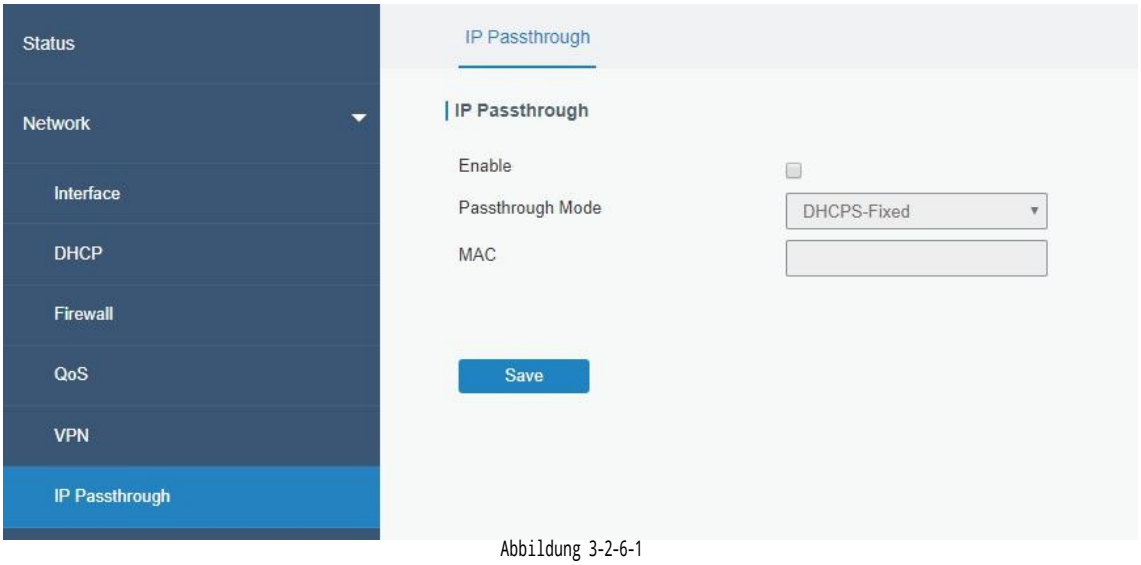


Abbildung 3-2-6-1

IP-Passthrough	
Element	Beschreibung
Aktivieren	IP-Passthrough aktivieren oder deaktivieren.
Passthrough-Modus	Wählen Sie den Passthrough-Modus aus „DHCPS-Fixed" und „DHCPS-Dynamic".
MAC	Legen Sie die MAC-Adresse fest.

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 bezogen. Nach der Einrichtung des statischen Routings wird das Paket für das angegebene Ziel an den vom Benutzer festgelegten Pfad weitergeleitet.

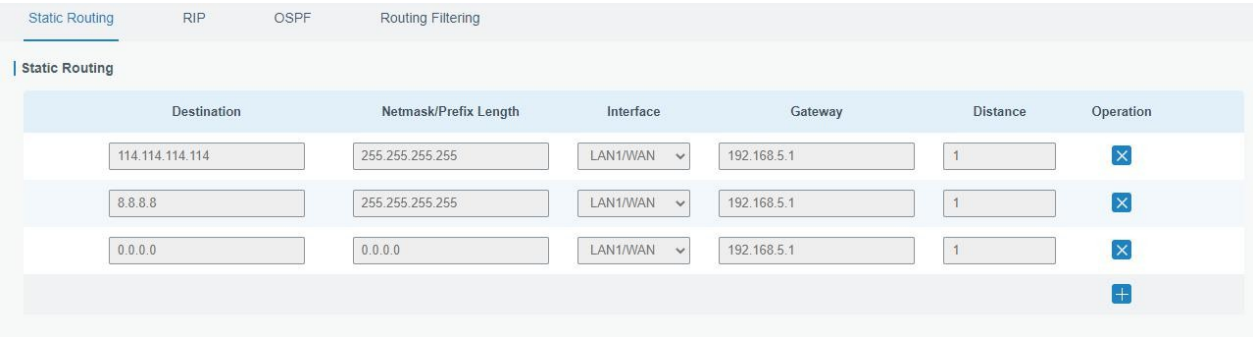


Abbildung 3-2-7-1

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.
Entfernung	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 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.

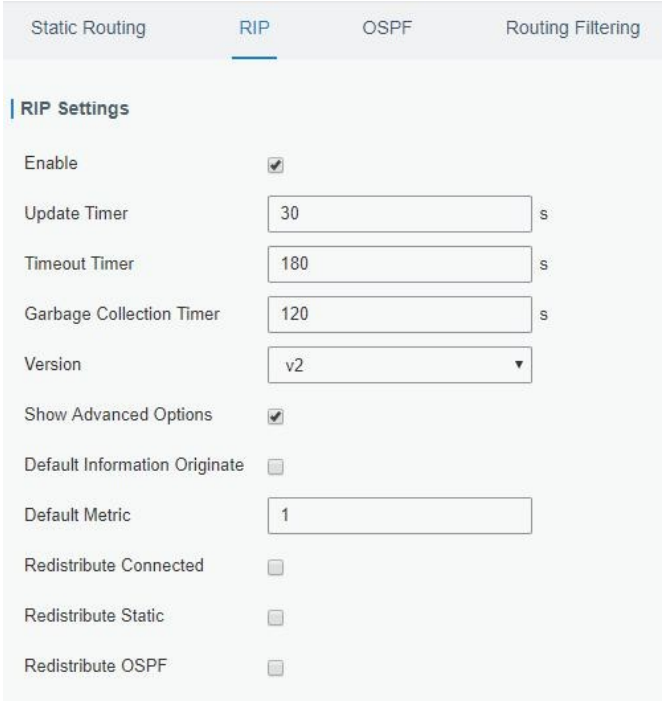


Abbildung 3-2-7-2

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.
Zeitüberschreitungstimer	Legt die Routing-Verfallszeit fest. Wenn innerhalb der Verfallszeit kein Aktualisierungspaket für ein Routing empfangen wird, wird die Routing-Kosten 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 „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

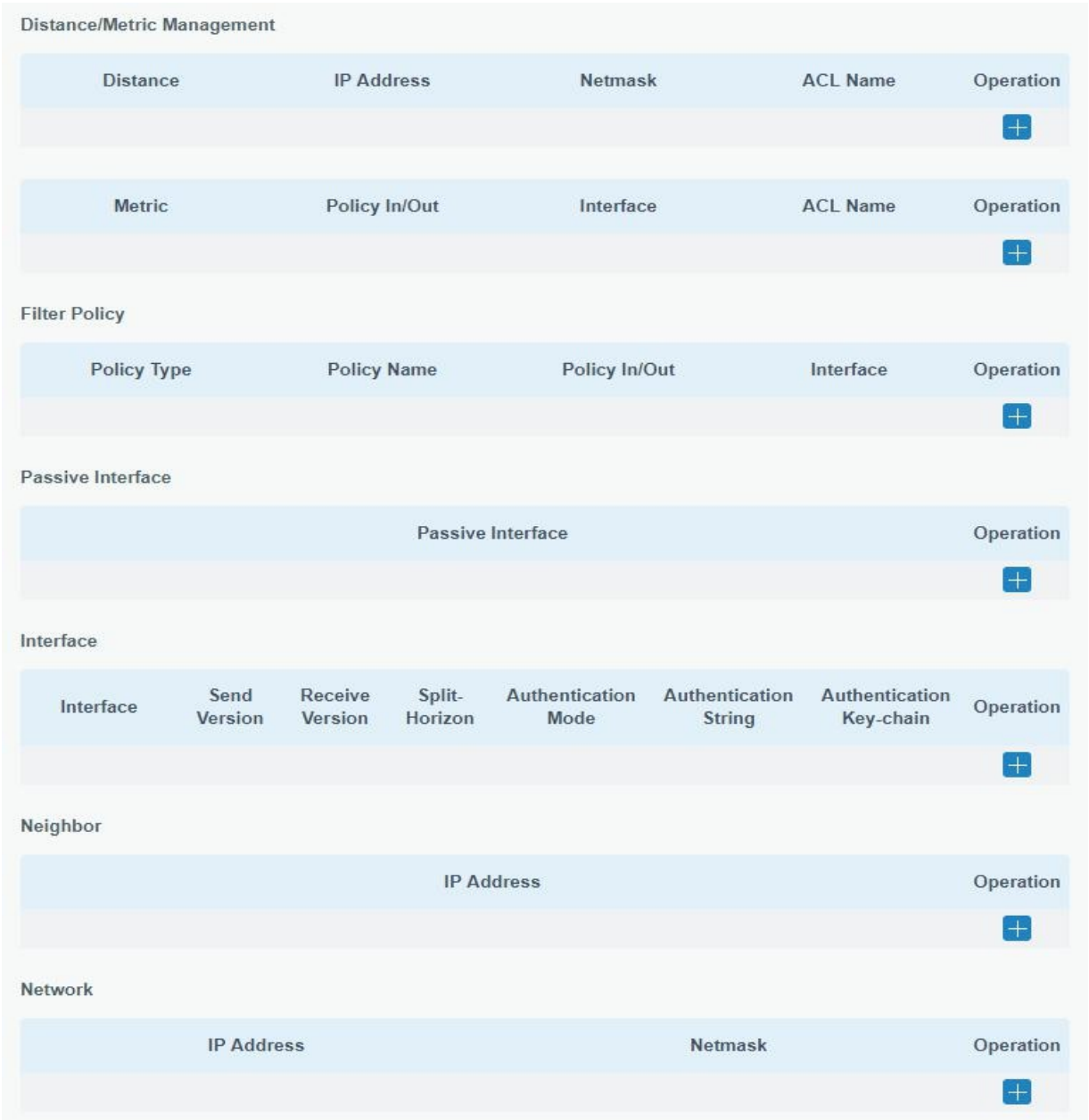


Abbildung 3-2-7-3

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“, „LAN1/WAN“ und „Bridge0“ aus.
Passive Schnittstelle	
Passive Schnittstelle	Wählen Sie die Schnittstelle aus „cellular0“, „LAN1/WAN“ und „Bridge0“ aus.
Schnittstelle	
Schnittstelle	Wählen Sie die Schnittstelle aus „cellular0“, „LAN1/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.

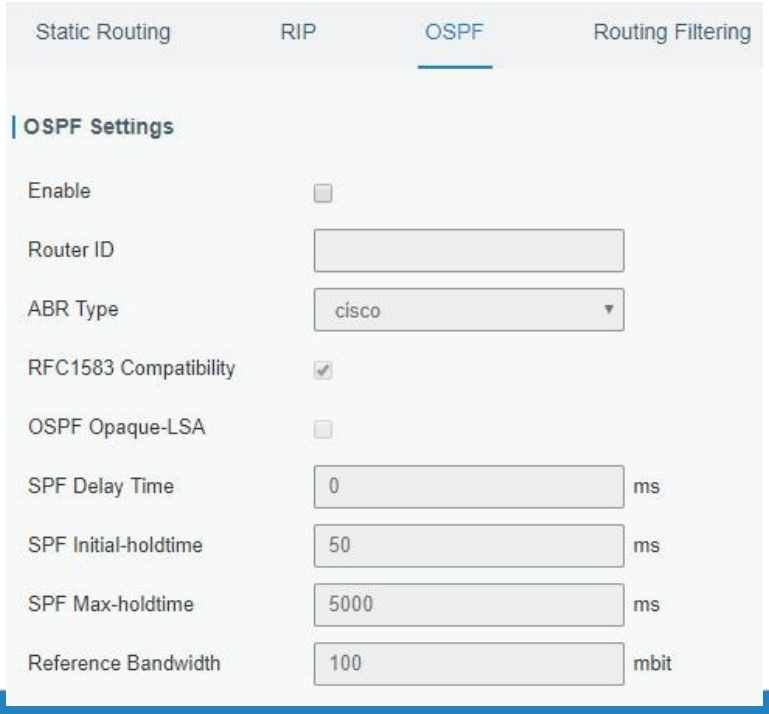
Fünf Arten von OSPF-Paketen:

- Hello-Paket

- DD-Paket (Datenbankbeschreibungspaket)
- 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. Erst wenn beide Seiten erfolgreich DD-Pakete ausgetauscht haben und die LSDB-Synchronisation erreicht ist, kann eine echte Nachbarschaftsbeziehung hergestellt werden. LSA beschreibt die Netzwerktopologie um einen Router herum, LSDB beschreibt die gesamte Netzwerktopologie.



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 Max-Holdtime	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.
Hallo-Intervall (s)	Sendeintervall des Hello-Pakets. Wenn die Hello-Zeit zwischen zwei benachbarten Routern unterschiedlich ist, kann keine Nachbarbeziehung hergestellt werden. Bereich: 1-65535.
Dead-Intervall (s)	Dead Time. Wenn innerhalb der Dead Time kein Hello-Paket von den Nachbarn empfangen wird, gilt der Nachbar als ausgefallen. Wenn die Dead Times 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“, „LAN1/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	
Bereichskennung	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	Das Intervall für die erneute Übertragung von LSA. Bereich: 1-65535.
Sendeverzögerung	Die Verzögerungszeit für die LSA-Übertragung. Bereich: 1-65535.

Tabelle 3-2-7-7 OSPF-Parameter

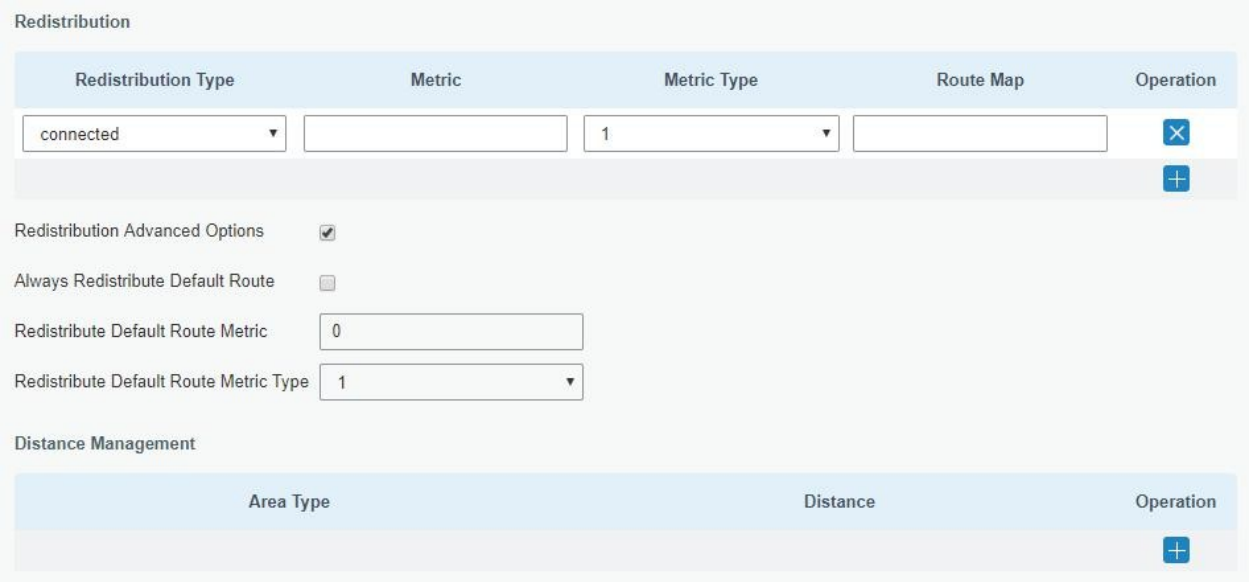


Abbildung 3-2-7-8

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 nach dem Start neu verteilen.
Standardroute neu verteilen Routenmetrik	Standardroute-Metrik für die Neuverteilung senden. Bereich: 0-16777214.
Standardroute 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

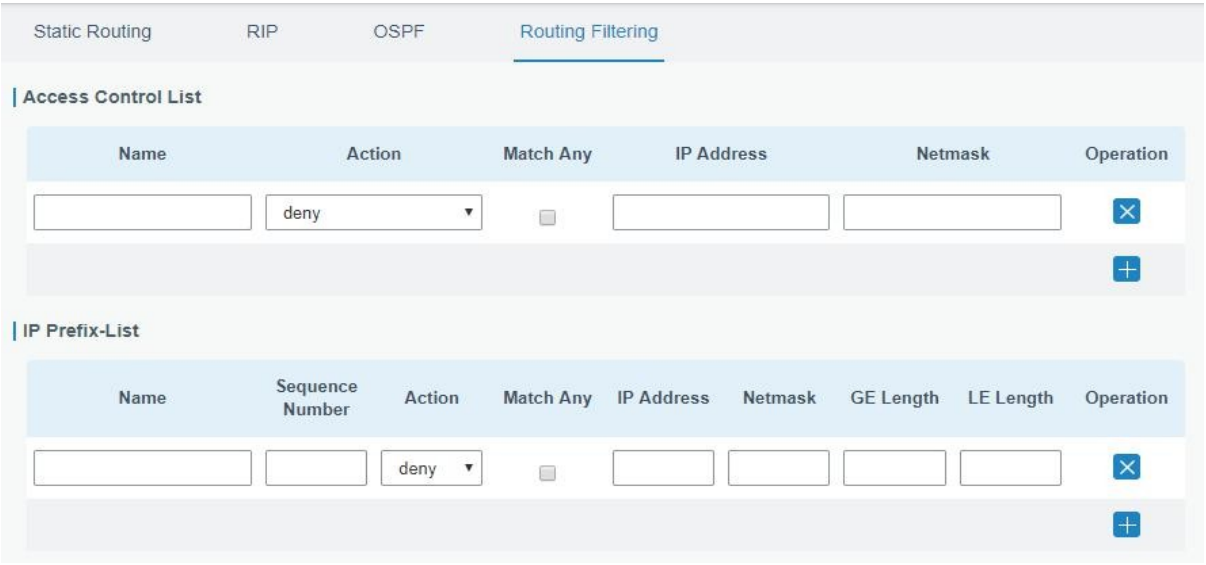


Abbildung 3-2-7-9

Routing-Filterung	
Element	Beschreibung
Zugriffskontrollliste	
Name	Benutzerdefinierter Name muss mit einem Buchstaben beginnen. Es sind nur Buchstaben, Ziffern und Unterstriche (_) sind zulässig.
Aktion	Wählen Sie zwischen „zulassen" und „verweigern".
Beliebige Übereinstimmung	IP-Adresse und Subnetzmaske müssen nicht festgelegt werden.
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, IP-Adresse, Subnetzmaske, FE-Länge und 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 der 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-Subnetzwerk.

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 über Ausfälle des virtuellen Master-Routers informiert sein. 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.

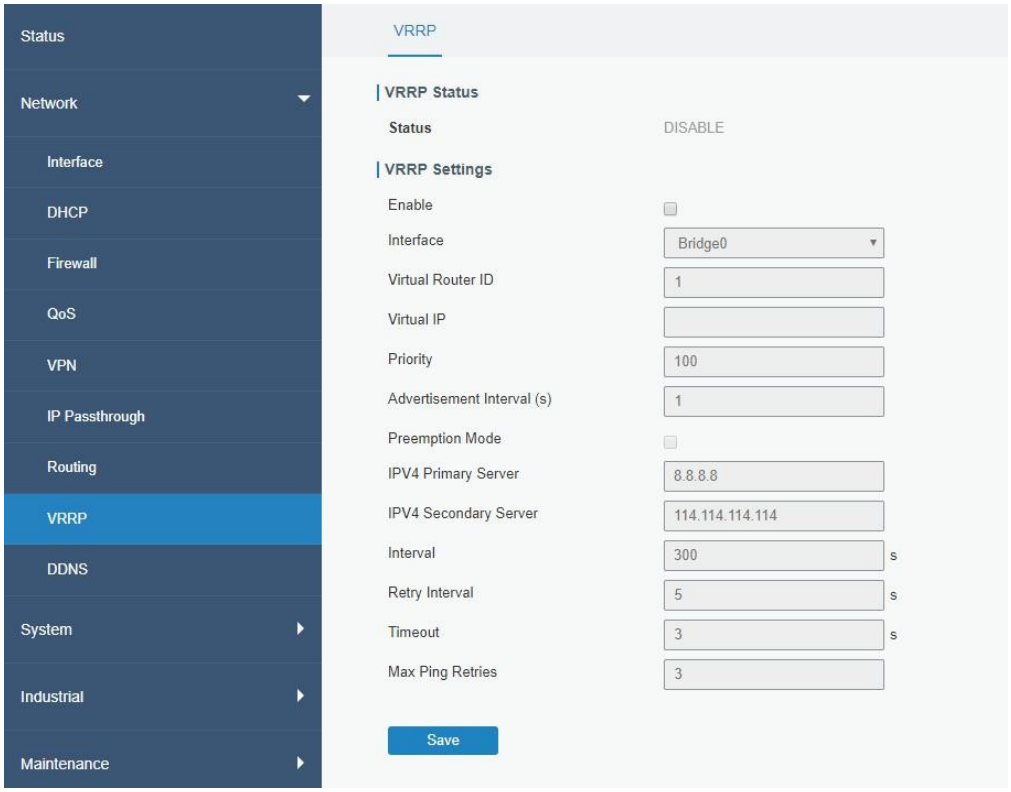


Abbildung 3-2-8-1

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
Preemption-Modus	Wenn der Router im Präemptionsmodus arbeitet,sendet er, sobald er feststellt, dass seine eigene Priorität höher ist als die des aktuellen Gateway-Routers, ein VRRP-Benachrichtigungspaket, was zur 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 Server nicht verfügbar ist. Sekundärserver nicht verfügbar ist.	114.114.114.114
Intervall	Zeitintervall (in Sekunden) zwischen zwei Pings.	300
Wiederholungsintervall	Legen Sie das Intervall für Ping-Wiederholungen 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.

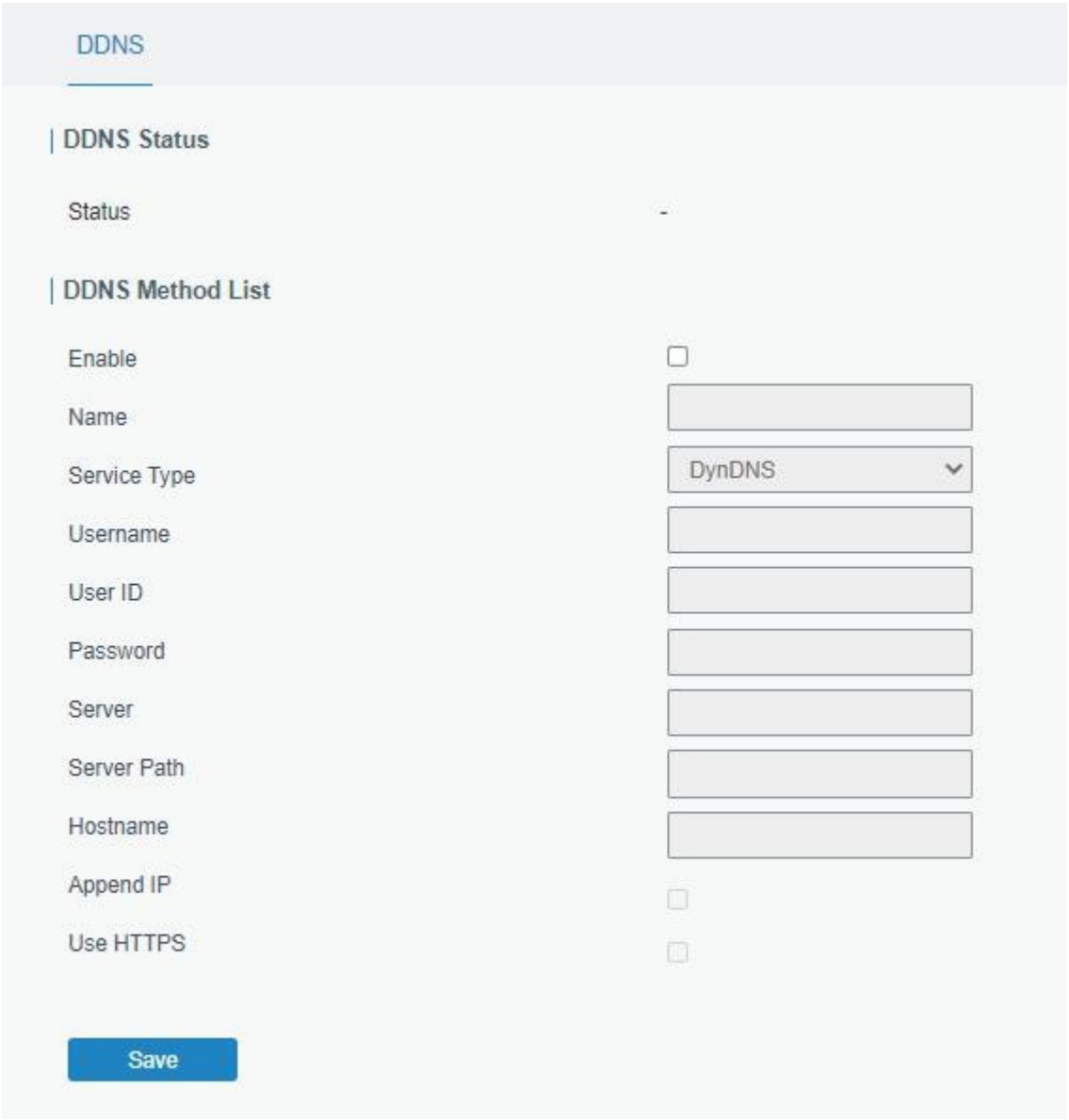


Abbildung 3-2-9-1

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

In diesem Abschnitt wird beschrieben, wie Sie allgemeine Einstellungen konfigurieren, z. B. Administratorkonto, Zugriffsservice, Systemzeit, allgemeine Benutzerverwaltung, SNMP, AAA, Ereignisalarme usw.

3.3.1 Allgemeine Einstellungen

3.3.1.1 Allgemein

Zu den allgemeinen Einstellungen gehören Systeminformationen und HTTPS-Zertifikate.

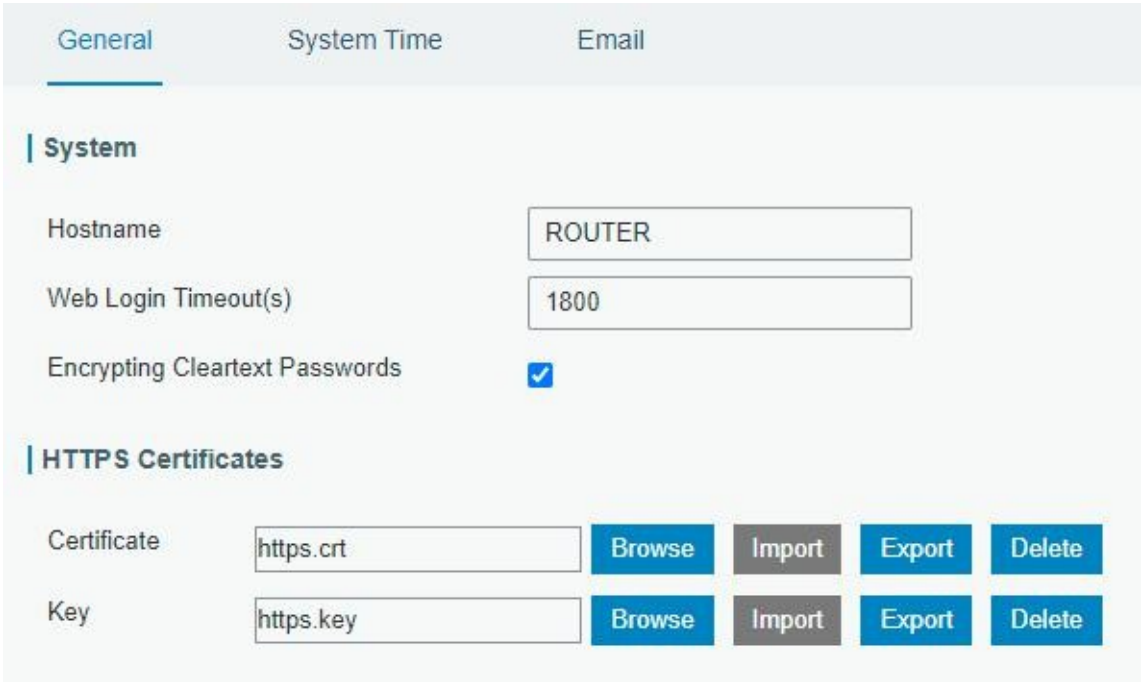


Abbildung 3-3-1-1

Allgemein		
Element	Beschreibung	Standard
System		
Hostname	Benutzerdefinierter Router-Name, muss mit einem Buchstaben beginnen.	ROUTER
Zeitlimit für Web-Anmeldung (s)	Bei Ablauf der Zeit müssen Sie sich erneut anmelden. Bereich: 100-3600.	1800
Verschlüsselung von Klartext Passwörter	Diese Funktion verschlüsselt alle Klartext-Passwörter in Verschlüsselungstext-Passwörter.	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. Durch Klicken auf die Schaltfläche „Löschen“ wird die Datei gelöscht.	--
Taste	Klicken Sie auf die Schaltfläche „Durchsuchen“, wählen Sie die Schlüsseldatei auf dem PC aus und klicken Sie dann auf	--

	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 Zeit läuft, wird empfohlen, die Systemzeit bei der Konfiguration des Routers einzustellen.

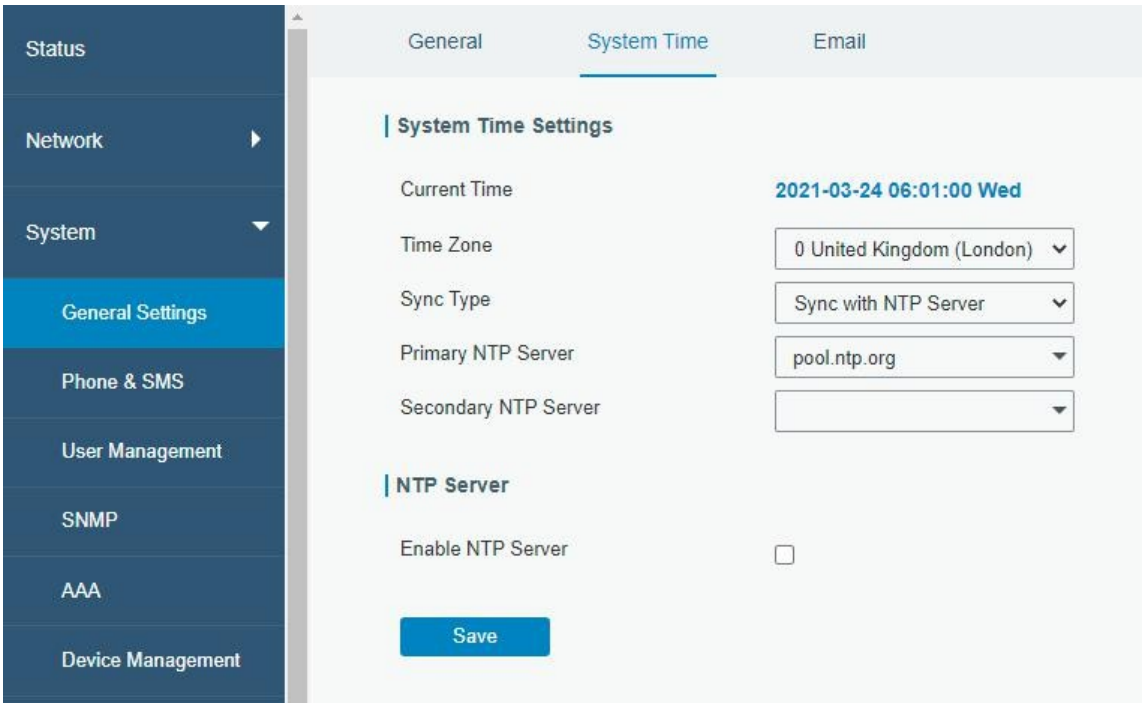


Abbildung 3-3-1-2

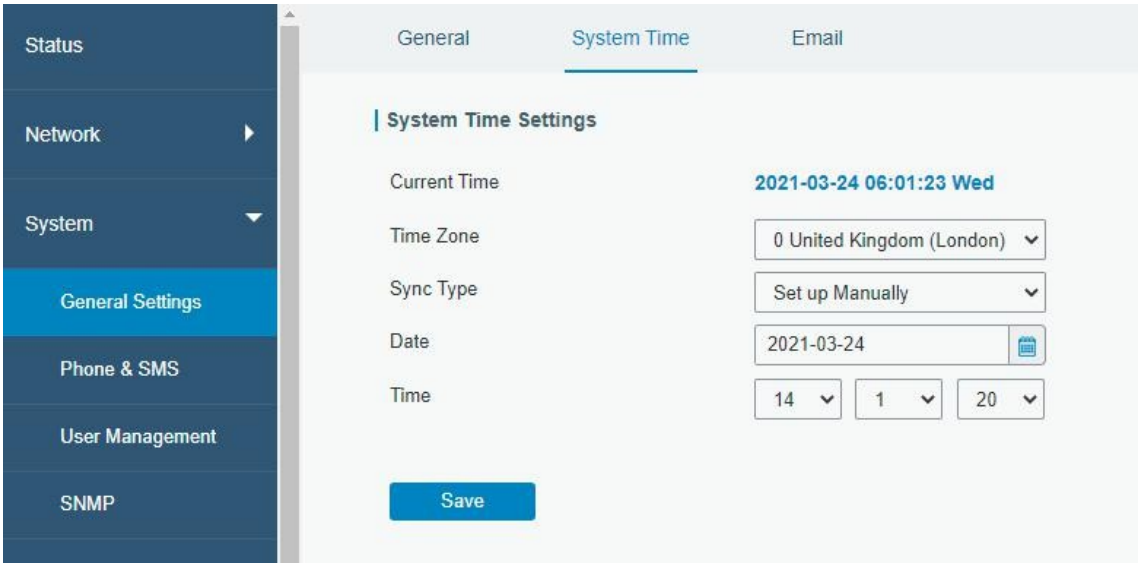


Abbildung 3-3-1-3

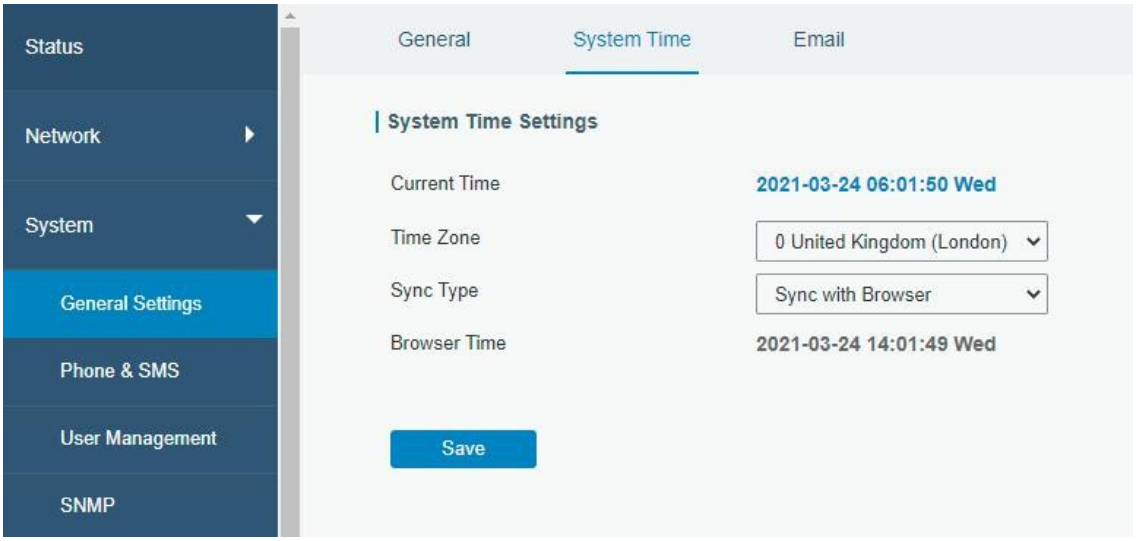


Abbildung 3-3-1-4

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 Typ der Zeitsynchronisierung auszuwählen.
Mit Browser synchronisieren	Zeit mit Browser synchronisieren.
Browserzeit	Zeigt die aktuelle Zeit des Browsers an.
Manuell einrichten	Konfigurieren Sie die Systemzeit manuell.
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 die Zeitsynchronisation mit dem Router durchführen. nachdem die Option „NTP-Server aktivieren“ 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 E-Mails verwendet wird. In diesem Abschnitt wird beschrieben, wie Sie E-Mail-Einstellungen konfigurieren und E-Mail-Gruppen für Alarme und Ereignisse hinzufügen.

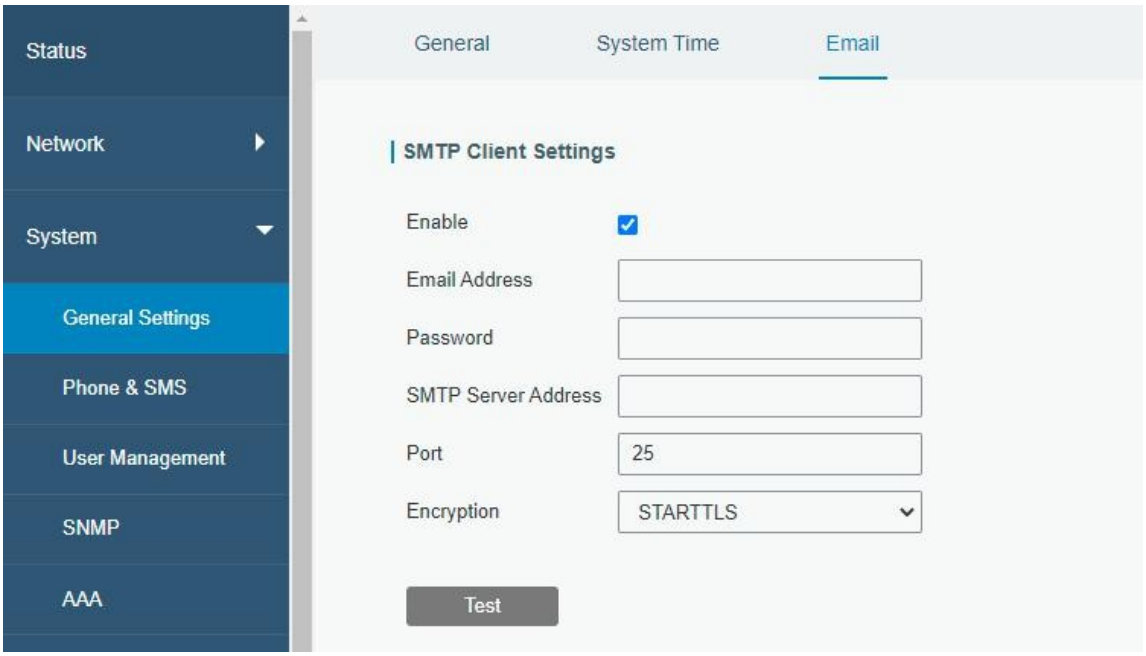


Abbildung 3-3-1-5

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	Wählen Sie aus: 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, sofern Sie sich nicht auf eine bestimmte Version des Protokolls beziehen. Der Standardport ist 465.

Tabelle 3-3-1-3 SMTP-Einstellung

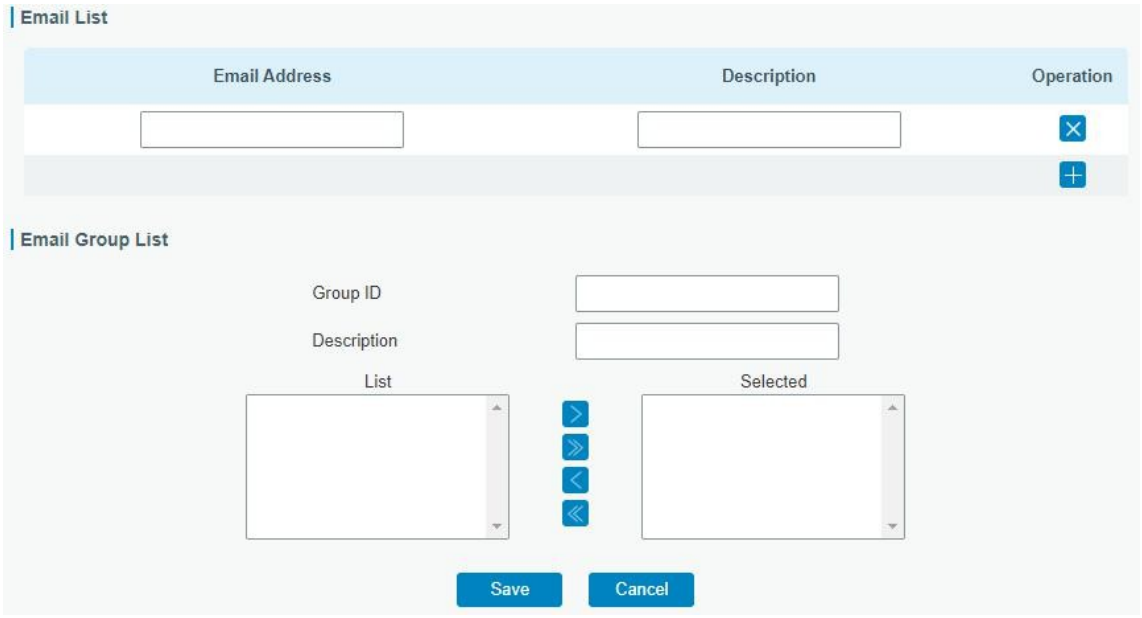


Abbildung 3-3-1-6

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

Ereigniseinstellungen

Anwendungsbeispiel für Ereignisse

3.3.2 Telefon und SMS

3.3.2.1 Telefon

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

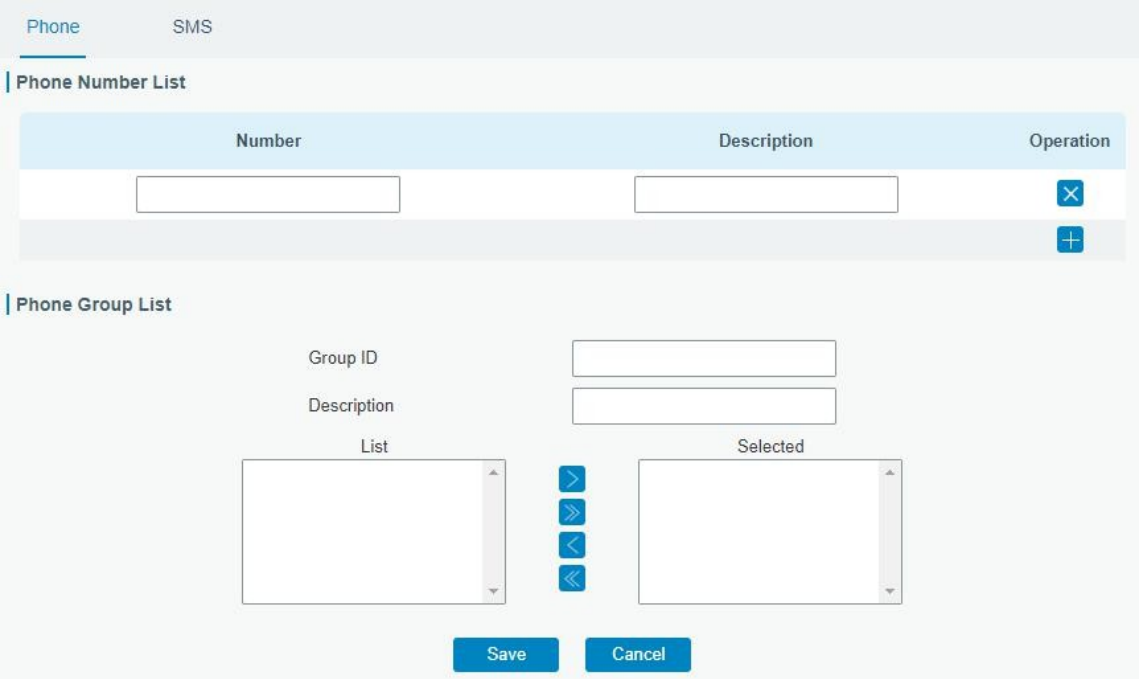


Abbildung 3-3-2-1

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.

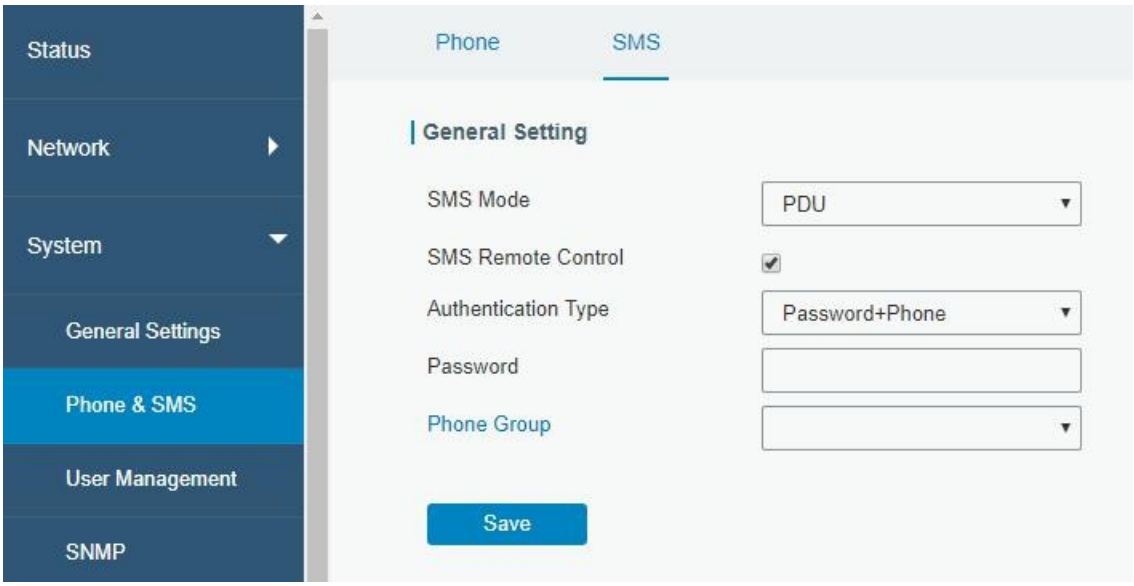


Abbildung 3-3-2-2

SMS-Einstellungen	
Element	Beschreibung
SMS-Modus	Wählen Sie den SMS-Modus aus „TEXT“ und „PDU“ aus.
SMS-Fernbedienung Steuerung	SMS-Fernsteuerung aktivieren/deaktivieren.
Authentifizierungstyp	Sie können zwischen „Telefonnummer“ und „Passwort + Telefonnummer“ wählen. Telefonnummer: Verwenden Sie die Telefonnummer zur Authentifizierung. Passwort + Telefonnummer: Verwenden Sie sowohl „Passwort“ als auch „Telefonnummer“ zur Authentifizierung. für die Authentifizierung.
Passwort	Legen Sie ein Passwort für die Authentifizierung fest.
Telefongruppe	Wählen Sie die Telefongruppe aus, die für die Fernsteuerung verwendet wird. Der Benutzer kann auf die Telefongruppe klicken und die Telefonnummer festlegen.

Tabelle 3-3-2-2 SMS-Fernsteuerungsparameter

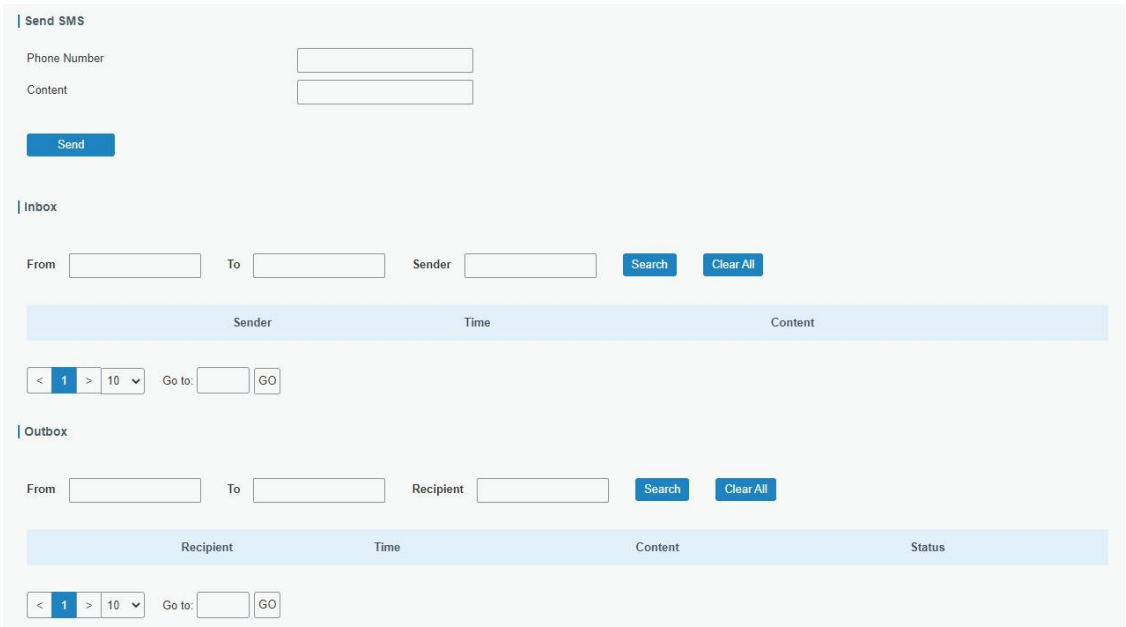


Abbildung 3-3-2-3

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 UR32L 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.

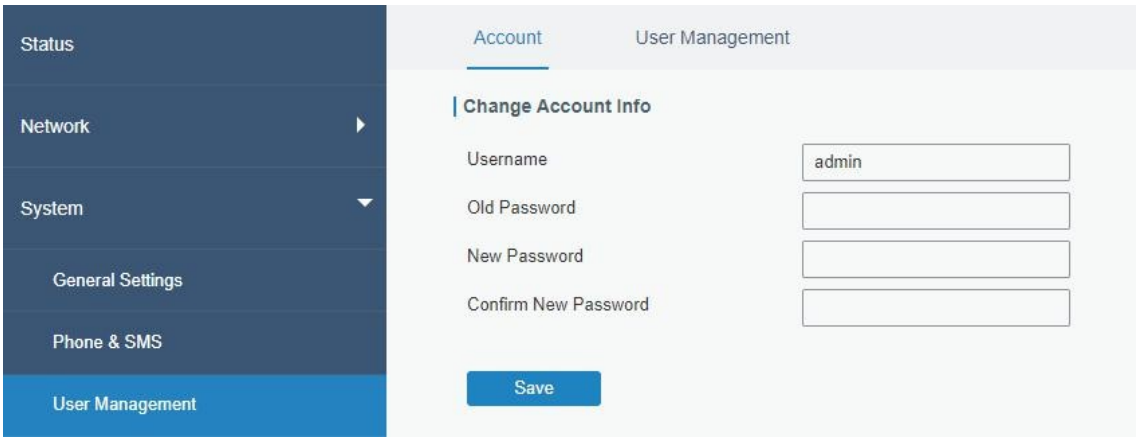


Abbildung 3-3-3-1

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.
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. Zu den allgemeinen Benutzerberechtigungen gehören „Nur Lesen“ und „Lesen/Schreiben“.

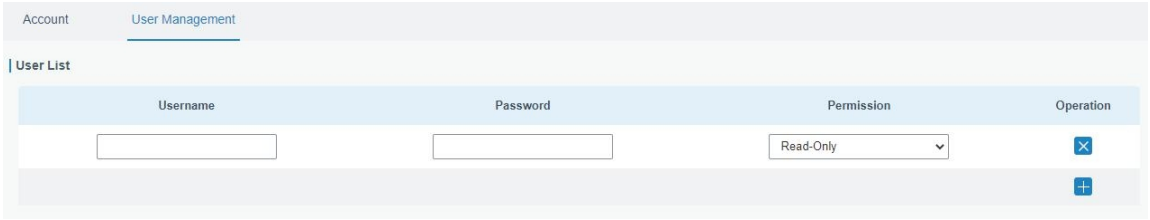


Abbildung 3-3-3-2

Benutzerverwaltung	
Element	Beschreibung
Benutzername	Geben Sie einen neuen Benutzernamen ein. Sie können Zeichen wie a-z, 0-9, „_“, „-“, „$“ verwenden. Das erste Zeichen darf keine Ziffer sein.
Passwort	Legen Sie ein Passwort fest.
Berechtigungen	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 auf dieser Ebene die Konfiguration des Routers anzeigen und festlegen.

Tabelle 3-3-3-2 Benutzerverwaltung

3.3.4 SNMP

SNMP wird häufig im Netzwerkmanagement für die Netzwerküberwachung eingesetzt. 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 Konfigurationsschritte für die Abfrage aus NMS sind nachfolgend aufgeführt:

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

Beispiel für eine zugehörige Konfiguration

SNMP-Anwendungsbeispiel

3.3.4.1 SNMP

UR32L 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.

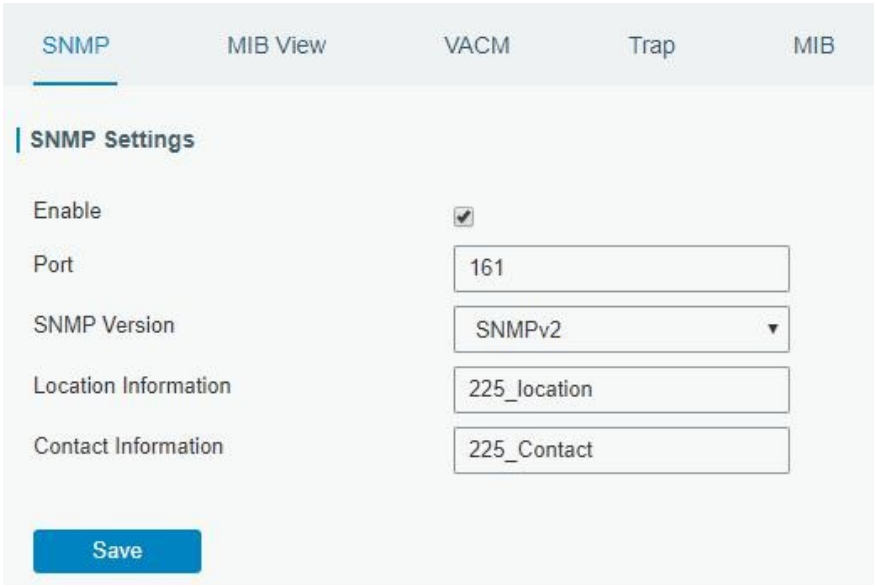


Abbildung 3-3-4-1

SNMP-Einstellungen	
Element	Beschreibung
Aktivieren	Aktivieren oder deaktivieren Sie die SNMP-Funktion.
Port	Legen Sie den SNMP-Port fest. 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 3-3-4-1 SNMP-Parameter

3.3.4.2 MIB-Ansicht

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

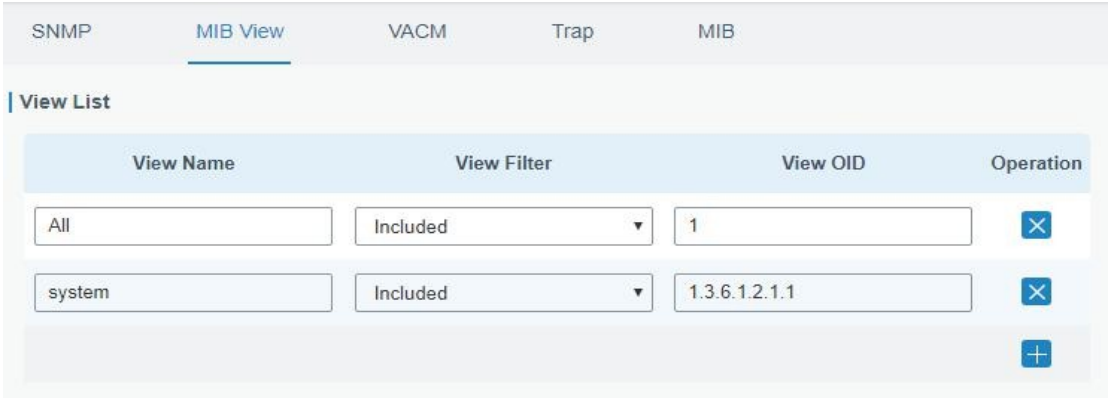


Abbildung 3-3-4-2

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 3-3-4-2 MIB-Ansichtsparameter

3.3.4.3 VACM

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

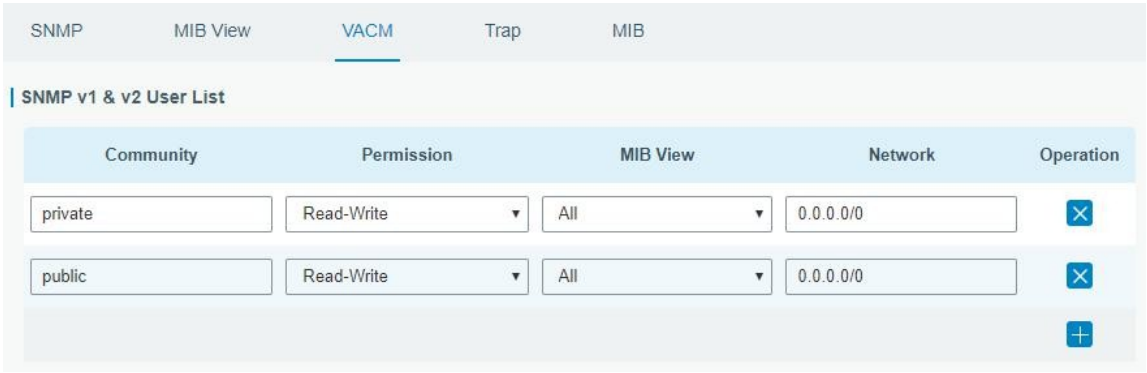


Abbildung 3-3-4-3

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" festzulegen.
Inform-Ansicht	Wählen Sie eine MIB-Ansicht aus der MIB-Ansichtsliste aus, um die Berechtigung auf „Informieren" zu setzen.
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".
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" und „DES" ist.

Tabelle 3-3-4-3 VACM-Parameter

3.3.4.4 Trap

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

Abbildung 3-3-3-4

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 3-3-4-4 Trap-Parameter

3.3.4.5 MIB

In diesem Abschnitt wird beschrieben, wie Sie MIB-Dateien herunterladen können. Die letzte MIB-Datei „LTE-ROUTER-MIB.txt“ ist für den UR32L-Router bestimmt.

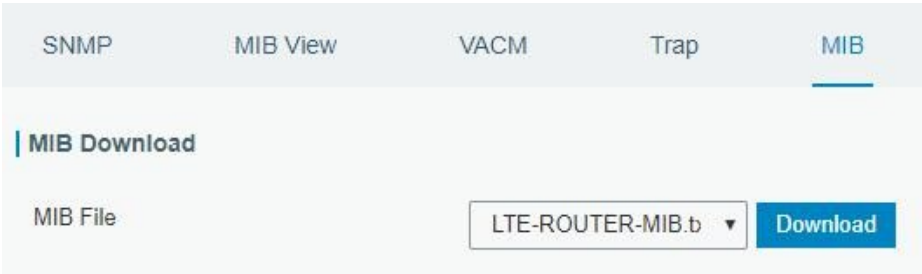


Abbildung 3-3-4-5

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

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

Tabelle 3-3-4-5 MIB-Download

3.3.5 AAA

Die AAA-Zugriffskontrolle wird für die Besucherkontrolle und die verfügbaren entsprechenden Dienste verwendet, sobald der Zugriff gewährt wurde. Sie verwendet dieselbe Methode zur Konfiguration von drei unabhängigen Sicherheitsfunktionen. Sie bietet Modularisierungsmethoden für folgende Dienste:

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

3.3.5.1 Radius

Radius verwendet UDP für den Transport und wird in der Regel in verschiedenen Netzwerkumgebungen mit höheren Anforderungen an die Sicherheit und die Berechtigung des Fernzugriffs von Benutzern eingesetzt.

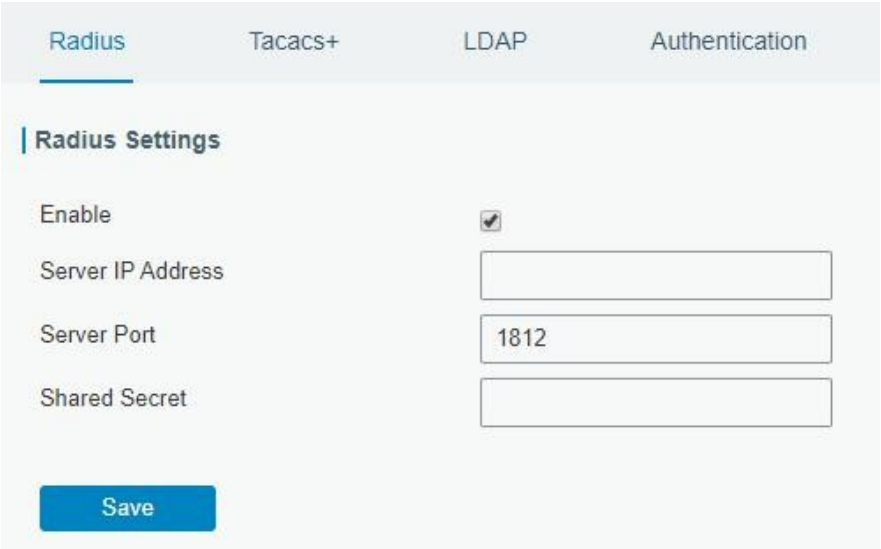


Abbildung 3-3-5-1

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 eine Verbindung zum Radius-Server herzustellen.

Tabelle 3-3-5-1 Radius-Parameter

3.3.5.2 TACACS+

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

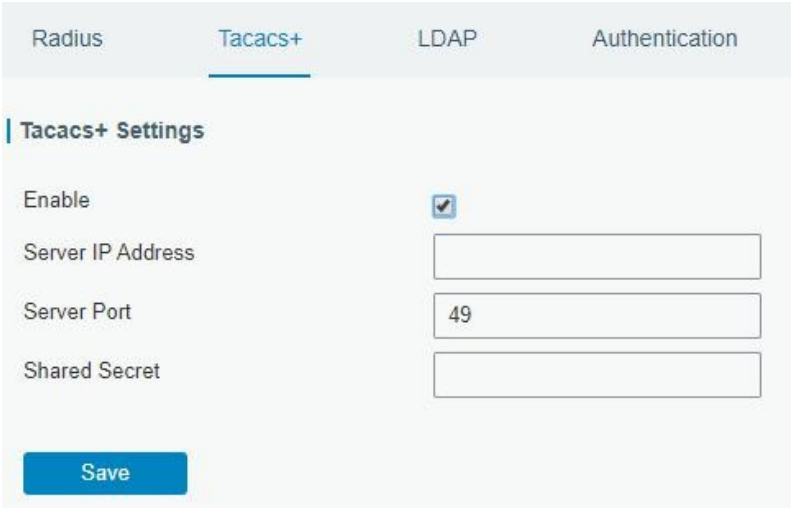


Abbildung 3-3-5-2

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 TACACS+-Serverport 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 3-3-5-2 TACACS+-Parameter

3.3.5.3 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.

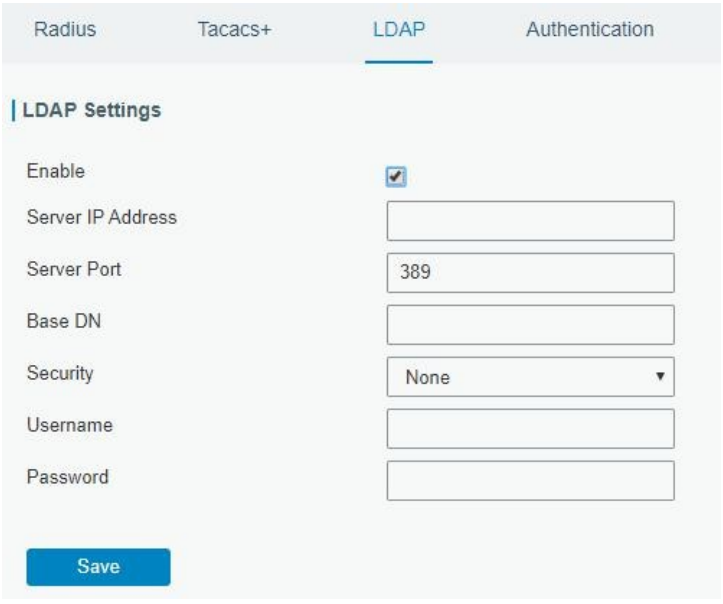


Abbildung 3-3-5-3

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 oberste Ebene der LDAP-Verzeichnisstruktur.
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

3.3.5.4 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 3-3-5-4

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 3-3-5-4 Authentifizierungsparameter

3.3.6 Geräteverwaltung

3.3.6.1 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 [illegible]

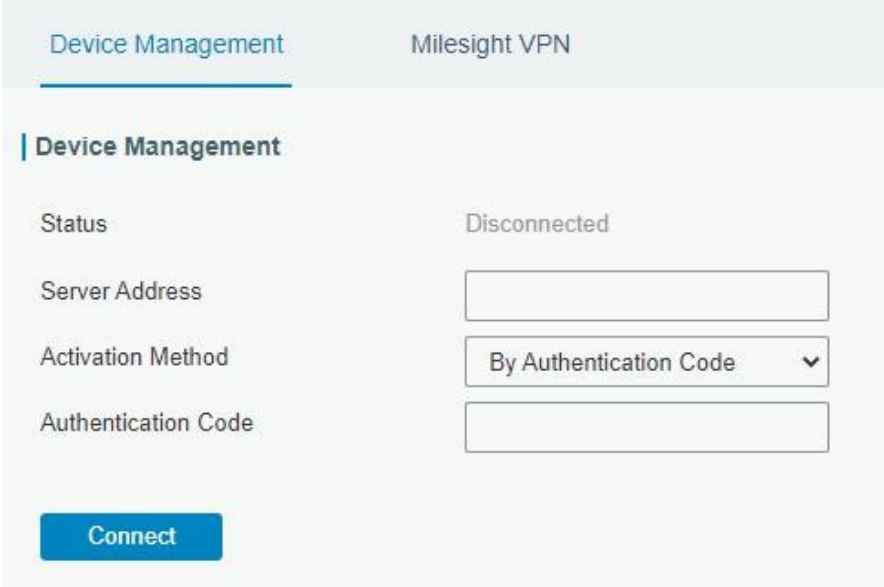


Abbildung 3-3-6-1

Geräte-Hub	
Artikel	Beschreibung
Status	Zeigt den Verbindungsstatus zwischen dem Router und dem DeviceHub anzeigen.
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, um den Router mit dem DeviceHub-Server zu verbinden. Die Optionen sind „Per Authentifizierungscode“ und „Über den Kontonamen“.
Authentifizierungscode	Geben Sie den vom DeviceHub generierte Authentifizierungscode ein.
Kontoname	Geben Sie das registrierte DeviceHub-Konto (E-Mail) ein und Passwort.
Passwort	

Tabelle 3-3-6-1

3.3.6.2 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 [illegible]

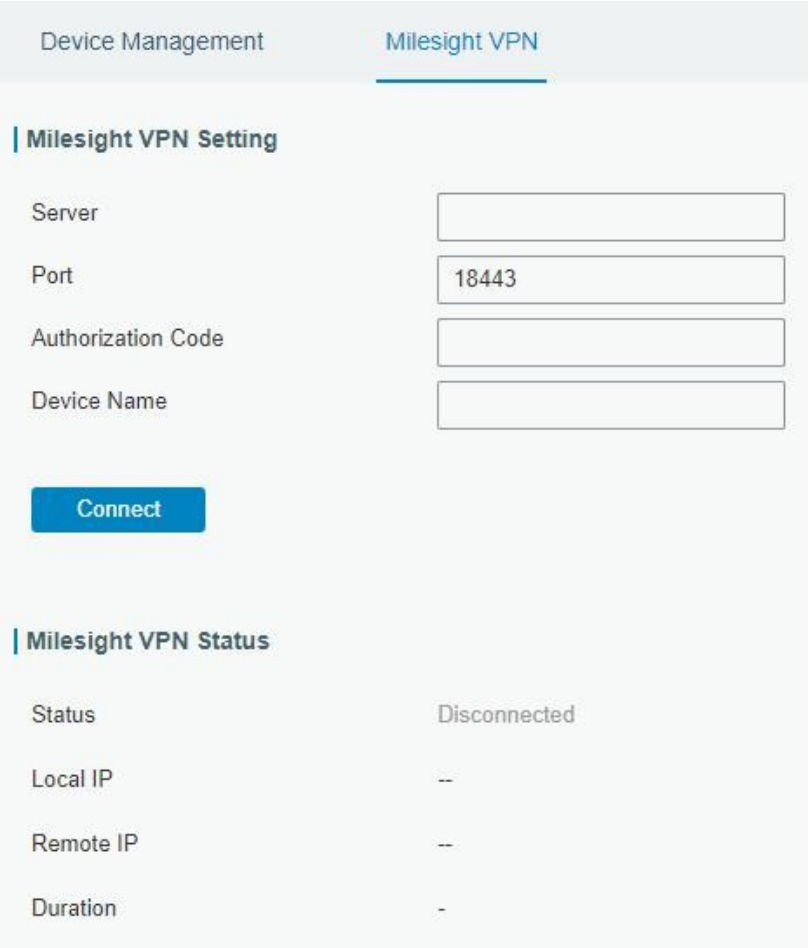


Abbildung 3-3-6-2

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 3-3-6-2

3.3.7 Ereignisse

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

3.3.7.1 Ereignisse

Auf dieser Seite können Sie Alarmmeldungen anzeigen.

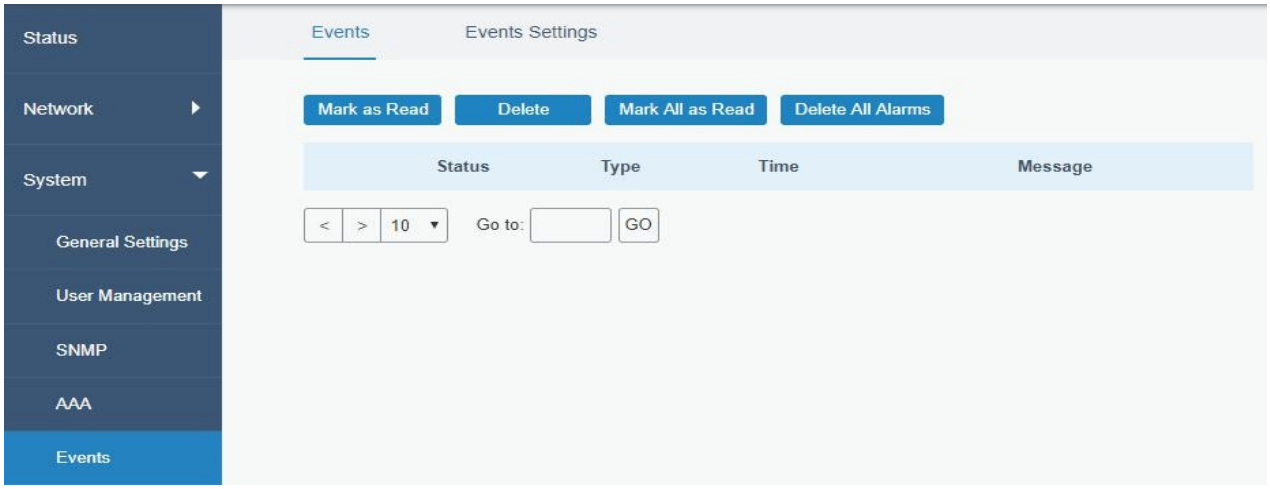


Abbildung 3-3-7-1

Ereignisse	
Element	Beschreibung
Als gelesen markieren	Markieren Sie den ausgewählten Ereignisalarm als „ ead" (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	Zeigt die Alarmzeit an.
Meldung	Zeigt den Inhalt des Alarms an.

Tabelle 3-3-7-1 Ereignisparameter

3.3.7.2 Ereigniseinstellungen

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

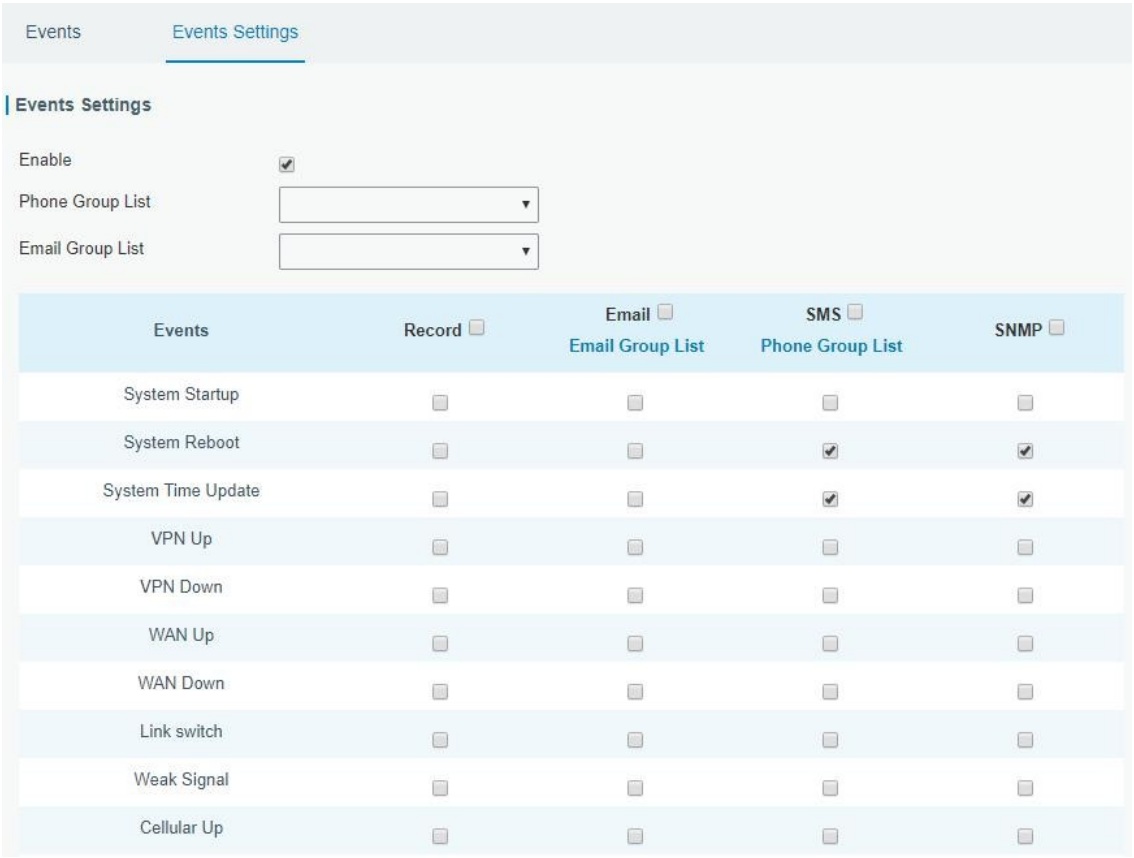


Abbildung 3-3-7-2

Abbildung 3-3-7-3

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 die E-Mail-Gruppe aus, die den Alarm erhalten soll.
Aufzeichnung	Der relevante Inhalt des Ereignisalarms wird auf der Seite 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 zu konfigurieren.
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.
Mobilfunk aktiv	Das Mobilfunknetz ist verbunden.
Mobilfunkverbindung unterbrochen	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.

Tabelle 4-3-7-2 Ereignisparameter

Verwandte Themen

E-Mail-Einstellungen

Anwendungsbeispiel für Ereignisse

3.4 Wartung

In diesem Abschnitt werden die Tools und die Verwaltung für die Systemwartung beschrieben.

3.4.1 Tools

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

3.4.1.1 Ping

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

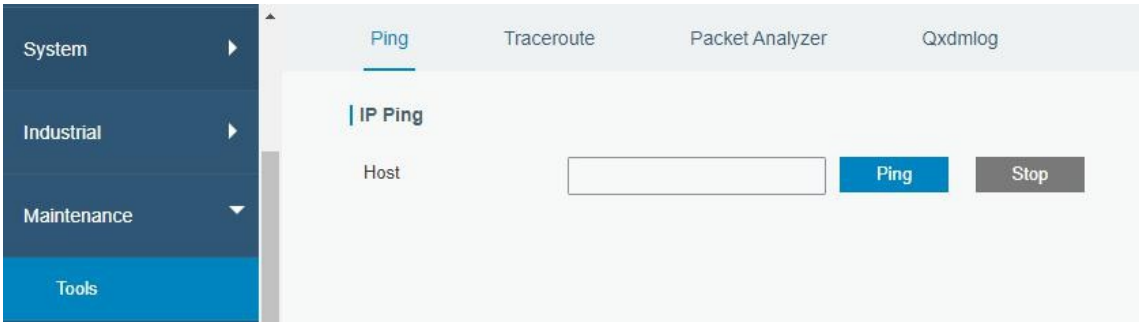


Abbildung 3-4-1-1

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

Tabelle 3-4-1-1 IP-Ping-Parameter

3.4.1.2 Traceroute

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

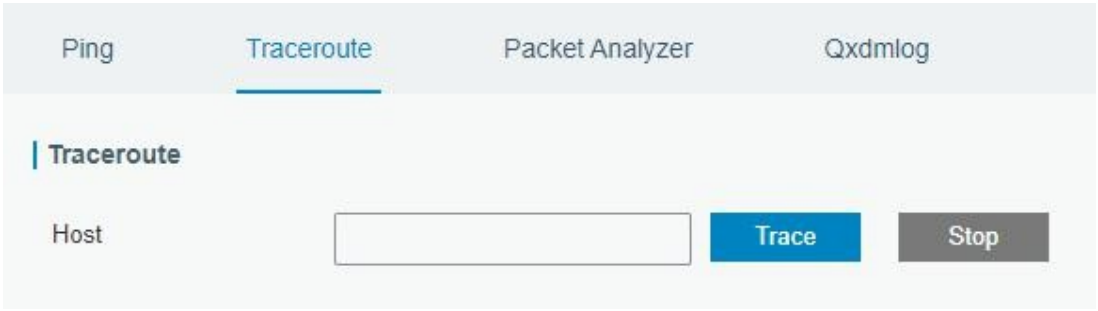


Abbildung 3-4-1-2

Traceroute	
Element	Beschreibung
Host	Adresse des zu ermittelnden Zielhosts.

Tabelle 3-4-1-2 Traceroute-Parameter

3.4.1.3 Paketanalysator

Der Paketanalysator wird zum Erfassen der Pakete verschiedener Schnittstellen verwendet.

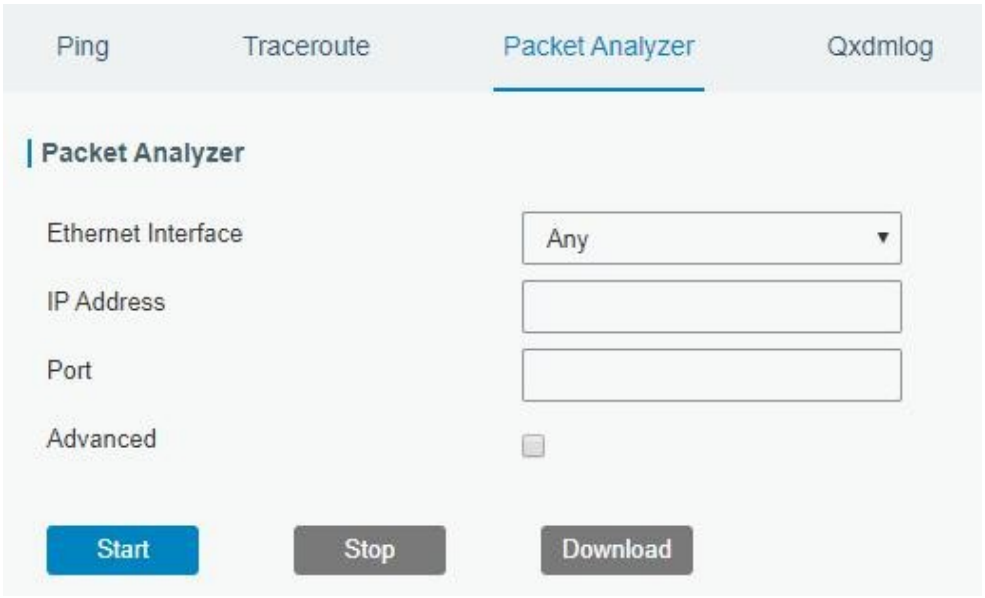


Abbildung 3-4-1-3

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 3-4-1-3 Parameter des Paketanalysators

3.4.1.4 Qxdmlog

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

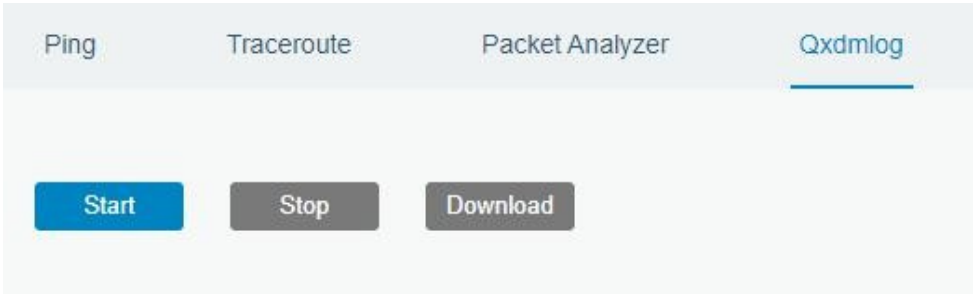
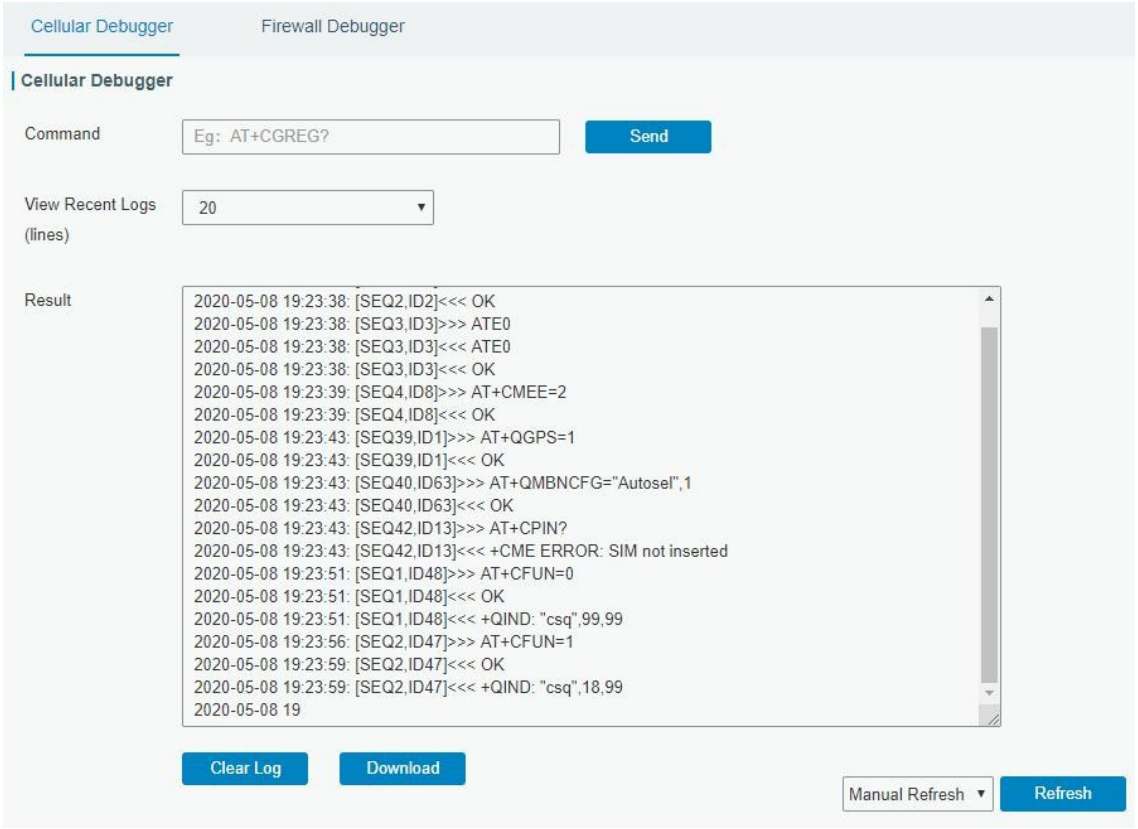


Abbildung 3-4-1-4

3.4.2 Debugger

3.4.2.1 Mobilfunk-Debugger

In diesem Abschnitt wird erläutert, wie Sie AT-Befehle an den Router senden und die Debug-Informationen des



Mobilfunknetzes überprüfen können.

Abbildung 3-4-2-1

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 3-4-2-1 Parameter des Mobilfunk-Debuggers

3.4.2.2 Firewall-Debugger

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

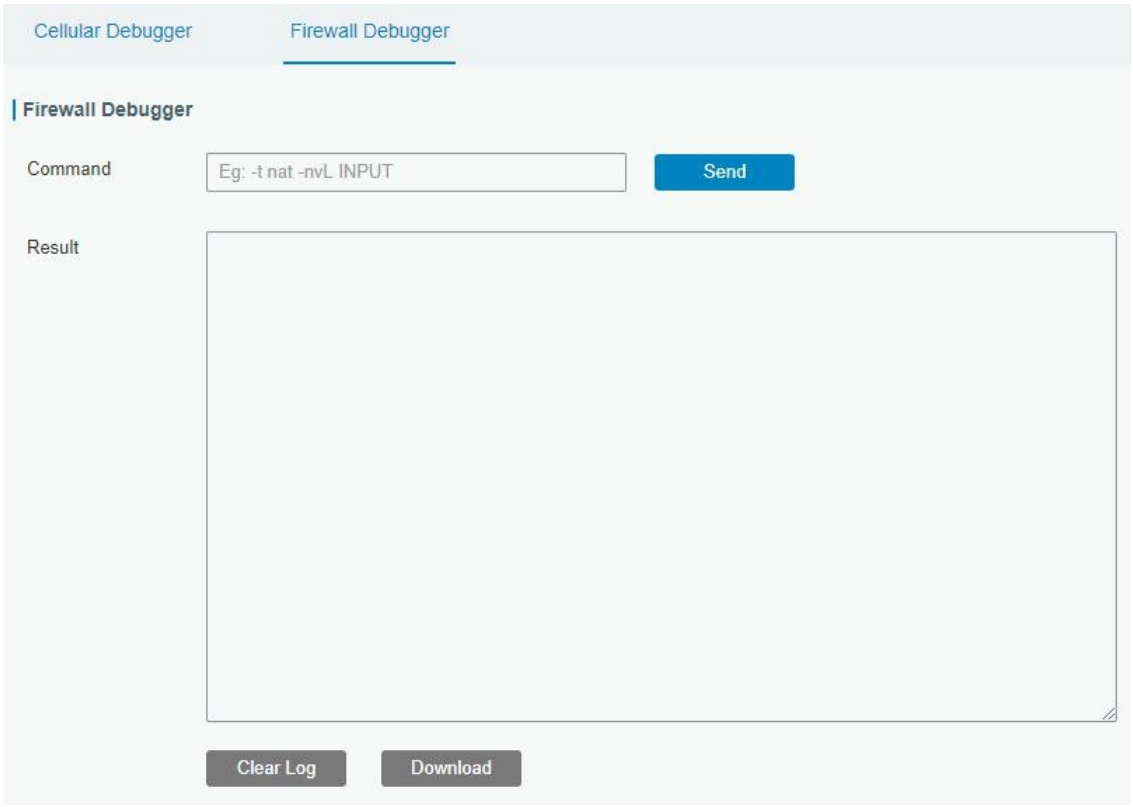


Abbildung 3-4-2-2

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 3-4-2-2 Firewall-Debugger-Parameter

3.4.3 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 Fehlerbehebungen am System vornimmt, 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.

3.4.3.1 Systemprotokoll

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

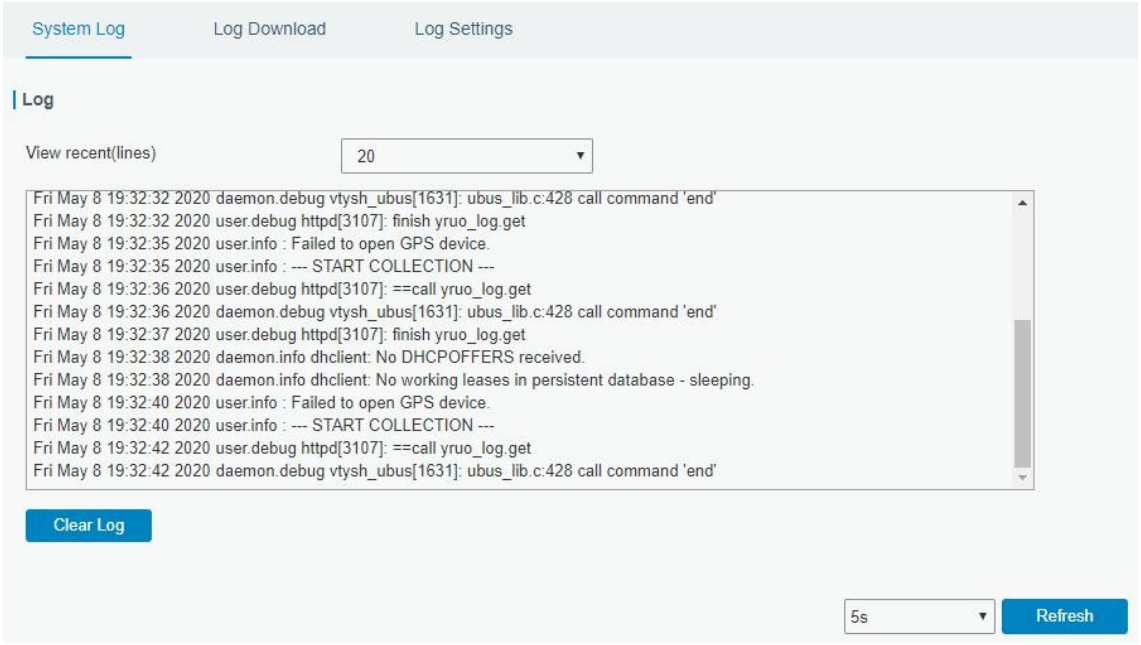


Abbildung 3-4-3-1

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

Tabelle 3-4-3-1 Parameter für das Systemprotokoll

3.4.3.2 Protokoll herunterladen

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

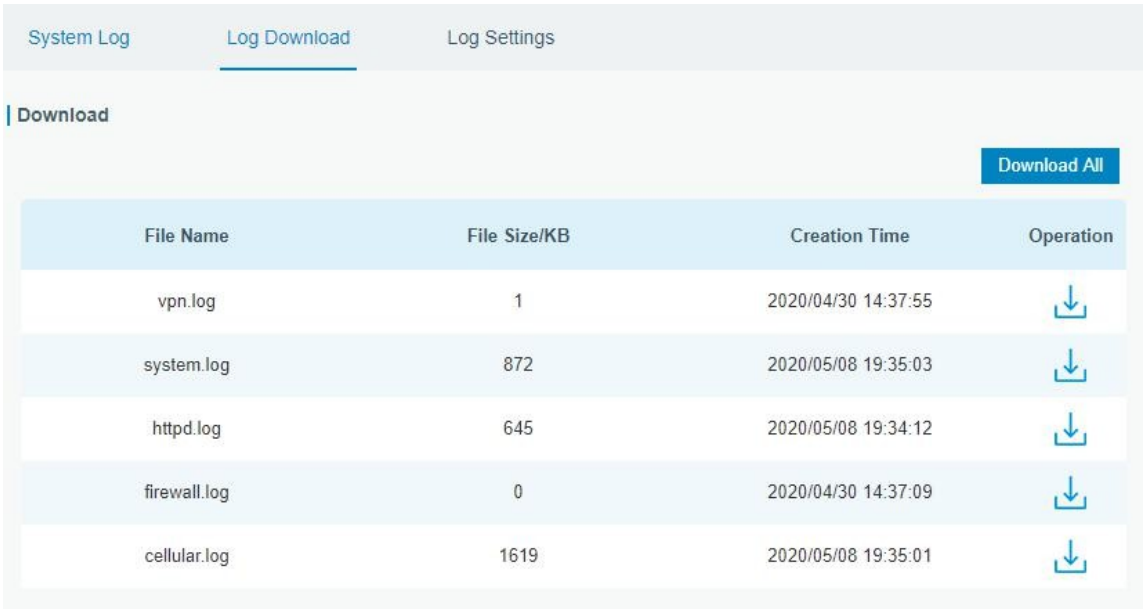


Abbildung 3-4-3-2

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 Protokolldatei s an.
Vorgang	Klicken Sie hier, um alle Protokolldateien herunterzuladen.

Tabelle 3-4-3-2 Systemprotokollparameter

3.4.3.3 Protokolleinstellungen

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

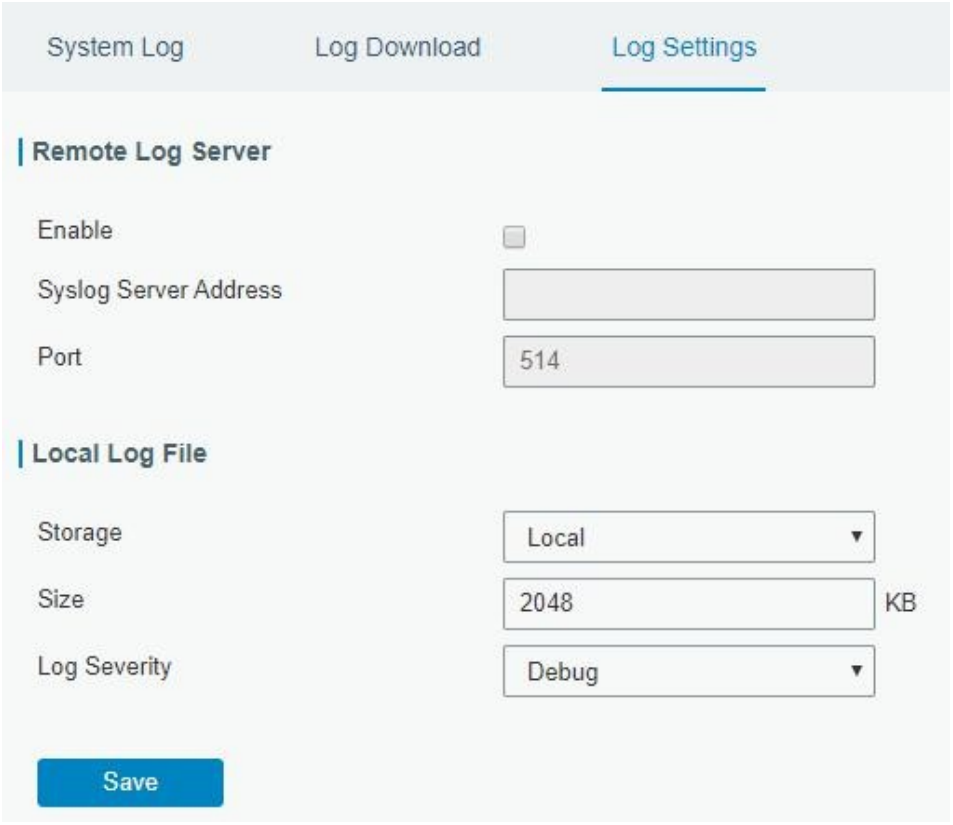


Abbildung 3-4-3-3

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 3-4-3-3 Protokolleinstellungsparameter

3.4.4 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.

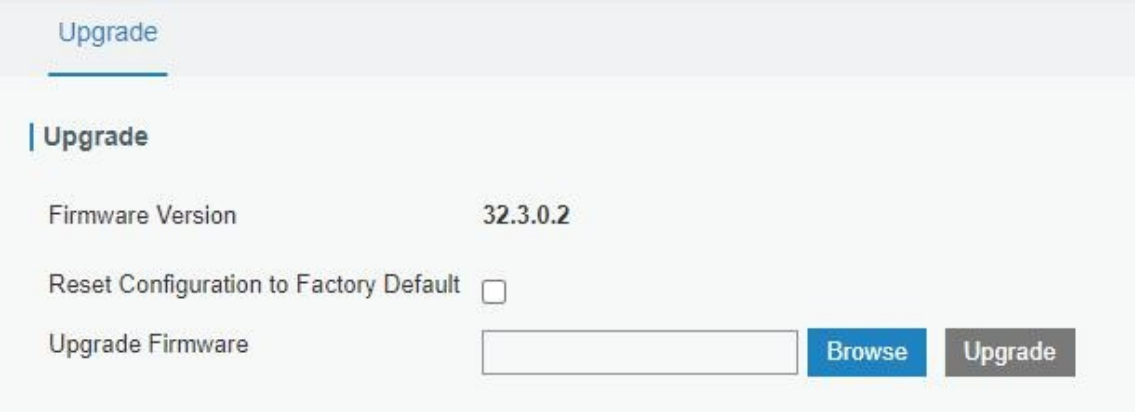


Abbildung 3-4-4-1

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 3-4-4-1 Upgrade-Parameter

Beispiel für die zugehörige Konfiguration

Firmware-Upgrade

3.4.5 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.

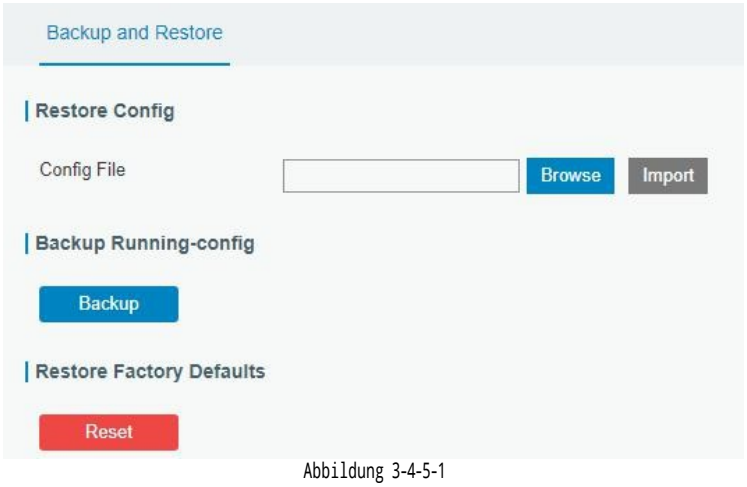


Abbildung 3-4-5-1

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 3-4-5-1 Parameter für Sicherung und Wiederherstellung

Beispiel für die entsprechende Konfiguration

Werkseinstellungen wiederherstellen

3.4.6 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.

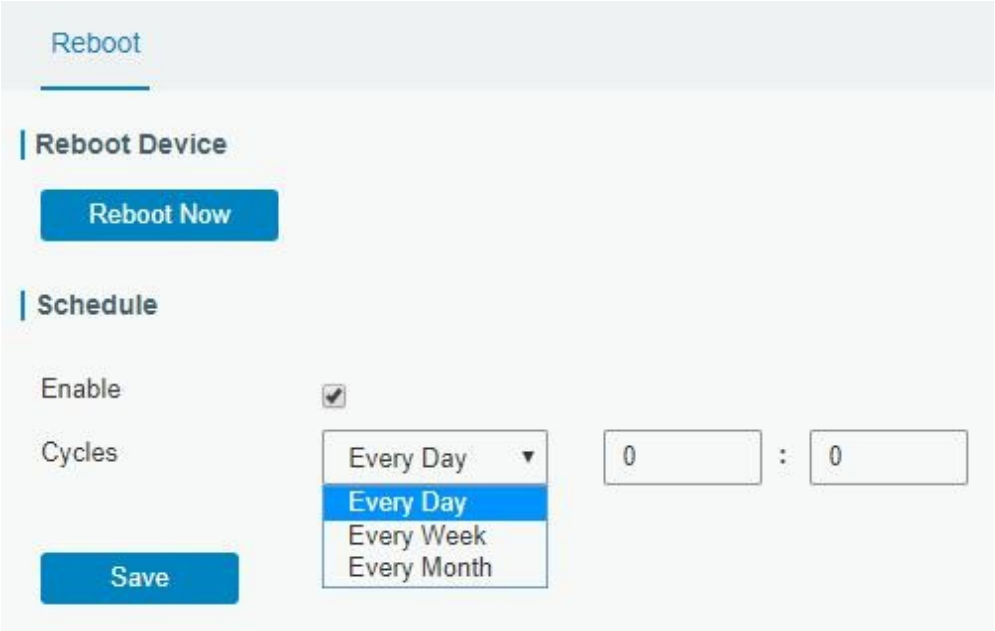


Abbildung 3-4-6-1

Neustart	
Element	Beschreibung
Jetzt neu starten	Starten Sie den Router sofort neu.
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 3-4-2-1 Zeitplanparameter

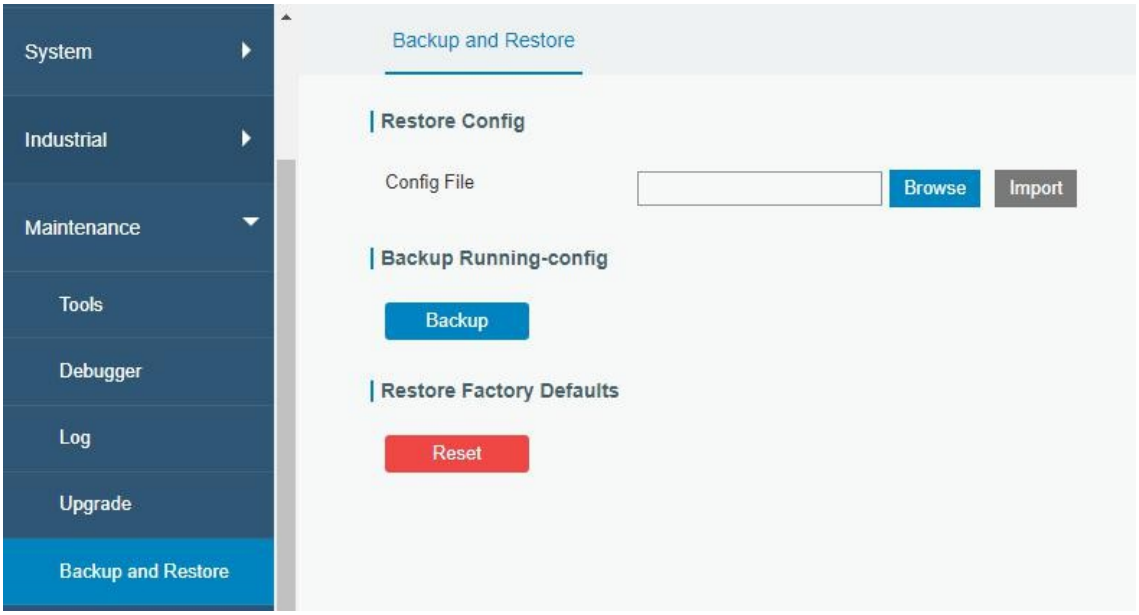
Kapitel 4 Anwendungsbeispiele

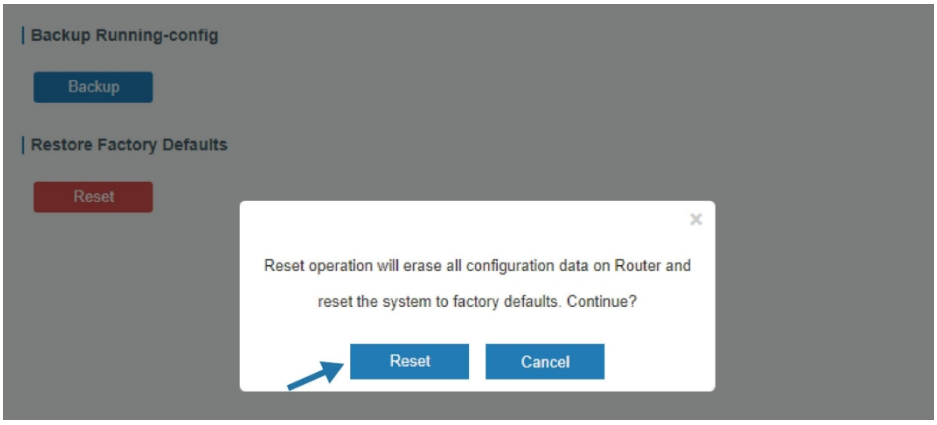
4.1 Werkseinstellungen wiederherstellen

4.1.1 Über die Webschnittstelle

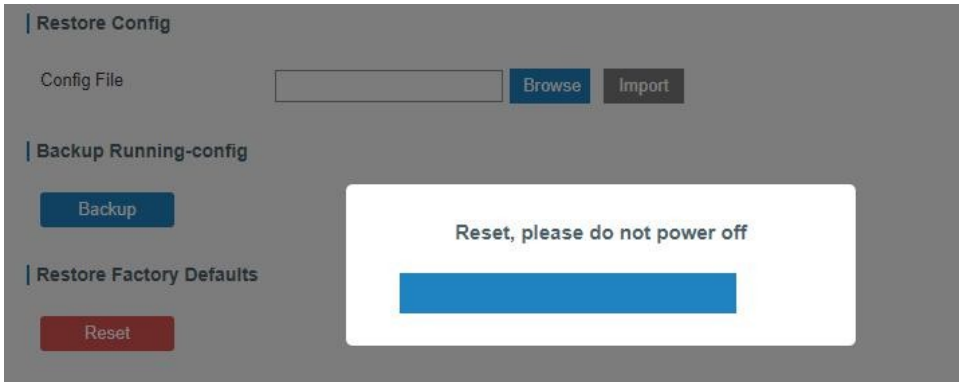
1. Melden Sie sich bei der Webschnittstelle an und gehen Sie zu „Wartung > Sichern und Wiederherstellen“.
2. Klicken Sie unter „Werkseinstellungen wiederherstellen“ auf die Schaltfläche „Zurücksetzen“.

Sie werden gefragt, ob Sie das Gerät auf die Werkseinstellungen zurücksetzen möchten. Klicken Sie anschließend auf die Schaltfläche „Zurücksetzen“.





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



Bitte 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

4.2.2 Über die Hardware

Suchen Sie die Reset-Taste am Router und führen Sie je nach Status der SYSTEM-LED die entsprechenden Maßnahmen durch.

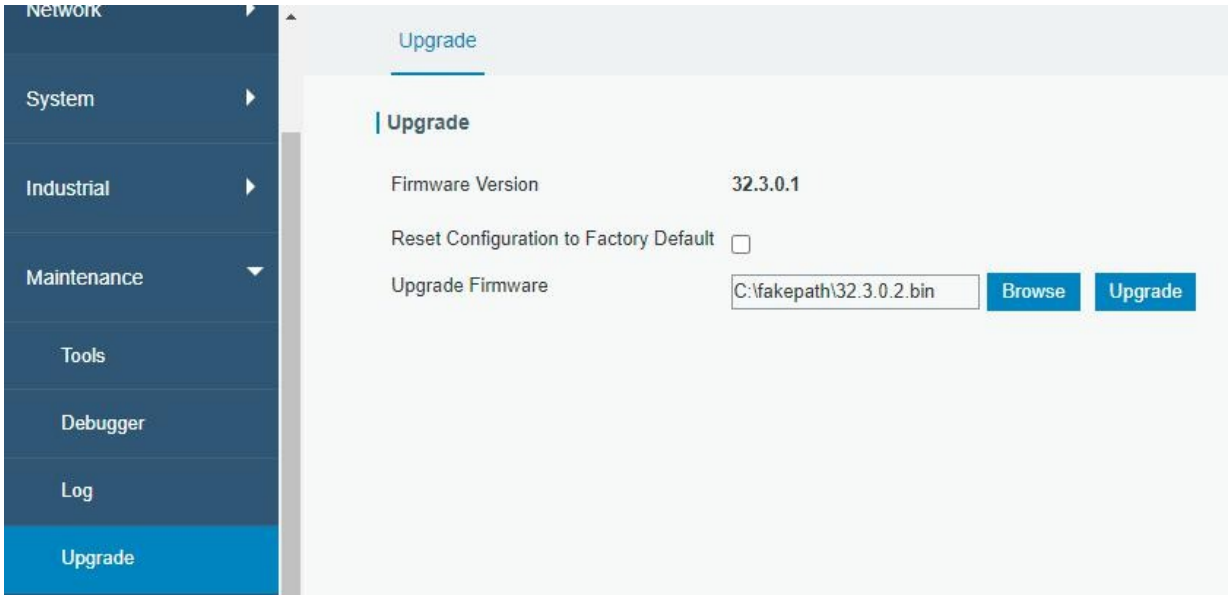
SYSTEM-LED	Maßnahme
Blinkt	Halten Sie die Reset-Taste länger als 5 Sekunden gedrückt.
Statisch grün → Schnell blinkend	Lassen Sie die Taste los und warten Sie.
Aus → Blinkt	Der Router ist nun auf die Werkseinstellungen zurückgesetzt.

4.2 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 > Aktualisieren“.
2. Klicken Sie auf „Durchsuchen“ und wählen Sie die richtige Firmware-Datei auf Ihrem PC aus.
3. 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

Aktualisierung

4.3 Ereignisse Anwendungsbeispiel

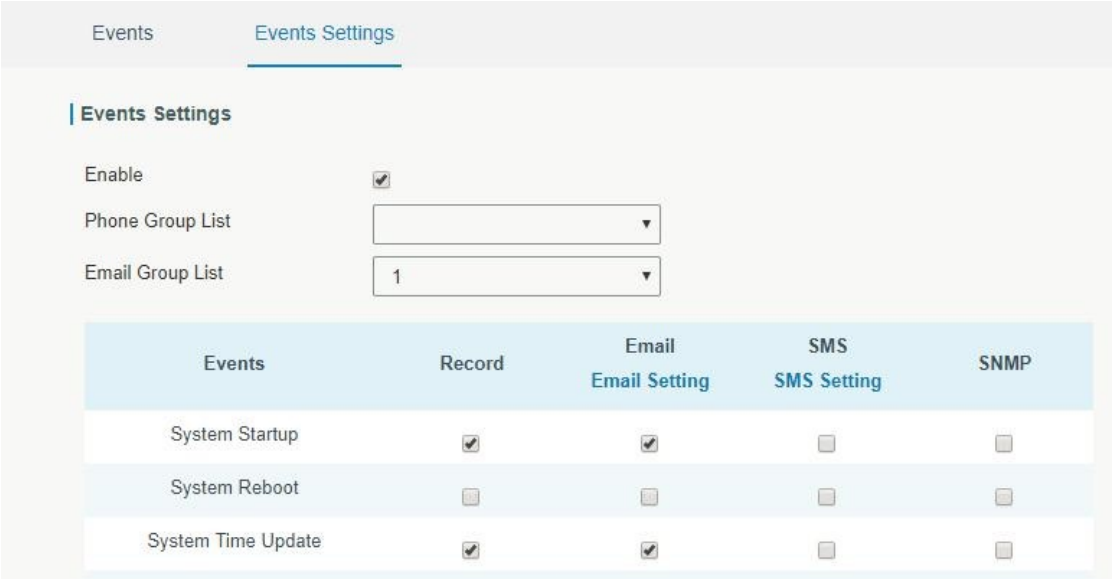
Beispiel

In diesem Abschnitt wird ein Beispiel für das Senden von Alarmmeldungen per E-Mail bei Auftreten der folgenden Ereignisse und das Aufzeichnen der Ereignisalarme in der Web-GUI vorgestellt.

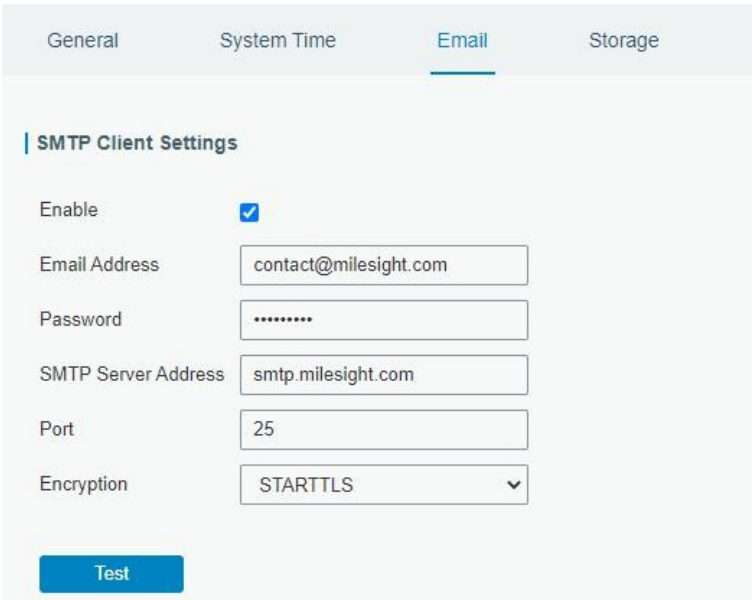
Ereignisse	Maßnahmen zur Auslösung von Ereignissen (zu Testzwecken)
Router-System starten.	Stromversorgung des Routers anschließen.
Aktualisierung der Systemzeit des Routers.	Systemzeit manuell einstellen.

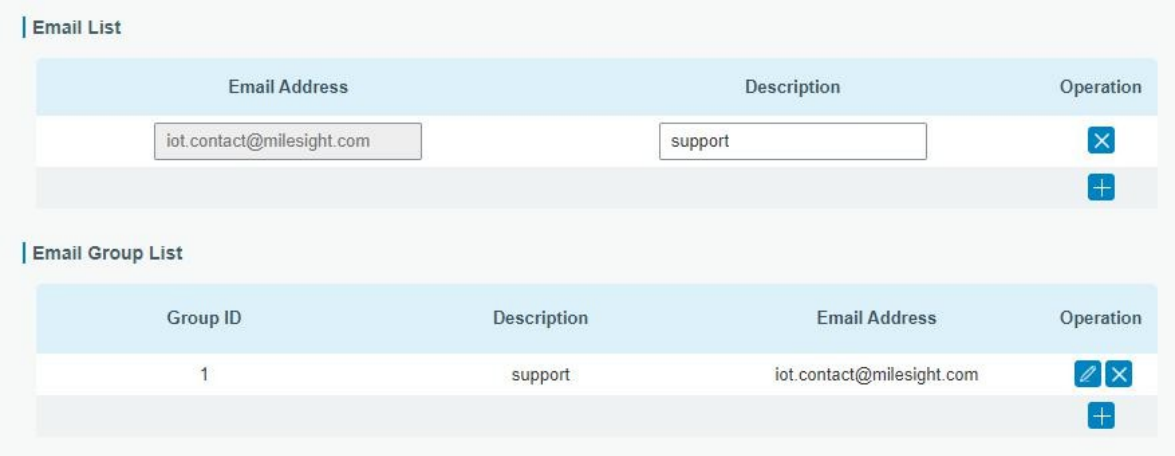
Konfigurationsschritte

1. Gehen Sie zu „System > Ereignisse > Ereigniseinstellungen“ und aktivieren Sie die Ereigniseinstellungen.
2. Überprüfen Sie die entsprechenden Ereignisse für die Aufzeichnung und E-Mail-Alarme und klicken Sie dann wie unten gezeigt auf die Schaltfläche „Speichern“.

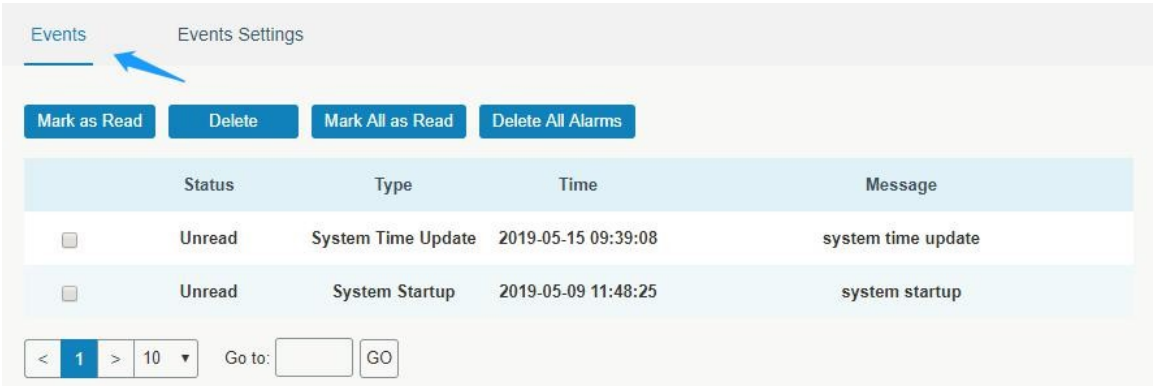


3. Konfigurieren Sie die entsprechenden Parameter, einschließlich der Einstellungen für den E-Mail-Versand und der E-Mail-Gruppen, wie unten beschrieben. Klicken Sie auf „Speichern“ und „Übernehmen“, damit die Änderungen wirksam werden.





4. Um die Funktionalität des Alarms zu testen, führen Sie bitte die oben aufgeführten entsprechenden Maßnahmen durch. Bei Auftreten des entsprechenden Ereignisses wird Ihnen eine Alarm-E-Mail gesendet.
Aktualisieren Sie die Web-GUI, gehen Sie zu „Ereignisse > Ereignisse“ und Sie finden die Ereignisaufzeichnungen.



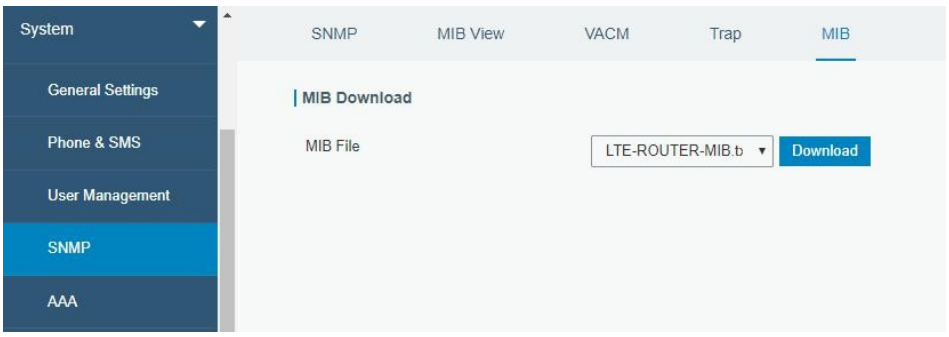
Verwandte Themen

Ereignis-E-Mail-Einstellungen

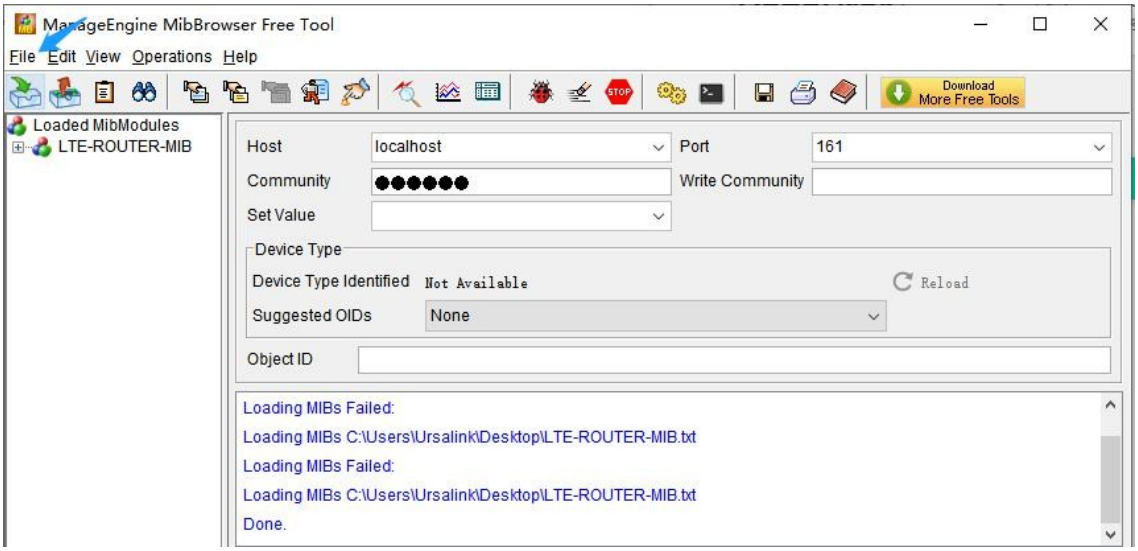
4.4 SNMP-Anwendungsbeispiel

Bevor Sie die SNMP-Parameter konfigurieren, laden Sie bitte zunächst die entsprechende „MIB“-Datei aus der WEB-GUI des UR32L herunter und laden Sie sie dann in eine beliebige Software oder ein Tool hoch, das das Standard-SNMP-Protokoll unterstützt. Hier verwenden wir als Beispiel das „ManageEngine MibBrowser Free Tool“, um auf den Router zuzugreifen und Mobilfunkdaten abzufragen.

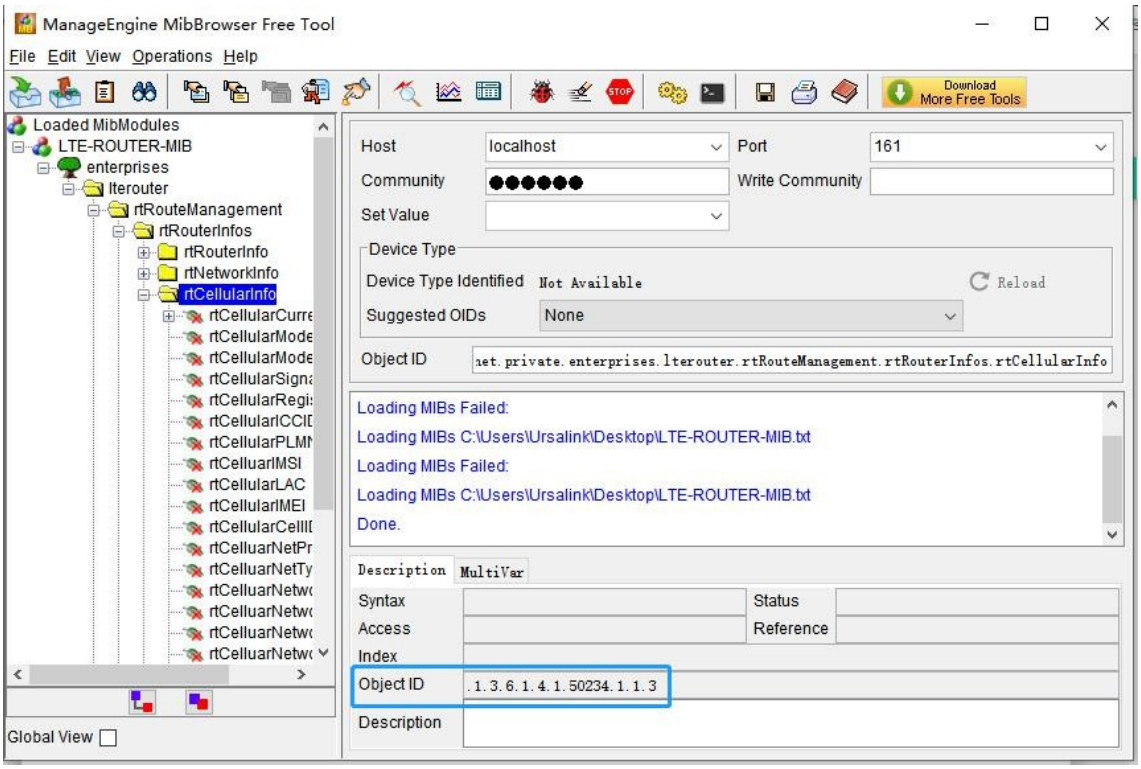
1. Gehen Sie zu „System > SNMP > MIB“ und laden Sie die MIB-Datei „LTE-ROUTER-MIB.txt“ auf den PC herunter.



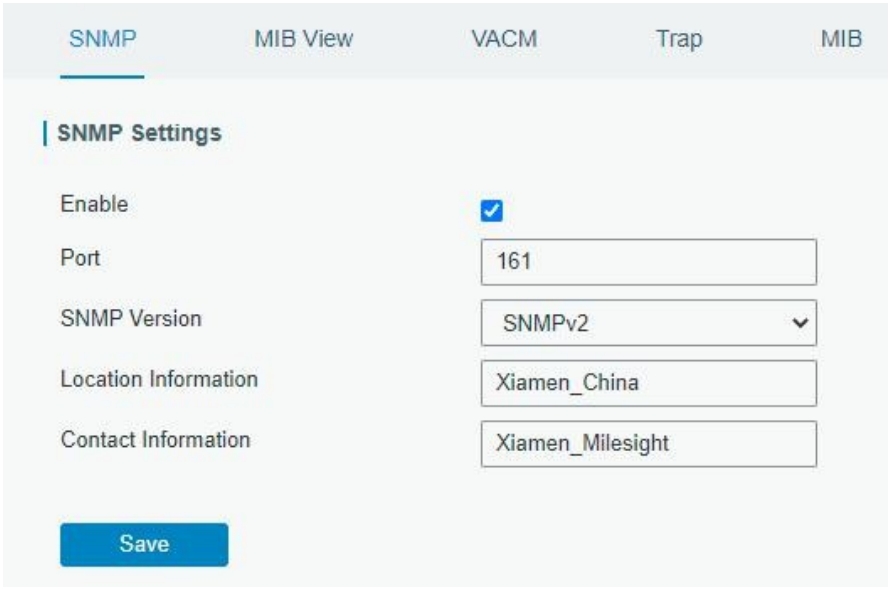
2. Starten Sie „ManageEngine MibBrowser Free Tool“ auf dem PC. Klicken Sie in der Menüleiste auf „Datei > MIB laden“. Wählen Sie dann die Datei „LTE-ROUTER-MIB.txt“ vom PC aus und laden Sie sie in die Software hoch.



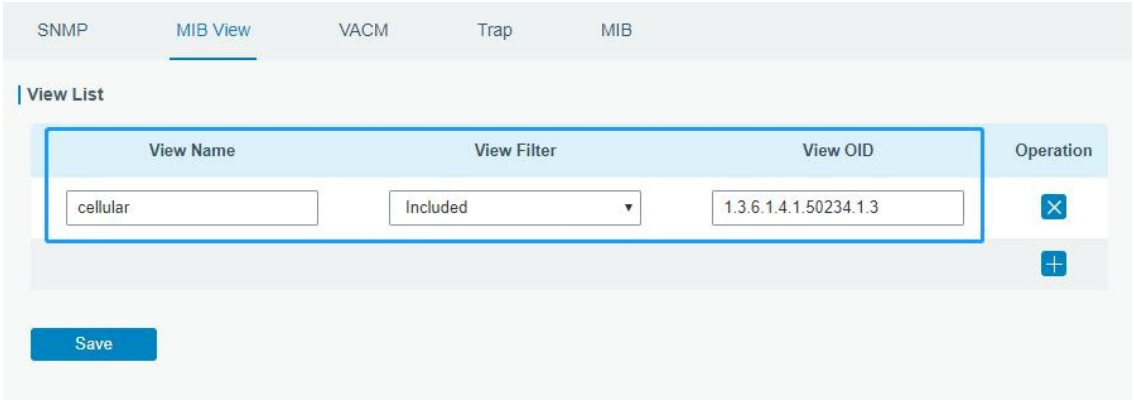
Klicken Sie auf die Schaltfläche „+“ neben „LTE-ROUTER-MIB“ im Menü „Loaded MibModules“ und suchen Sie „usCellularinfo“. Daraufhin wird die OID der Mobilfunkdaten „.1.3.6.1.4.1.50234“ angezeigt, die in die MIB-Ansichtseinstellungen eingegeben wird.



3. Gehen Sie in der WEB-GUI des Routers zu „System > SNMP > SNMP“. Aktivieren Sie die Option „Enable“ und klicken Sie dann auf die Schaltfläche „Save“.

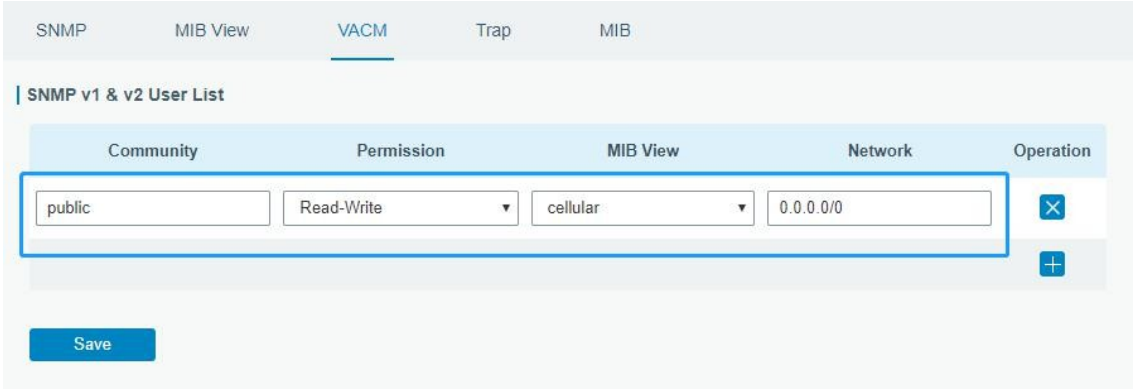


4. Gehen Sie zu „System > SNMP > MIB View“. Klicken Sie auf „ “ , um eine neue MIB-Ansicht hinzuzufügen und die Ansicht zu definieren, auf die von außerhalb des Netzwerks zugegriffen werden



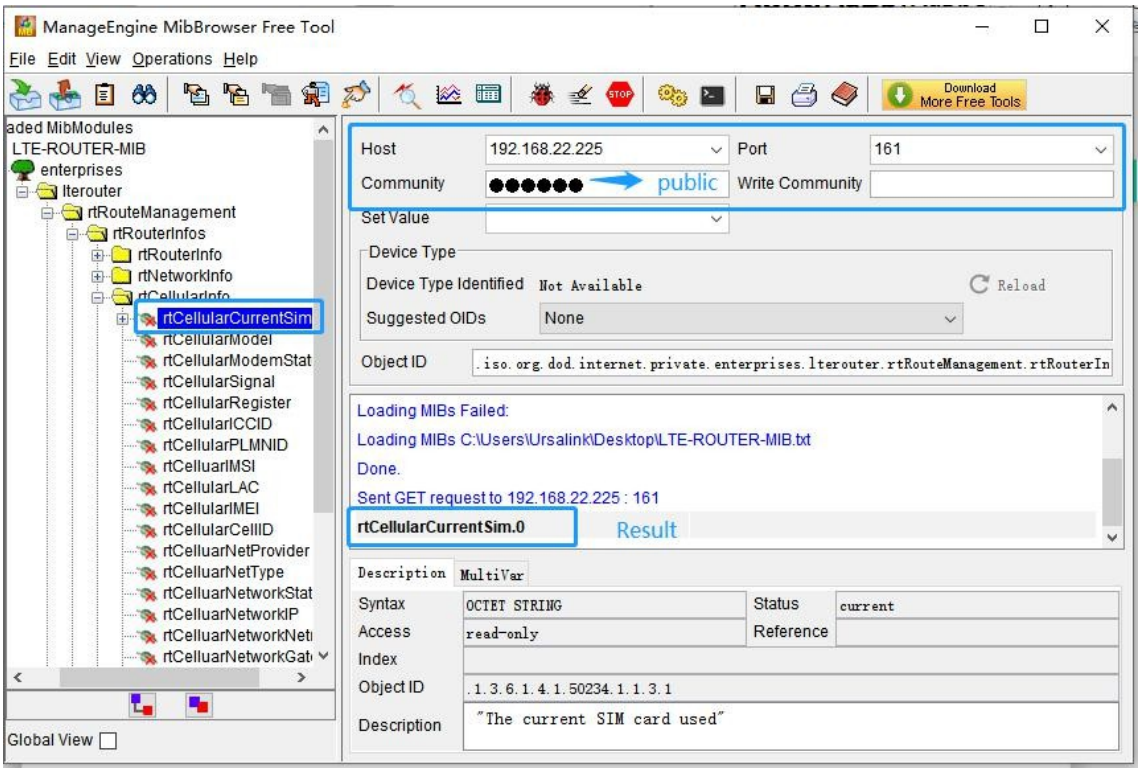
soll. Klicken Sie anschließend auf die Schaltfläche „Save“.

5. Gehen Sie zu „System > SNMP > VACM“. Klicken Sie auf „ “ , um eine neue VACM-Einstellung hinzuzufügen und die Zugriffsberechtigung für die angegebene Ansicht vom angegebenen externen Netzwerk aus zu definieren. Klicken Sie auf „Save“ und „Apply“, um die Änderungen zu übernehmen.



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 dann auf „FET". Daraufhin werden die aktuellen SIM-Informationen im Ergebnisfeld angezeigt. Auf die gleiche Weise können Sie auch andere Mobilfunkdaten abrufen.



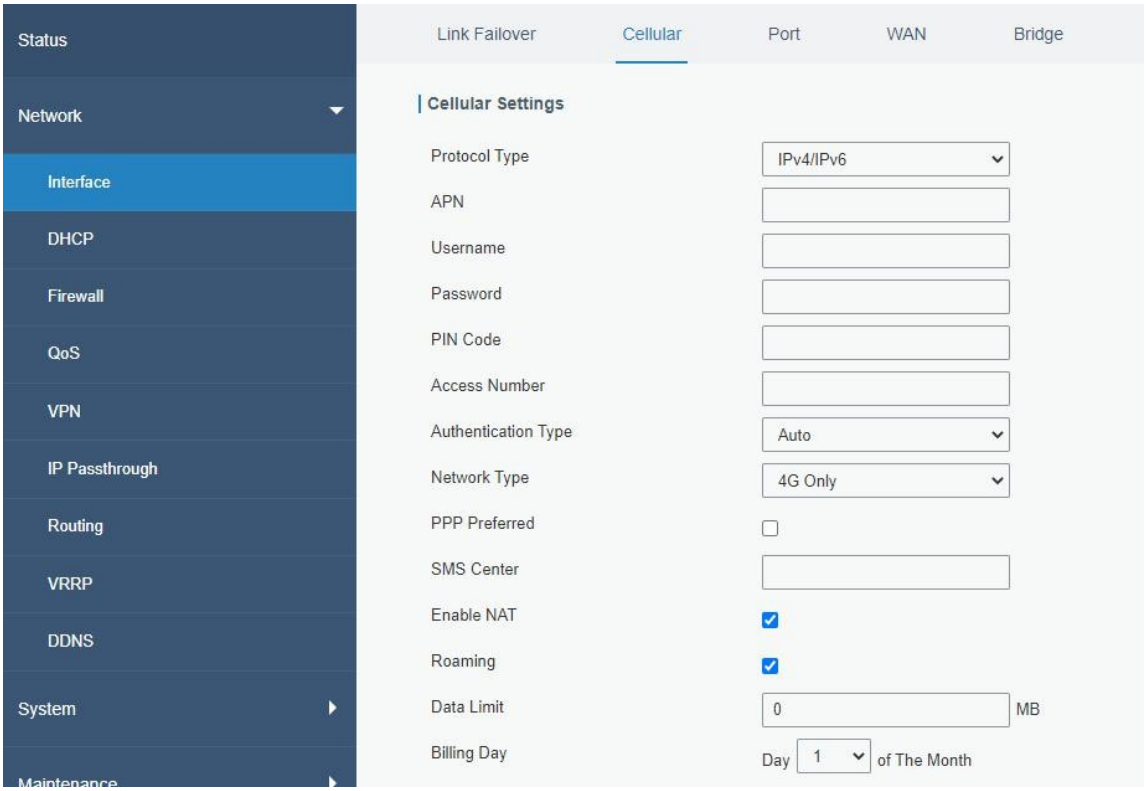
Verwandtes Thema

SNMP

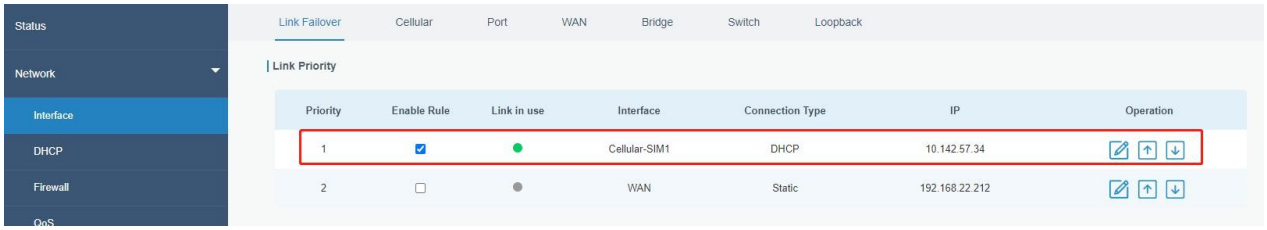
4.5 Netzwerkverbindung

4.5.1 Mobilfunkverbindung

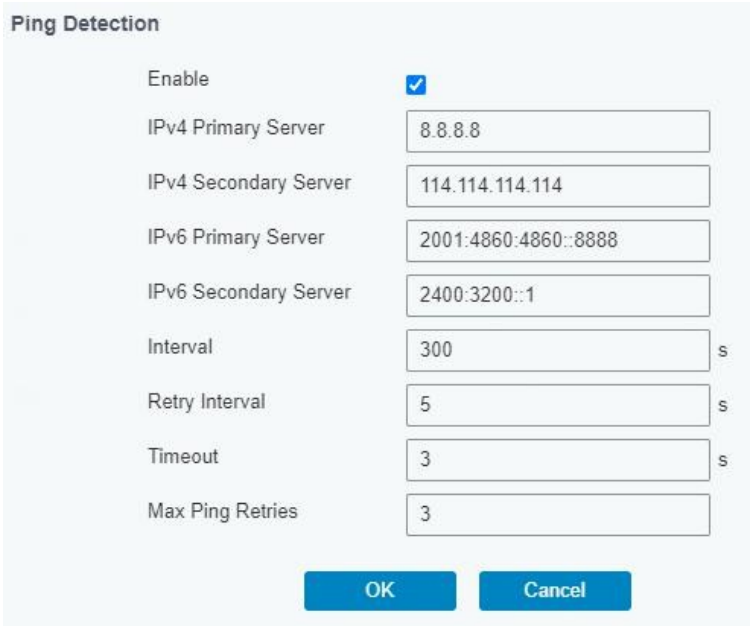
1. Gehen Sie zu „Netzwerk > Schnittstelle > Mobilfunk > Mobilfunkeinstellungen" und konfigurieren Sie die Mobilfunkdaten. Klicken Sie anschließend auf „Speichern" und „Übernehmen", damit die Konfiguration wirksam wird.



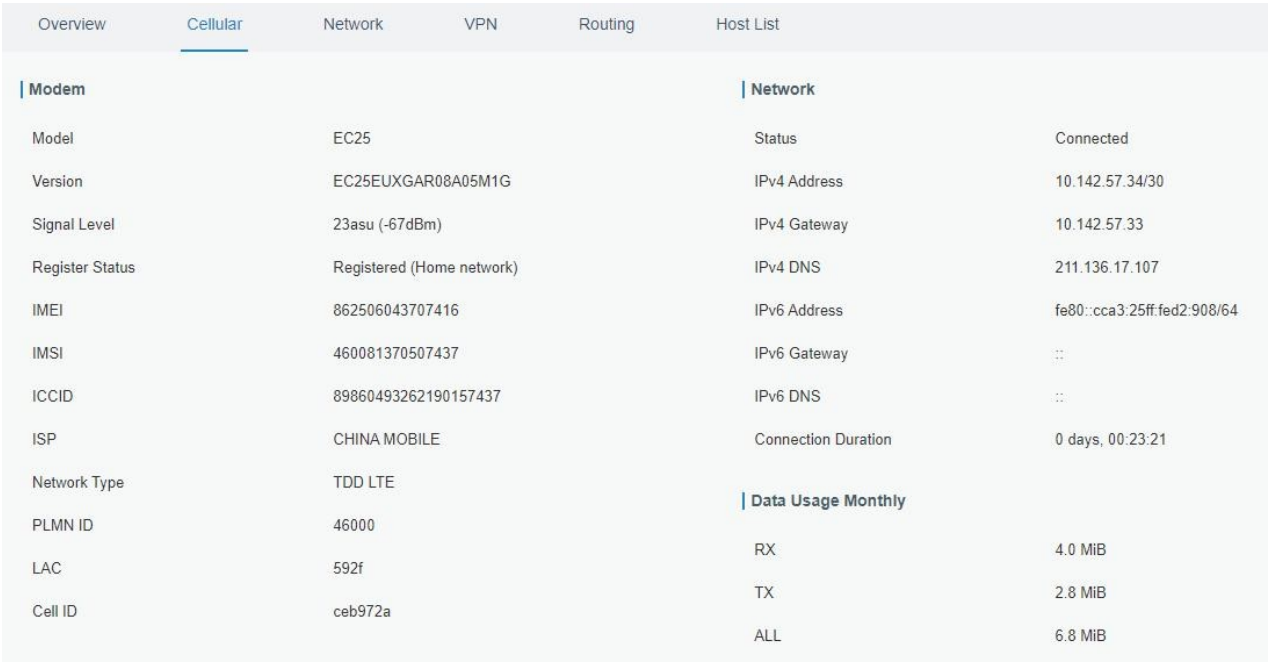
2. Gehen Sie zu „Netzwerk > Schnittstelle > Link-Failover“, um die Mobilfunkschnittstelle zu aktivieren und die Link-Priorität zu ändern.



3. Klicken Sie auf „ “ , um die ICMP-Ping-Erkennungsinformationen zu konfigurieren.



4. Überprüfen Sie den Status der Mobilfunkverbindung über die WEB-GUI des Routers.
Klicken Sie auf „Status > Mobilfunk“, um den Status der Mobilfunkverbindung anzuzeigen. Wenn „Verbunden“ angezeigt wird, hat die SIM-Karte erfolgreich eine Verbindung hergestellt.



5. Überprüfen Sie mit dem Browser Ihres PCs, ob das Netzwerk ordnungsgemäß funktioniert.
Öffnen Sie Ihren bevorzugten Browser auf dem PC, geben Sie eine beliebige verfügbare Webadresse in die Adressleiste ein und prüfen Sie, ob Sie über den UR32L-Router auf das Internet zugreifen können.

Verwandtes

Thema Mobilfunk-Einstellungen
Mobilfunk-Status

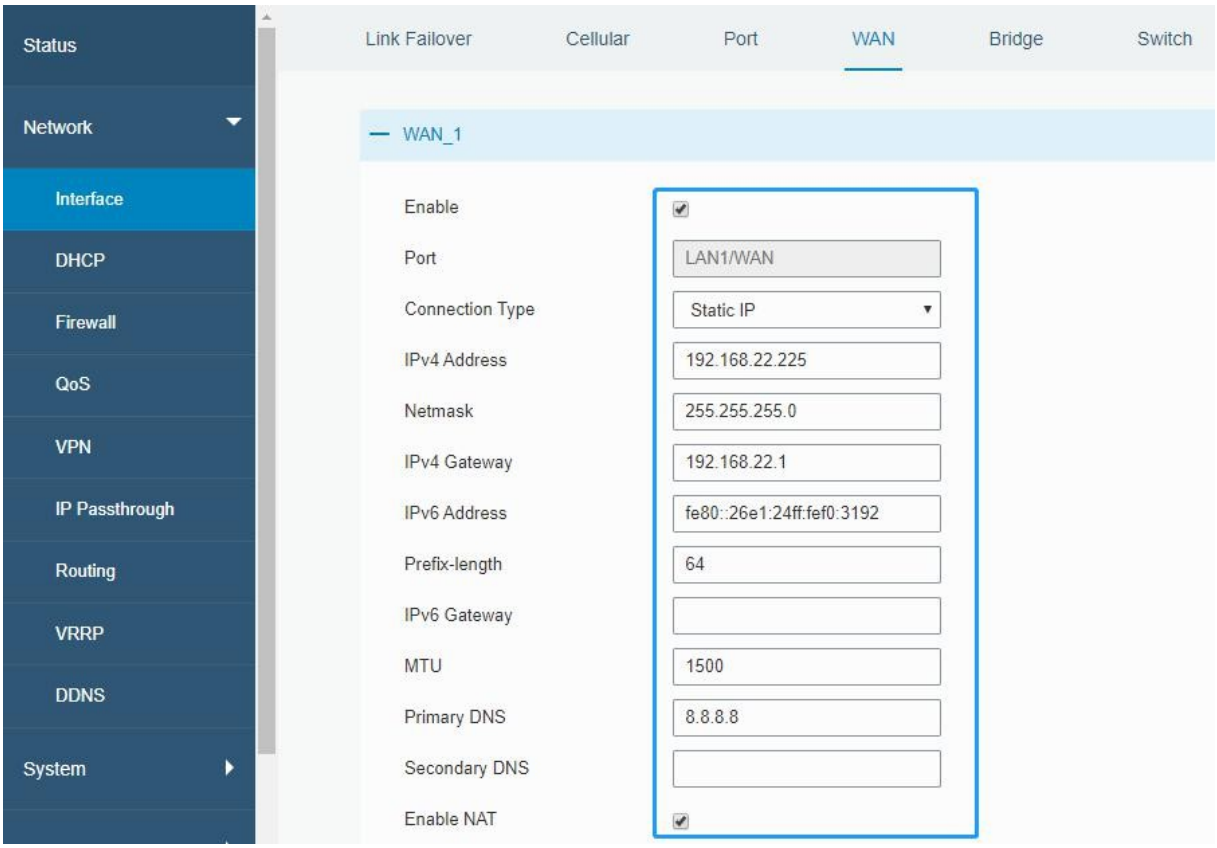
4.5.2 Beispiel für eine Ethernet-WAN-Verbindung

Der WAN-Port des UR32L ist über ein Ethernet-Kabel mit dem Internet verbunden.

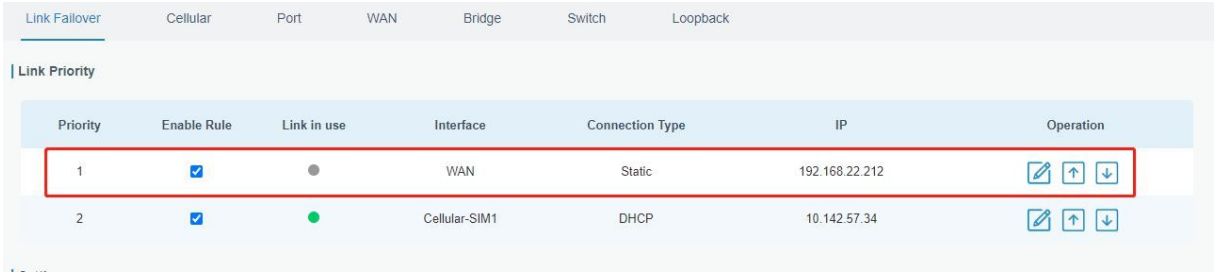
Konfigurationsschritte

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

Hinweis: Wenn Sie den PPPoE-Typ auswählen, überprüfen Sie bitte den „Benutzernamen“ und das „Passwort“ bei Ihrem lokalen Internetdienstanbieter. Klicken Sie auf die Schaltfläche „Speichern und übernehmen“, damit die Änderungen wirksam werden.



2. Gehen Sie zu „Netzwerk > Schnittstelle > Link-Failover“, um die WAN-Priorität auf 1 zu ändern.



Verwandtes Thema [WAN-Einstellung](#) [WAN-Status](#)

4.6 VRRP-Anwendungsbeispiel

Anwendungsbeispiel

Ein Webserver benötigt einen Internetzugang über den UR32L-Router. Um Datenverluste aufgrund eines Routerausfalls zu vermeiden, können zwei UR32L-Router als VRRP-Backup-Gruppe eingesetzt werden, um die Netzwerkzuverlässigkeit zu verbessern.

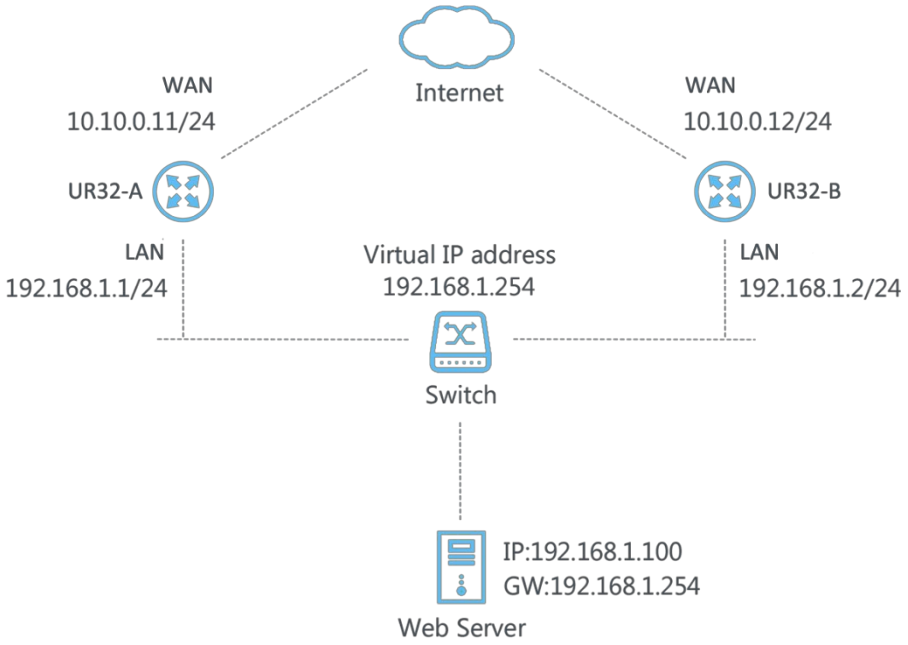
VRRP-Gruppe:

Die WAN-Ports des UR32L-Routers A und des Routers B sind über ein kabelgebundenes Netzwerk mit dem Internet verbunden. Die LAN-Ports dieser Router sind mit einem Switch verbunden.

Die virtuelle IP lautet 192.168.1.254/24.

UR32L Router	Virtuelle Router-ID (gleich für A und B)	Anschluss verbunden mit Switch	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.



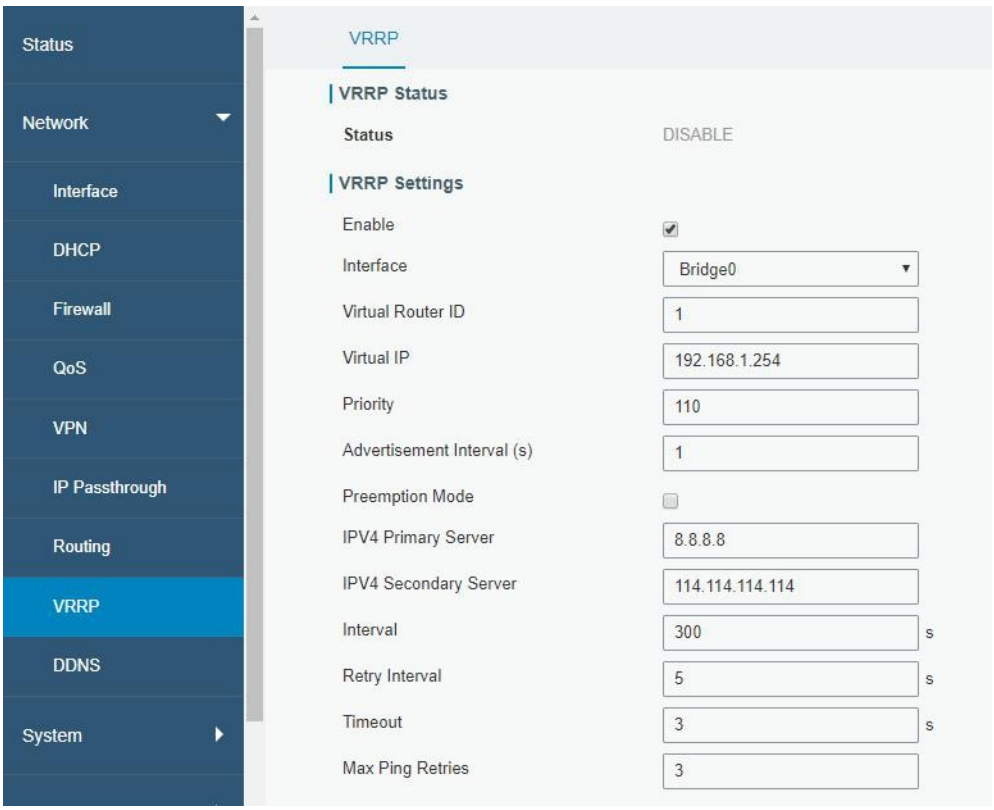
Konfigurationsschritte

Konfiguration von Router

A

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

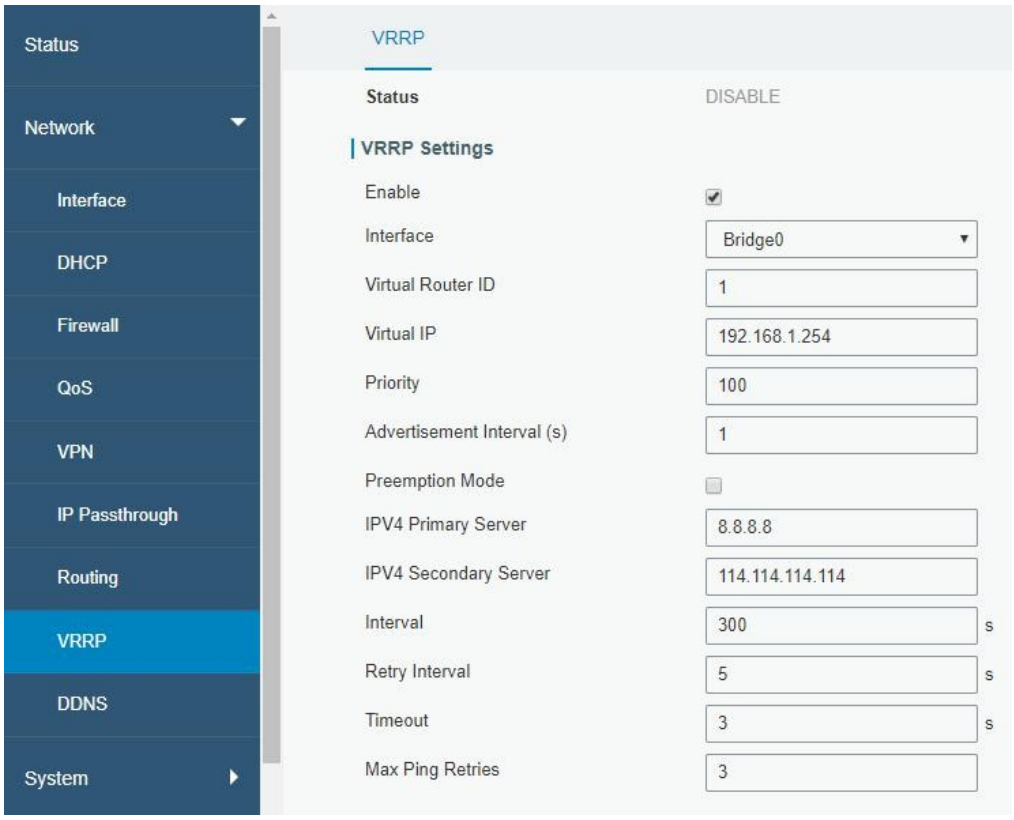
2. Gehen Sie zu „Netzwerk > VRRP > VRRP“ und konfigurieren Sie die VRRP-Parameter wie unten angegeben.



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 eine Störung aufweist, 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, sobald Router A wieder auf das Internet zugreifen kann.

Verwandte Themen

VRRP-Einstellung

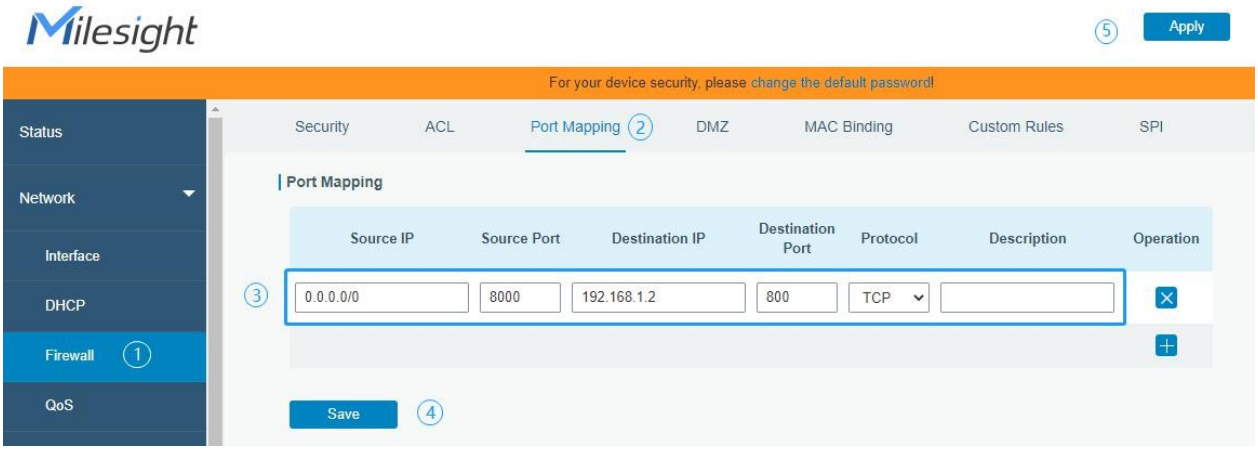
4.7 NAT-Anwendungsbeispiel

Beispiel

Ein UR32L-Router kann über Mobilfunk auf das Internet zugreifen. Der LAN-Port ist mit einem Webserver verbunden, dessen IP-Adresse 192.168.1.2 und dessen Port 8000 ist. Konfigurieren Sie den Router so, dass das öffentliche Netzwerk auf den Server zugreifen kann.

Konfigurationsschritte

Gehen Sie zu „Firewall > Portzuordnung“ und konfigurieren Sie die Parameter für die Portzuordnung.



Klicken Sie auf „Speichern“ und „Übernehmen“.

Verwandtes Thema

Portzuordnung

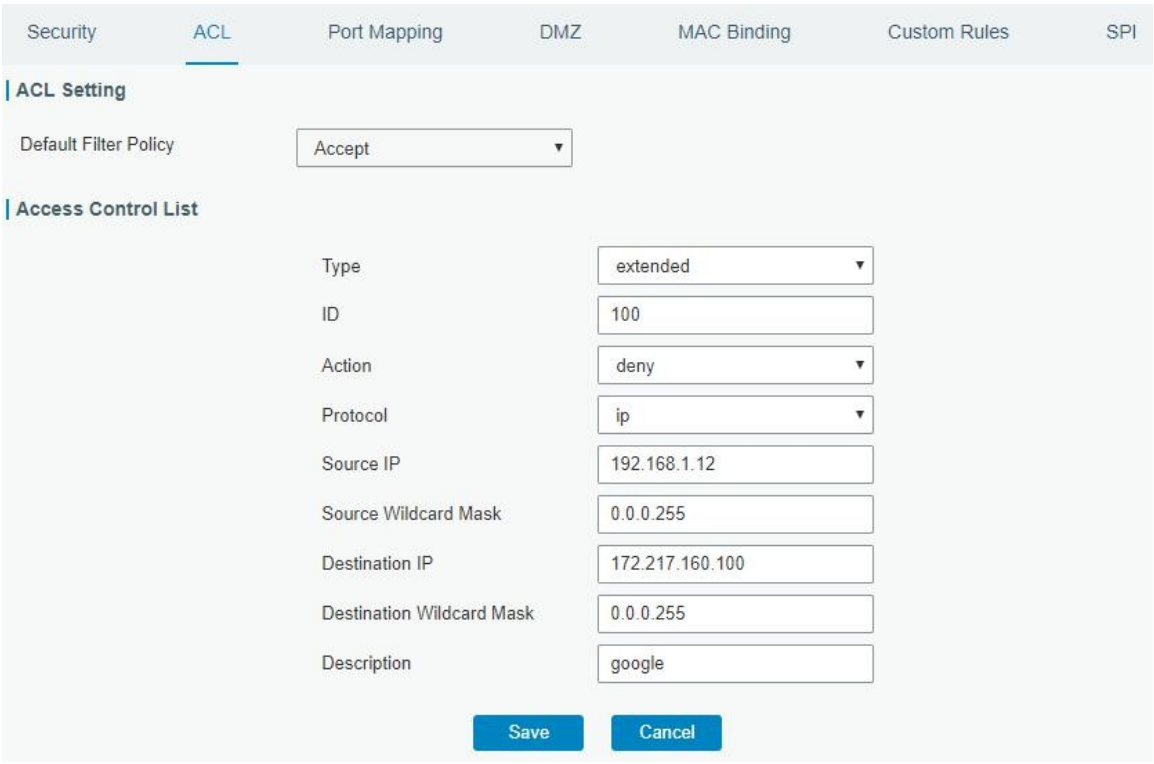
4.8 Beispiel für eine Zugriffskontrollanwendung

Anwendungsbeispiel

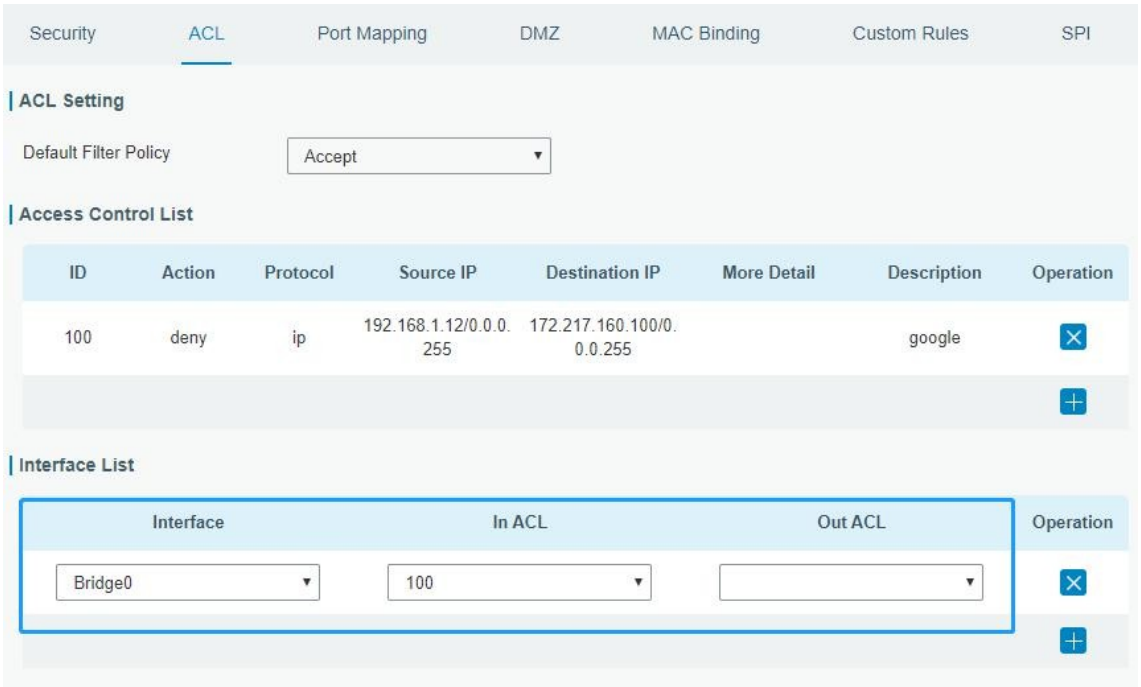
Der LAN-Port des UR32L ist mit der IP-Adresse 192.168.1.0/24 konfiguriert. Konfigurieren Sie dann den Router so, dass der Zugriff auf die Google-IP-Adresse 172.217.160.100 von einem lokalen Gerät mit der IP-Adresse 192.168.1.12 aus verweigert wird.

Konfigurationsschritte

1. Gehen Sie zu „Netzwerk > Firewall > ACL“, um die Zugriffskontrollliste zu konfigurieren. Klicken Sie auf die Schaltfläche „ “, um die folgenden Parameter festzulegen. Klicken Sie anschließend auf die Schaltfläche „Speichern“.



2. Konfigurieren Sie die Schnittstellenliste. Klicken Sie anschließend auf „Speichern“ und „Übernehmen“.



Verwandtes Thema

ACL

4.9 QoS-Anwendungsbeispiel

Beispiel

Konfigurieren Sie den UR32L-Router so, dass er lokale Präferenzen 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 Mobilfunkschnittstelle.

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. Suchen Sie die Option „Service Category“ (Dienstkategorie) und klicken Sie auf „ “ (Dienstkategorien), um Dienstklassen einzurichten. Hinweis: Die Prozentsätze müssen zusammen 100 % ergeben.

3. Suchen Sie die Option „Service Category Rules“ (Dienstkategorieregeln) und klicken Sie auf „ “ (Neue Regel hinzufügen), um Regeln einzurichten.

Hinweis:

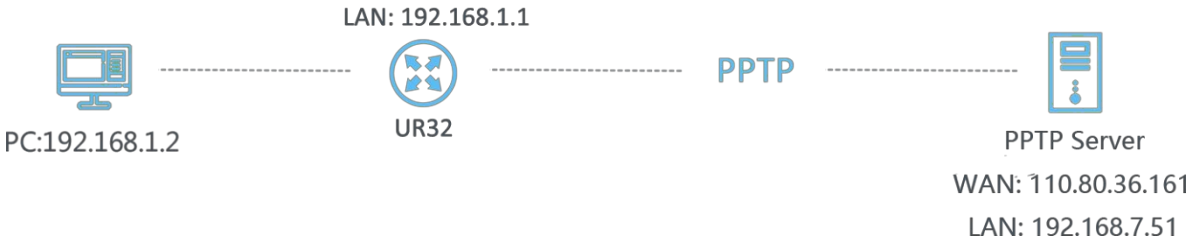
IP/Port: null bezieht sich auf jede IP-Adresse/jeden Port. Klicken Sie auf die Schaltflächen „Save“ (Speichern) und „Apply“ (Anwenden).

Verwandtes Thema

QoS-Einstellung

4.10 PPTP-Anwendungsbeispiel

Beispiel

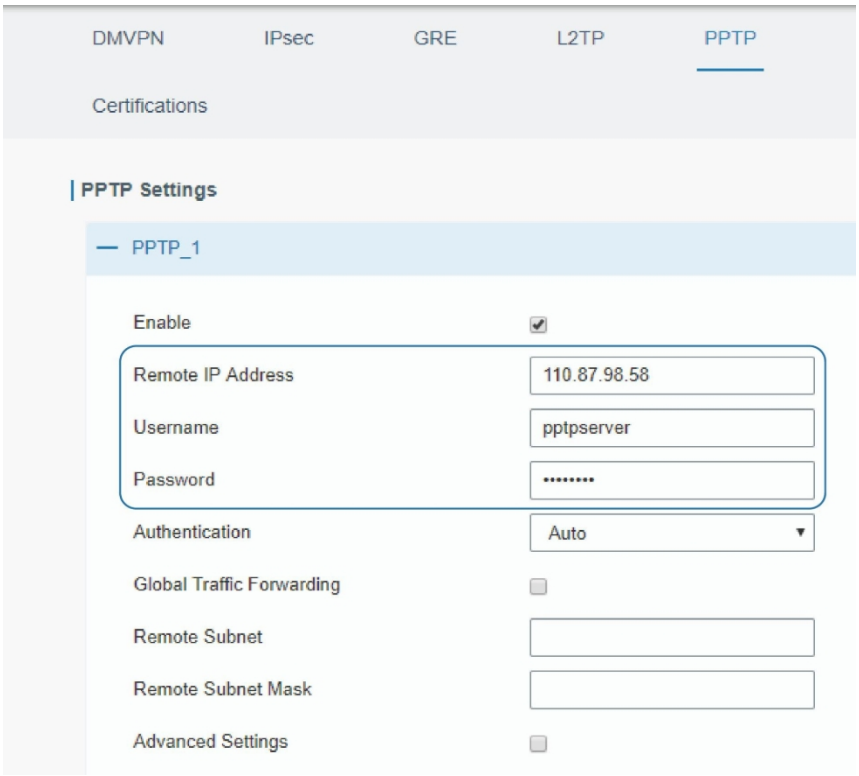


Konfigurieren Sie den UR32L als PPTP-Client, um eine Verbindung zu einem PPTP-Server herzustellen und Daten sicher zu übertragen. Beachten Sie dazu die folgende Topologiegrafik.

Konfigurationsschritte

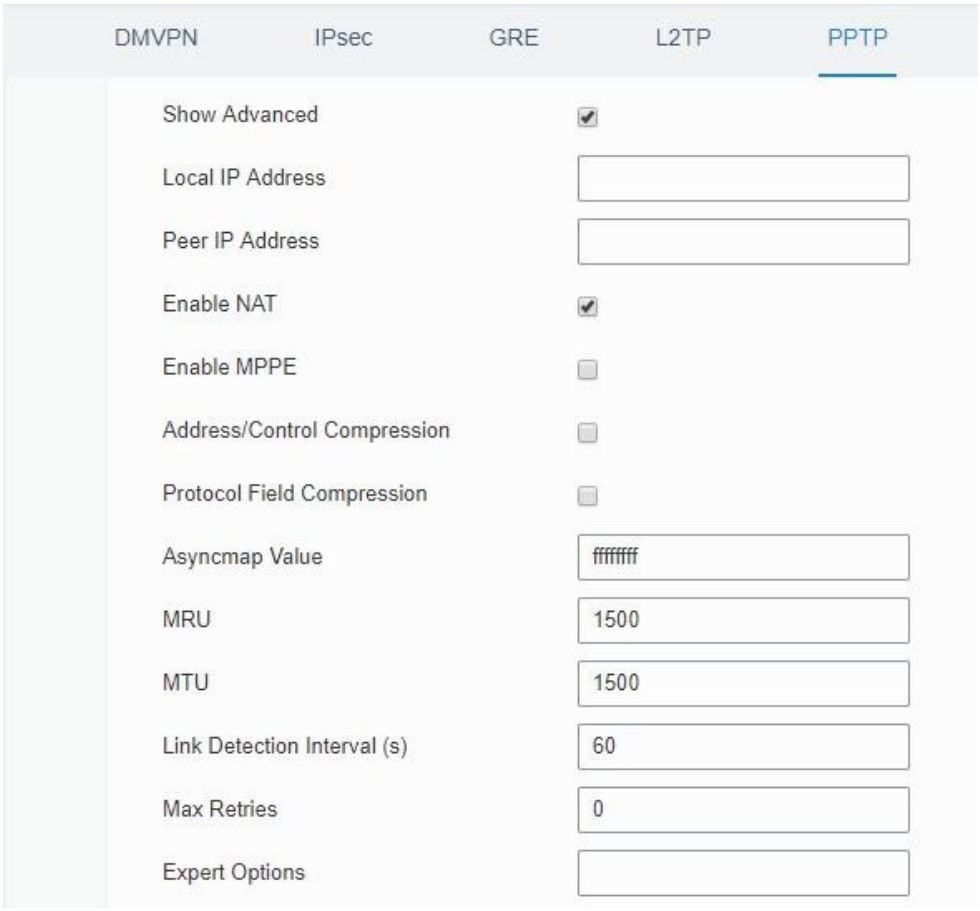
1. Gehen Sie zu „Netzwerk > VPN > PPTP“ und konfigurieren Sie die IP-Adresse des PPTP-Servers, den Benutzernamen und das Passwort, die vom PPTP-Server bereitgestellt werden.

Hinweis: Wenn Sie möchten, dass alle Daten über den VPN-Tunnel übertragen werden, aktivieren Sie die Option „Globale Datenweiterleitung“.



Wenn Sie auf ein Peer-Subnetz wie 192.168.3.0/24 zugreifen möchten, müssen Sie das Subnetz und die Maske konfigurieren, um die Route hinzuzufügen.

2. Aktivieren Sie die Option „Show Advanced“ (Erweitert anzeigen), um die erweiterten Einstellungen anzuzeigen.



Wenn der PPTP-Server eine MPPE-Verschlüsselung erfordert, müssen Sie die Option „MPPE aktivieren“ aktivieren.

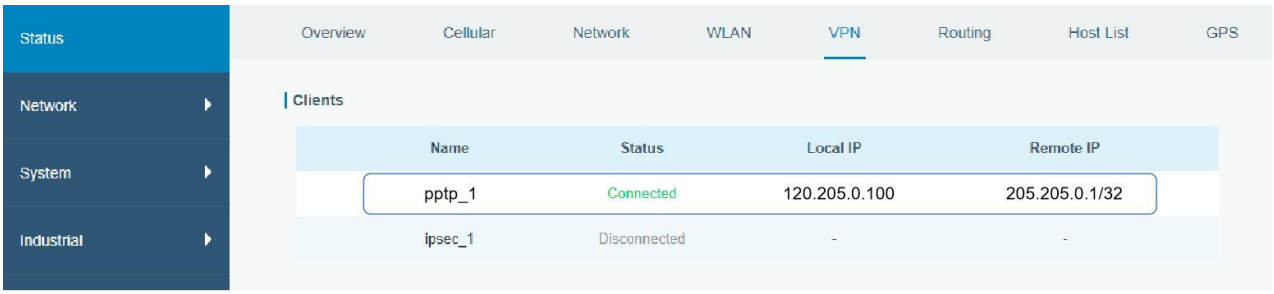
Wenn der PPTP-Server dem Client eine feste Tunnel-IP zuweist, können Sie die lokale Tunnel-IP und die entfernte Tunnel-IP wie unten gezeigt eingeben.

Andernfalls weist der PPTP-Server die Tunnel-IP-Adresse nach dem Zufallsprinzip zu.

Klicken Sie auf die Schaltfläche „Speichern“, wenn Sie alle Einstellungen vorgenommen haben. Daraufhin werden die erweiterten Einstellungen wieder ausgeblendet. Klicken Sie anschließend auf die Schaltfläche „Übernehmen“, damit die Konfigurationen wirksam werden.

3. Gehen Sie zu „Status > VPN“ und überprüfen Sie den PPTP-Verbindungsstatus. PPTP wird wie unten gezeigt hergestellt.

Lokale IP: Die IP-Adresse des Client-Tunnels. Remote-IP: Die IP-Adresse des Server-Tunnels.



Verwandte Themen

PPTP-Einstellungen

PPTP-Status

[ENDE]