

Industrieller Router Ultra-Serie UR75

Benutzerhandbuch



Sicherheitshinweise

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

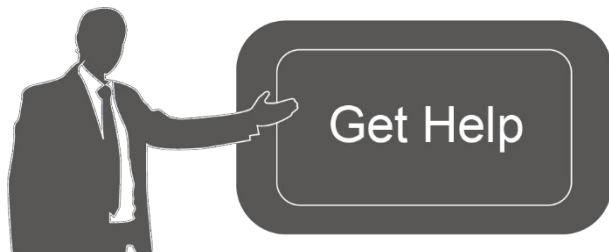
- ❖ Das Gerät darf in keiner Weise zerlegt oder umgebaut werden.
- ❖ Um die Gefahr von Bränden und Stromschlägen zu vermeiden, halten Sie das Produkt vor der Installation von Regen und Feuchtigkeit fern.
- ❖ Stellen Sie das Gerät nicht an Orten auf, an denen die Temperatur oder Luftfeuchtigkeit unterhalb/oberhalb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

© 2011-2024 Xiamen Milesight IoT Co., Ltd. Alle Rechte vorbehalten.

Alle Informationen in dieser Bedienungsanleitung sind urheberrechtlich geschützt. Daher darf keine Organisation oder Einzelperson Es ist untersagt, diese Bedienungsanleitung ohne schriftliche Genehmigung von Xiamen Milesight IoT Co., Ltd. ganz oder teilweise zu kopieren oder zu reproduzieren.

Konformitätserklärung

UR75 entspricht den grundlegenden Anforderungen und anderen relevanten Bestimmungen der CE- und RoHS-Richtlinien.



Für Unterstützung wenden Sie sich bitte an den technischen Support von Milesight:

E-Mail: iot.support@milesight.com Support-Portal: support.milesight-iot.com Tel.: 86-592-5085280

Fax: 86-592-5023065

Adresse: Gebäude C09, Software Park III, Xiamen 361024, China

Revisionsverlauf

Datum	Dokumentversion	Beschreibung
25. November 2022	V 3.0	Erstversion basierend auf Hardware 3.x
17. Januar 2023	V 3.1	1. Änderung des Web-GUI-Designs 2. LT2P- und PPTP-VPN-Client-Funktion hinzufügen 3. VLAN-Funktion hinzufügen 4. HTTPS-Zertifikat-Importfunktion hinzufügen
20. April 2024	V 3.2	1. Node-RED-, DDNS-, IP-Passthrough-, SMS- und SNMP-Funktion hinzufügen 2. Umbenennung von Modbus Master in Modbus Client 3. Unterstützung für benutzerdefinierte Mobilfunk-MTU, IMS und SMS-Zentralnummer 4. Hinzufügen der NAT-Option auf WAN- und Mobilfunk-Schnittstellen 5. Unterstützung für die Anpassung des AT-Debug-Befehls 6. Unterstützung für Hard-Reset
20. September 2024	V3.3	1. Hinzufügen des WLAN-Client-Modus und Unterstützung für die Konfiguration des WLAN-Ländercodes; 2. WLAN-Statusseite hinzufügen; 3. Funktion zum Zurücksetzen der Verbindung mit hoher Priorität bei zwei Karten hinzufügen; 4. MQTT-Ereignisalarm und Multi-User-Funktion hinzufügen; 5. Anpassen des Systemmenüs.

Inhalt

Kapitel 1 Produktvorstellung.....	7
1.1 Übersicht.....	7
1.2 Vorteile.....	7
Kapitel 2 Hardware-Einführung.....	8
2.1 Packliste.....	8
2.2 Hardware-Übersicht.....	9
2.3 Serielle & IO- & Stromversorgungs-Pinbelegungen.....	10
2.4 LED-Anzeigen.....	10
2.5 Abmessungen (mm).....	11
2.6 Reset-Taste.....	11
Kapitel 3 Hardware-Installation.....	11
3.1 SIM-Installation.....	11
3.2 Antenneninstallation.....	12
3.3 Geräteinstallation.....	12
3.4 Installation der Schutzterdung.....	12
Kapitel 4 Zugriff auf die Web-GUI.....	13
Kapitel 5 Anwendungsbeispiele.....	15
5.1 Mobilfunkverbindung konfigurieren.....	15
5.2 Ethernet-Verbindung konfigurieren.....	17
5.3 WLAN-Zugangspunkt konfigurieren.....	19
5.4 OpenVPN-Client konfigurieren.....	20
5.6 Serielle DTU-Verbindung konfigurieren.....	22
5.5 NAT-Regel konfigurieren.....	25
5.7 Werkseinstellungen wiederherstellen.....	26
5.8 Firmware-Upgrade.....	27
Kapitel 6 Webkonfiguration.....	28
6.1 Status.....	28
6.1.1 Übersicht.....	28
6.1.2 Mobilfunk.....	30
6.1.3 WLAN.....	33
6.1.4 GPS.....	34
6.1.5 Firewall.....	35
6.1.6 Routing-Tabelle.....	36
6.1.7 VPN.....	37
6.2 Netzwerk.....	37
6.2.1 Schnittstellen.....	37
6.2.1.1 WAN.....	38
6.2.1.2 LAN/DHCP-Server.....	41
6.2.1.3 Mobilfunk.....	44
6.2.1.4 Schnittstelleneinstellungen.....	45
6.2.1.5 Link-Failover.....	46
6.2.1.6 Switch (VLAN).....	48
6.2.1.7 Zuweisung einer statischen IP-Adresse.....	49

6.2.2	WLAN	50
6.2.2.1	WLAN	50
6.2.2.2	Erweiterte Einstellungen	52
6.2.3	Firewall	53
6.2.3.1	Allgemeine Einstellungen	53
6.2.3.2	ACL	54
6.2.3.3	Portzuordnung (DNAT)	56
6.2.3.4	DMZ	56
6.2.3.5	Benutzerdefinierte Regeln	57
6.2.3.6	Zertifikate	57
6.2.4	Statische Routen	57
6.2.5	IP-Passthrough	58
6.2.6	DDNS	58
6.2.7	Diagnose	59
6.3	VPN	60
6.3.1	OpenVPN	60
6.3.1.1	OpenVPN-Server	60
6.3.1.2	OpenVPN-Client	63
6.3.1.3	Zertifikat	66
6.3.2	IPsecVPN	67
6.3.2.1	IPSec-Server	67
6.3.2.2	IPSec-Client	70
6.3.2.3	Zertifikat	73
6.3.3	L2TP	74
6.3.4	PPTP	76
6.4	Dienst	77
6.4.1	Serieller Anschluss	77
6.4.2	E/A	81
6.4.2.1	DI	81
6.4.2.2	DO	83
6.4.3	Modbus-Client (Master)	83
6.4.3.1	Modbus-Client	83
6.4.3.2	Kanal	84
6.4.4	GPS	87
6.4.4.1	GPS-IP-Weiterleitung	88
6.4.4.2	GPS-Serienweiterleitung	89
6.4.4.3	GPS-MQTT-Weiterleitung	90
6.4.5	Telefon & SMS	91
6.4.5.1	Telefon	91
6.4.5.2	SMS	92
6.4.6	SNMP	93
6.4.6.1	SNMP	94
6.4.6.2	MIB-Ansicht	94
6.4.6.3	VACM	95
6.4.6.4	Falleinstellungen	95
6.4.6.5	MIB-Download	96

6.4.7	MQTT	96
6.5	App.....	99
6.5.1	Node-RED	99
6.6	System.....	101
6.6.1	Verwaltung.....	102
6.6.1.1	Systemeinstellungen.....	102
6.6.1.2	Benutzereinstellungen.....	103
6.6.1.3	Verwaltung mehrerer Benutzer.....	103
6.6.2	Wartung.....	104
6.6.2.1	Protokoll.....	104
6.6.2.2	Mobilfunk-Debugger	105
6.6.2.3	Firewall-Debugger.....	106
6.6.2.4	Sicherung/Aktualisierung.....	107
6.6.2.5	Neustart.....	107
6.6.3	Ereignisalarm	108
6.6.3.1	Ereignisalarm.....	108
6.6.3.2	Ereigniseinstellungen.....	108
6.6.4	Geräteverwaltung	109
6.6.4.1	Geräteverwaltung	109
6.6.4.2	Cloud-VPN.....	110

Kapitel 1 Produktvorstellung

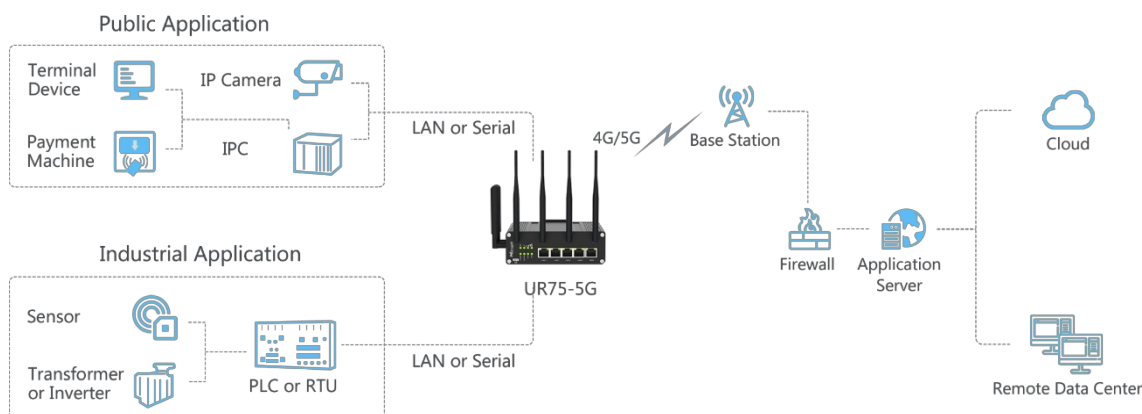
1.1 Übersicht

Der UR75 ist ein industrieller Mobilfunkrouter mit integrierten intelligenten Softwarefunktionen, der für vielfältige M2M/IoT-Anwendungen entwickelt wurde. Der UR75 wurde auf die neueste Mobilfunktechnologie - 5G - aufgerüstet und ermöglicht so einen ultraschnellen Breitbandzugang über ein 5G-Mobilfunknetz.

Dank der Verwendung einer leistungsstarken und stromsparenden CPU in Industriequalität sowie eines Funkmoduls bietet der UR75 ein Netzwerk mit Wire-Speed bei geringem Stromverbrauch und einer extrem kompakten Bauweise, um eine äußerst sichere und zuverlässige Verbindung zum Funknetzwerk zu gewährleisten.

Gleichzeitig unterstützt der UR75 auch Gigabit-Ethernet-Ports, serielle Ports (RS232/RS485) und I/O (Input/Output), wodurch Sie M2M-Anwendungen durch die Kombination von Daten und Videos in begrenzter Zeit und mit begrenztem Budget skalieren können.

Der UR75 eignet sich besonders für intelligente Stromnetze, digitale Medieninstallationen, industrielle Automatisierung, Telemetriegeräte, medizinische Geräte, digitale Fabriken, Finanzwesen, Zahlungsgeräte, Umweltschutz, Wasserwirtschaft und vieles mehr.



1.2 Vorteile

Ultraschnelle Konnektivität

- Industrietaugliche Quad-Core-CPU ARM Cortex-A55 mit großem Speicher, die eine hohe Leistung für die Datenübertragung bietet
- Globales 5G (NSA/SA)/4G LTE-Netzwerk mit zwei SIM-Karten für die Sicherung zwischen mehreren Netzbetreibern
- Dual Carrier Aggregation (2CC CA) wird im 5G Sub-6GHz unterstützt und ermöglicht eine größere Signalabdeckung mit einer hervorragenden Download-Geschwindigkeit von bis zu 4,67 Gbps
- Plug&Play, blitzschnelle Übertragung über Gigabit-Ethernet-Ports oder USB-Typ-C-Schnittstelle

- Unterstützt Wi-Fi 6 und ermöglicht gleichzeitige 2,4G- und 5G-Dualband-Verbindungen mit einer Download-Geschwindigkeit von bis zu 1,8 Gbit/s

Sicherheit und Zuverlässigkeit

- Automatische Failover-/Failback-Sicherung über Ethernet, Mobilfunk (Dual-SIM) und WLAN
- Sichere Übertragung mit VPN-Tunneln wie IPsec/OpenVPN/L2TP/PPTP
- Integrierte Hardware-Überwachung zur automatischen Wiederherstellung nach verschiedenen Ausfällen, wodurch ein Höchstmaß an Verfügbarkeit gewährleistet wird
- Ausgestattet mit mehreren Sicherheitsmaßnahmen wie ACL, DMZ, SYN-Flood-Schutz und Datenfilterung, um die Sicherheit des Netzwerks zu gewährleisten
- Unterstützt Policy Routing und NAT für einen sichereren Intranetzugang

Einfache Wartung

- Milesight DeviceHub ermöglicht eine einfache Einrichtung, Massenkfiguration und zentralisierte Verwaltung von Remote-Geräten
- Das benutzerfreundliche Design der Weboberfläche und mehrere Upgrade-Optionen helfen Administratoren bei der einfachen Verwaltung der Geräte
- Unterstützt mehrstufige Benutzerberechtigungen für die Sicherheitsverwaltung
- Schnelle und benutzerfreundliche Programmierung mit dem Entwicklungstool Node-RED

Industrielles Design

- Breiter Betriebstemperaturbereich von -30 °C bis 60 °C und industrielles Design für raue Umgebungen
- Robustes Gehäuse mit Schutzart IP30, optimiert für die Montage auf DIN-Schienen oder in Regalen.
- Ausgestattet mit E/A, serieller Schnittstelle und GPS für industrielle Übertragungsanwendungen
- 3 Jahre Garantie inklusive

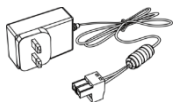
Kapitel 2 Hardware-Einführung

2.1 Packliste



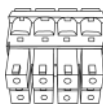
1 ×

UR75-Gerät



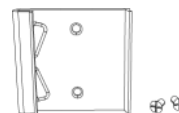
1 ×

Netzteil

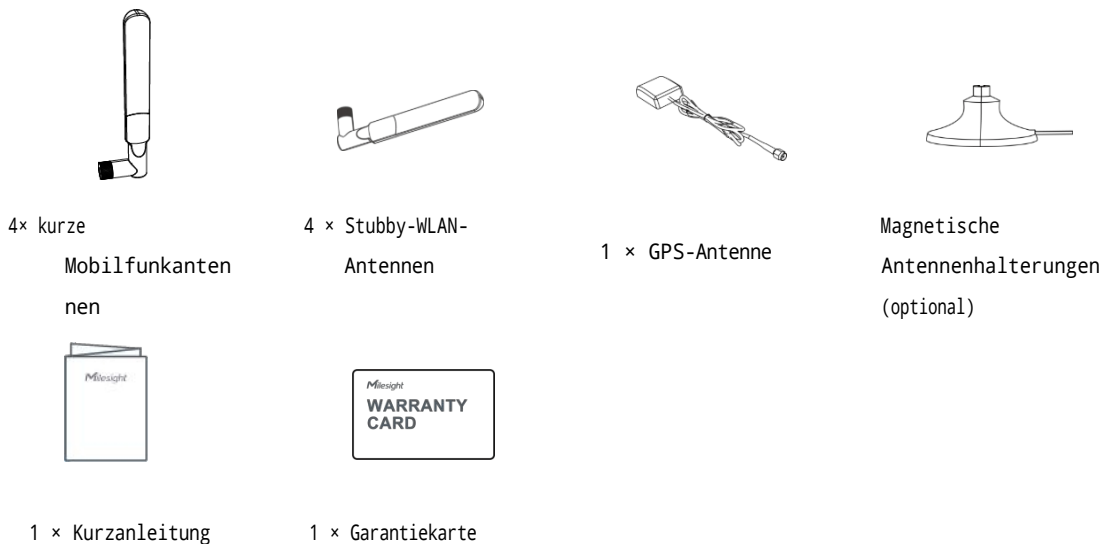


1 × 8-poliger steckbarer

Anschluss



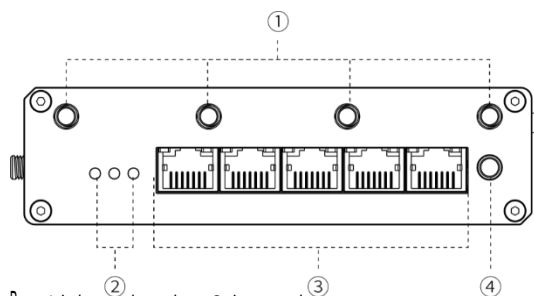
1 × DIN-Schienen-Kit



Wenn eines der oben genannten Teile fehlt oder beschädigt ist, wenden Sie sich bitte an Ihren Vertriebsmitarbeiter.

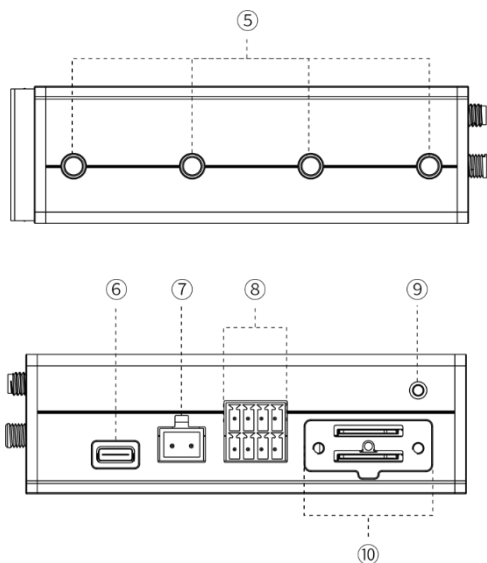
2.2 Übersicht über die Hardware

A. Frontblende



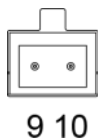
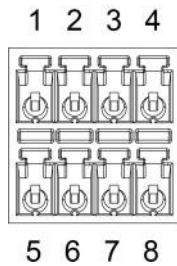
- ① Wi-Fi-Antennenanschlüsse (nur Wi-Fi-Version) LED-Anzeigefeld
- ② SYSTEM: Strom- und Statusanzeige SIM 1 und SIM 2: SIM-Statusanzeige Ethernet-Anschlüsse und Anzeigen
- ④ GPS-Antennenanschluss

B. Linke und rechte Seitenwand



- ⑤ Mobilfunkantennenanschlüsse USB-Typ-C-Anschluss
- ⑥ Stromanschluss Serielle Anschlüsse und E/A-Anschlüsse
- ⑧ Erdungsbolzen
- ⑩ SIM-Steckplätze und Reset-Taste

2.3 Serielle & IO- & Stromversorgungs-Pinbelegungen



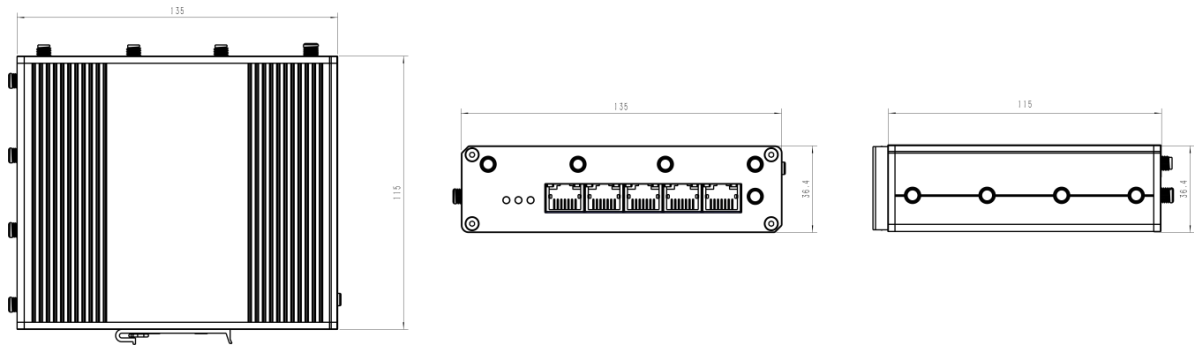
PIN	RS232	RS485	DI	DO	Beschreibung
1	---	---	IN	---	Digitaler Eingang
2	GND	---	GND	---	Masse
3	---	B	---	---	Daten -
4	TXD	---	---	---	Daten übertragen
5	---	---	---	COM	Gemeinsame Grundlage
6	---	---	---	OUT	Digitalausgang
7	---	A	---	---	Daten +
8	RXD	---	---	---	Daten empfangen

PIN	Beschreibung	Drahtfarbe
9	Positiv	Rot
10	Negativ	Schwarz

2.4 LED-Anzeigen

LED	Anzeige	Status	Beschreibung
SYSTEM	Stromversorgung und Systemstatus	Aus	Der Strom ist ausgeschaltet
		Orange	Statisch: Das System wird gerade hochgefahren
		Grün	Statisch: Das System läuft ordnungsgemäß
		Rot	Statisch: Das System funktioniert nicht richtig
SIM1/SIM2	Mobilfunk- und Signalstatus	Aus	SIM-Karte wird registriert oder kann nicht registriert werden (oder es sind keine SIM-Karten eingelegt)
		Grün	Blinkt schnell: SIM-Karte wurde registriert und wählt sich gerade ein
			Leuchtet konstant: SIM-Karte wurde registriert und wählt sich mit dem 5G-Netzwerk verbunden
		Orange	Statisch: SIM-Karte wurde registriert und wählt sich ein zum 4G-Netzwerk
Ethernet-Anschluss	Verbindungsanzeige (orange)	Aus	Getrennt oder Verbindungsfehler
		Ein	Verbunden
		Blinkt	Daten werden übertragen
	Geschwindigkeitsanzeige (Grün)	Aus	100-Mbps-Modus
		Ein	1000-Mbps-Modus

2.5 Abmessungen (mm)



2.6 Reset-Taste

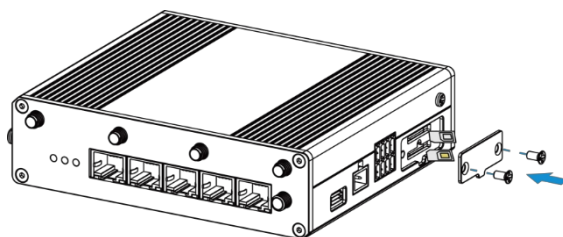
Die Reset-Taste befindet sich neben den SIM-Steckplätzen.

Funktion	Beschreibung	
	LED-Anzeige	Aktion
Soft-Reset	Statisch	Halten Sie beim Einschalten des Geräts die Reset-Taste länger als 5 Sekunden gedrückt.
	Statisch → Alle blinken	Lassen Sie die Taste los und warten Sie.
	Aus → SYSTEM Statisch Grün	Das Gerät wird auf die Werkseinstellungen zurückgesetzt.
Hard-Reset	Aus	Wenn das Gerät ausgeschaltet ist, halten Sie die Reset-Taste gedrückt.
	Statisch → Alle blinken	Schalten Sie das Gerät ein, während Sie die Reset-Taste mehr als 5 Sekunden gedrückt halten und dann loslassen.
	Aus → SYSTEM Statisch Grün	Das Gerät wird auf die Werkseinstellungen zurückgesetzt.

Kapitel 3 Hardware-Installation

3.1 SIM-Installation

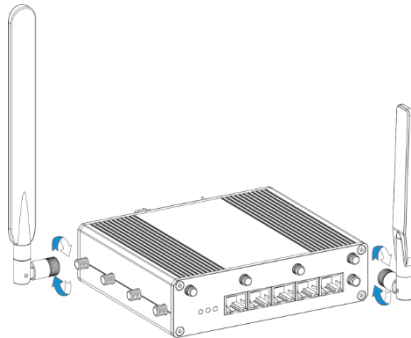
Schrauben Sie die Halterung der SIM-Karte ab, legen Sie die SIM-Karte gemäß dem Richtungssymbol auf dem Gerät in den Steckplatz ein und befestigen Sie die Halterung wieder mit Schrauben am Gerät.



3.2 Antenneninstallation

Drehen Sie die Antenne entsprechend in den Antennenanschluss. Antennen sollten vertikal installiert werden und sich immer an einem Standort mit gutem Empfang befinden.

Hinweis: Die Mobilfunkantennen 1, 2 und 3 sind Hauptantennen, Antenne 4 ist eine Diversity-Antenne.

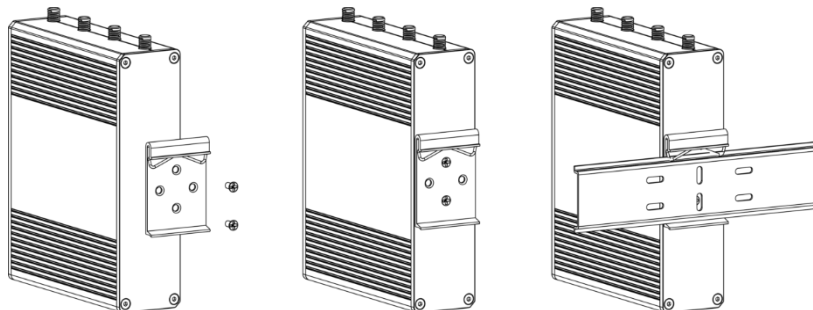


3.3 Geräteinstallation

Das UR75-Gerät kann auf einem Tisch aufgestellt oder an einer DIN-Schiene montiert werden. Verwenden Sie für die Montage an einer DIN-Schiene zwei M3 × 6-Flachkopf-Kreuzschlitzschrauben, um die Befestigungsklammer am Gerät zu befestigen, und hängen Sie das Gerät dann an die DIN-Schiene. Die Breite der DIN-Schiene beträgt 3,5 cm.

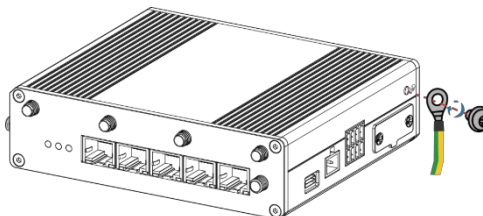


Das empfohlene Drehmoment für die Befestigung beträgt 1,0 N·m, das maximal zulässige Drehmoment 1,2 N·m.



3.4 Installation der Schutzerdung

Verbinden Sie den Erdungsring des Erdungskabels des Gehäuses mit dem Erdungsbolzen und schrauben Sie die Erdungsmutter fest.



Kapitel 4 Zugriff auf die Web-GUI

Der UR75 bietet eine benutzerfreundliche Web-GUI für die Konfiguration, auf die Benutzer über den LAN-Port zugreifen können. In diesem Kapitel wird erläutert, wie Sie auf die Web-GUI des UR75-Routers zugreifen können.

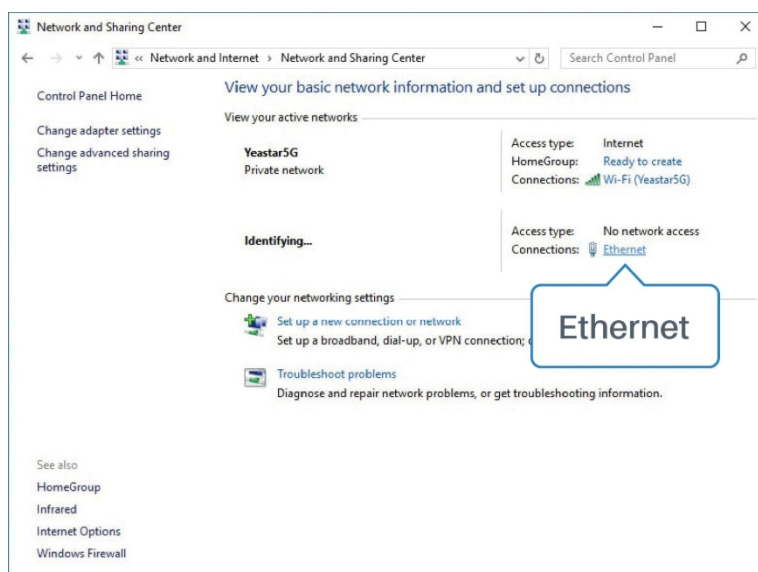
Benutzername: **admin**

Passwort: **password**

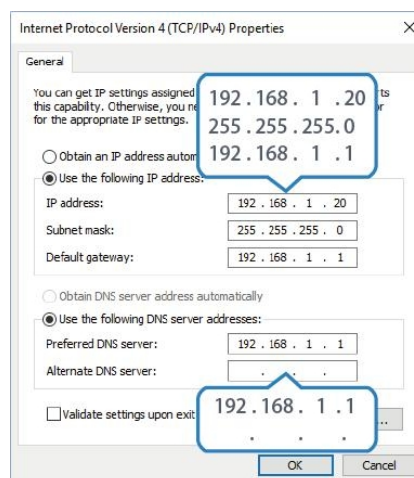
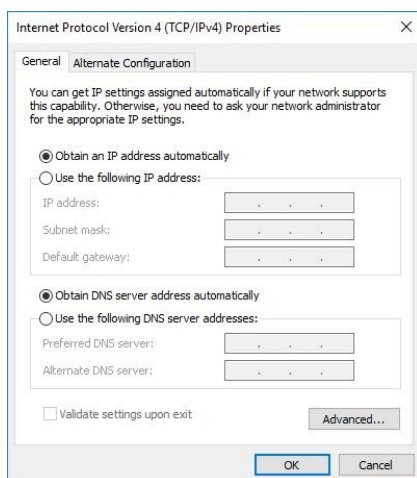
IP-Adresse: **192.168.1.1**

Verbinden Sie den PC direkt mit dem LAN-Port oder USB-Port des UR75-Routers. Die folgenden Schritte basieren auf dem Betriebssystem Windows 10 und dienen als Referenz.

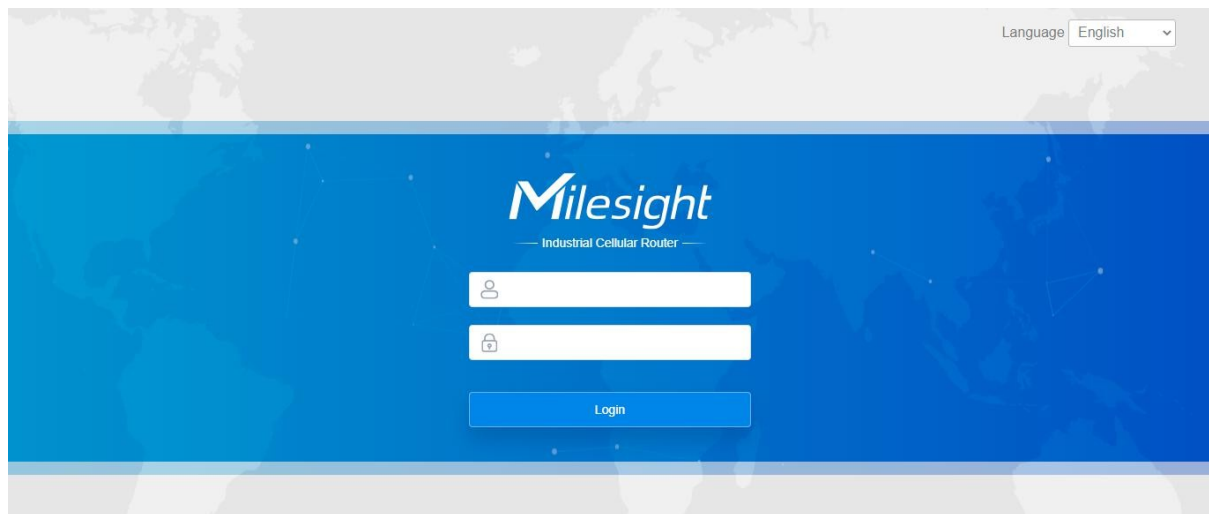
1. Gehen Sie zu **Systemsteuerung → Netzwerk und Internet → Netzwerk- und Freigabecenter** und klicken Sie dann auf **Ethernet** (kann auch anders heißen).



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



3. Öffnen Sie einen Webbrowser auf Ihrem PC (Chrome wird empfohlen), geben Sie die IP-Adresse 192.168.1.1 ein, um auf die Web-GUI zuzugreifen, geben Sie dann den Standardbenutzernamen und das Standardkennwort ein und klicken Sie auf



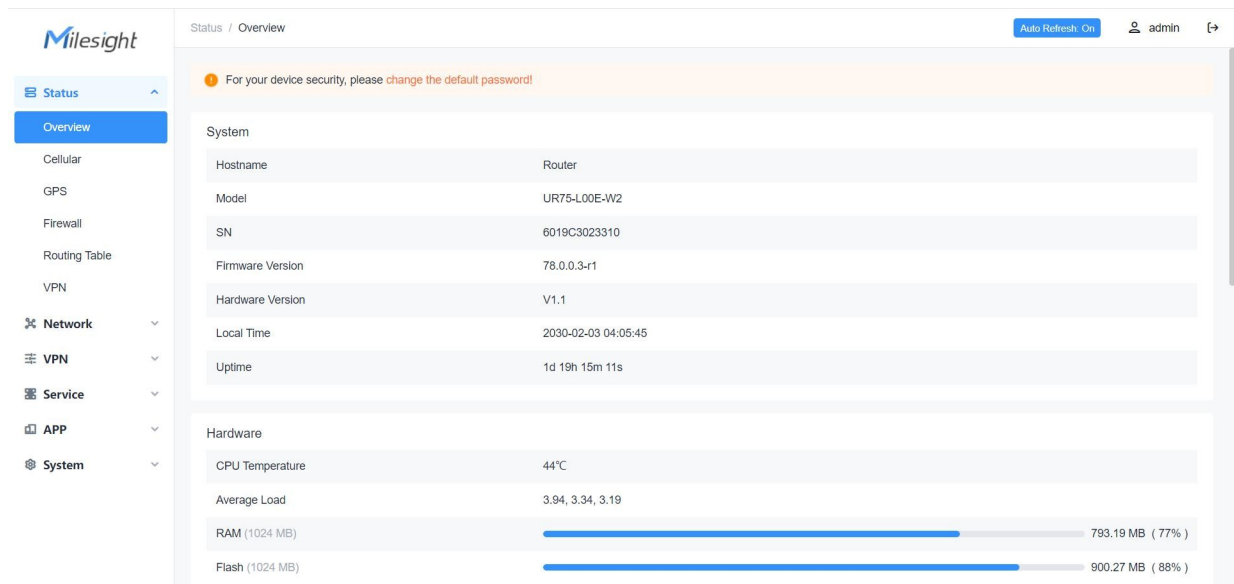
The image shows the login page of the Milesight Industrial Cellular Router web GUI. The page has a blue header with the Milesight logo and the text 'Industrial Cellular Router'. Below the header, there are two input fields for username and password, each with an icon (a person for username and a lock for password). A blue 'Login' button is positioned below the password field. In the top right corner, there is a language dropdown menu set to 'English'.

„Anmelden“.



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

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



The image shows the 'Status / Overview' page of the Milesight router web GUI. The page has a sidebar on the left with navigation links: Status, Overview, Cellular, GPS, Firewall, Routing Table, VPN, Network, VPN, Service, APP, and System. The main content area displays system and hardware information. At the top, there is a warning message: 'For your device security, please change the default password!'. Below this, the 'System' section lists various parameters:

Parameter	Value
Hostname	Router
Model	UR75-L00E-W2
SN	6019C3023310
Firmware Version	78.0.0.3-r1
Hardware Version	V1.1
Local Time	2030-02-03 04:05:45
Uptime	1d 19h 15m 11s

Below the system information, the 'Hardware' section displays various metrics:

Parameter	Value
CPU Temperature	44°C
Average Load	3.94, 3.34, 3.19
RAM (1024 MB)	793.19 MB (77%)
Flash (1024 MB)	900.27 MB (88%)

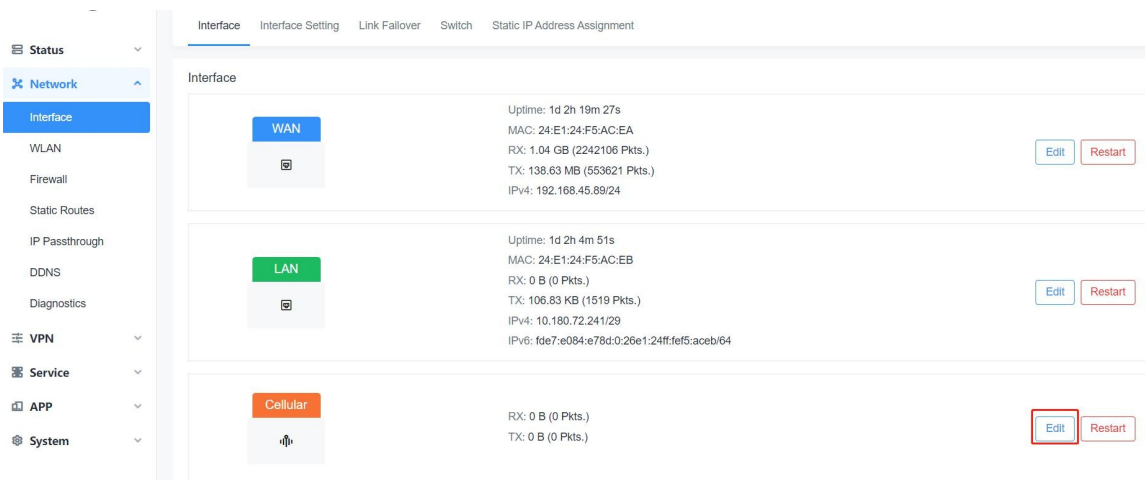
Kapitel 5 Anwendungsbeispiele

5.1 Mobilfunkverbindung konfigurieren

UR75-Router verfügen über zwei Mobilfunk-Schnittstellen: SIM1 und SIM2. Es ist jeweils nur eine Mobilfunk-Schnittstelle aktiv. Wir zeigen Ihnen anhand eines Beispiels, wie Sie eine SIM-Karte in den SIM1-Steckplatz des UR75 einlegen und den Router so konfigurieren, dass Sie über Mobilfunk Zugang zum Internet erhalten.

Konfigurationsschritte

1. Stellen Sie sicher, dass die SIM-Karte richtig eingelegt ist und alle Mobilfunkantennen an den richtigen Anschlüssen angeschlossen sind.
2. Gehen Sie zu **Netzwerk > Schnittstelle > Schnittstellenseite**, suchen Sie die Mobilfunkschnittstelle und klicken Sie auf die Schaltfläche **Bearbeiten**.



3. Wählen Sie die SIM-Karte aus, die Sie konfigurieren möchten, geben Sie die erforderlichen Informationen zur SIM-Karte ein und speichern Sie alle Einstellungen.

Select SIM Card

SIM1

If not filled in, use the default configuration in the SIM card

IP Type

IPv4

APN

PIN

Authentication Type

NONE

Network Type

Auto

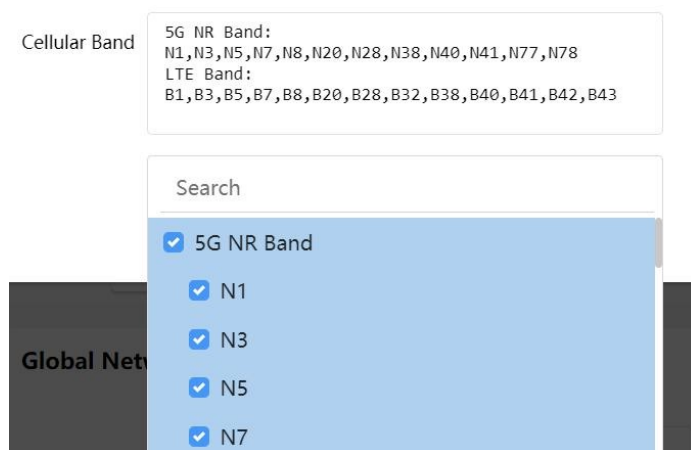
Roaming

☒

IMS

☒

Für eine 5G-Verbindung können Sie bestimmte Frequenzbänder auswählen, um eine hohe Netzwerkgeschwindigkeit zu gewährleisten.



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

Interface Interface Setting Link Failover Switch Static IP Address Assignment						
Link Priority Link failover enables the device to switch to the next link automatically following the order of the priority list when it detects that the current link is unavailable. Tables from top to bottom, priority from high to low						
Priority	Enable Rule	Link In Use	Interface	Connection Type	IP	
1	☒	●	Cellular-SIM1	DHCP Client	-	≡ Edit
2	☒	●	Cellular-SIM2	DHCP Client	-	≡ Edit
3	☒	●	WAN	Static Address	192.168.45.89	≡ Edit

5. Klicken Sie auf „**Bearbeiten**“ eines Links, um die ICMP-Ping-Erkennungsinformationen zu konfigurieren. Wenn die Ping-Prüfung aktiviert ist, sendet der Router ICMP-Pakete an den Erkennungsserver, um zu überprüfen, ob dieser Link gültig ist. Wenn keine Antwort erfolgt und die maximale Anzahl an Wiederholungsversuchen überschritten wird, wechselt er zu dem Link mit niedrigerer Priorität.

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

Enable ☒

When off, the default ping probe passes

IPv4 Primary Server

IPv4 Secondary Server

IPv6 Primary Server

IPv6 Secondary Server

Interval s

Retry Interval s

Timeout s

Max Retries

6. Gehen Sie zu „**Status**“ > „**Mobilfunk**“, um den Status der Mobilfunkverbindung zu überprüfen. Wenn der Modemstatus „Bereit“ und der Netzwerkstatus „**Verbunden**“ lautet, wurde die SIM-Karte erfolgreich gewählt.

Network	
Status	Connected
IPv4 Address	10.21.123.198/29
IPv4 Gateway	10.21.123.197
IPv4 DNS	112.5.230.54
IPv6 Address	2409:8934:2294:acfe:1/128
IPv6 Gateway	fe80::2
IPv6 DNS	2409:8034:2000::3
Connection Duration	0days, 00:08:06

Verwandtes Thema

[Mobilfunk-](#)

[Einstellungen](#)

[Mobilfunkstatus](#)

5.2 Ethernet-Verbindung konfigurieren

UR75-Router unterstützen den Netzwerkzugang über den WAN-Port.

Konfigurationsschritte

1. Gehen Sie zu **Netzwerk > Schnittstelle** > Schnittstellenseite, suchen Sie die WAN-Schnittstelle und klicken Sie auf die Schaltfläche **Bearbeiten**.

2. Wählen Sie das Protokoll entsprechend Ihrem Netzwerkrouter-Modus oder Netzwerkanbieter-Typ aus, konfigurieren Sie die entsprechenden Parameter und speichern Sie anschließend alle Einstellungen.

- **DHCP:** Der übergeordnete Netzwerkrouter weist dem WAN-Port des UR75 eine IP-Adresse zu. Dies ist die einfachste Methode und erfordert, dass der übergeordnete Router den DHCP-Server aktiviert.
- **Statusadresse:** Weisen Sie eine statische IP-Adresse mit demselben Subnetz wie das LAN-Subnetz des oberen Netzwerkrouters zu. Außerdem muss mindestens ein DNS-Server konfiguriert werden.
- **PPPoE:** Geben Sie den Benutzernamen und das Passwort Ihres PPPoE-Kontos ein. Wenden Sie sich dazu an Ihren Netzwerkanbieter.

Protocol	Static Address
IP Type	Static Address
IPv4 Address	192.168.45.89
IPv4 Netmask	255.255.255.0
IPv4 Gateway	192.168.45.1
IPv4 Primary DNS	8.8.8.8
IPv4 Secondary DNS	223.5.5.5

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

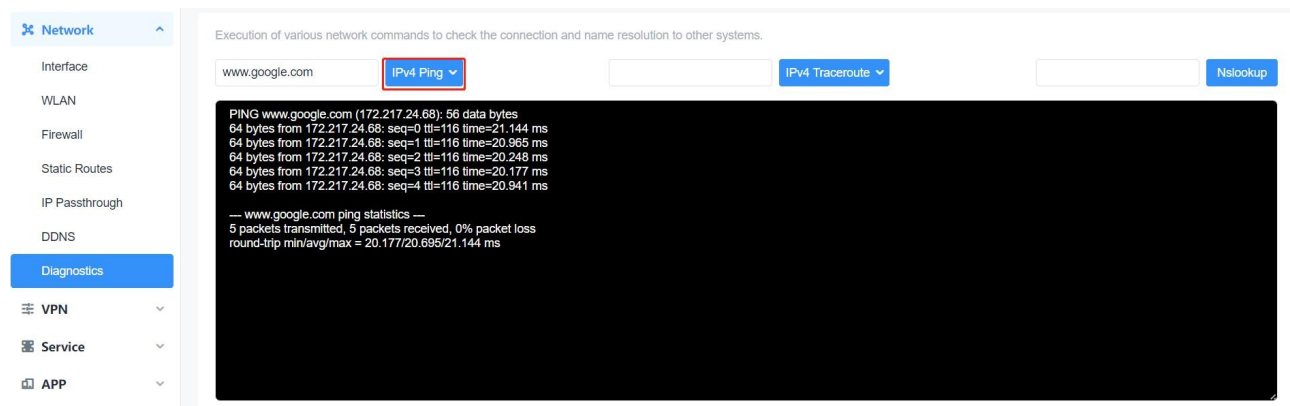
Priority	Enable Rule	Link in Use	Interface	Connection Type	IP	
1	☒	●	Cellular-SIM1	DHCP Client	-	Edit
2	☒	●	Cellular-SIM2	DHCP Client	-	Edit
3	☒	●	WAN	Static Address	192.168.45.89	Edit

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

Hinweis: Wenn Sie ein privates Netzwerk verwenden, ändern Sie bitte die Adresse des privaten Servers oder deaktivieren Sie die Ping-Prüfung.

Enable	☒
When off, the default ping probe passes	
IPv4 Primary Server	8.8.8.8
IPv4 Secondary Server	223.5.5.5
IPv6 Primary Server	2001:4860:4860::8888
IPv6 Secondary Server	2400:3200::1
Interval	180 s
Retry Interval	3 s
Timeout	5 s
Max Retries	3

5. Klicken Sie auf „**Netzwerk > Diagnose**“, um die Netzwerkverbindung zu überprüfen.



Verwandtes Thema

[WAN-Einstellungen](#)

5.3 WLAN-Zugangspunkt konfigurieren

UR75-Router unterstützen sowohl 2,4-GHz- als auch 5-GHz-WLAN und können als Zugangspunkte fungieren, um gleichzeitig anderen Geräten Netzwerkzugang zu gewähren. Wir werden nun ein Beispiel für die Konfiguration eines 2,4-GHz-WLAN-Zugangspunkts betrachten.

Konfigurationsschritte

1. Stellen Sie sicher, dass der Router WLAN unterstützt und die WLAN-Antennen an die richtigen Anschlüsse angeschlossen sind.
2. Gehen Sie zur Seite „**Netzwerk > WLAN**“, um den 2,4-GHz-WLAN-Modus zu aktivieren. Anschließend können Benutzer den Funktyp, die SSID und andere Parameter ändern. Aus Sicherheitsgründen wird empfohlen, einen Verschlüsselungsmodus auszuwählen und einen Schlüssel für Geräte festzulegen, die eine Verbindung zum WLAN herstellen sollen.

WLAN1-2.4G

WLAN2-5G

Enable	☒
_Type	AP
BSSID	24:e1:24:f5:ac:ec
Radio Type	802.11bgn/ax mixed
Channel	Auto
Bandwidth	40 MHz
SSID	Router_F5ACEC_2.4G
Encryption Mode	WPA-PSK/WPA2-PSK
Cipher	AES/TKIP
Key	
Group Rekey Interval	3600 s

3. Verwenden Sie ein Smartphone, um eine Verbindung zum Zugangspunkt des UR75 herzustellen. Sie können die Informationen zum verbundenen Client/Benutzer auf der Seite „**Status > Übersicht**“ überprüfen.

Active DHCP Leases			
Hostname	IPv4-Address	MAC-Address	Remaining Lease Time
BRA-AL00	10.0.0.171	22:89:DF:97:25:09	23h 59m 47s

Verwandtes Thema

[WLAN-Einstellungen](#)

5.4 OpenVPN-Client konfigurieren

UR75-Router können als OpenVPN-Clients oder OpenVPN-Server fungieren. Wir zeigen Ihnen anhand eines Beispiels, wie Sie einen OpenVPN-Client für die Verbindung mit CloudConnexa konfigurieren.

Konfigurationsschritte

1. Stellen Sie sicher, dass der UR75 Zugang zum Internet hat.
2. Melden Sie sich bei Ihrem CloudConnexa-Konto an, wählen Sie den Abschnitt „Netzwerk“ und wählen Sie den gewünschten Dienst entsprechend Ihren Anforderungen aus. Folgen Sie dann den Anweisungen des Assistenten, um mit den Einstellungen fortzufahren.

Select Network Scenarios

Please select all applicable scenarios for the network you are going to create.

Remote Access 
Connect your private resources to CloudConnexa. Provide remote access to your resources, which are hosted on IaaS Cloud, and on premises resources.
[Read more](#)

Site-to-site 
Connect multiple private networks to CloudConnexa (site-to-site connectivity). This wizard will assist you in adding a single network. You can use this wizard to connect all of your networks.
[Read more](#)

Secure Internet Access 
Provide secure access to public resources. Use this network as an Internet Gateway for all internet traffic or only for selected public resources. You can then apply whitelisting rules to your public resources.
[Read more](#)

If you would like to connect a single server you can create a [host](#) and connect your server directly to CloudConnexa

[Skip Wizard](#)[Continue](#)

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

Deploy Network Connector (connector01)

Connector Details

Name
connector01

Region
 Singapore

Each Connector must be installed and connected to CloudConnexa. Select where you would like to deploy Network Connector.

OpenVPN Compatible Router : OpenWrt

1 Download .ovpn Profile

[Download OVPN Profile](#)

2 Use .ovpn Profile

Use .ovpn Profile on your router and connect it to CloudConnexa

[Read how to use .ovpn Profile and connect OpenWrt router to CloudConnexa](#)

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

Network Configuration

Selected Scenarios: Remote Access

Add route

Routes define public and private subnets that will be routed to this Network. Routes are pushed to the routing table of User Devices and Connectors, so that they can access IP Services.

No Route defined yet.

[Add Route](#)

Add IP Service

IP Services are defined as access to specific IP address ranges and protocols.

No IP Service defined yet.

[Add IP Service](#)

- ✓ Define Network
- ✓ Deploy Network Connector
connector01 ✓
- ✓ Add Application
- 4 Add Routes and IP Services**
- 5 Configure Access Group (Optional)

5. Gehen Sie auf der UR75 zur Seite „VPN > OpenVPN > OpenVPN-Client“, wählen Sie als Konfigurationsmethode „Dateikonfiguration“ aus und importieren Sie dann die OVPN-Datei.

Client_2

Enable ☒

Configuration Method File Configuration

Configuration File openvpn-custom-client2.conf BROWSE EDIT EXPORT DELETE

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

VPN

Clients

Name	Status	Local IP	Remote IP
openvpn_2	Connected	100.96.1.18	100.96.1.1

Sie können den Verbindungsstatus auch auf CloudConnexa überprüfen.

CloudConnexa

221028
openvpn.com

Status

Users

Networks

Networks

Applications

IP Services

Connectors

Networks

Configure a Network to connect physical and virtual networks, including distributed networks.

Add Network

All Online Offline Online with Issues Filter

Connection Status	Name	Internet Access	Internet Gateway (Egress)	Applications	IP Services
Offline	Milesight device	Split Tunnel On	Off		
Online	test	Split Tunnel On	Off		test

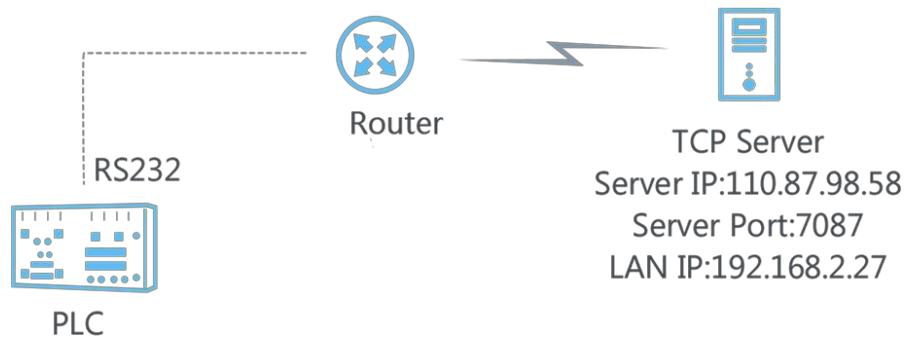
Verwandtes Thema

[OpenVPN-Client](#)

5.6 Serielle DTU-Verbindung konfigurieren

Beispiel

Eine SPS ist über RS232 mit dem UR75 verbunden und muss die Daten transparent an einen Remote-TCP-Server übertragen.



Konfigurationsschritte

1. Gehen Sie zu „**Service**“ > „**Serielle Schnittstelle**“, aktivieren Sie „Seriell 1“ und konfigurieren Sie die Parameter der seriellen Schnittstelle. Die Parameter der seriellen Schnittstelle müssen mit denen der SPS übereinstimmen, wie in der Abbildung unten gezeigt.

Serial 1 Serial 2

Enable ☒

Serial Type RS232 ▼

Baud Rate 9600 ▼

Data Bits 8 Bits ▼

Stop Bits 1 Bits ▼

Parity None ▼

2. Konfigurieren Sie den seriellen Modus als **DTU-Modus** und das Protokoll als **TCP-Client**.

Serial Mode DTU ▼

DTU Protocol TCP Client ▼

Keepalive Interval 75 s

Keepalive Retry Times 9

Reconnect Interval 10 s

Specific Protocol ☐

Packet Size 1024 Byte

Serial Frame Interval 100 ms

Register String

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

Destination IP Address

Server Address	Server Port	Status	
110.87.98.58	7087	Disconnected	Delete Add

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

Settings

(1) Protocol
TCP Server

(2) Local host IP
192.168.2.27

(3) Local host port
7087

Disconnect

5. Verbinden Sie den UR75 über RS232 mit dem PC für die SPS-Simulation. Starten Sie dann die sscom-Software auf dem PC, um die Kommunikation über die serielle Schnittstelle zu testen.

ComNum COM9

BaudRate 9600

DataBits 8

StopBits 1

Verify None

FlowControl None

☐ DTR

☐ Send even 100

☐ Send HEX

Data input: hello

CloseCom

6. Nachdem die Verbindung zwischen dem UR75 und dem TCP-Server hergestellt wurde, können Sie Daten zwischen sscom und Netassist senden.

PC-Seite

SSCOM3.2

testtesttesttesttesttesttesttesttesttesttest

OpenFile FileNm SendFile SaveData Clear HexData

ComNum COM13

BaudRate 9600

DataBits 8

StopBits 1

Verify None

FlowControl None

☐ DTR

☐ Send even 1000 ms/Time

☐ Send HEX

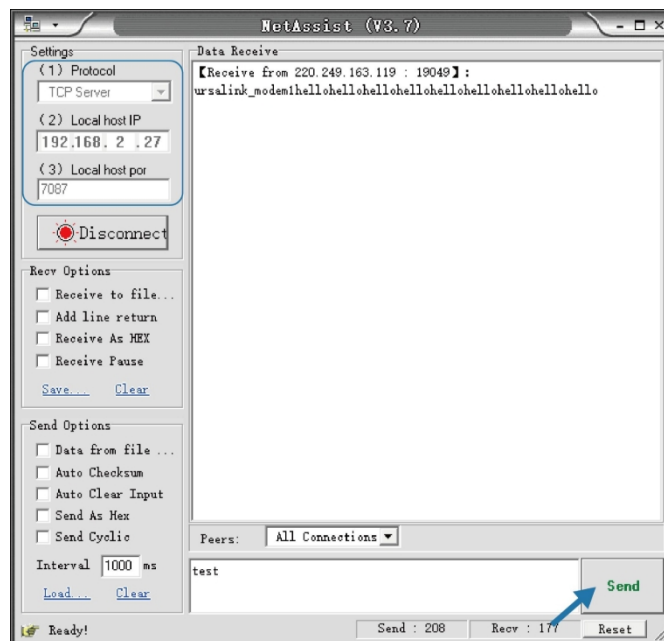
☐ Send New

Data input: hello

SEND

www.mcu51.com S:42 R:48 COM13 opened 9600bps CTS=1 DSR=0 RL

TCP-Serverseite



7. Nachdem der Test der seriellen Kommunikation abgeschlossen ist, können Sie die SPS zum Testen an den RS232-Anschluss des UR75 anschließen.

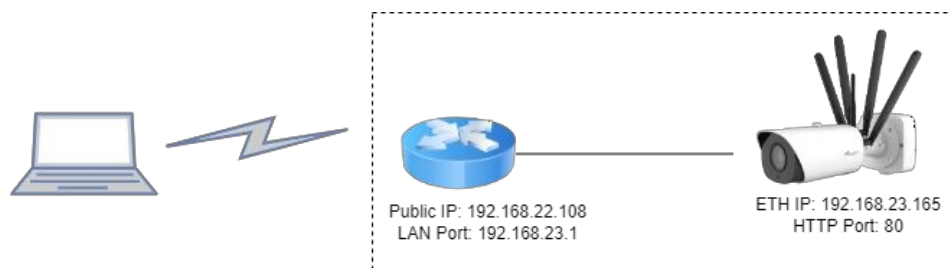
Verwandtes Thema

[Serieller Port](#)

5.5 NAT-Regel konfigurieren

Beispiel

Ein UR75-Router kann über Mobilfunk auf das Internet zugreifen und eine öffentliche IP-Adresse erhalten. Der LAN-Port ist mit einer IP-Kamera verbunden, deren IP-Adresse 192.168.23.165 lautet und deren HTTP-Port 80 ist. Auf diese IP-Kamera kann über die folgenden Port-Mapping-Einstellungen mit der öffentlichen IP-Adresse zugegriffen werden.



Konfigurationsschritte

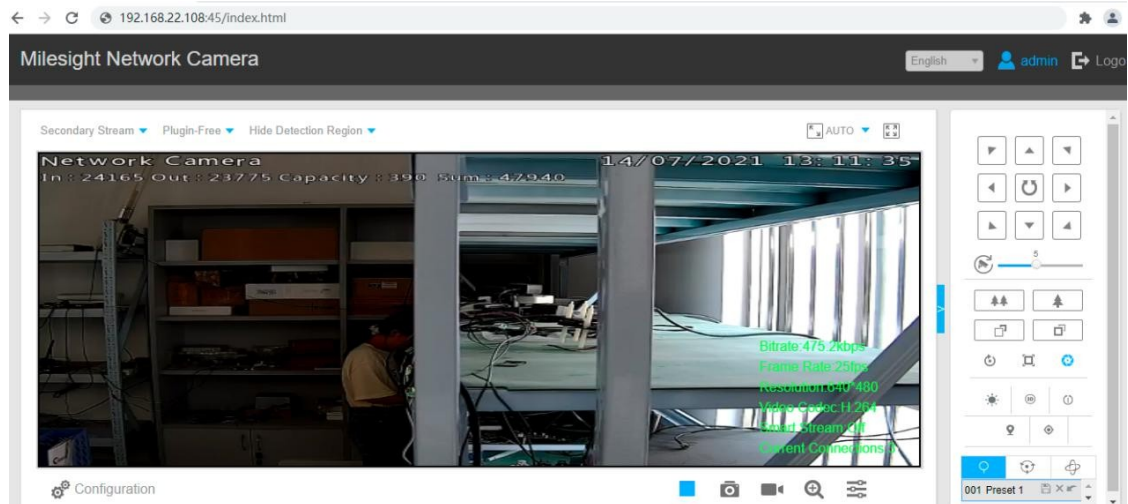
Gehen Sie zu **Netzwerk > Firewall > Portzuordnung** und konfigurieren Sie die Portzuordnungsparameter wie unten angegeben. Die externe IP-Adresse 0.0.0.0/0 bedeutet, dass alle externen Adressen Zugriff haben. Danach können Benutzer die öffentliche IP-Adresse: externen Port verwenden, um auf die IP-Kamera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

Port Mapping(DNAT)

When external services are needed internally (for example, when a website is published externally), the external address initiates an active connection. And, the router or the gateway on the firewall receives the connection. Then it will convert the connection to the internal. This conversion is called DNAT, which is mainly used for external and internal services.

List Priority: The priority is lowered in accordance with the table from top to bottom.

Name	Protocol	External IP Address	External Port	Internal IP Address	Internal Port	Enable	
Camera	TCP UDP	0.0.0.0/0	45	192.168.23.165	80	☒	⋮ Delete
							Add



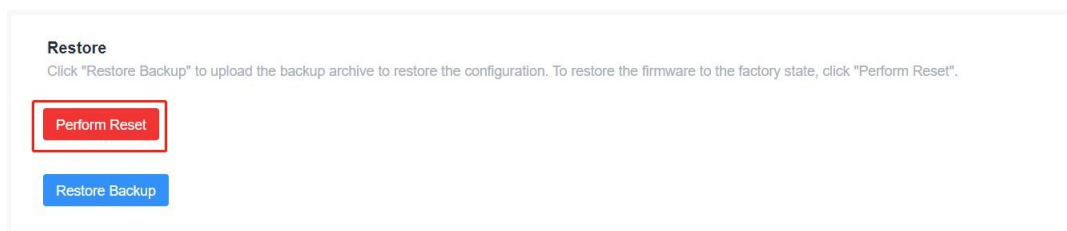
Verwandtes Thema

[Portzuordnung](#)

5.7 Werkseinstellungen wiederherstellen

Methode 1:

Gehen Sie zur Seite „**System > Wartung > Sicherung/Upgrade**“, klicken Sie auf die Schaltfläche „**Zurücksetzen**“ und bestätigen Sie, dass Sie das Gerät auf die Werkseinstellungen zurücksetzen möchten. Klicken Sie anschließend auf die Schaltfläche „**OK**“.



Das Gerät wird dann neu gestartet und sofort auf die Werkseinstellungen zurückgesetzt.



Bitte warten Sie, bis die SYSTEM-LED grün leuchtet. Dies bedeutet, dass das Gerät erfolgreich auf die Werkseinstellungen zurückgesetzt wurde.

Verwandtes Thema

[Sicherung/Flash-Firmware](#)

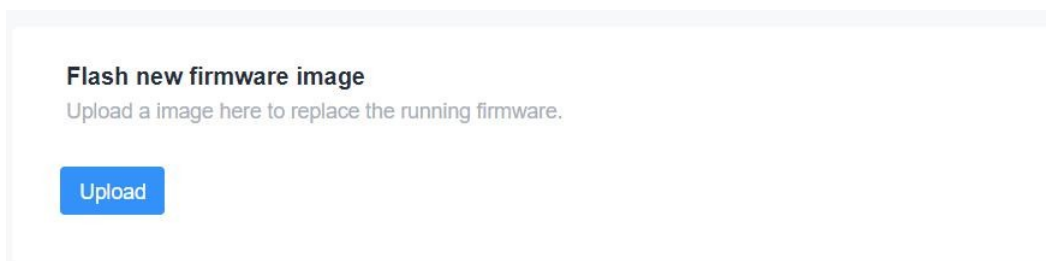
Methode 2:

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

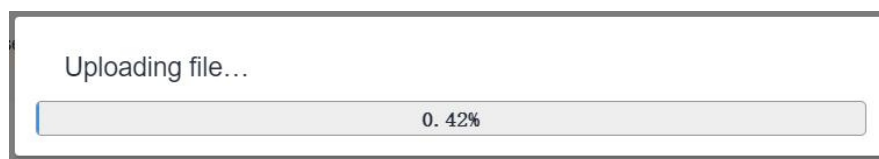
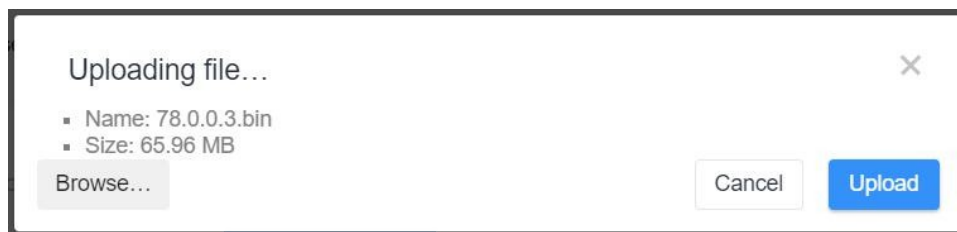
5.8 Firmware-Upgrade

Es wird empfohlen, vor dem Upgrade des Geräts zunächst den technischen Support von Milesight zu kontaktieren. Nachdem Sie die Bilddatei erhalten haben, führen Sie bitte die folgenden Schritte aus, um das Upgrade abzuschließen.

1. Gehen Sie zur Seite „**System > Wartung > Sicherung/Aktualisierung**“ und klicken Sie auf „**Hochladen**“.



2. Suchen Sie die richtige Firmware-Datei auf dem PC, klicken Sie auf „**Hochladen**“ und das Gerät überprüft, ob die Firmware-Datei korrekt ist. Wenn sie korrekt ist, wird die Firmware auf das Gerät importiert.



3. Klicken Sie nach dem Hochladen auf „**Weiter**“, um das Gerät zu aktualisieren. Wenn die SYS-LED von orange auf grün wechselt und statisch leuchtet, ist die Aktualisierung abgeschlossen. Führen Sie während der Aktualisierung keine Vorgänge durch und trennen Sie das Gerät nicht vom Stromnetz.

Flash image?

The flash mirror image was uploaded. The listed information below is the checksum and file size, compare them with the original file to ensure data integrity.
Click "Proceed" below to start the flash procedure.

- Size: 66.86 MB
- MD5: bf733fb3ea296cea485f539f91e253a1
- SHA256: ad04e4338f4bc8b0c47f77ce25be066c9f2b6003dc793dbe885d07775af06e5c

☒ Keep Current Configuration

CancelContinue

Flashing...

The system is flashing now.
DO NOT POWER OFF THE DEVICE!
Wait a few minutes until you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.

Verwandtes Thema

[Sichern/Flashen der Firmware](#)

Kapitel 6 Webkonfiguration

6.1 Status

6.1.1 Übersicht

Die Registerkarte „System“ enthält die grundlegenden Informationen zum Router auf dieser Seite.

System

Hostname	Router
Model	UR75-L00E-W2
SN	6019C3023310
Firmware Version	78.0.0.3-r1
Hardware Version	V1.1
Local Time	2030-02-03 04:18:01
Uptime	1d 19h 27m 27s

System	
Artikel	Beschreibung
Hostname	Der Hostname des Geräts kann unter „System > Verwaltung > Systemeinstellungen geändert werden .
Modell	Der Modellname des Geräts.
SN	Die Seriennummer des Geräts.
Firmware-Version	Die aktuelle Firmware-Version des Geräts.
Hardware-Version	Die aktuelle Hardwareversion des Geräts.
Lokale Zeit	Die aktuelle Systemzeit des Geräts kann unter System > Verwaltung > Systemeinstellungen geändert werden .
Betriebszeit	Die Zeit, seitdem das Gerät eingeschaltet ist und läuft.

Hardware

CPU Temperature	45°C
Average Load	4.15, 3.50, 3.29
RAM (1024 MB)	778.70 MB (76%)
Flash (1024 MB)	901.46 MB (88%)

Hardware	
Element	Beschreibung
CPU-Temperatur	Die Temperatur der CPU.
Durchschnittliche Auslastung	Durchschnittswerte über zunehmend längere Zeiträume (1, 5 und 15 Minuten), je kleiner die Zahlen, desto besser.
RAM	Die RAM-Kapazität und der verfügbare RAM-Speicher.
Flash	Die Flash-Kapazität und der verfügbare Flash-Speicher.

Die Registerkarte **„Aktuelles Netzwerk“** zeigt die grundlegenden Informationen zur verwendeten Verbindung an. Klicken Sie für weitere Details auf das Kapitel „Schnittstelle“.

Current Network

- Accessible IP address of the Internet



Type: Static Address

● **IPv4:** 192.168.45.89

IPv6: -

IPv4 Gateway: 192.168.45.1

IPv6 Gateway: -

MAC: 24:E1:24:F5:AC:EA

Runtime: 1d 2h 31m 37s

Die Registerkarte **„Aktive DHCP-Leases“** zeigt die grundlegenden Informationen der verbundenen Geräte an.

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Remaining Lease Time
BRA-AL00	10.0.0.171	22:89:DF:97:25:09	23h 59m 47s

Aktive DHCP-Leases	
Element	Beschreibung
Hostname	Der Hostname des verbundenen Geräts.
IPv4-Adresse	Die IPv4-Adresse des verbundenen Geräts.
MAC-Adresse	Die MAC-Adresse des verbundenen Geräts.
Verbleibende Leasingdauer Zeit	Die verbleibende Zeit für diese Lease.

Wenn Milesight UPS mit dem Gerät verbunden ist, werden die grundlegenden Informationen zur USV ebenfalls auf der Statusseite angezeigt. Weitere Informationen finden Sie im *Milesight UPS-Benutzerhandbuch*.

UPS

Model	-
SN	-
Firmware Version	-
Hardware Version	-
Power Status	Disconnected_ups
Battery	-
Battery Temperature	-

6.1.2 Mobilfunk

Auf dieser Seite können Sie den Mobilfunknetzstatus des Routers anzeigen.

Cellular Status

SIM Status	Ready
Module Model	RG500L-EU
Version	RG500LEUACR04A01M8G_OCPU_20.001.20.001
Current SIM	SIM1
Cellular Band	N41
Signal Strength	-72dBm
Register Status	Registered(Home network)
IMEI	869263050069693
IMSI	460005970144201
ICCID	898600511318F2001680
ISP	CHINA MOBILE
Network Type	5G SA
PLMN ID	46000
LAC	3259E7
Cell ID	203959107
CQI	-
DL Bandwidth	100MHz
UL Bandwidth	100MHz
SINR	26dB
PCI	23F
RSRP	-71dBm
RSRQ	-11dB
EARFCN	7B49E

Modem-Informationen

Element	Beschreibung
Status	Entsprechender Erkennungsstatus von Modul und SIM-Karte. ● Keine SIM-Karte: Die SIM-Karte ist nicht eingelegt. ● PIN-Fehler: Der PIN-Code ist fehlerhaft ● PIN erforderlich: Für die SIM-Karte muss ein PIN-Code eingegeben werden ● PUK erforderlich: Die SIM-Karte muss mit dem PUK-Code entsperrt werden ● Kein Signal: kein Mobilfunksignal ● Bereit: Die SIM-Karte ist eingelegt

	● Aus: Die SIM-Karte ist deaktiviert oder das Datenvolumen ist überschritten
Modell	Der Modellname des Mobilfunkmoduls.
Version	Die Firmware-Version des Mobilfunkmoduls.
Aktuelle SIM	Die aktuell verwendete SIM-Karte.
Mobilfunkband	Das Mobilfunkband, über das sich der Router beim Netzwerk angemeldet hat.
Signalstärke	Der RSSI-Wert (Received Signal Indicator) des registrierten Mobilfunknetzes.
Registrierungsstatus	Der Registrierungsstatus der SIM-Karte.
IMEI	Die IMEI des Mobilfunkmoduls.
IMSI	Die IMSI der SIM-Karte.
ICCID	Die ICCID der SIM-Karte.
ISP	Der Netzbetreiber, bei dem die SIM-Karte registriert ist.
Netzwerktyp	Der verbundene Netzwerktyp, z. B. LTE, 3G usw.
PLMN-ID	Die aktuelle PLMN-ID, einschließlich MCC,MNC,LAC und Cell ID.
LAC	Der Standortbereichscode der SIM-Karte.
Cell-ID	Die Zell-ID des Standorts der SIM-Karte.
CQI	Der Kanalqualitätsindikator des Mobilfunknetzes.
DL-Bandbreite	Die DL-Bandbreite des Mobilfunknetzes.
UL-Bandbreite	Die UL-Bandbreite des Mobilfunknetzes.
SINR	Das Signal-Interferenz-Rausch-Verhältnis des Mobilfunknetzes.
PCI	Die physikalische Zellenkennung des Mobilfunknetzes.
RSRP	Die Referenzsignalempfangsleistung des Mobilfunknetzes.
RSRQ	Die Referenzempfangsqualität des Mobilfunknetzes.
EARFCN	Die absolute Funkkanalnummer von E-UTRA.

Network

Status	Connected
IPv4 Address	10.192.129.188/29
IPv4 Gateway	10.192.129.189
IPv4 DNS	211.143.147.120
IPv6 Address	-
IPv6 Gateway	-
IPv6 DNS	-
Connection Duration	0days, 00:36:58

Monthly Data Statistics

The traffic statistics here are for reference only, and the actual traffic is subject to the charging bill provided by the operator.

SIM-1	RX: 0.0 MiB	TX: 0.3 MiB	ALL: 0.3 MiB
SIM-2	RX: 0.0 MiB	TX: 0.0 MiB	ALL: 0.0 MiB

Netzwerk

Element	Beschreibung
Status	Der Verbindungsstatus des Mobilfunknetzes.
IPv4/IPv6-Adresse	Die IPv4/IPv6-Adresse und Netzmaske des Mobilfunknetzes.
IPv4/IPv6-Gateway	Das IPv4/IPv6-Gateway und die Netzmaske des Mobilfunknetzes.
IPv4/IPv6-DNS	Der DNS-Server des Mobilfunknetzes.
Verbindungsdauer	Die Information darüber, wie lange das Mobilfunknetz verbunden war verbunden ist.
RX	Das Datenvolumen und die empfangenen Pakete dieses Monats.
TX	Das Datenvolumen und die übertragenen Pakete dieses Monats.
ALL	Gesamtdatenvolumen und Pakete dieses Monats.

6.1.3 WLAN

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

Base Info

Work Mode	AP
Status	● Enable
SSID	Router_F5AFCD_5G
BSSID	24:E1:24:F5:AF:CD
Channel	149
Encryption Mode	WPA2-PSK/WPA3-PSK
IP Address	192.168.1.1

Access Device List

Host Name	MAC	IP Address	Connect Time
-----------	-----	------------	--------------

This section contains no values now.

WLAN-Status – AP-Modus	
Element	Beschreibung
Grundlegende Informationen	
Arbeitsmodus	Zeigt den Arbeitsmodus dieser WLAN-Schnittstelle an.
Status	Zeigt den Aktivierungsstatus dieser WLAN-Schnittstelle an.
Typ	Zeigt den Typ der WLAN-Schnittstelle an.
SSID	Zeigt die SSID dieses Geräts an.
Kanal	Zeigen Sie den verwendeten Kanal dieser WLAN-Schnittstelle an.
Verschlüsselungsmodus	Zeigen Sie den Verschlüsselungsmodus dieser WLAN-Schnittstelle an.
IP-Adresse	Zeigt die IP-Adresse dieses Geräts an.
Liste der zugehörigen Geräte	
Hostname	Zeigt den Hostnamen des Clients an, der mit diesem Gerät verbunden ist.
MAC-Adresse	Zeigen Sie die MAC-Adresse des Clients an, der mit diesem Gerät verbunden hat.
IP-Adresse	Zeigt die IP-Adresse des Clients an, der mit diesem Gerät verbunden ist.
Verbindungszeit	Zeigen Sie die Verbindungsdauer zwischen dem Client-Gerät und diesem

Gerät an.

Base Info

Work Mode	Client
Status	● Connected
SSID	RedmiK60
BSSID	4e:c2:25:0a:ed:6a
Channel	11
RSSI	-28dBm
IP Address	192.168.23.112
Netmask	255.255.255.0
Gateway	192.168.23.127

WLAN-Status – Client-Modus	
Element	Beschreibung
Grundlegende Informationen	
Arbeitsmodus	Zeigt den Arbeitsmodus dieser WLAN-Schnittstelle an.
Status	Zeigt den Verbindungsstatus mit dem WLAN-Zugangspunkt an.
SSID	Zeigt die SSID des AP an, mit dem das Gerät verbunden ist.
BSSID	Zeigt die MAC-Adresse des AP an, mit dem das Gerät verbunden ist.
Kanal	Zeigt den verwendeten Kanal dieser WLAN-Schnittstelle an.
RSSI	Zeigt das Signal dieser WLAN-Schnittstelle an.
IP	Zeigen Sie die IP-Adresse dieses Geräts an, die vom WLAN-AP zugewiesen wurde.
Netzmaske	Zeigt die vom WLAN-AP zugewiesene Netzmaske dieses Geräts an.
Gateway	Zeigt die IP-Adresse des WLAN-AP an.

6.1.4 GPS

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

GPS Status

Status	Obtained
Time for Locating	2022/11/24 05:51:05
Satellites In Use	36
Satellites In View	71
Latitude	24.624043 N
Longitude	118.030530 E
Altitude	83.6 M
Speed	0.000000 km/h

GPS-Status

Element	Beschreibung
Status	Der Status der GPS-Erfassung.
Zeit für die Ortung	Die Zeit für die Ortung.
Verwendete Satelliten	Die Anzahl der eingesetzten Satelliten.
Sichtbare Satelliten	Die Anzahl der sichtbaren Satelliten.
Breitengrad	Der Breitengrad des Standorts.
Längengrad	Der Längengrad des Standorts.
Höhe	Die Höhe des Standorts.
Geschwindigkeit	Die Bewegungsgeschwindigkeit.

6.1.5 Firewall

Auf dieser Seite können Sie alle IPv4/IPv6-Ketten von iptables überprüfen. Benutzer können auf die Ziele mit gestrichelten Linien klicken, um zu den entsprechenden Ketten zu springen.

IPv4 Firewall		IPv6 Firewall		Show Empty Chain		Reset Counts		Restart Firewall	
Table: Filter									
Chain <i>INPUT</i> (Policy: <i>ACCEPT</i> , 0 Packets, 0 B Traffic)									
Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Remark
1.44 K	123.47 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
16.84 K	2.06 MB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
15.88 K	2.00 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
370	19.24 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
0	0 B	zone_wan_input	all	eth1	*	0.0.0.0/0	0.0.0.0/0	-	-
959	60.27 KB	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_eth_input	all	eth1	*	0.0.0.0/0	0.0.0.0/0	-	-
Chain <i>FORWARD</i> (Policy: <i>ACCEPT</i> , 0 Packets, 0 B Traffic)									
Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Remark
0	0 B	forwarding_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom forwarding rule chain
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-

Firewall-Status	
Element	Beschreibung
Tabelle: Filter	Die Standardtabelle für die Verarbeitung von Netzwerkpaketen.
Tabelle: NAT	Wird verwendet, um Pakete zu ändern, die eine neue Verbindung herstellen, und für die Netzwerkadressübersetzung (NAT) verwendet.
Tabelle: Mangle	Wird für bestimmte Arten der Paketänderung verwendet.
Leere Kette anzeigen/ausblenden	Zeigt/verbirgt die Kette ohne Regeln.
Zählungen zurücksetzen	Setzt die Verkehrszählungen aller Ketten zurück.
Firewall neu starten	Den gesamten Firewall-Prozess neu starten.

6.1.6 Routing-Tabelle

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

IPv4 Router

Interface	Destination Network	IPv4 Gateway	Priority
WAN	8.8.8.8	192.168.45.1	0
LAN	192.168.1.0/24	-	0
WAN	192.168.45.0/24	-	0
WAN	192.168.45.0/24	192.168.45.1	1
WAN	223.5.5.5	192.168.45.1	0

ARP

Interface	IPv4 Address	MAC Address
LAN	192.168.1.119	7E:03:C0:70:98:5F

Active IPv6 Router

Interface	Destination Network	IPv6 Gateway	Priority
LAN	fdcd:8701:29c0::/64	-	1024

IPv6 Neighbor

Interface	IPv6 Address	MAC Address
-----------	--------------	-------------

This section contains no values now.

Artikel	Beschreibung
Aktiver IPv4/IPv6-Router	
Schnittstelle	Die ausgehende Schnittstelle der Route.
Ziel Netzwerk	Die IP-Adresse und Netzmaske des Zielhosts oder des Zielnetzwerks Netzwerks.
IPv4/IPv6 Gateway	Die IP-Adresse des Gateways, von dem aus Pakete gesendet werden sollen.
Priorität	Die Metriknummer, die die Priorität der Schnittstelle angibt.
ARP-Cache	
Schnittstelle	Die Bindungsschnittstelle von ARP.
IPv4-Adresse	Die IP-Adresse des ARP-Pools.
MAC-Adresse	Die der IP-Adresse zugeordnete MAC-Adresse.

IPv6-Nachbar	
Schnittstelle	Die Bindungsschnittstelle des Nachbarn.
IPv6-Adresse	Die IP-Adresse des Nachbarn.
MAC-Adresse	Die der IP-Adresse entsprechende MAC-Adresse.

6.1.7 VPN

Auf dieser Seite können Sie den VPN-Status überprüfen.

Clients

Name	Status	Local IP	Remote IP
This section contains no values now.			

IPsec Server

Status	Server IP	Connected Clients IP
This section contains no values now.		

OpenVPN Server

Status	Server IP	Connected Clients IP
This section contains no values now.		

VPN-Status	
Element	Beschreibung
Clients	
Name	Der Name der aktivierten VPN-Clients.
Status	Der Verbindungsstatus des Clients.
Lokale IP	Die lokale IP-Adresse und das Subnetz des VPN-Tunnels.
Remote-IP	Die tatsächliche Remote-IP-Adresse und das Subnetz des VPN-Tunnels.
IPsec/OpenVPN-Server	
Status	Der Status des Servers.
Server-IP	Die Server-IP-Adresse und das Subnetz des VPN-Tunnels.
IP-Adresse der verbundenen Clients	Die IP-Adresse des Clients, der mit dem Server verbunden ist.

6.2 Netzwerk

6.2.1 Schnittstellen

In diesem Menü können Sie die Grundeinstellungen für Mobilfunk-, WAN- und LAN-Schnittstellen konfigurieren.

Interface

WAN

Uptime: 0h 25m 56s
MAC: 24:E1:24:F6:96:1A
RX: 7.68 MB (20917 Pkts.)
TX: 9.15 MB (9617 Pkts.)
IPv4: 192.168.45.192/24

Edit Restart

LAN

Uptime: 0h 25m 56s
MAC: 24:E1:24:F6:96:1B
RX: 101.23 KB (472 Pkts.)
TX: 180.69 KB (446 Pkts.)
IPv4: 10.0.0.1/24
IPv6: fd64:173c:6368:0:26e1:24ff:fe6:961b/64

Edit Restart

Cellular

RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

Edit Restart

Schnittstellen	
Element	Beschreibung
Neustart	Klicken Sie hier, um diese Netzwerkschnittstelle neu zu starten.
Bearbeiten	Klicken Sie hier, um die allgemeinen Einstellungen dieser Netzwerkschnittstelle zu bearbeiten.

Global Network Option

IPv6 ULA-Prefix

Globale Netzwerkooptionen	
Element	Beschreibung
IPv6-ULA-Präfix	Das IPv6-Präfix für die eindeutige lokale Adresse (ULA) dieses Geräts.

6.2.1.1 WAN

Der WAN-Port kann über ein Ethernet-Kabel mit dem Internet verbunden werden. Er unterstützt drei Verbindungstypen, die sowohl mit IPv4 als auch mit IPv6 funktionieren.

- **Statische IP:** Konfigurieren Sie die IPv4-Adresse, die Netzmaske und das Gateway für die Ethernet-WAN-Schnittstelle.
- **DHCP-Client:** Konfigurieren Sie die Ethernet-WAN-Schnittstelle als DHCP-Client, um automatisch eine IPv4-Adresse zu erhalten.
- **PPPoE:** Konfigurieren Sie die Ethernet-WAN-Schnittstelle als PPPoE- oder PPPoEv6-Client.

General Setting

Advanced Setting

Status

 Uptime: 0h 55m 16s
MAC: 24:E1:24:F5:AC:EA
RX: 0 B (0 Pkts.)
TX: 67.54 KB (1048 Pkts.)
IPv4: 192.168.45.182/24

WAN – Status	
Element	Beschreibung
Betriebszeit	Wie lange ist das Gerät bereits in Betrieb?
MAC	MAC-Adresse der WAN-Schnittstelle.
RX	RX: Das Datenvolumen und die Pakete, die über diese Schnittstelle empfangen wurden.
TX	TX: Das Datenvolumen und die Pakete, die von dieser Schnittstelle übertragen wurden.
IPv4	IPv4-Adresse der WAN-Schnittstelle.

1. Statische IP-Konfiguration

Wenn das externe Netzwerk der WAN-Schnittstelle eine feste IP-Adresse zuweist, wählen Sie bitte diesen Modus.

Protocol

IP Type

IPv4 Address

IPv4 Netmask

IPv4 Gateway

IPv4 Primary DNS

IPv4 Secondary DNS

Statische Adresse – Allgemeine Einstellungen		
Element	Beschreibung	Standard
IP-Typ	Ist fest auf IPv4 eingestellt.	IPv4
IPv4-Adresse	Legen Sie die IPv4-Adresse des WAN-Ports fest.	--
IPv4-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.	--
Primärer IPv4-DNS	Legen Sie den primären IPv4-DNS-Server fest.	8.8.8.8
Sekundärer IPv4-DNS	Legen Sie den sekundären IPv4-DNS-Server fest.	223.5.5.5

General Setting

Advanced Setting

NAT ☒

MTU

Statische Adresse – Erweiterte Einstellungen	
Element	Beschreibung

NAT	Aktivieren oder deaktivieren Sie die NAT-Funktion. Wenn diese Funktion aktiviert ist, kann eine private IP-Adresse in eine öffentliche IP übersetzt werden.
MTU	Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500.

2. DHCP-Client

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

General Setting

Advanced Setting

Status

 Uptime: 0h 56m 21s
MAC: 24:E1:24:F5:AC:EA
RX: 0 B (0 Pkts.)
TX: 69.14 KB (1073 Pkts.)
IPv4: 192.168.45.182/24

Protocol

DHCP Client

General Setting

Advanced Setting

Obtain DNS server automatically

☒

NAT

☒

MTU

1500

DHCP-Client – Erweiterte Einstellungen	
Element	Beschreibung
DNS-Server abrufen automatisch	Peer-DNS automatisch beziehen. DNS ist erforderlich, wenn Sie eine Domänenname.
NAT	Aktivieren oder deaktivieren Sie die NAT-Funktion. Wenn sie aktiviert ist, kann eine private IP-Adresse in eine öffentliche IP übersetzt werden.
MTU	Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500.

3. PPPoE/PPPoEv6

PPPoE bezieht sich auf ein Punkt-zu-Punkt-Protokoll über Ethernet. Wenn die IPv6-Aushandlung aktiviert ist, kann der Router sowohl IPv4- als auch IPv6-Adressen erhalten.

Protocol

PPPoE

Username

Password

PPPoE – Allgemeine Einstellungen	
Element	Beschreibung
PAP/CHAP-Benutzername	Geben Sie den von Ihrem Internetdienstanbieter (ISP) bereitgestellten Benutzernamen ein.
PAP/CHAP-Passwort	Geben Sie das von Ihrem Internetdienstanbieter (ISP) bereitgestellte Passwort ein.

Obtain IPv6-Address 

Enable IPv6 negotiation on the PPP link

Obtain DNS server automatically ☒

Max Retries

Heartbeat Interval s

NAT ☒

MTU

PPPoE – Erweiterte Einstellungen	
Element	Beschreibung
IPv6-Adresse beziehen	Aktivieren Sie die IPv6-Aushandlung auf der PPP-Verbindung.
DNS-Server abrufen automatisch	Peer-DNS automatisch während des PPP-Wählvorgangs abrufen. DNS ist erforderlich beim Aufrufen von Domainnamen.
Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl der Wiederholungsversuche nach einem fehlgeschlagenen Verbindungsaufbau fest. Bereich: 0-9.
Heartbeat-Intervall (s)	Legen Sie das Heartbeat-Intervall für die Verbindungserkennung fest. Bereich: 1-600.
NAT	Aktivieren oder deaktivieren Sie die NAT-Funktion. Wenn diese Funktion aktiviert ist, kann eine private IP-Adresse in eine öffentliche IP übersetzt werden.
MTU	Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500.

Beispiel für eine zugehörige Konfiguration

[Ethernet-WAN-Verbindung](#)

6.2.1.2 LAN/DHCP-Server

General Setting
Advanced Setting
DHCP Server

Status
 Uptime: 0h 53m 46s
MAC: 24:E1:24:F5:AC:EB
RX: 2.17 MB (17646 Pkts.)
TX: 23.04 MB (18893 Pkts.)
IPv4: 192.168.1.1/24
IPv6: fdcd:8701:29c0:0:26e1:24ff:fe5:aceb/64

IPv4 Address

IPv4 Netmask

IPv6 Prefix Length

Assign the given length part of every public IPv6-prefix to this interface.

IPv6 Prefix Identifier

Assign the prefix part of this hexadecimal sub ID to this interface.

LAN – Allgemeine Einstellungen	
Element	Beschreibung
Status	Betriebszeit: Wie lange ist das Gerät bereits in Betrieb?
	MAC: MAC-Adresse der LAN-Schnittstellen.
	RX: Das Datenvolumen und die Pakete, die über diese Schnittstelle empfangen wurden.
	TX: Das Datenvolumen und die Pakete, die von dieser Schnittstelle übertragen wurden.
	IPv4/IPv6: IPv4/IPv6-Adresse der LAN-Schnittstellen.
IPv4-Adresse	Legen Sie die IPv4-Adresse der LAN-Schnittstelle fest.
IPv4-Netzmaske	Legen Sie die Netzmaske für die LAN-Schnittstelle fest.
IPv6-Präfixlänge	Weisen Sie dieser Schnittstelle einen Teil der angegebenen Länge jedes öffentlichen IPv6-Präfixes zu.
IPv6-Präfix Kennung	Weisen Sie dieser Schnittstelle Präfixteile unter Verwendung dieser hexadezimalen Subpräfix-ID zu.

General Setting
Advanced Setting
DHCP Server

MTU

LAN – Erweiterte Einstellungen	
Element	Beschreibung
MTU	Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500.

General Setup

Enable ☒

Start Address

End Address

IPv4 Lease Time m

IPv4 Netmask

DNS Server  

DHCP-Server – Allgemeine Einrichtung	
Element	Beschreibung
Aktivieren	Aktivieren Sie diese Option, um DHCP für diese Schnittstelle zu deaktivieren.
Startadresse	Definieren Sie den Anfang des Pools von IP-Adressen, die an DHCP-Clients vergeben werden.
Endadresse	Legen Sie das Ende des Pools von IP-Adressen fest, die an DHCP-Clients vermietet werden.
IPv4-Lease-Zeit	Legen Sie die Ablaufzeit der vermieteten Adressen fest, das Minimum beträgt 2 Minuten (2m).
IPv4-Netzmaske	Legen Sie diese fest, um die an Clients gesendete Netzmaske zu überschreiben. Normalerweise ist sie berechnet aus dem bedienten Subnetz.
DNS-Server	Legen Sie die DNS-Serverliste für Clients fest.

IPv6 Settings

Enable ☒

Router Announcement Service

DHCPv6 Service

DHCPv6 Mode

Announced DNS Servers 

DHCP-Server-IPv6-Einstellungen	
Element	Beschreibung
Aktivieren	Wählen Sie diese Option, um den DHCPv6-Server bei Verwendung von Mobilfunk IPv6 oder PPPoE v6 verwenden.
Router-Advertisement-Dienst	Er ist als Servermodus festgelegt.
DHCPv6-Dienst	Er ist als Servermodus festgelegt.

DHCPv6-Modus	Er ist als zustandsloser Modus festgelegt.
Angekündigte DNS-Server	Legen Sie die DNS-Serverliste für Clients fest.

6.2.1.3 Mobilfunk

Select SIM Card SIM1 
If not filled in, use the default configuration in the SIM card

IP Type IPv4/IPv6 

APN

PIN 

Authentication Type NONE 

Network Type Auto 

Roaming ☒

IMS ☒

SMS Center Number

NAT ☒

Customized MTU ☐

MTU

Data Limit MB

Billing Day Day 1 

Cellular Band

5G NR Band:

N1,N3,N5,N7,N8,N20,N28,N38,N40,N41,N77,N78

LTE Band:

B1,B3,B5,B7,B8,B20,B28,B32,B38,B40,B41,B42,B43

Mobilfunk	
Element	Beschreibung
SIM auswählen Karte	Wählen Sie die SIM-Karte aus, für die Sie die Einstellungen konfigurieren möchten.
IP-Typ	Zeigen Sie den für diese Schnittstelle zu verwendenden Internetprotokolltyp an. Option: IPv4, IPv6 und IPv4/IPv6.
APN	Geben Sie den Zugangspunktnamen für die Mobilfunk-Einwahlverbindung ein, der von

	lokalen Internetdienstanbieters bereitgestellt wird.
PIN	Geben Sie einen 4- bis 8-stelligen PIN-Code ein, um die SIM-Karte zu entsperren.
Authentifizierung Typ	Wählen Sie zwischen KEINE, PAP, CHAP und PAP/CHAP.
Netzwerktyp	Wählen Sie zwischen Auto, Nur 5G, Nur 4G und Nur 3G. Auto: Automatische Verbindung zum Netzwerk mit dem stärksten Signal. Nur 5G: Verbindung nur zum 5G-Netzwerk. Und so weiter.
Roaming	Roaming aktivieren oder deaktivieren.
IMS	IMS-Funktion aktivieren oder deaktivieren.
SMS-Zentrale Nummer	Geben Sie die Nummer des lokalen SMS-Centers ein, um SMS-Nachrichten zu speichern, weiterzuleiten, zu konvertieren und Zustellung von SMS-Nachrichten.
NAT	Aktivieren oder deaktivieren Sie die NAT-Funktion.
Benutzerdefiniert MTU	Aktivieren oder deaktivieren Sie diese Option, um die maximalen Übertragungseinheiten anzupassen. Wenn deaktiviert, verwendet das Gerät die MTU-Einstellungen des Betreibers.
MTU	Legen Sie die maximalen Übertragungseinheiten fest. Bereich: 68-1500.
Datenlimit	Legen Sie das Datenlimit für diesen Monat fest. Wenn der Datenverkehr das Limit überschreitet, wird die SIM-Karte in diesem Monat gesperrt. Die Standardeinstellung ist leer (keine Begrenzung).
Abrechnungstag	Löschen Sie die monatlichen Datenstatistiken, wenn der Abrechnungstag dieses Monats erreicht ist Monats erreicht ist.
Mobilfunkband	Wählen Sie die 5G NR- und 4G LTE-Bänder aus, die zur Registrierung im Mobilfunknetz verwendet werden. Es kann zur Optimierung der Mobilfunkgeschwindigkeit durch Auswahl bestimmter Frequenzbänder verwendet werden.

Verwandte Anwendung

[Mobilfunk-Anwendung](#)

6.2.1.4 Schnittstelleneinstellungen

Der Mobilfunkrouter UR75 unterstützt 5 Gigabit-Ethernet-Ports. Auf dieser Seite werden die Eigenschaften aller Ethernet-Ports angezeigt und Sie können den Status dieser Ports steuern.

Interface Setting

Interface	Status	Property	Interface Speed	Interface Mode
LAN1	Up	LAN	Auto	Auto
LAN2	Up	LAN	Auto	Auto
LAN3	Up	LAN	Auto	Auto
LAN4	Up	LAN	Auto	Auto
WAN	Up	WAN	Auto	Auto

Schnittstelleneinstellung	
Element	Beschreibung
Schnittstelle	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

	zu deaktivieren.
Eigenschaft	Der Typ des Ethernet-Ports, festgelegt als WAN-Port oder LAN-Port.
Schnittstellengeschwindigkeit	Die Geschwindigkeit des Ethernet-Ports ist auf „Auto“ festgelegt.
Schnittstellenmodus	Der Modus des Ethernet-Ports ist auf „Auto“ festgelegt.

6.2.1.5 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 anhand 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 UR75 einen zweiten Link aus, in dem IPv6 als primärer IPv6-Link fungiert, und umgekehrt.

Link-Failover

Link Priority

Link failover enables the device to switch to the next link automatically following the order of the priority list when it detects that the current link is unavailable.
Tables from top to bottom, priority from high to low

Priority	Enable Rule	Link in Use	Interface	Connection Type	IP	
1	☒		Cellular-SIM1	DHCP Client	-	 Edit
2	☒		Cellular-SIM2	DHCP Client	-	 Edit
3	☒		WAN	Static Address	192.168.40.137	 Edit

Settings

Revert to High Priority Link ☒

After checking, it will periodically detect whether the higher priority link is available. If a higher priority link is available, it will switch to the link with a higher priority.

Revert Interval

10 s

The interval for trying to switch to a link with a higher priority. If it is set to 0, it will not switch actively and will not take effect on switching between SIM cards.

Dual-card Switch Delay ☐

Reconnect high priority SIM card ☐

Emergency Reboot ☐

After enabling, if all interfaces are unavailable, the system will reboot.

Element	Beschreibung
Verbindungspriorität	
Priorität	Zeigen Sie die Priorität jeder Schnittstelle an. Sie können sie mit der 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 Mobilfunkschnittstelle hier nicht aktiviert ist, wird die Schnittstelle ebenfalls deaktiviert.
Verbindung in Gebrauch	Markieren Sie mit grüner Farbe, ob diese Schnittstelle verwendet wird.
Schnittstelle	Zeigen Sie den Namen der Schnittstelle an.
Verbindungstyp	Zeigen Sie an, wie die IP-Adresse in dieser Schnittstelle abgerufen werden kann, z. B. statische IP oder DHCP. Bei Mobilfunk-Schnittstellen wird nur DHCP-Client unterstützt.
IP	Zeigen Sie die IP-Adresse der Schnittstelle an.
	Ziehen Sie diese Schaltfläche, um die Priorität der Netzwerkverbindungen anzupassen. Der oberste Eintrag der Liste hat die höchste Priorität.
Bearbeiten	Klicken Sie hier, um die Ping-Probe-Einstellungen jeder Netzwerkverbindung zu bearbeiten.
Einstellungen	
Auf „Hoch“ zurücksetzen	Wenn diese Option aktiviert ist, wird regelmäßig überprüft, ob die Verbindung mit hoher Priorität

Prioritätsverbindung	pingt werden, und wenn ja, die Verbindung mit einer höheren Priorität umschalten.
Rückstellintervall	Geben Sie die Anzahl der Sekunden an, die Sie warten sollten, bevor Sie zu die Verbindung mit höherer Priorität zu wechseln. 0 bedeutet, dass nicht aktiv gewechselt wird.
Dual-Karten-Umschaltung Verzögerung	Aktivieren oder deaktivieren Sie diese Option, um die Verzögerungszeit für den Wechsel zur Karte mit niedrigerer Karte zu wechseln, wenn die Mobilfunkverbindung mit hoher Priorität fehlschlägt.
Hochprioritäre SIM-Karte erneut verbinden	Aktivieren oder deaktivieren Sie diese Option, um das Intervall für die Erkennung einer Mobilfunkverbindung mit hoher Priorität zu konfigurieren. Wenn die Verbindung wiederhergestellt ist, wird wieder auf die Mobilfunkverbindung mit hoher Priorität zurück.
Notfall-Neustart	Aktivieren Sie diese Option, um das Gerät neu zu starten, wenn keine Verbindung verfügbar ist.

Ping Probe

Enable ☒

When off, the default ping probe passes

IPv4 Primary Server IPv4 Secondary Server IPv6 Primary Server IPv6 Secondary Server Interval sRetry Interval sTimeout sMax Retries

Ping-Prüfung	
Element	Beschreibung
Aktivieren	Wenn diese Option aktiviert ist, überprüft der Router regelmäßig den Verbindungsstatus des Links durch Senden von ICMP-Paketen.
IPv4/IPv6-Primärserver	Der Router sendet ein ICMP-Paket an die IPv4/IPv6-Adresse, um festzustellen, ob die Netzwerkverbindung noch verfügbar ist oder nicht.
IPv4/IPv6-Sekundär Server	Der Router versucht, die alternative Serveradresse anzupingen, wenn Primärserver nicht verfügbar ist.
Intervall	Zeitintervall (in Sekunden) zwischen zwei Pings.
Wiederholungsintervall	Legen Sie das Intervall für Ping-Wiederholungen fest. Wenn der Ping fehlgeschlagen ist, sendet der Router erneut in jedem Wiederholungsintervall.
Zeitlimit	Die maximale Zeit, die der Router auf eine Antwort auf eine Ping-Anfrage wartet. Wenn er innerhalb der in diesem Feld vordefinierten Zeit keine Antwort erhält, wird die Ping-Anfrage als fehlgeschlagen betrachtet.

Maximale Wiederholungsversuche	Die Anzahl der Wiederholungsversuche, die der Router beim Senden von Ping-Anfragen unternimmt, bis feststellt, dass die Verbindung fehlgeschlagen ist.
--------------------------------	--

6.2.1.6 Switch (VLAN)

VLAN ist eine neue Datenaustauschtechnologie, die virtuelle Arbeitsgruppen realisiert, indem sie die LAN-Geräte logisch in Netzwerksegmente unterteilt.

VLAN

Enable
☒

VLAN Setting

VLAN ID	LAN 1	LAN 2	LAN 3	LAN 4	CPU
1	Untagged	Untagged	Untagged	Untagged	Untagged

Add

LAN Setting

Name	VLAN ID	IP Address	Subnet Mask	MTU
LAN	1	192.168.1.1	255.255.255.0	1500

DHCP Server

Name	Interface	Address	IPv4 Lease Time	IPv4 Netmask
DHCP_3	LAN	Start Address: 192.168.1.100 End Address: 192.168.1.199	1440m	255.255.255.0

Edit

Switch	
Element	Beschreibung
VLAN	Aktivieren oder deaktivieren Sie die VLAN-Funktion.
VLAN-Einstellungen	
VLAN-ID	Legen Sie die Label-ID des VLAN fest. Bereich: 3-4094.
LAN 1/2/3/4	Binden Sie das VLAN an die entsprechenden Ports und wählen Sie den Status aus „Getaggt“, „Nicht getaggt“ und „Schließen für Ethernet-Frame auf Trunk-Verbindung“.
CPU	Steuerung der Kommunikation zwischen VLAN und anderen Netzwerken.
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, die sich von WANLAN und andere VLANs.
Subnetzmaske	Legen Sie die Netzmaske des LAN-Ports fest.
MTU	Legen Sie die maximale Übertragungseinheit des LAN-Ports fest. Bereich: 68-1500.

Enable ☒

Interface LAN

Start Address 192.168.1.100

End Address 192.168.1.199

IPv4 Lease Time 1440 m

IPv4 Netmask 255.255.255.0

DNS Server 192.168.1.1  

Switch – DHCP-Server	
Element	Beschreibung
Aktiv	Aktivieren Sie diese Option, um DHCP für diese VLAN-Schnittstelle zu deaktivieren. Der DHCP-Server kann nur gelöscht werden, wenn Sie die entsprechenden LAN-Einstellungen gelöscht haben.
Schnittstelle	Zeigt den VLAN-Schnittstellennamen des DHCP-Servers an.
Startadresse	Definieren Sie den Anfang des Pools von IP-Adressen, die an DHCP-Clients vergeben werden.
Endadresse	Definieren Sie das Ende des Pools von IP-Adressen, die an DHCP-Clients vermietet werden.
IPv4-Lease-Zeit	Legen Sie die Ablaufzeit der vermieteten Adressen fest, das Minimum beträgt 2 Minuten (2m).
IPv4-Netzmaske	Legen Sie diese fest, um die an Clients gesendete Netzmaske zu überschreiben. Normalerweise wird sie aus dem bedienten Subnetz berechnet.
DNS-Server	Legen Sie die DNS-Serverliste für Clients fest.

6.2.1.7 Zuweisung statischer IP-Adressen

Wenn die LAN/VLAN-Schnittstelle als DHCP-Server fungiert, können Benutzer Geräten mit festen MAC-Adressen feste IP-Adressen und symbolische Hostnamen zuweisen.

Static IP Address Assignment

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. It can be connected by the assigned host via the interface with a non-dynamic configuration. Add new lease items with Add Button. The address and the value of the hostname field will be assigned to the host identified by the MAC address field. The tenancy term, an optional field, is able to set the duration of DHCP tenancy term for every host individually.

Hostname	MAC Address	IPv4 Address	IPv4 Lease Time	
			m	
				

Zuweisung statischer IP-Adressen	
Element	Beschreibung
Hostname	Der Hostname statischer Leases.

MAC-Adresse	Die MAC-Adresse des DHCP-Clients.
IPv4-Adresse	Die dem Client zugewiesene IPv4-Adresse.
IPv4-Lease-Zeit	Verbleibende Zeit für den Client.

6.2.2 WLAN

6.2.2.1 WLAN

In diesem Abschnitt wird erläutert, wie Sie die entsprechenden Parameter für ein WLAN-Netzwerk einstellen. Der UR75 unterstützt sowohl 2,4-GHz- als auch 5-GHz-WLAN, die gleichzeitig betrieben werden können.

WLAN1-2.4G
WLAN2-5G
Advanced Settings

Enable ☒

Work Mode

AP

BSSID

24:e1:24:f5:af:cc

Radio Type

802.11bgn/ax mixed

Channel

Channel 11 (2462 GHz)

Bandwidth

40 MHz

SSID

Router_F5AFCC_2.4G

Encryption Mode

WPA2-PSK/WPA3-PSK

Cipher

AES

Key

.....

Group Rekey Interval

3600

 s

SSID Broadcast ☒

AP Isolation ☐

Max Client Number

128

WLAN	
Element	Beschreibung
Aktivieren	WLAN aktivieren/deaktivieren.

Arbeitsmodus	Wählen Sie den Arbeitsmodus des Routers aus. Die Optionen sind „Client“ oder „AP“.
AP-Modus	
BSSID	Zeigt die MAC-Adresse dieser WLAN-Schnittstelle an.
Funkmodus	Wählen Sie den Funktyp aus.
Kanal	Wählen Sie einen Funkkanal zwischen 1 und 13 oder wählen Sie „Auto“.
Bandbreite	Wählen Sie die Bandbreite aus. Die Optionen sind 20 MHz und 40 MHz.
SSID	Geben Sie die SSID des Zugangspunkts ein.
Verschlüsselungsmodus	Wählen Sie den Verschlüsselungsmodus aus. Die Optionen sind Keine Verschlüsselung, WEP Open System, WEP Auto, WEP Shared Key, WPA-PSK, WPA2-PSK, WPA3-PSK, WPA-PSK/WPA2-PSK und WPA2-PSK/WPA3-PSK.
Verschlüsselung	Wählen Sie die Verschlüsselung aus, wenn Sie den PSK-Verschlüsselungsmodus verwenden. Die Optionen sind AES, TKIP und AES/TKIP.
Schlüssel	Geben Sie den Schlüssel ein, um eine Verbindung zu diesem Zugangspunkt herzustellen. Der Standardschlüssel lautet „ iotpassword “.
Gruppen-Schlüsselaktualisierung Intervall	Das Intervall für die Änderung des Verschlüsselungsschlüssels.
SSID Übertragung	Wenn die SSID-Übertragung deaktiviert ist, können andere drahtlose Geräte die SSID nicht finden, und Benutzer müssen die SSID manuell eingeben, um auf das drahtlose Netzwerk zugreifen zu können. .
AP-Isolation	Wenn die AP-Isolation aktiviert ist, werden alle Benutzer, die auf den AP zugreifen, isoliert und können nicht miteinander kommunizieren.
Max. Client Anzahl	Legen Sie die maximale Anzahl von Clients fest, die zugreifen können, wenn der Router als AP konfiguriert ist.
MAC-Filterung	Aktivieren Sie diese Option, um die Clients zu filtern, die sich mit diesem Zugangspunkt verbinden dürfen.
Typ	Wählen Sie den Filtertyp für Geräte, die mit dem WLAN-Zugangspunkt dieses Routers verbunden sind. Whitelist: Nur die aufgeführten MAC-Adressen dürfen eine Verbindung zum WLAN-Zugangspunkt des Routers herstellen. Blacklist: Die aufgeführten MAC-Adressen dürfen keine Verbindung zum WLAN-Zugangspunkt des Routers verbinden.
MAC Adresse	Die MAC-Adressen der Geräte, die blockiert oder zugelassen werden sollen.
Beschreibung	Die Beschreibung dieser MAC-Adresse.
Client-Modus	
Scannen	Klicken Sie hier, um die Zugangspunkte in der Umgebung dieses Geräts zu scannen.
SSID	Geben Sie die SSID des Zugangspunkts ein.
BSSID	Geben Sie die MAC-Adresse des Zugangspunkts ein. Entweder die SSID oder die BSSID kann eingegeben werden, um sich mit dem Netzwerk zu verbinden.
Kanal	Wählen Sie einen WLAN-Kanal von 1 bis 13 oder wählen Sie „Auto“.
Verschlüsselungsmodus	Wählen Sie den Verschlüsselungsmodus aus. Die Optionen sind „Keine Verschlüsselung“, „WPA-PSK“, WPA2-PSK, WPA3-PSK, WPA-PSK/WPA2-PSK und WPA2-PSK/WPA3-PSK.
Verschlüsselung	Wählen Sie die Verschlüsselungsmethode für die WPA-Verschlüsselung aus. Die Optionen sind „AES“, „TKIP“ und „AES/TKIP“.
Schlüssel	Geben Sie den Schlüssel ein, um eine Verbindung zu diesem Zugangspunkt herzustellen.

IP-Einstellung	
Protokoll	Legen Sie das Protokoll fest, um die WLAN-IP-Adresse zu erhalten.
IPv4-Adresse	Legen Sie die IP-Adresse im drahtlosen Netzwerk fest, wenn das Protokoll „Statische IP“ lautet. Beachten Sie, dass das Subnetz dieser IP-Adresse sich vom WAN-Port unterscheiden sollte.
Netzmaske	Stellen Sie die Netzmaske im drahtlosen Netzwerk ein, wenn das Protokoll „Statische IP“ lautet.
Gateway	Stellen Sie das Gateway im drahtlosen Netzwerk ein, wenn das Protokoll „Statische IP“ lautet.
Bevorzugt DNS	Legen Sie den primären IPv4-DNS-Server fest.
Alternativ DNS	Legen Sie den sekundären IPv4-DNS-Server fest.

SSIDs							
SSID	BSSID	Encryption Mode	Cipher	Channel	Frequency	Signal	
Router_F5AD14_2.4G	24:E1:24:F5:AD:14	WPA2-PSK/WPA3-PSK	AES	9	2452MHz	-9dBm	Join Network
235-ttt	24:E1:24:F8:83:45	No Encryption	NONE	11	2462MHz	-20dBm	Join Network
AnshinNEO_5G_F8CA9E_RPT	04:42:1A:DC:BA:30	WPA2-PSK	AES	2	2417MHz	-39dBm	Join Network
9F5AFCC_2.4G11	24:E1:24:F5:AF:CC	No Encryption	NONE	8	2447MHz	-40dBm	Join Network
Gateway_556689	22:33:44:55:66:89	No Encryption	NONE	1	2412MHz	-42dBm	Join Network

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

Verwandtes Thema

[Beispiel für eine WLAN-Anwendung](#)

6.2.2.2 Erweiterte Einstellungen

Das Gerät unterstützt die Auswahl des Ländercodes zur Anpassung des Kanals und der Sendeleistung.

WLAN1-2.4G WLAN2-5G **Advanced Settings**

Country Code AT-AUSTRIA

If the selected country code does not support the originally set channel, the channel will change to Auto after restarting the wireless.

6.2.3 Firewall

In diesem Abschnitt wird beschrieben, wie Sie die Firewall-Parameter einstellen, darunter Sicherheit, ACL, DMZ Port-Zuordnung und benutzerdefinierte iptables-Regeln. Nach der Einstellung können Sie unter „Status > Firewall“ überprüfen, ob die Firewall-Einstellungen funktionieren.

6.2.3.1 Allgemeine Einstellungen

Security Configuration

Enable SYN-flood protection ☒

Log in via HTTPS by default ☒

Access Control

Name	Port	Local Access	Remote Access
HTTP	80	☒	☐
HTTPS	443	☒	☐
SSH	22	☒	☐
TELNET	23	☒	☐

URL Filter

Domain Name Keyword Filter

Example: To filter www.google.com, enter google.

Allgemeine Einstellungen		
Element	Beschreibung	Standard
Sicherheitskonfiguration		
SYN-Flood-Schutz aktivieren	Aktivieren/Deaktivieren Sie den SYN-Flood-Schutz. Der SYN-Flood-Schutz schützt vor DDoS-Angriffen, die einen Teil des normalen TCP-Drei-Wege-Handshakes ausnutzen, um Ressourcen auf dem Zielserver zu verbrauchen und ihn unbrauchbar zu machen.	Aktivieren
Standardmäßig über HTTPS anmelden standardmäßig	Standardmäßig über HTTPS in die Web-GUI des Geräts einloggen.	Aktivieren
Zugriffskontrolle		
Port	Legen Sie die Portnummer der Dienste fest. Bereich: 1-65535.	--
Lokaler Zugriff	Greifen Sie lokal auf den Router zu.	Aktivieren
Fernzugriff	Greifen Sie remote auf den Router zu.	Deaktivieren
HTTP	Benutzer können sich lokal über HTTP beim Gerät anmelden, um und es über das Web steuern, nachdem die Option	80

	aktiviert ist.	
HTTPS	Benutzer können sich lokal und remote über HTTPS beim Gerät anmelden, um über das Web darauf zuzugreifen und es zu steuern , nachdem die Option aktiviert wurde.	443
TELNET	Benutzer können sich lokal und remote über Telnet beim Gerät anmelden über Telnet anmelden, nachdem die Option aktiviert wurde.	23
SSH	Benutzer können sich lokal und remote über SSH, nachdem die Option aktiviert wurde.	22
URL-Filter		
Domainname-Stichwortfilter	Sie können bestimmte Websites blockieren, indem Sie ein Schlüsselwort aus einem Domainnamen eingeben. Nach dem Filtern können die Geräte unter den LAN-Ports nicht mehr auf die entsprechenden Websites zugreifen. Die maximal zulässige Anzahl von Zulässige Zeichenanzahl: 64.	

6.2.3.2 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 ein Router ein Paket empfängt, wird das Feld gemäß der für die aktuelle Schnittstelle geltenden ACL-Regel analysiert. Nachdem das spezielle Paket identifiziert wurde, wird die Erlaubnis oder Verweigerung des entsprechenden Pakets gemäß der voreingestellten Strategie implementiert. Die von der ACL definierten Datenpaket-Übereinstimmungsregeln können auch von anderen Funktionen verwendet werden, die eine Unterscheidung des Datenflusses erfordern.

ACL

Policy Priority: DMZ > DNAT > Access Service Control > ACL

List Priority: The priority is lowered in accordance with the table from top to bottom.

Default Filter Policy: Accept

Name	Match Rule	Action	Enable
Rule1	Forwarded IPv4, protocol TCP, UDP, ICMP From WAN(WAN, Cellular) IP 0.0.0.0/0 To LAN IP 0.0.0.0/0	Accept forward	☒

⋮ Edit Delete Add

ACL	
Element	Beschreibung
Standardfilterrichtlinie	Pakete, die nicht in der Zugriffskontrollliste enthalten sind, werden gemäß der Standardfilterrichtlinie verarbeitet. Akzeptieren: Erlaubt den gesamten Datenverkehr aus Geräten unter LAN-Ports. Verwerfen: Verweigern Sie den gesamten Datenverkehr aus Geräten unter LAN-Ports.
Aktivieren	Aktivieren Sie diese ACL-Regel.
⋮	Ziehen Sie diese Schaltfläche, um die Priorität der ACL-Regeln anzupassen. Der Anfang der Liste hat die höchste Priorität.
Bearbeiten	Klicken Sie hier, um die Details dieser ACL-Regel zu bearbeiten.
Löschen	Diese ACL-Regel löschen.

Name	Rule1
IP Type	IPv4
Protocol	TCP UDP ICMP
Source Interface	WAN(WAN, Cellular)
Source Type	IP
Source IP Address	0.0.0.0/0 Eg:192.168.1.1 or 192.168.1.1/24
Source port	Any Port You can enter the port number, or enter 20-300
Destination Interface	LAN
Destination IP Address	0.0.0.0/0 Eg:192.168.1.1 or 192.168.1.1/24
Destination port	Any Port You can enter the port number, or enter 20-300
Action	Accept

ACL – Hinzufügen/Bearbeiten	
Name	Legen Sie einen eindeutigen Namen für diese ACL-Regel fest.
Typ	Wählen Sie den Typ IPv4 oder IPv6 aus.
Protokoll	Wählen Sie das Protokoll aus TCP, UDP und ICMP aus.
Quellschnittstelle	Wählen Sie den Quellschnittstellentyp aus „Geräteausgang“, „LAN“, „VLAN“ oder „WAN“ (WAN, Mobilfunk, WLAN). „Geräteausgang“ bedeutet, dass die Pakete vom Router selbst kommen.
Quellentyp	Bei Verwendung des IPv4-Typs wählen Sie den Adresstyp als IP, MAC oder IP+MAC aus.
Quell-IP/MAC Adresse	Quellnetzwerkadresse entsprechend dem Adresstyp festlegen. (0.0.0.0/0 bedeutet alle).
Quellport	Legen Sie eine bestimmte Quellportnummer oder einen Portbereich fest, Beispiel: 20-300.
Zielschnittstelle	Wählen Sie den Zielschnittstellentyp aus LAN, WAN (WAN, Mobilfunk, WLAN), VLAN oder Geräteeingang. Geräteeingang bedeutet, dass die Pakete an den Router selbst gesendet werden.
Ziel-IP Adresse	Legen Sie die Zielnetzwerkadresse fest (0.0.0.0/0 bedeutet alle).
Zielport	Legen Sie eine bestimmte Quellportnummer oder einen Portbereich fest, Beispiel: 20-300.
Aktion	Wählen Sie die Aktion „Akzeptieren“ oder „Ablehnen“.

6.2.3.3 Portzuordnung (DNAT)

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

Port Mapping(DNAT)

When external services are needed internally (for example, when a website is published externally), the external address initiates an active connection. And, the router or the gateway on the firewall receives the connection. Then it will convert the connection to the internal. This conversion is called DNAT, which is mainly used for external and internal services.

List Priority: The priority is lowered in accordance with the table from top to bottom.

Name	Protocol	External IP Address	External Port	Internal IP Address	Internal Port	Enable	
	TCP UDP ▼	0.0.0.0/0		192.168.1.1		☒	☰ Delete

[Add](#)

Portzuordnung (DNAT)	
Artikel	Beschreibung
Name	Legen Sie einen eindeutigen Namen für die Portzuordnungsregel fest.
Protokoll	Wählen Sie TCP oder UDP entsprechend den Anforderungen Ihrer Anwendung aus.
Externe IP-Adresse	Geben Sie den Host oder das Netzwerk an, das auf die lokale IP-Adresse zugreifen kann. 0.0.0.0/0 bedeutet alle.
Externer Port	Legen Sie den Port oder Portbereich fest, von dem aus eingehende Pakete weitergeleitet werden, Beispiel: 20-300.
Interne IP-Adresse	Geben Sie die IP-Adresse ein, an die Pakete weitergeleitet werden, nachdem Empfang über die eingehende Schnittstelle weitergeleitet werden.
Interner Port	Geben Sie den Port oder Portbereich ein, an den Pakete nach dem Empfang vom/von den eingehenden Port(s) weitergeleitet werden. Bei der Einstellung des Portbereichs sollte der Wert mit dem externen Portbereich übereinstimmen.
Aktivieren	Aktivieren oder deaktivieren Sie diese Portzuordnungsregel.
☰	Ziehen Sie diese Schaltfläche, um die Priorität der Portzuordnungsregeln anzupassen. Die oberste Eintrag in der Liste hat die höchste Priorität.
Löschen	Löschen Sie diese Regel.

Beispiel für eine zugehörige Konfiguration

[NAT-Anwendungsbeispiel](#)

6.2.3.4 DMZ

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

DMZ

The DMZ host is an intranet host whose ports are only open to the specific addresses except for the occupied and forwarded ports. After enabling DMZ, all data received from the source IP address by the router will be forwarded to the DMZ host IP address filled in.

Enable ☒

DMZ Host

Source IP Address

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

6.2.3.5 Benutzerdefinierte Regeln

Auf dieser Seite können Sie Ihre eigenen benutzerdefinierten Firewall-iptables-Regeln eingeben, die als Linux-Shell-Skript ausgeführt werden.

Firewall - Custom Rules

Custom rules allow you to execute the iptables commands of firewall. Note that the URL filtering command is invalid.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
```

6.2.3.6 Zertifikate

Auf dieser Seite können Sie die HTTPS-Zertifikate für den sicheren Zugriff auf die Web-GUI des Routers importieren.

HTTPS Certificate

Certificate		Browse	Export	Delete
Key		Browse	Export	Delete

6.2.4 Statische Routen

Eine statische Route ist ein manuell konfigurierter Routing-Eintrag. Die Informationen zum Routing werden manuell eingegeben und nicht aus dem dynamischen Routing-Verkehr abgerufen. Nach der Einrichtung der statischen Route wird das Paket für das angegebene Ziel an den vom Benutzer festgelegten Pfad weitergeleitet.

Static IPv4 Routes

Interface	Destination Network	IPv4 Netmask	IPv4 Gateway	Priority	MTU	
WAN	192.168.45.0	255.255.255.0	192.168.45.1	1	1500	Delete
Add						

Static IPv6 Routes				
Interface	Destination Network	IPv6 Gateway	Priority	MTU
This section contains no values now.				

Statische Routen	
Element	Beschreibung
Schnittstelle	Über die Schnittstelle gelangen die Daten zur Zieladresse.
Ziel Netzwerk	Geben Sie die Ziel-IPv4/IPv6-Adresse ein.
IPv4-Netzmaske	Geben Sie die Subnetzmaske der IPv4-Zieladresse ein.
IPv4/IPv6 Gateway	IPv4/IPv6-Adresse des nächsten Routers, der passiert wird, bevor die Eingangsdaten die Zieladresse erreichen.
Priorität	Ein kleinerer Wert bedeutet eine höhere Priorität. Bereich: 1-255.
MTU	Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500.

6.2.5 IP-Passthrough

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

Enable	☒
Passthrough Mode	DHCPs-Fixed
MAC	

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, wenn der Passthrough-Modus „DHCPs-Fixed“ ist.

6.2.6 DDNS

Dynamic DNS (DDNS) ist eine Methode, die einen Nameserver in der Domain Name

System, mit dem Benutzer eine dynamische IP-Adresse einem statischen Domainnamen zuordnen 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.

Status Disconnected

Enable ☒

Service Provider Custom

User name

User ID

Password

Server

Server Path

Host Name

Append IP ☐

HTTPS ☐

DDNS	
Element	Beschreibung
Status	Zeigt den Verbindungsstatus von DDNS an.
Aktiv	DDNS aktivieren/deaktivieren.
Dienstanbieter	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 zum DDNS-Server-Update-Pfad hinzu.
HTTPS	Aktivieren Sie HTTPS für einige DDNS-Anbieter.

6.2.7 Diagnose

Netzwerkdienstprogramme umfassen IPv4/IPv6-Ping, IPv4/IPv6-Traceroute und das Befehlszeilentool nslookup.

Execution of various network commands to check the connection and name resolution to other systems.

IPv4 Ping
 IPv4 Traceroute
 Nslookup

Netzwerkdienstprogramme	
Element	Beschreibung
IPv4-Ping	Klicken Sie hier, um vom Gerät in IPv4 aus ein Ping an das externe Netzwerk zu senden.
IPv6-Ping	Klicken Sie hier, um das externe Netzwerk vom Gerät in IPv6 aus anzupingen.
IPv4-Traceroute	Adresse des Zielhosts, der in IPv4 erkannt werden soll.
IPv6-Traceroute	Adresse des Zielhosts, der in IPv6 erkannt werden soll.
Nslookup	Klicken Sie hier, um die Zuordnung zwischen Domänenname und IP-Adresse oder andere DNS-Einträge anzuzeigen.

6.3 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.

6.3.1 OpenVPN

OpenVPN ist ein Open-Source-Produkt für virtuelle private Netzwerke (VPN), das ein vereinfachtes Sicherheitsframework, ein modulares Netzwerkdesign und plattformübergreifende Portabilität bietet. Die Standardversion von OpenVPN für UR75 ist 2.5.3.

6.3.1.1 OpenVPN-Server

UR75 unterstützt OpenVPN-Server, um sichere Punkt-zu-Punkt- oder Standort-zu-Standort-Verbindungen in gerouteten oder gebrückten Konfigurationen und Fernzugriffsfunktionen zu erstellen. Sie können die ovpn-Datei direkt importieren oder die Parameter auf dieser Seite konfigurieren, um diesen Server einzurichten.

OpenVPN Server

Enable ☒

Configuration Method

Configuration File **Browse** **Edit** **Export** **Delete**

OpenVPN-Server – Dateikonfiguration

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

Configuration Method	Page Configuration	▼
Protocol	UDP	▼
Port	1194	
Listening IP		
Network Interface	tun	▼
Authentication Type	None	▼
Local Virtual IP	10.8.0.1	
Remote Virtual IP	10.8.1.1	
Compression	LZO	▼
Ping Detection Interval	60	s
Ping Detection Timeout	300	s
Encryption Mode	None	▼
MTU	1500	
Max Frame Size	1500	
Log Level	Notice	▼
Expert Options		

Account

Username	Password
This section contains no values now.	

Add Account

Local Router

Subnet	Subnet Mask
This section contains no values now.	

Add Router

Client Subnet

Name	Subnet	Subnet Mask
This section contains no values now.		

Add Subnet

OpenVPN-Server – Seitenkonfiguration	
Element	Beschreibung
Protokoll	Wählen Sie ein Transportprotokoll für die Verbindung aus UDP und TCP aus.
Zuhörende IP	Geben Sie den lokalen Hostnamen oder die IP-Adresse für die Bindung ein. Wenn das Feld leer bleibt, verbindet sich der OpenVPN-Server an alle Schnittstellen gebunden.
Port	Geben Sie die TCP/UDP-Servicenummer für die OpenVPN-Clientverbindung ein. Bereich: 1-65535.
Netzwerkschnittstelle	Wählen Sie den Typ der virtuellen VPN-Netzwerkschnittstelle aus TUN und TAP aus. TUN-Geräte kapseln IPv4 oder IPv6 (OSI-Schicht 3), während TAP-Geräte Ethernet 802.3 (OSI-Schicht 2) kapseln.
Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird. Vorab geteilt: Verwenden Sie denselben geheimen Schlüssel wie der Server, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite VPN > OpenVPN > Zertifikate, um eine statische Datei (static.key) in das Feld PSK zu importieren. Benutzername/Passwort: Verwenden Sie den auf der Serverseite voreingestellten Benutzernamen/das Passwort, um die Authentifizierung abzuschließen. X.509-Zertifikat: Verwenden Sie ein Zertifikat vom Typ X.509, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite VPN > OpenVPN > Zertifizierungen, um das CA-Zertifikat, das Client-Zertifikat und den privaten Client-Schlüssel in die entsprechenden Felder zu importieren. X.509-Zertifikat + Benutzer: Verwenden Sie sowohl Benutzername/Passwort als auch X.509-Zertifikat als Authentifizierungstyp verwenden.
Lokale virtuelle IP	Legen Sie die lokale Tunneladresse fest, wenn der Authentifizierungstyp „Keine“ oder „Vorab geteilt“ ist.
Virtuelle Remote-IP	Legen Sie die Remote-Tunneladresse fest, wenn der Authentifizierungstyp „Keine“ oder „Vorab geteilt“ lautet. „Vorab geteilt“ ist.
Client-Subnetz	Definieren Sie einen IP-Adresspool für den OpenVPN-Client.
Client-Netzmaske	Legen Sie die Netzmaske des Client-Subnetzes fest, um den IP-Adressbereich zu begrenzen.
Neuverhandlungsintervall	Verhandeln Sie den Datenkanalschlüssel nach diesem Intervall neu. 0 bedeutet deaktivieren.
Maximale Anzahl von Clients	Begrenzen Sie den Server auf eine maximale Anzahl gleichzeitiger Clients, Bereich: 1-128. Hinweis: Bitte stellen Sie die Protokollierungsstufe auf „Info“ ein, wenn Sie viele Clients verbinden müssen.
CRL aktivieren	CRL-Überprüfung aktivieren oder deaktivieren.
Client-zu-Client aktivieren	Wenn diese Option aktiviert ist, können OpenVPN-Clients miteinander kommunizieren.

Dup-Client aktivieren	Ermöglicht mehreren Clients, sich mit demselben gemeinsamen Namen oder derselben gemeinsamen Zertifizierung zu verbinden. Zertifizierung.
TLS-Authentifizierung aktivieren	Deaktivieren oder aktivieren Sie die TLS-Authentifizierung, wenn der Authentifizierungstyp „X.509-Zertifikat“ ist. Nach der Aktivierung gehen Sie zur Seite „VPN > OpenVPN > Zertifikate“, um eine ta.key-Datei in das Feld „TA“ zu importieren. Hinweis: Diese Option unterstützt nur tls-auth. Für tls-crypt fügen Sie bitte diese Formatzeichenfolge in der Expertenoption hinzu: tls-crypt /etc/openvpn/openvpn-client1-ta.key
Komprimierung	Wählen Sie diese Option, um LZO zur Komprimierung von Daten zu aktivieren oder zu deaktivieren.
Ping-Erkennungsintervall	Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Wenn dies festgelegt ist Sowohl auf dem Server als auch auf dem Client überschreibt der vom Server übertragene Wert die lokalen Werte des Clients. Bereich: 10-1800 s.
Zeitlimit für Ping-Erkennung	OpenVPN wird nach Ablauf des Zeitlimits neu aufgebaut. Wenn dies sowohl auf dem Server und dem Client festgelegt ist, überschreibt der vom Server übermittelte Wert die lokalen Werte des Clients. Bereich: 60-3600 s.
Verschlüsselungsmodus	Wählen Sie zwischen NONE, 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: 68-1500.
Maximale Frame-Größe	Legen Sie die maximale Frame-Größe fest. Bereich: 64-1500.
Ausführlichkeitsstufe	Wählen Sie zwischen ERROR, WARNING, NOTICE und DEBUG.
Expertenoptionen	Der Benutzer kann in diesem Feld einige Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen. Beispiel: auth SHA256; key direction 1
Konto	
Benutzername und Passwort	Legen Sie den Benutzernamen und das Passwort für den OpenVPN-Client fest, wenn der Authentifizierungstyp „Benutzername/Passwort“ ist.
Lokaler Router	
Subnetz	Legen Sie die IP-Adresse der lokalen Route fest.
Subnetzmaske	Legen Sie die Netzmaske der lokalen Route fest.
Client-Subnetz	
Name	Legen Sie den Namen als allgemeinen Namen des OpenVPN-Client-Zertifikats fest.
Subnetz	Legen Sie das Subnetz des OpenVPN-Clients fest.
Subnetzmaske	Legen Sie die Subnetzmaske des OpenVPN-Clients fest.

6.3.1.2 OpenVPN-Client

UR75 unterstützt die gleichzeitige Ausführung von maximal 3 OpenVPN-Clients. Sie können die ovpn-Datei direkt importieren oder die Parameter auf dieser Seite konfigurieren, um Clients einzurichten.

Client_1

Enable ☒

Configuration Method

File Configuration

Configuration File

Browse

Edit

Export

Delete

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

Configuration Method

Page Configuration

Protocol

UDP

Port

1194

Remote Address

Network Interface

tun

Authentication Type

None

Local Virtual IP

Remote Virtual IP

Compression

LZO

Ping Detection Interval

60

s

Ping Detection Timeout

300

s

Encryption Mode

None

MTU

1500

Max Frame Size

1500

Log Level

Notice

Expert Options

Local Router

Subnet

Subnet Mask

This section contains no values now.

Add Router

OpenVPN-Client – Seitenkonfiguration

Element	Beschreibung
Protokoll	Wählen Sie ein Transportprotokoll aus, das durch die Verbindung von UDP und TCP verwendet wird.
Remote-IP-Adresse	Geben Sie die IP-Adresse oder den Domännennamen des Remote-OpenVPN-Servers ein.
Port	Geben Sie die TCP/UDP-Servicenummer des Remote-OpenVPN-Servers ein. Bereich: 1-65535.
Netzwerkschnittstelle	Wählen Sie den Typ der virtuellen VPN-Netzwerkschnittstelle aus TUN und TAP aus. TUN-Geräte kapseln IPv4 oder IPv6 (OSI-Schicht 3), während TAP-Geräte Ethernet 802.3 (OSI-Schicht 2) kapseln.
Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird. Vorab geteilt: Verwenden Sie denselben geheimen Schlüssel wie der Server, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite VPN > OpenVPN > Zertifikate , um eine statische Datei (static.key) in das Feld PSK zu importieren. Benutzername/Passwort: Verwenden Sie den auf der Serverseite voreingestellten Benutzernamen/das Passwort, um die Authentifizierung abzuschließen. X.509-Zertifikat: Verwenden Sie ein Zertifikat vom Typ X.509, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite VPN > OpenVPN > Zertifizierungen , um das CA-Zertifikat, das Client-Zertifikat und den privaten Client-Schlüssel in die entsprechenden Felder zu importieren. X.509-Zertifikat + Benutzer: Verwenden Sie sowohl Benutzername/Passwort als auch X.509-Zertifikat als Authentifizierungstyp verwenden.
Lokale virtuelle IP	Legen Sie die lokale Tunneladresse fest, wenn der Authentifizierungstyp „Keine“ oder „Vorab geteilt“ ist.
Virtuelle Remote-IP	Legen Sie die Remote-Tunneladresse fest, wenn der Authentifizierungstyp „Keine“ oder „Vorab geteilt“ lautet. „Vorab geteilt“ .
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über den OpenVPN-Tunnel gesendet, wenn diese Funktion aktiviert ist.
TLS-Authentifizierung aktivieren	Deaktivieren oder aktivieren Sie die TLS-Authentifizierung, wenn der Authentifizierungstyp „X.509-Zertifikat“ ist. Nach der Aktivierung gehen Sie zur Seite „VPN > OpenVPN > Zertifikate“ , um eine ta.key-Datei in das Feld „TA“ zu importieren. Hinweis: Diese Option unterstützt nur tls-auth. Für tls-crypt fügen Sie bitte diese Formatzeichenfolge in der Expertenoption hinzu: tls-crypt /etc/openvpn/openvpn-client1-ta.key
Komprimierung	Wählen Sie diese Option, um LZO zur Komprimierung von Daten zu aktivieren oder zu deaktivieren.
Ping-Erkennungsintervall	Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Wenn dies festgelegt ist Sowohl auf dem Server als auch auf dem Client überschreibt der vom Server übertragene Wert die

	lokalen Werte des Clients. Bereich: 10-1800 s.
Zeitlimit für Ping-Erkennung	OpenVPN wird nach Ablauf des Zeitlimits neu aufgebaut. Wenn dies sowohl auf dem Server als auch auf dem Client eingestellt ist, überschreibt der vom Server übermittelte Wert die lokalen Werte des Clients . Bereich: 60-3600 s.
Verschlüsselungsmodus	Wählen Sie zwischen NONE, 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: 128-1500.
Maximale Frame-Größe	Legen Sie die maximale Bildgröße fest. Bereich: 128-1500.
Ausführlichkeitsstufe	Wählen Sie zwischen ERROR, WARNING, NOTICE und DEBUG.
Expertenoptionen	Der Benutzer kann in diesem Feld einige Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen. Beispiel: auth SHA256; key direction 1
Lokale Route	
Subnetz	Legen Sie die IP-Adresse der lokalen Route fest.
Subnetzmaske	Legen Sie die Netzmaske der lokalen Route fest.

Beispiel für eine zugehörige Konfiguration

[Beispiel für eine OpenVPN-Client-Anwendung](#)

6.3.1.3 Zertifikat

Bei Verwendung der Seitenkonfiguration des OpenVPN-Servers oder -Clients kann der Benutzer die erforderlichen Zertifikats- und Schlüsseldateien entsprechend den Authentifizierungstypen auf diese Seite importieren/exportieren.

Server

CA Certificate

Browse

Export

Delete

Certificate

Browse

Export

Delete

Private key

Browse

Export

Delete

DH

Browse

Export

Delete

TA

Browse

Export

Delete

CRL

Browse

Export

Delete

PSK

Browse

Export

Delete

Client_1

CA Certificate

Browse

Export

Delete

Certificate

Browse

Export

Delete

Private key

Browse

Export

Delete

TA

Browse

Export

Delete

PSK

Browse

Export

Delete

6.3.2 IPsecVPN

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 einzelnen Computern 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.

6.3.2.1 IPSec-Server

Enable ☒

IPsec Mode

IPsec Protocol

Local Subnet

Local Subnet Mask

Local ID Type

Remote Subnet

Remote Subnet Mask

Remote ID Type

SA Encryption Algorithm

SA Authentication Algorithm

PFS Group

SA Lifetime s

DPD Time Interval s

DPD Timeout s

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

	FQDN: Vollständig qualifizierter Domänenname, Beispiel: test.user.com Benutzer-FQDN: Vollständig qualifizierte Benutzername-Zeichenfolge im E-Mail-Adressformat, Beispiel: test@user.com
SA-Verschlüsselungsalgorithmus	Wählen Sie AES128, AES192 oder AES256.
SA-Authentifizierung Algorithmus	Wählen Sie SHA1 oder SHA2-256.
PFS-Gruppe	Wählen Sie NULL, MODP768_1, MODP1024_2 oder MODP1536_5.
SA-Lebensdauer	Legen Sie die Lebensdauer der IPsec-SA fest. Bereich: 60-86400 s.
DPD-Intervallzeit	Legen Sie das DPD-Wiederholungsintervall für das Senden von DPD-Anfragen fest. Bereich: 2-60 s
DPD-Zeitlimit	Bei Verwendung von IKE V1 legen Sie das DPD-Zeitlimit fest, um den Ausfall der Gegenstelle zu erkennen . Bereich: 10-3600 s.

IKE Parameter ☒

IKE Version

Negotiation Mode

Encryption Algorithm

Authentication Algorithm

DH Group

Local Authentication

XAUTH ☐

Lifetime s

PSK List

Selector	PSK
This section contains no values now.	

[Add](#)

IPsec Advanced ☒

Enable Compression ☐

Margintime s

Expert Options

IKE-Parameter	
Element	Beschreibung
IKE-Version	Wählen Sie die Methode für den Schlüsselaustausch aus IKEv1 und IKEv2 aus.
Verhandlungsmodus	Bei Verwendung von IKEv1 wählen Sie „Main“ oder „Aggressive“.
Verschlüsselungsalgorithmus	Wählen Sie DES, 3DES, AES128, AES192 oder AES256.
Authentifizierungsalgorithmus	Wählen Sie MD5, SHA1 oder SHA2-256.
DH-Gruppe	Wählen Sie MODP768_1, MODP1024_2 oder MODP1536_5.
Lokale Authentifizierung	Wählen Sie PSK oder CA. PSK: Verwenden Sie einen vorab geteilten Schlüssel, um die Authentifizierung abzuschließen. CA: Verwenden Sie ein Zertifikat, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite VPN > IPsec > Zertifizierungen, um das CA-Zertifikat, das lokale Zertifikat und den privaten Schlüssel in die entsprechenden Felder zu importieren.
Remote-Authentifizierung	Bei Verwendung von IKEv2 wählen Sie PSK oder CA. PSK: Verwenden Sie einen vorab geteilten Schlüssel, um die Authentifizierung abzuschließen. CA: Verwenden Sie ein Zertifikat, um die Authentifizierung abzuschließen.

XAUTH	Bei Verwendung von IKEv1 definieren Sie den XAUTH-Benutzernamen und das Passwort nach XAUTH aktiviert ist.
Lebensdauer	Legen Sie die Lebensdauer in der IKE-Verhandlung fest. Bereich: 60-86400 s.
XAUTH-Liste	
Benutzername	Definieren Sie den Benutzernamen, der für die Client-Xauth-Authentifizierung verwendet wird.
Passwort	Legen Sie das Passwort fest, das für die Client-Xauth-Authentifizierung verwendet wird.
PSK-Liste	
Selektor	Stellen Sie den Selektor als IP-Adresse oder lokale ID des IPsec-Clients ein. Wenn er leer bleibt leer gelassen wird, können alle Clients diesen PSK zur Authentifizierung verwenden.
PSK	Definieren Sie den vorab geteilten Schlüssel.
IPsec erweitert	
Komprimierung aktivieren	Der Kopf des IP-Pakets wird nach der Aktivierung komprimiert.
Margintime	Legen Sie eine erweiterte Zeit vor Ablauf der Lebensdauer fest, um die Neuverhandlung zu beginnen.
Expertenoptionen	Der Benutzer kann in diesem Feld einige andere Initialisierungszeichenfolgen eingeben, um zusätzliche Einstellungen und trennen Sie die Zeichenfolgen durch Semikolons.

6.3.2.2 IPsec-Client

UR75 unterstützt die gleichzeitige Ausführung von maximal 3 IPsec-Clients.

Enable ☒

IPsec Gateway Address

IPsec Mode

IPsec Protocol

Local Subnet

Local Subnet Mask

Local ID Type

Remote Subnet

Remote Subnet Mask

Remote ID Type

SA Encryption Algorithm

SA Authentication Algorithm

PFS Group

SA Lifetime s

DPD Time Interval s

IPSec-Client	
Element	Beschreibung
Aktivieren	Aktivieren oder deaktivieren Sie den IPsec-Client-Modus. Es sind maximal 3 Tunnel zulässig.
IP-Gateway-Adresse	Geben Sie die Adresse des Remote-IPsec-Servers ein.
IPsec-Modus	Wählen Sie „Tunnel“ oder „Transport“.
IPsec-Protokoll	Wählen Sie „ESP“ oder „AH“.
Lokales Subnetz	Geben Sie die IP-Adresse des lokalen LAN-Subnetzes im IPsec-Tunnel ein.
Lokale Subnetz-Netzmaske	Geben Sie die lokale LAN-Netzmaske im IPsec-Tunnel ein.
Lokaler ID-Typ	Wählen Sie den Identifizierungstyp aus, der an den Remote-Peer gesendet werden soll. Standard: Keine ID: Verwenden Sie die lokale Subnetz-IP-Adresse als ID FQDN: Vollständig qualifizierter Domänenname, Beispiel: test.user.com Benutzer-FQDN: Vollständig qualifizierte Benutzername-Zeichenfolge im E-Mail-Adressformat, example:test@user.com
Remote-Subnetz	Legen Sie das Remote-LAN-Subnetz fest, das sich im IPsec-Tunnel befindet.
Remote-Subnetzmaske	Geben Sie die Remote-LAN-Netzmaske für den IPsec-Tunnel ein.

Remote-ID-Typ	Wählen Sie den Identifizierungstyp aus, der mit der lokalen ID des Remote-Peers übereinstimmt. Standard: Keine ID: Remote-Subnetz-IP-Adresse als ID verwenden FQDN: Vollständig qualifizierter Domänenname, Beispiel: test.user.com Benutzer-FQDN: Vollständig qualifizierte Benutzername-Zeichenfolge im E-Mail-Adressformat, Beispiel: test@user.com
SA-Verschlüsselungsalgorithmus	Wählen Sie AES128, AES192 oder AES256.
SA-Authentifizierung Algorithmus	Wählen Sie SHA1 oder SHA2-256.
PFS-Gruppe	Wählen Sie NULL, MODP768_1, MODP1024_2 oder MODP1536_5.
SA-Lebensdauer	Legen Sie die Lebensdauer von IPsec SA fest. Bereich: 60-86400 s.
DPD-Intervallzeit	Legen Sie das DPD-Wiederholungsintervall für das Senden von DPD-Anfragen fest. Bereich: 2-60 s
DPD-Zeitlimit	Bei Verwendung von IKEv1 legen Sie das DPD-Zeitlimit fest, um den Ausfall der Gegenstelle zu erkennen . Bereich: 10-3600 s.

IKE Parameter ☒

IKE Version

Negotiation Mode

Encryption Algorithm

Authentication Algorithm

DH Group

Local Authentication

Local Secret Key

XAUTH ☐

Lifetime s

IPsec Advanced ☒

Enable Compression ☐

Margintime s

Expert Options

IKE-Parameter	
Element	Beschreibung
IKE-Version	Wählen Sie die Methode für den Schlüsselaustausch von IKEv1 oder IKEv2.
Verhandlungsmodus	Bei Verwendung von IKEv1 wählen Sie „Main“ oder „Aggressive“.
Verschlüsselungsalgorithmus	Wählen Sie „DES“, „3DES“, „AES128“, „AES192“ oder „AES256“.
Authentifizierungsalgorithmus	Wählen Sie MD5, SHA1 oder SHA2-256.

DH-Gruppe	Wählen Sie MODP768_1, MODP1024_2 oder MODP1536_5.
Lokale Authentifizierung	Wählen Sie PSK oder CA. PSK: Verwenden Sie einen vorab geteilten Schlüssel, um die Authentifizierung abzuschließen. CA: Verwenden Sie ein Zertifikat, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite „VPN > IPsec > Zertifizierungen“, um das CA-Zertifikat, das lokale Zertifikat und den privaten Schlüssel in die entsprechenden Felder zu importieren.
Lokaler geheimer Schlüssel	Geben Sie den vorab geteilten Schlüssel ein, der auf der Serverseite definiert ist.
Remote-Authentifizierung	Wählen Sie PSK oder CA. PSK: Verwenden Sie einen vorab geteilten Schlüssel, um die Authentifizierung abzuschließen. CA: Verwenden Sie ein Zertifikat, um die Authentifizierung abzuschließen.
Remote-Schlüssel	Geben Sie den vorab geteilten Schlüssel ein, der auf der Serverseite definiert ist.
XAUTH	Bei Verwendung von IKEv1 definieren Sie den XAUTH-Benutzernamen und das Passwort nach XAUTH aktiviert ist.
Lebensdauer	Legen Sie die Lebensdauer in der IKE-Verhandlung fest. Bereich: 60-86400 s.
IPsec Advanced	
Komprimierung aktivieren	Der Kopf des IP-Pakets wird nach der Aktivierung komprimiert.
Marginalzeit	Legen Sie eine erweiterte Zeit vor Ablauf der Lebensdauer fest, um den Vorgang zu starten. Neuverhandlung.
Expertenoptionen	Der Benutzer kann in diesem Feld einige andere Initialisierungszeichenfolgen eingeben, um zusätzliche Einstellungen hinzuzufügen. Die Zeichenfolgen müssen durch Semikolons getrennt werden.

6.3.2.3 Zertifikat

Bei Verwendung der lokalen Authentifizierung des IPsec-Servers oder -Clients als CA kann der Benutzer die erforderlichen Zertifikats- und Schlüsseldateien auf dieser Seite importieren/exportieren.

IPsec Server

CA Certificate

Browse

Export

Delete

Local Certificate

Browse

Export

Delete

Private key

Browse

Export

Delete

IPsec_1

CA Certificate

Browse

Export

Delete

Local Certificate

Browse

Export

Delete

Remote Certificate

Browse

Export

Delete

Private key

Browse

Export

Delete

6.3.3 L2TP

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

Enable

☒

Server IP Address

Username

Password

Authentication Type

Auto

▼

Global Traffic Forwarding

☐

Remote Subnet

Remote Subnet Mask

Tunnel Key

Show Advanced Setting	☒
Local Tunnel Ip Address	
Peer IP Address	
Enable MPPE	☒
Address/Control Compression	☐
Protocol Field Compression	☐
Asyncmap Value	ffffff
MRU	1440
MTU	1440
Link Detection Interval	60 s
Max Retries	1
Expert Options	

L2TP	
Element	Beschreibung
Aktivieren	L2TP-Client aktivieren oder deaktivieren.
Server-IP-Adresse	Geben Sie die IP-Adresse oder den Domännennamen des Remote-L2TP-Servers ein.
Benutzername	Geben Sie den Benutzernamen ein, den der L2TP-Server bereitstellt.
Passwort	Geben Sie das vom L2TP-Server bereitgestellte Passwort ein.
Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird.
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über den L2TP-VPN-Tunnel gesendet, wenn diese Funktion aktiviert ist.
Remote-Subnetz	Geben Sie das Remote-Subnetz des L2TP-VPN-Servers ein.
Remote-Subnetzmaske	Geben Sie die Remote-Netzmaske des L2TP-VPN-Servers ein.
Tunnelschlüssel	Geben Sie das Passwort für den L2TP-Tunnel ein.
Lokale Tunnel-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 ist.
Peer-IP-Adresse	Geben Sie die Tunnel-IP-Adresse des L2TP-Servers ein.
MPPE aktivieren	MPPE (Microsoft Point to Point Encryption) aktivieren oder deaktivieren.
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 L2TP-Initialisierungszeichenfolgen. Der Benutzer kann den Standardwert beibehalten. Bereich: 0-ffffff.
MRU	Legt die maximale Empfangseinheit fest. Bereich: 64-1500.

MTU	Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500.
Link-Erkennungsintervall	Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Bereich: 0-600.
Expertenoptionen	Der Benutzer kann in diesem Feld einige Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen.

6.3.4 PPTP

Das Point-to-Point Tunneling Protocol (PPTP) ist ein Protokoll, das einen TCP-Steuerkanal und einen Generic Routing Encapsulation-Tunnel verwendet, um PPP-Pakete zu kapseln.

Enable	☒
Server IP Address	
Username	
Password	
Authentication Type	MS-CHAP
Global Traffic Forwarding	☐
Remote Subnet	
Remote Subnet Mask	
Show Advanced Setting	☒
Local Tunnel Ip Address	
Peer IP Address	
Enable MPPE	☒
Address/Control Compression	☐
Protocol Field Compression	☐
Asynmap Value	ffffff
MRU	1440
MTU	1440
Link Detection Interval	60 s
Max Retries	1
Expert Options	

PPTP	
Element	Beschreibung
Aktivieren	Aktivieren oder deaktivieren Sie den PPTP-Client.
Server-IP-Adresse	Geben Sie die IP-Adresse oder den Domännennamen des Remote-PPTP-Servers ein.
Benutzername	Geben Sie den Benutzernamen ein, den der PPTP-Server bereitstellt.
Passwort	Geben Sie das vom PPTP-Server bereitgestellte Passwort ein.
Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird.
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über einen PPTP-VPN-Tunnel gesendet, wenn diese Funktion aktiviert ist.
Remote-Subnetz	Geben Sie das Remote-Subnetz des PPTP-VPN-Servers ein.
Remote-Subnetzmaske	Geben Sie die Remote-Netzmaske des PPTP-VPN-Servers ein.
Lokale Tunnel-IP Adresse	Legen Sie die Tunnel-IP-Adresse des PPTP-Clients fest. Der Client erhält die Tunnel-IP-Adresse automatisch vom Server, wenn sie null ist.
Peer-IP-Adresse	Geben Sie die Tunnel-IP-Adresse des PPTP-Servers ein.
MPPE aktivieren	MPPE (Microsoft Point-to-Point-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 PPTP-Initialisierungszeichenfolgen. Der Benutzer kann den Standardwert beibehalten. Bereich: 0-ffffff.
MRU	Legt die maximale Empfangseinheit fest. Bereich: 64-1440.
MTU	Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1440.
Link-Erkennungsintervall	Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Bereich: 0-600.
Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl der Wiederholungsversuche fest, um den Ausfall der PPTP-Verbindung zu erkennen. Bereich: 0-10.
Expertenoptionen	Der Benutzer kann in diesem Feld einige Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen.

6.4 Dienst

6.4.1 Serielle Schnittstelle

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

Enable



Serial Type

RS232



Baud Rate

9600



Data Bits

8 Bits



Stop Bits

1 Bits



Parity

None



Software Flow Control



Serial Mode

Modbus Client



Serielle Einstellung		
Element	Beschreibung	Standard
Aktivieren	Serielle Schnittstelle aktivieren oder deaktivieren.	Deaktivieren
Serieller Typ	Der serielle Anschluss 1 ist ein RS232-Anschluss und der serielle Anschluss 2 ist ein RS485-Anschluss.	--
Baudrate	Der Bereich liegt zwischen 300 und 230400. Entspricht der Baudrate des angeschlossenen Endgerätes.	9600
Datenbits	8 Bits oder 7 Bits optional. Entspricht den Datenbits des angeschlossenen Endgerät.	8
Stoppbits	1 Bit oder 2 Bit optional. Gleich wie bei den Stoppbits des angeschlossenen Endgerät.	1
Parität	Die Optionen sind „Keine“, „Ungerade“ und „Gerade“. Das Gleiche gilt für die Parität des angeschlossenen Endgeräts.	Keine
Software-Ablauf Steuerung	Aktivieren oder deaktivieren Sie die Software-Flusskontrolle.	Deaktivieren
Serieller Modus	Wählen Sie den Arbeitsmodus der seriellen Schnittstelle aus. DTU-Modus: Im DTU-Modus kann die serielle Schnittstelle eine Kommunikation mit dem Remote-Server/Client herstellen. GPS: Im GPS-Modus gehen Sie zu Service > GPS > GPS-Serienweiterleitung, um die grundlegenden Parameter für die Übertragung von GPS-Daten an die serielle Schnittstelle zu konfigurieren. Modbus-Client: Im Modbus-Client-Modus gehen Sie zu „Service“ > „Modbus-Client“, um grundlegende Parameter und Kanäle zu konfigurieren.	Deaktivieren

Serial Mode

DTU Protocol

Keepalive Interval s

Keepalive Retry Times

Reconnect Interval s

Specific Protocol ☐

Packet Size Byte

Serial Frame Interval ms

Register String

Destination IP Address

Server Address	Server Port	Status
----------------	-------------	--------

This section contains no values now.

DTU-Modus		
Element	Beschreibung	Standard
DTU-Protokoll	Wählen Sie aus den folgenden Protokollen aus: TCP-Client: Der Router wird als TCP-Client verwendet und überträgt Daten transparent an den TCP-Server. UDP-Client: Der Router wird als UDP-Client verwendet und überträgt Daten transparent an den UDP-Server. TCP-Server: Der Router wird als TCP-Server verwendet, um auf Abfragedaten zu warten. UDP-Server: Der Router wird als UDP-Server verwendet, um auf Abfragedaten zu warten. Modbus: Der Router wird als Modbus-Gateway verwendet, das die Konvertierung zwischen Modbus RTU und Modbus TCP ermöglicht. Node-RED: Der Router leitet die Daten an den seriellen Eingangs-Knoten weiter, wenn Node-RED installiert ist. MQTT: Der Router wird als MQTT-Client verwendet, um Daten an den MQTT-Broker weiterzuleiten oder den Downlink an den seriellen Port weiterzuleiten.	--
TCP/UDP-Server		
Lokaler Port	Legen Sie den lokalen Port dieses TCP/UDP-Servers fest. Bereich: 1-65535.	502
Keepalive Intervall	Nachdem die TCP-Verbindung hergestellt wurde, sendet der Client regelmäßig Heartbeat-Pakete, um die Verbindung aufrechtzuerhalten. Der Intervallbereich liegt zwischen 1 und 3600 Sekunden.	75
Maximale Wiederholungsversuche	Wenn der TCP-Heartbeat-Zeitüberschreitung erreicht ist, sendet der Router den Heartbeat erneut. Nachdem die voreingestellte Anzahl an Wiederholungsversuchen erreicht ist, wird die TCP-Verbindung neu aufgebaut. Der Bereich für die Wiederholungsversuche liegt zwischen 1 und 16.	9
Paketgröße	Legen Sie die Größe des seriellen Datenrahmens fest. Das Paket wird gesendet, wenn die voreingestellte Rahmengröße die Grenze erreicht. Der Größenbereich liegt zwischen 1 und 1024 Byte.	1024
Serieller Rahmenintervall	Das Intervall, in dem der Router die im Pufferbereich gespeicherten realen seriellen Daten an das öffentliche Netzwerk sendet. Der Bereich liegt zwischen 10 und 65535 ms. Hinweis: Die Daten werden an das öffentliche Netzwerk gesendet, wenn die Größe der tatsächlichen seriellen Daten die voreingestellte Paketgröße erreicht, auch wenn sie innerhalb der seriellen	100

	Rahmenintervall liegen.	
TCP/UDP-Client		
Keepalive-Intervall	Nachdem der TCP-Client mit dem TCP-Server verbunden ist, sendet der Client regelmäßig Heartbeat-Pakete über TCP, um die Verbindung aufrechtzuerhalten. Der Intervallbereich liegt zwischen 1-3600 s.	75
Keepalive-Wiederholungszeiten	Wenn die TCP-Heartbeat-Zeiten abgelaufen sind, sendet der Router den Heartbeat erneut. Nachdem die voreingestellten Wiederholungsversuche erreicht sind, stellt der Router die Verbindung zum TCP-Server wieder her. Der Bereich liegt zwischen 1 und 16.	9
Wiederverbindungsintervall	Wenn die Verbindung fehlschlägt, stellt der Router die Verbindung zum Server erneut her, und zwar im voreingestellten Intervall. Der Bereich liegt zwischen 10 und 60 Sekunden.	10
Spezifisches Protokoll	Mit dem spezifischen Protokoll kann der Router eine Verbindung zur TCP2COM-Software verbinden.	Deaktivieren
Heartbeat Intervall	Mit einem bestimmten Protokoll sendet der Router regelmäßig Heartbeat-Pakete an den Server, um die Verbindung aufrechtzuerhalten. Der Intervallbereich liegt zwischen 1 und 3600 Sekunden.	30
ID	Definieren Sie eine eindeutige ID für jeden Router. Diese darf nicht länger als 63 Zeichen sein und enthalten keine Leerzeichen.	--
Paketgröße	Legen Sie die Größe des seriellen Datenrahmens fest. Das Paket wird gesendet, wenn die voreingestellte Rahmengröße erreicht ist. Der Bereich liegt zwischen 1 und 1024 Byte.	1024
Serieller Rahmenintervall	Das Intervall, in dem der Router die im Pufferbereich gespeicherten realen seriellen Daten an das öffentliche Netzwerk sendet. Der Bereich liegt zwischen 10 und 65535 ms. Hinweis: Die Daten werden an das öffentliche Netzwerk gesendet, wenn die Größe der tatsächlichen seriellen Daten die voreingestellte Paketgröße erreicht, auch wenn sie innerhalb des seriellen Bereichs liegt.	100
Registerzeichenfolge	Bei der Einrichtung des UDP-Clients definieren Sie die Registrierungszeichenfolge für die Verbindung mit dem Server.	Null
Serveradresse	Geben Sie die TCP- oder UDP-Serveradresse (IP/Domänenname) ein.	Null
Server-Port	Geben Sie den TCP- oder UDP-Serverport ein. Bereich: 1-65535.	Null
Status	Zeigt den Verbindungsstatus zwischen dem Router und dem Server an.	--
Modbus		
Lokaler Port	Legen Sie den Listening-Port des Routers fest. Bereich: 1-65535.	502
Max. TCP-Clients	Geben Sie die maximale Anzahl von TCP-Clients an, die eine Verbindung zum Router, der als TCP-Server fungiert.	32
Verbindungszeitlimit Zeitüberschreitung	Wenn der TCP-Server innerhalb der Verbindungszeitüberschreitung keine Daten vom Slave-Gerät empfängt innerhalb der Verbindungszeitüberschreitung keine Daten vom Slave-Gerät, wird die TCP-Verbindung unterbrochen.	60
Leseintervall	Legen Sie das Intervall für das Auslesen der Fernkanäle fest. Wenn ein Lesezyklus endet, beginnt der neue Lesezyklus, bis dieses Intervall abgelaufen ist. Wenn es auf 0 gesetzt ist, startet das Gerät den neuen Lesezyklus neu, nachdem alle Kanäle ausgelesen wurden.	100
Zeitüberschreitung bei der Antwort	Legen Sie die maximale Antwortzeit fest, die der Router auf die Antwort auf den Befehl wartet. Wenn das Gerät nach Ablauf der maximalen Antwortzeit keine Antwort erhält, wird davon ausgegangen, dass die Zeit für den Befehl abgelaufen ist.	3000
Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl von Wiederholungsversuchen fest, nachdem das Lesen fehlgeschlagen ist.	3
Node-RED		

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

Beispiel für eine zugehörige Konfiguration

[DTU-Anwendungsbeispiel](#)

6.4.2 E/A

6.4.2.1 DI

In diesem Abschnitt wird erläutert, wie Sie Überwachungsbedingungen für digitale Eingänge konfigurieren und bestimmte Aktionen ausführen können, sobald die Bedingungen erfüllt sind.

Enable ☒

Mode High Level ▼

Duration 100 ms

DO ☐SMS ☐Node-RED ☐MQTT ☐

DI	
Element	Beschreibung
Aktivieren	DI aktivieren oder deaktivieren.
Modus	Wählen Sie den Arbeitsmodus von DI aus. Hoher Pegel: Wenn ein hoher Pegel erkannt wird, wird die Aktion ausgelöst. Niedriger Pegel: Wenn ein niedriger Pegel erkannt wird, wird die Aktion ausgelöst. Zähler: Wenn ein Impuls erkannt wird, erhöht sich der Zählerwert um 1.
Dauer (ms)	Wenn der Modus auf High/Low-Pegel eingestellt ist, legen Sie die Dauer des High/Low-Pegels fest. Bereich: 1-10000.
Auslösebedingung	Wenn der Modus auf Zähler eingestellt ist, wählen Sie die Zähler-Auslösebedingung aus. Niedrig->Hoch: Der Zählerwert erhöht sich um 1, wenn sich der Status des digitalen Eingangs von niedrigem auf hohen Pegel ändert. Hoch->Niedrig: Der Zählerwert erhöht sich um 1, wenn sich der Status des digitalen Eingangs ändert. von hohem Niveau zu niedrigem Niveau.
Auslöser Zähler	Das System ergreift entsprechende Maßnahmen, wenn der Zählerwert den voreingestellten Wert erreicht erreicht hat, und setzt dann den Zählerwert auf 0 zurück. Bereich: 1-100.
Aktion	Wählen Sie die entsprechenden Maßnahmen aus, die das System ergreifen soll, wenn der digitale Eingangsmodus die voreingestellte Bedingung oder Dauer erfüllt. DO: Steuerung des Ausgangsstatus von DO. SMS: Wählen Sie die Telefongruppe aus, an die SMS-Alarme gesendet werden sollen. Node-RED: Senden Sie den DI-Status an den Knoten „Digital Input“, wenn Node-RED installiert ist. MQTT: Aktivieren Sie diese Option, um Nachrichten an den MQTT-Broker zu senden. Die MQTT-Verbindung wird auf der Seite „ Service > MQTT “ eingerichtet.

MQTT Connections	Topic	QoS	Retain
This section contains no values now.			

[Add](#)

6.4.2.2 DO

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

Enable ☒

Mode Pulse

Initial Status High Level

Duration of High Level 100 *10 ms

Duration of Low Level 100 *10 ms

The Number of Pulse 10

DO	
Element	Beschreibung
Aktivieren	DO aktivieren oder deaktivieren.
Modus	Wählen Sie den Arbeitsmodus von DO aus. High Level: Löst den DO aus, um ein High-Level-Signal zu senden. Low Level: Löst den DO aus, um ein Low-Level-Signal zu senden. Zähler: Löst den DO aus, um Impulse zu senden.
Anfangszustand	Wählen Sie High Level oder Low Level als Anfangszustand des Impulses.
Dauer des hohen Pegels (*10 ms)	Legen Sie die Dauer des hohen Pegels des Impulses fest. Bereich: 1-10000.
Dauer des niedrigen Pegels (*10 ms)	Stellen Sie die Dauer des niedrigen Pegels des Impulses ein. Bereich: 1-10000.
Anzahl der Impulse	Stellen Sie die Impulsanzahl ein. Bereich: 1-100.

6.4.3 Modbus-Client (Master)

Der UR75-Router kann als Modbus RTU/TCP-Client konfiguriert werden, um den Remote-Modbus-Server abzufragen und Daten an den TCP-Server zu senden.

6.4.3.1 Modbus-Client

Auf dieser Seite können Sie die Parameter des Modbus-Clients konfigurieren.

Enable ☒

Read Interval s

Max Retries

Max Response Time ms

Execution Interval ms

Channel

Modbus-Client		
Element	Beschreibung	Standard
Aktivieren	Modbus-Master aktivieren/deaktivieren.	--
Leseintervall	Legen Sie das Intervall für das Lesen von Remote-Kanälen fest. Wenn der Lesezyklus endet, werden die Befehle, die nicht gesendet wurden, verworfen und der neue Lesezyklus beginnt. Wenn der Wert auf 0 gesetzt ist, startet das Gerät den neuen Lesezyklus, nachdem alle Kanäle gelesen wurden. Bereich: 0-600 s.	0
Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl der Wiederholungsversuche fest, wenn das Lesen fehlschlägt, Bereich: 0-5.	3
Maximale Antwortzeit	Legen Sie die maximale Antwortzeit fest, die der Router auf die Antwort auf den Befehl wartet. Wenn das Gerät nach Ablauf der maximalen Antwortzeit keine Antwort erhält, wird davon ausgegangen, dass die Zeit für den Befehl abgelaufen ist. Bereich: 10-1000 ms.	500
Ausführungsintervall	Das Ausführungsintervall zwischen den einzelnen Befehlen. Bereich: 10-1000 ms.	50
Kanal	Wählen Sie einen lesbaren Kanal aus „ Service > Channel > Kanal. “	--

6.4.3.2 Kanal

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

Channel Setting

Channel Name	Server ID	Register Address	Number	Command Type	Link Type	Remote Device IP	Port	Sign	Decimal Place	
	1	0	1	Holding Regis: ▾	TCP ▾			☐	0	Delete
										Add

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

Alarm Setting

Name	Condition	Alarm
------	-----------	-------

This section contains no values now.

Add

Add Alarm Setting

Name

Condition

Max. Threshold

SMS ☒

Phone Group

Abnormal Content
 Note: \$YEAR/\$MON/\$DAY \$TIME, get ABERRANT data \$VALUE from address \$ADDRESS of channel \$NAME. (Abnormal scope is \$CONDITION)
 125 / 255

Normal Content
 Note: \$YEAR/\$MON/\$DAY \$TIME, get NORMAL data \$VALUE from address \$ADDRESS of channel \$NAME. (Abnormal scope is \$CONDITION)
 123 / 255

Continuous Alarm ☐

Alarameinstellung	
Element	Beschreibung
Kanal Name	Wählen Sie den Modbus-Kanal aus.
Bedingung	Die Bedingung, die den Alarm auslöst.
Min. Schwellenwert	Legen Sie den Mindestwert fest, bei dem der Alarm ausgelöst wird. Wenn der tatsächliche Wert unter diesem Wert liegt, wird der Alarm ausgelöst.
Max. Schwellenwert	Stellen Sie den Maximalwert ein, bei dem der Alarm ausgelöst werden soll. Wenn der tatsächliche Wert diesen Wert überschreitet diesem Wert liegt, wird der Alarm ausgelöst.
SMS	Aktivieren oder deaktivieren Sie den SMS-Alarm, wenn der Modbus-Kanal die Bedingung erfüllt.
Telefon Gruppe	Wählen Sie die Telefongruppe aus, die die Alarm-SMS erhalten soll. Die Telefongruppe kann auf der Seite „Service > Telefon & SMS > Telefon“ hinzugefügt werden.
Anormaler Inhalt	Wenn der tatsächliche Wert die voreingestellte Bedingung erfüllt, löst der Router automatisch den Alarm aus und sendet den voreingestellten abnormalen Inhalt an die angegebene Telefongruppe.
Normaler Inhalt	Wenn der tatsächliche Wert nach Überschreiten des Schwellenwert wieder auf den Normalwert zurückkehrt, hebt der Router automatisch den Alarm wegen einer Anomalie auf und sendet den voreingestellten normalen Inhalt an die angegebene Telefongruppe.
Kontinuierlich Alarm	Einmal aktiviert, wird derselbe Alarm kontinuierlich gemeldet. Andernfalls Der gleiche Alarm wird nur einmal gemeldet.

TCP Forwarding

Name	IP	Port
All		

Delete

Add

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

MQTT Forwarding

Channel Name	MQTT Connections	Topic	QoS	Retain
All	111	111	0	☒
All	111	22	0	☒
All	111		0	☐

Delete

Add

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

6.4.4 GPS

Benutzer können hier die GPS-Funktion aktivieren. Für weitere Debug-Informationen aktivieren Sie bitte auch das GPS-Protokoll.

Enable
☒

Enable GPS Log
☐

6.4.4.1 GPS-IP-Weiterleitung

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

Enable	☒
Type	Client
Protocol	TCP Protocol
GPS Keepalive Interval	75 s
Keepalive Retry	9
Reconnect Interval	10 s
Report Interval	30 s
Stable Report Interval	120 s
Stable Decision Threshold	25 mi
Include RMC Message	☒
Include GSA Message	☒
Include GGA Message	☒
Include GSV Message	☒
Include VTG Message	☒
Message Prefix	
Message Suffix	

Destination Address

Server Address	Server Port	Status	
		-	Delete
			Add

GPS-IP-Weiterleitung		
Element	Beschreibung	Standard
Aktivieren	Leiten Sie die GPS-Daten an den Client oder Server weiter.	Deaktivieren
Typ	Wählen Sie den Verbindungstyp des Routers als Client oder Server aus.	Client
Protokoll	Wählen Sie das Protokoll für die Datenübertragung als TCP oder UDP.	TCP

GPS-Keepalive-Intervall	Wenn das Gerät mit dem Server/Client verbunden ist, sendet es regelmäßig ein Heartbeat-Paket an den Server/Client, um die Verbindung aufrechtzuerhalten. Der Intervallbereich liegt zwischen 1 und 3600 Sekunden.	75
Keepalive-Wiederholungsversuche	Wenn die TCP-Heartbeat-Zeiten abgelaufen sind, sendet der Router den Heartbeat erneut. Nachdem die voreingestellten Wiederholungszeiten erreicht sind, stellt der Router die Verbindung zum TCP-Server wieder her. Der Bereich liegt zwischen 1 und 16.	9
Lokaler Port	Legen Sie den Listening-Port des Routers fest, wenn Sie ihn als Server verwenden. Bereich: 1-65535.	
Wiederverbinden Intervall	Wenn die Verbindung fehlschlägt, stellt der Router die Verbindung zum Server nach dem voreingestellten Intervall erneut mit dem Server. Der Bereich liegt zwischen 10 und 60 Sekunden.	10
Meldeintervall	Das Gerät sendet GPS-Daten entsprechend diesem Intervall an den Server/Client, wenn es den stabilen Entscheidungsschwellenwert erreicht. Der Bereich liegt zwischen 1-65535 s.	30
Stabiles Berichtsintervall	Das Gerät sendet GPS-Daten entsprechend diesem Intervall an den Server/Client, wenn es den stabilen Entscheidungsschwellenwert nicht erreicht. Der Bereich 1-65535 s.	120
Stabile Entscheidungsschwellenwert	Die GPS-Standortabweichung innerhalb dieser Entfernung kann als unverlässlich angesehen werden. Der Bereich liegt zwischen 1 und 65535 m.	25
RMC einbeziehen Nachricht	RMC umfasst Daten zu Uhrzeit, Datum, Position, Kurs und Geschwindigkeit.	Aktivieren
GSA einbeziehen Nachricht	GSA enthält den Betriebsmodus des GPS-Empfängers, die für die Positionsbestimmung verwendeten Satelliten und die DOP-Werte.	Aktivieren
GGA einschließen Nachricht	GGA umfasst Zeit-, Positions- und Fix-Typ-Daten.	Aktivieren
GSV einbeziehen Nachricht	GSV enthält die Anzahl, Höhe und Azimut der GPS-Satelliten sowie SNR-Werte.	Aktivieren
VTG einbeziehen Meldung	VTG enthält Kurs- und Geschwindigkeitsinformationen relativ zum Boden.	Aktivieren
Meldung Präfix	Fügen Sie den GPS-Daten ein Präfix hinzu.	Null
Nachricht Suffix	Fügen Sie den GPS-Daten ein Suffix hinzu.	Null
Zieladresse		
Server Adresse	Geben Sie die Serveradresse ein, um GPS-Daten zu empfangen (IP/Domänenname).	--
Server-Port	Geben Sie den Server-Port ein, um GPS-Daten zu empfangen. Bereich: 1-65535.	--
Status	Zeigt den Verbindungsstatus zwischen dem Router und dem Server an.	--

6.4.4.2 GPS-Serienweiterleitung

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

Enable ☒

Serial Type

Report Interval s

Include RMC Message ☒

Include GSA Message ☒

Include GGA Message ☒

Include GSV Message ☒

Include VTG Message ☒

Serielle GPS-Weiterleitung		
Element	Beschreibung	Standard
Aktiv	Leitet die GPS-Daten an den voreingestellten seriellen Anschluss weiter.	Deaktivieren
Serieller Typ	Wählen Sie den seriellen Anschluss aus, der die GPS-Daten empfangen soll. Stellen Sie sicher, dass der serieller Anschluss unter „Service > Serieller Anschluss“ aktiviert ist.	--
Berichtsintervall	Das Gerät leitet die GPS-Daten entsprechend diesem Intervall an den seriellen Anschluss weiter gemäß diesem Intervall an den seriellen Anschluss weiter. Der Bereich liegt zwischen 1 und 65535 Sekunden.	30
RMC einbeziehen Nachricht	RMC umfasst Daten zu Uhrzeit, Datum, Position, Kurs und Geschwindigkeit.	Aktivieren
GSA einbeziehen Nachricht	GSA umfasst den Betriebsmodus des GPS-Empfängers, die verwendeten Satelliten in der Positionsbestimmung verwendeten Satelliten und DOP-Werte.	Aktivieren
GGA einschließen Nachricht	GGA enthält Zeit-, Positions- und Fix-Typ-Daten.	Aktivieren
GSV einbeziehen Nachricht	GSV enthält die Anzahl, Höhe und Azimut der GPS-Satelliten und SNR-Werte.	Aktivieren
VTG einbeziehen Nachricht	VTG enthält Kurs- und Geschwindigkeitsinformationen relativ zum Boden.	Aktivieren

6.4.4.3 GPS-MQTT-Weiterleitung

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

Enable ☒

Report Interval s

Include RMC Message ☒

Include GSA Message ☒

Include GGA Message ☒

Include GSV Message ☒

Include VTG Message ☒

MQTT Connections

MQTT Connections	Topic	QoS	Retain
111	111	0	☐

Delete

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

6.4.5 Telefon & SMS

6.4.5.1 Telefon

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

Phone Book

Phone Number

Description

+123456

Delete

Add

Phone Group

Name

Description

Phone List

+123456

▼

Delete

Add

Element	Beschreibung
Telefonbuch	
Telefonnummer	Geben Sie die Telefonnummer ein. Ziffern, „+“ und „-“ sind zulässig.
Beschreibung	Die Beschreibung der Telefonnummer.
Telefon-Gruppenliste	
Gruppenname	Name für Telefongruppe festlegen.
Beschreibung	Die Beschreibung der Telefongruppe.
Telefonliste	Wählen Sie die Telefonnummern für die Liste aus.

6.4.5.2 SMS

Die SMS-Einstellungen umfassen die Fernsteuerung per SMS, das Senden von SMS sowie den Status des SMS-Empfangs und -Versands.

General Setting

SMS Mode

PDU

▼

SMS Remote Control

☒

Authentication Type

Password + Phone Number

▼

Password

👁

Phone Group

▼

SMS	
Element	Beschreibung
SMS-Modus	SMS-Modus auswählen: Text: Reiner Textmodus, der hauptsächlich in Europa und Amerika verwendet wird. Technisch gesehen kann er auch zum Versenden von Kurznachrichten in chinesischer Sprache verwendet werden. PDU: Dies ist der Standard-Kodierungsmodus für Mobiltelefone, der mit dem SMS-Format aller Mobiltelefone kompatibel ist und beliebige Zeichen verwenden kann. mit dem SMS-Format aller Mobiltelefone übereinstimmt und alle Zeichen verwenden kann.
SMS-Fernbedienung Steuerung	Aktivieren/Deaktivieren der SMS-Fernsteuerung. Klicken Sie hier , um die SMS-Steuerbefehle zu überprüfen
Authentifizierung Typ	Wählen Sie den Authentifizierungstyp, um zu überprüfen, ob die SMS von einem gültigen Controllers stammt.

	Telefonnummer: Nur die Telefonnummern in Telefongruppen unterstützen die Fernsteuerung. Passwort + Telefonnummer: Nur die Telefonnummern in der Telefongruppe Gruppen unterstützen die Fernsteuerung; außerdem sollte die Steuerungs-SMS im Format „Passwort+“;“+Befehlsinhalt gesendet werden.
Passwort	Legen Sie ein Passwort für die Authentifizierung fest.
Telefongruppe	Wählen Sie die Telefongruppe aus, die für die Fernsteuerung verwendet werden soll.

SMS Sending

Recipient Phone Number

Content

0 / 255

SEND

Inbox **Outbox**

Start Time End Time Sender **SEARCH** **CLEAR ALL**

Sender	Time	Content
🔄 Total: 0 < 1 > 10/Page Go To Page		

SMS	
Element	Beschreibung
SMS-Versand	
Empfänger-Telefon Nummer	Geben Sie die Nummer ein, an die die SMS gesendet werden soll.
Inhalt	Inhalt der SMS.
Posteingang/Postausgang	
Suche	Suche nach SMS-Datensatz.
Alle löschen	Löschen Sie die SMS-Eingangs-/Ausgangsbox-Datensätze.

6.4.6 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. Konfigurieren Sie die MIB-Ansicht.
4. VCAM konfigurieren.

6.4.6.1 SNMP

UR75 unterstützt die Versionen SNMPv1, SNMPv2c und SNMPv3. SNMPv3 verwendet eine Authentifizierungsverschlüsselung mit Benutzername und Passwort.

Enable ☒

Port

SNMP Version

Location Information

Contact Information

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	Ist fest auf SNMP v3 eingestellt.
Standortinformationen	Geben Sie die Standortinformationen ein.
Kontakt	Geben Sie die Kontaktinformationen ein.

6.4.6.2 MIB-Ansicht

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

SNMP Settings **MIB view** VACM Trap Settings MIB Download

MIB view

View Name	View Filter	View OID	
All	Include	1	Delete
System	Include	1.3.6.1.2.1.1	Delete

Add

MIB-Ansicht	
Artikel	Beschreibung
Ansichtsname	Legen Sie den Namen der MIB-Ansicht fest.
Ansichtsfiler	Wählen Sie zwischen „Eingeschlossen“ und „Ausgeschlossen“. Eingeschlossen: Alle Knoten innerhalb des angegebenen MIB-Knotens abfragen. Ausgeschlossen: Alle Knoten außer dem angegebenen MIB-Knoten abfragen.
Ansicht-OID	Geben Sie die OID-Nummer ein.
Hinzufügen/Löschen	Klicken Sie hier, um eine MIB-Ansicht hinzuzufügen oder zu löschen.

6.4.6.3 VACM

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

SNMP Settings
MIB view
VACM
Trap Settings
MIB Download

SNMP Community

Community	Supported network	MIB View	Access Permission
private	0.0.0.0/0	System	rw

Edit
Delete

Add

VACM	
Element	Beschreibung
SNMP v1 & v2c Unterstütztes Netzwerk	
Community	Legen Sie den Community-Namen fest.
IP Adresse/Netzmaske	Der externe IP-Adressbereich für den Zugriff auf diese MIB-Ansicht.
MIB-Ansicht	Wählen Sie eine MIB-Ansicht aus der MIB-Ansichtsliste aus, um Berechtigungen festzulegen.
Zugriffsberechtigung	Wählen Sie zwischen „Nur Lesen“ und „Lesen/Schreiben“.
SNMP v3-Benutzer	
Benutzername	Legen Sie den Namen des SNMPv3-Benutzers fest.
Sicherheitsstufe	Wählen Sie zwischen „Keine“, „Auth/NoPriv“ und „Auth/Priv“.
Authentifizierung Algorithmus	Wählen Sie „MD5“ oder „SHA“, wenn „Auth“ ausgewählt ist.
Authentifizierung Passwort	Das Passwort muss eingegeben werden.
Verschlüsselung Algorithmus	Wählen Sie zwischen „AES“ und „DES“, wenn „Auth/Priv“ ausgewählt ist.
Verschlüsselung Passwort	Das Passwort muss eingegeben werden.
Nur-Lesen-Ansicht	Wählen Sie eine MIB-Ansicht aus, um die Berechtigung als „Nur Lesen“ aus der MIB-Ansicht festzulegen.
Lese-/Schreibansicht	Wählen Sie eine MIB-Ansicht aus, um die Berechtigung als „Lesen-Schreiben“ aus der MIB-Ansicht festzulegen.
Benachrichtigungsansicht	Wählen Sie eine MIB-Ansicht aus, um die Berechtigung als „Benachrichtigen“ aus der MIB-Ansichtsliste festzulegen.

6.4.6.4 Trap-Einstellungen

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

Enable ☒

Community

None

Server Address

Port

SNMP-Trap	
Element	Beschreibung
Aktivieren	Aktivieren oder deaktivieren Sie die SNMP-Trap-Funktion.
Community	Wählen Sie die Community von SNMP v1/v2c aus.
Benutzer	Wählen Sie den Benutzer von SNMPv3 aus.
Serveradresse	Geben Sie die IP-Adresse oder den Domännennamen des NMS ein.
Port	Geben Sie den UDP-Port ein. Der Portbereich liegt zwischen 1 und 65535.

6.4.6.5 MIB-Download

In diesem Abschnitt wird beschrieben, wie Sie MIB-Dateien herunterladen können.

MIB File

Open_Router_MIB.txt

Download

6.4.7 MQTT

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

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

MQTT Channel				
Name	Address	Status	Enable Status	
111	111:1883	● Disabled	☐	Edit Delete
111111	111111111111:1883	● Disabled	☐	Edit Delete
				Add

MQTT-Kanal	
Element	Beschreibung
Name	Der eindeutige Name des MQTT-Kanals.
Adresse	Adresse und Port des MQTT-Brokers zum Empfang von Daten.
Status	Zeigt den Verbindungsstatus zwischen Router und MQTT-Broker an.
Status aktivieren	Aktivieren oder deaktivieren Sie diesen MQTT-Kanal.
Bearbeiten	Diesen MQTT-Kanal bearbeiten.

Löschen	Löschen Sie diesen MQTT-Kanal.
Hinzufügen	Einen neuen MQTT-Kanal hinzufügen.

General

Name	
Broker Address	
Broker Port	1883
Client ID	24:E1:24:F5:AF:CA_m0z6w79u
Connection Timeout	30 s
Keep Alive Interval	60 s
Auto Reconnect	☒
Reconnect Period	4 s
Clean Session	☐

User Credentials

Enable	☒
Username	admin
Password	 

TLS

Enable	☒
Mode	CA Signed Server Certificate 

Last Will and Testament

Enable ☐

Request Topic

Data Type	Topic	Retain	QoS
Request		☐	0
Response		☐	0

System Status Publish Topic

Data Type	Topic	Publish Interval(s)	Retain	QoS
System Info			☐	0
System Status			☐	0
Cellular			☐	0
Ethernet			☐	0
GPS			☐	0

MQTT-Einstellungen**Element** **Beschreibung****Allgemein**

Name	Passen Sie einen eindeutigen Verbindungsnamen an.
Broker-Adresse	MQTT-Broker-Adresse zum Empfangen von Daten.
Broker-Port	MQTT-Broker-Port zum Empfangen von Daten.
Client-ID	Die Client-ID ist die eindeutige Identität des Clients gegenüber dem Server. Sie muss eindeutig sein, wenn alle Clients mit demselben Server verbunden sind, und es ist der Schlüssel zur Verarbeitung von Nachrichten mit QoS 1 und 2.
Verbindung Zeitüberschreitung/s	Wenn der Client nach Ablauf des Verbindungszeitlimits keine Antwort erhält, Verbindung als unterbrochen betrachtet. Der Bereich: 1-65535.
Keep Alive Intervall/s	Nachdem der Client mit dem Server verbunden ist, sendet der Client regelmäßig Heartbeat-Pakete an den Server, um die Verbindung aufrechtzuerhalten. Bereich: 1-65535.
Auto Wiederverbinden	Wenn die Verbindung unterbrochen wird, versuchen Sie, die Verbindung zum Server automatisch wiederherzustellen.
Wiederverbinden Zeitraum	Wenn die Verbindung unterbrochen wird, wird der Zeitraum für die erneute Verbindung mit dem Server.
Sitzung bereinigen	Wenn diese Option aktiviert ist, erstellt die Verbindung eine temporäre Sitzung, und alle Informationen gehen verloren, wenn die Verbindung des Clients zum Broker unterbrochen wird. Wenn diese Option deaktiviert ist, erstellt die Verbindung eine dauerhafte Sitzung, die bestehen bleibt und speichert Offline-Nachrichten, bis die Sitzung nach Ablauf der Zeit abgemeldet wird.

Benutzeranmeldedaten

Aktivieren	Benutzeranmeldedaten aktivieren.
Benutzername	Der Benutzername, der für die Verbindung mit dem MQTT-Broker verwendet wird.
Passwort	Das Passwort, das für die Verbindung mit dem MQTT-Broker verwendet wird.

TLS

Aktivieren	Aktivieren Sie die TLS-Verschlüsselung in der MQTT-Kommunikation.
Modus	Wählen Sie zwischen selbstsignierten Zertifikaten und CA-signierten Serverzertifikaten. Von einer Zertifizierungsstelle signiertes Serverzertifikat: Überprüfen Sie das vom Gerät vorinstallierte Zertifikat der

	Zertifizierungsstelle (CA) überprüfen, das auf dem Gerät vorinstalliert ist. Selbstsignierte Zertifikate: Laden Sie die benutzerdefinierten CA-Zertifikate, Client-Zertifikate und den geheimen Schlüssel zur Überprüfung hoch.
Letzter Wille und Testament	
Aktivieren	Die Last-Will-Nachricht wird automatisch gesendet, wenn die Verbindung zum MQTT-Client abnormal getrennt wird. Sie wird in der Regel verwendet, um Geräte-Statusinformationen zu senden oder andere Geräte oder Proxy-Server über den Offline-Status des Geräts zu informieren. .
Last-Will-Thema	Passen Sie das Thema an, um Last-Will-Nachrichten zu empfangen.
Last-Will-QoS	QoS0, QoS1 oder QoS2 sind optional.
Last-Will-Beibehaltung	Aktivieren Sie diese Option, um die Last-Will-Nachricht als Retain-Nachricht festzulegen.
Letzter Wille Nutzlast	Passen Sie den Inhalt der Last-Will-Nachricht an.
Anfrage- und Antwortthema	
Thema	Der Router unterstützt das Senden von Anfragen zur Abfrage von Router-Informationen. Anfrage: Benutzer können Anfragen an dieses Thema senden, um Router-Informationen abzufragen. Anfrageformat: <pre>{ "id": "1", "status": "systeminfo", "sn": "64E1213132456", „need_response“:1 //1 bedeutet, dass eine Antwort erforderlich ist }</pre> Die ID ist ein Zufallswert, und der Status kann auf fünf Arten festgelegt werden: systeminfo, systemstatus, cellular, ethernet, gps. Antwort: Benutzer können dieses Thema abonnieren, um die Antworten zu erhalten.
Beibehalten	Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als gespeicherte Nachricht festzulegen.
QoS	QoS0, QoS1 oder QoS2 sind optional.
Systemstatus-Veröffentlichungsthema	
Datentyp	Datentyp, der automatisch an den MQTT-Broker gesendet wird. Beachten Sie, dass es sich bei den GPS-Daten auf dieser Seite keine Rohdaten, sondern dekodierte Standortdaten sind.
Thema	Themenname des für die Veröffentlichung verwendeten Datentyps.
Veröffentlichungsintervall (s)	Das Intervall, in dem Daten automatisch an den MQTT-Broker veröffentlicht werden.
Beibehalten	Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als gespeicherte Nachricht festzulegen.
QoS	QoS0, QoS1 oder QoS2 sind optional.

6.5 App

6.5.1 Node-RED

Node-RED ist ein flussbasiertes Entwicklungstool für die visuelle Programmierung und Verknüpfung von Hardwaregeräten, APIs und Online-Diensten als Teil des Internets der Dinge. Node-RED bietet einen

webbrowserbasierten Flusseditor, mit dem sich Flüsse mithilfe der zahlreichen Knoten in der Palette einfach miteinander verbinden lassen. Weitere Anleitungen und Dokumentationen finden Sie auf [der offiziellen Website von Node-RED](#). Wenn Node-RED nicht installiert ist, laden Sie bitte die Node-RED-App von der Milesight-Website herunter und installieren Sie sie auf dem Gerät.

Node-RED Installation

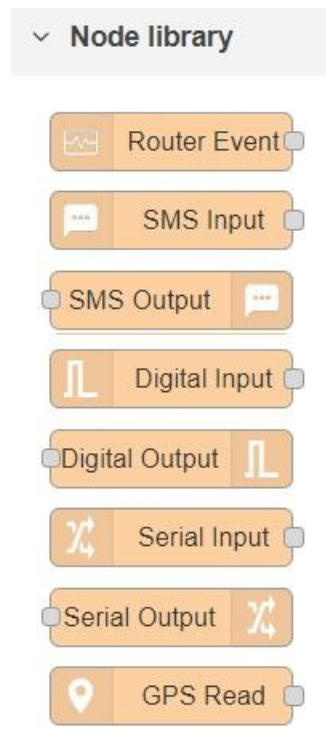
Browse

Nach der Installation wird der folgende Status angezeigt.

Enable	☐	Launch
Node-RED Version	3.0.2	
Node Library Version	1.0.1	
Upgrade Node Library	Browse	
All Flows	Export	
Restore to factory settings	Reset	
Uninstall	Uninstall	

Node-RED	
Element	Beschreibung
Aktivieren	Aktivieren Sie Node-RED.
Starten	Klicken Sie hier, um die Web-GUI von Node-RED zu starten. Die Anmeldeberechtigung für die Web-GUI von Node RED entspricht der des Admin-Kontos der Web-GUI.
Node-RED-Version	Zeigen Sie die Version von Node-RED an.
Node-Bibliotheksversion	Zeigt die Version der von Milesight bereitgestellten Node-Bibliothek an.
Node-Bibliothek aktualisieren	Aktualisieren Sie die Node-Bibliothek, indem Sie das Bibliothekspaket importieren.
Alle Flows exportieren	Alle Flows als JSON-Datei exportieren.
Auf Werkseinstellungen zurücksetzen	Löschen Sie alle Flows-Daten von Node-RED.
Einstellungen	
Deinstallieren	Deinstallieren Sie die Node-RED-App von diesem Gerät.

Milesight bietet eine angepasste Knotenbibliothek zur Verwendung der Schnittstellen des Routers.



Knotenbibliothek	
Knoten	Beschreibung
Router-Ereignis	Überwachen Sie Alarmereignisse des Geräts.
SMS-Eingabe	Empfangen von SMS-Nachrichten. Dies funktioniert nur, wenn das Mobilfunknetz verbunden ist.
SMS-Ausgabe	Eine SMS-Nachricht senden. Dies funktioniert nur, wenn das Mobiltelefon verbunden ist.
Digitaler Eingang	DI-Status empfangen. Dies funktioniert nur, wenn DI aktiviert ist und die Aktion Node-RED unter Service > I/O > DI-Web-GUI .
Digitaler Ausgang	DO-Status auslösen. Dies funktioniert nur, wenn DO unter „ Service > I/O > DO Web-GUI “ aktiviert ist.
Serieller Eingang	Serielle Schnittstellendaten empfangen. Dies funktioniert nur, wenn die serielle Schnittstelle aktiviert ist, der serielle Modus auf DTU eingestellt ist und das DTU-Protokoll auf Node-RED unter Service > Serieller Anschluss > Web-GUI für seriellen Anschluss
Serielle Ausgabe	Befehl an die serielle Schnittstelle senden. Dies funktioniert nur, wenn die serielle Schnittstelle aktiviert ist, der serielle Modus DTU ist und das DTU-Protokoll Node-RED unter Service > Serieller Anschluss > Serieller Anschluss Web-GUI .
GPS lesen	GPS-Daten empfangen. Dies funktioniert nur, wenn GPS unter „ Service > GPS > GPS-Web-GUI “ aktiviert ist.

6.6 System

In diesem Abschnitt wird beschrieben, wie Sie allgemeine Einstellungen und Debugging-Funktionen konfigurieren, z. B. Administratorkonto, Systemzeit, allgemeine Benutzerverwaltung, Geräteverwaltung, Download-Protokolle usw.

6.6.1 Verwaltung

6.6.1.1 Systemeinstellungen

General Settings

Host Name Router

Time Synchronization

Local Time 2024/09/23 01:52:28

Time Zone UTC

Time Sync Sync with NTP Server

System – Allgemeine Einstellungen	
Element	Beschreibung
Hostname	Definieren Sie den Gerätenamen, mit einem Buchstaben beginnen muss.
Ortszeit	Zeigt die aktuelle Systemzeit an.
Zeitzone	Klicken Sie auf die Dropdown-Liste, um die Zeitzone auszuwählen, in der Sie sich befinden.
Zeitsynchronisation	Wählen Sie den Modus für die Zeitsynchronisierung aus. Browserzeit synchronisieren: Zeit mit dem Browser synchronisieren. Mit NTP-Server synchronisieren: Synchronisieren Sie die Zeit mit dem NTP-Server. GPS-Zeitsynchronisierung: Synchronisieren Sie die Zeit stündlich mit GPS. Stellen Sie sicher, dass GPS unter „Service > GPS > GPS“ aktiviert ist. Manuell: Konfigurieren Sie die Zeit manuell.

NTP Settings

Enable NTP Server ☐

Secondary NTP Server

pool.ntp.org

cn.pool.ntp.org

time.nist.gov

System – NTP-Einstellung	
Element	Beschreibung
NTP-Server aktivieren	Aktivieren Sie diese Option, um einen NTP-Server für verbundene Geräte bereitzustellen.
NTP-Server-Kandidaten	Geben Sie die IP-Adresse oder den Domännennamen des NTP-Servers ein, um die Zeit zu synchronisieren. Es können maximal 5 Server hinzugefügt werden.

6.6.1.2 Benutzereinstellungen

Sie können den Benutzernamen oder das Passwort des Administrators für den Zugriff auf das Gerät ändern.

Username	admin
Old Password	
New Password	
Confirmation	

Kontoinformationen ändern	
Element	Beschreibung
Benutzername	Geben Sie den Benutzernamen des Administratorkontos ein.
Altes Passwort	Geben Sie das alte Passwort ein, um die Berechtigung zu überprüfen.
Neues Passwort	Geben Sie ein neues Passwort ein. Sie können alle ASCII-Zeichen außer Leerzeichen.
Bestätigung	Geben Sie das neue Passwort erneut ein.

6.6.1.3 Verwaltung mehrerer Benutzer

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

User List

Username	Password	Permission	
user		Read-Write	Delete
user2		Read-Only	Delete
			Add

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

6.6.2 Wartung

6.6.2.1 Protokoll

Benutzer können Protokolle herunterladen, die Aufzeichnungen über Informations-, Fehler- und Warnereignisse enthalten, die Aufschluss über die Systemprozesse geben. Durch Überprüfen der Daten im Protokoll 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 das Gerät lädt alle Systemprotokolle auf einen Remote-Protokollserver wie Syslog Watcher hoch.

External System Log Server	0.0.0.0
External System Log Server Port	514
External System Log Server Protocol	UDP
Cron Log Level	Debug
AP Log	start
Start or Stop MD Log	stop
MD Log Save Mode	USB
MD Log Level	Debug

Protokoll – Allgemeine Einstellungen	
Element	Beschreibung
Externes Systemprotokoll Server	Geben Sie die Adresse des Remote-Protokoll-Servers (IP/Domänenname) ein, an den der Router sendet.
Externes Systemprotokoll Server-Port	Geben Sie den Port des Remote-Protokoll-Servers ein, an den der Router sendet.
Externes Systemprotokoll Serverprotokoll	Wählen Sie UDP oder TCP aus der Dropdown-Liste, um die Protokolldatei im entsprechenden Protokoll zu übertragen.
Cron-Protokollstufe	Die Schweregrade zum Drucken des AP-Protokolls: Normal, Warnung, Debug.
AP-Protokoll	Wählen Sie diese Option, um die Aufzeichnung des Systemprotokolls zu starten oder zu beenden.
MD starten oder stoppen Protokoll	Wählen Sie diese Option, um die Aufzeichnung des Mobilfunkmodulprotokolls zu starten oder zu stoppen.
MD-Protokoll-Speichermodus	Wählen Sie den Speicher- und Ausgabemodus des MD-Protokolls aus.
MD-Protokollstufe	Die Schweregrade zum Drucken des MD-Protokolls: Info, Hinweis, Warnung, Fehler, Kritisch, Alarm, Notfall, Debug.

AP Log

Download

Tcpdump Log

Start

Stop

Download

Protokoll – Erweiterte Einstellungen	
Element	Beschreibung
AP-Protokoll	
Herunterladen	Klicken Sie hier, um das zuletzt aufgezeichnete AP-Protokoll herunterzuladen.
Tcpdump-Protokoll	
Start	Klicken Sie hier, um die Aufzeichnung des Tcpdump-Protokolls zu starten.
Stopp	Klicken Sie hier, um die Aufzeichnung des tcpdump-Protokolls zu beenden.
Herunterladen	Klicken Sie hier, um das zuletzt aufgezeichnete tcpdump-Protokoll herunterzuladen.

6.6.2.2 Mobilfunk-Debugger

Mit diesem Tool können Sie AT-Befehle eingeben, indem Sie den AT-Befehl eingeben und **die Eingabetaste** drücken, um ihn auszuführen und die Debug-Informationen des Mobilfunknetzes zu überprüfen.

Cellular Debugger
Firewall Debugger

Enter the AT command that you want to send to cellular modem. Press "Enter" to execute.

Eg: AT+COPS?

AT+CSQ
AT+ECELL
AT+ERAT?
AT+EPBSEH?
AT+CREG?
AT+COPS?
Edit

Clear

Klicken Sie außerdem auf „**EDIT**“, um die allgemeinen AT-Befehle anzupassen, und drücken Sie dann direkt auf die Schaltflächen oben im schwarzen Rahmen, um allgemeine Befehle direkt auszuführen.

Edit AT Commands

AT Commands

AT+CSQ

Delete

AT+ECELL

Delete

AT+ERAT?

Delete

AT+EPBSEH?

Delete

AT+CREG?

Delete

AT+COPS?

Delete

Add

Save

Beschreibung der gängigen Befehle:

AT+CSQ? -----Mobilfunknetzsignal abrufen

AT+ECELL? -----Aktuelle Zellinformationen abrufen

AT+ERAT? -----RAT-Status und Netzwerktyp abrufen

AT+EPBSEH? -----Verwendete Frequenzbänder abrufen

AT+CREG? -----Netzwerkregistrierungsstatus abrufen

AT+COPS? -----Informationen zum Betreiber und zur Zugangstechnologie abrufen

6.6.2.3 Firewall-Debugger

Mit diesem Tool können Sie iptables-Befehle verwenden, um Firewall-Informationen zu überprüfen und Ergebnisse herunterzuladen.

Cellular Debugger

Firewall Debugger

Enter the command that you want to send to firewall module. Press "Enter" to execute.

Eg: -t nat -vL INPUT

Clear

Download

6.6.2.4 Sicherung/Upgrade

In diesem Abschnitt wird beschrieben, wie Sie eine vollständige Sicherung der Systemkonfigurationen in einer Datei erstellen, die Werkseinstellungen wiederherstellen, die Konfigurationsdatei auf dem Gerät wiederherstellen und das Flash-Image über das Internet aktualisieren können. In der Regel ist ein Firmware-Upgrade nicht erforderlich.

Hinweis: Während des Firmware-Upgrades sind keine Vorgänge auf der Webseite zulässig, da sonst das Upgrade unterbrochen wird oder das Gerät sogar ausfällt.

Backup

Click "Download" to download a tar archive of the current configuration file.

Download

Restore

Click "Restore Backup" to upload the backup archive to restore the configuration. To restore the firmware to the factory state, click "Perform Reset".

Perform Reset

Restore Backup

Flash new firmware image

Upload a image here to replace the running firmware.

Upload

Sicherung/Aktualisierung	
Element	Beschreibung
Sicherung erstellen	Klicken Sie hier, um ein Tar-Archiv der aktuellen Konfigurationsdatei herunterzuladen.
Zurücksetzen	Klicken Sie hier, um das Gerät auf die Werkseinstellungen zurückzusetzen.
Sicherung wiederherstellen	Um Konfigurationsdateien wiederherzustellen, können Sie hier ein zuvor erstelltes Sicherungsarchiv hochladen. Benutzerdefinierte Dateien (Zertifikate, Skripte) können auf dem System verbleiben. Um dies zu verhindern, können Sie zunächst einen Werksreset durchführen.
Hochladen	Laden Sie hier ein Image hoch, um die laufende Firmware zu ersetzen.

Verwandtes Konfigurationsbeispiel

[Firmware-Upgrade](#)

[Werkseinstellungen](#)

[wiederherstellen](#)

6.6.2.5 Neustart

Auf dieser Seite können Sie das Gerät sofort oder regelmäßig neu starten.

Reboot

Reboot Now

Reboot the system on your device

Scheduled Reboot



Cycles

Every Day



Time



Neustart	
Element	Beschreibung
Jetzt neu starten	Das Gerät sofort neu starten.
Zeitplan	
Aktivieren	Klicken Sie hier, um den Neustart-Zeitplan zu aktivieren.
Zyklen	Starten Sie das Gerät in einem festgelegten Zeitintervall neu.
Zeit	Wählen Sie die Uhrzeit für die Ausführung des Zeitplans aus.

6.6.3 Ereignisalarm

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

6.6.3.1 Ereignisalarm

Auf dieser Seite können Sie Alarmmeldungen anzeigen.

Cellular Up X

Cellular Down X

WAN Up X

WAN Down X

VPN Up X

VPN Down X

System Reboot X

System Startup X

Cellular Data Stats Clear X

Cellular Data Traffic is running out X

Export

Time	EventType	Description
2024-09-02 23:20:49	WiFi Connected	WLAN1-2.4G connected
2024-09-02 23:18:49	WiFi Disconnected	WLAN2-5G disconnected
2024-09-02 04:57:44	Link switch	Network switched from wlan_5g to wan
2024-09-02 04:57:28	Link switch	Network switched from wan to wlan_5g
2024-09-02 04:57:19	WAN Up	WAN up

Ereignisalarm	
Element	Beschreibung
Suche	Wählen Sie den Ereignisalarm aus, den Sie in dieser Liste anzeigen möchten.
Export	Exportieren Sie die Ereignisalarmliste in eine CSV-Datei.
Zeit	Zeigen Sie die Alarmzeit an.
Ereignistyp	Zeigen Sie den Typ der Ereignisalarme an.
Beschreibung	Zeigt die Details der Ereignisalarme an.

6.6.3.2 Ereigniseinstellungen

In diesem Abschnitt können Sie festlegen, ob Sie bei Änderungen Benachrichtigungen per SMS, SNMP oder MQTT erhalten möchten.

SMS Notification

Enable ☒

Phone Group List

group3 X group2 X

Event Type

WAN Up X WAN Down X

SNMP

Enable ☐

Event Type

MQTT Connections

Enable ☐

Event Type	MQTT Connections	Topic	Retain	QoS	
	111	/test1	☒	QoS 1	Delete
	111	/test	☐	QoS 0	Delete

Add

Ereigniseinstellungen	
Element	Beschreibung
SMS-Benachrichtigung	
Aktivieren	Aktivieren Sie die SMS-Benachrichtigung, wenn ein Ereignis ausgelöst wird.
Telefon-Gruppenliste	Wählen Sie die Telefongruppe aus, die SMS-Benachrichtigungen erhalten soll.
Ereignistyp	Wählen Sie den Ereignistyp aus, für den SMS-Benachrichtigungen gesendet werden sollen.
SNMP	
Aktivieren	Aktivieren Sie diese Option, um SNMP-Benachrichtigungen zu aktivieren, wenn ein Ereignis ausgelöst wird.
Ereignistyp	Wählen Sie den Ereignistyp aus, der über SNMP aufgezeichnet werden soll.
MQTT-Verbindungen	
Aktivieren	Aktivieren Sie diese Option, um MQTT-Benachrichtigungen zu aktivieren, wenn ein Ereignis ausgelöst wird.
Ereignistyp	Wählen Sie den Ereignistyp aus, der MQTT senden soll. Benachrichtigungen.
MQTT-Verbindung	Wählen Sie die MQTT-Verbindung zum Senden von Benachrichtigungen aus. Diese ist auf der Seite „ Service > MQTT “.
Thema	Themenname, der für die Veröffentlichung von Daten aus der seriellen Schnittstelle verwendet wird.
Beibehalten	Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als Retain-Nachricht festzulegen.
QoS	QoS0, QoS1 oder QoS2 sind optional.

6.6.4 Geräteverwaltung

6.6.4.1 Geräteverwaltung

Sie können das Gerät auf dieser Seite mit der Milesight DeviceHub-Verwaltungsplattform verbinden, um das Gerät zentral und aus der Ferne zu verwalten. Weitere Informationen finden Sie im [DeviceHub-Benutzerhandbuch](#).

Status Disconnected

Server Address

Activation Method By Account name 

Account name

Password 

[Connect](#)

Geräteverwaltung	
Element	Beschreibung
Status	Zeigt den Verbindungsstatus zwischen dem Gerät und dem DeviceHub.
Serveradresse	IP-Adresse oder Domäne des DeviceHub-Verwaltungsservers.
Aktivierungsmethode	Wählen Sie die Aktivierungsmethode, um das Gerät mit dem DeviceHub-Server zu verbinden. Die Optionen sind „Per Authentifizierungscode“ und „Per Kontoname “.
Authentifizierungscode	Geben Sie den vom DeviceHub generierten Authentifizierungscode ein.
Kontoname	Geben Sie den registrierten DeviceHub-Kontonamen (E-Mail-Adresse) und das Passwort ein.
Passwort	
Verbinden/Trennen	Klicken Sie auf diese Schaltfläche, um das Gerät mit dem DeviceHub zu verbinden/die Verbindung zum DeviceHub zu trennen. DeviceHub zu verbinden/zu trennen.

6.6.4.2 Cloud-VPN

Sie können das Gerät auf dieser Seite mit MilesightVPN verbinden, um den Router und die angeschlossenen Geräte zentral und aus der Ferne zu verwalten. Weitere Informationen finden Sie im [MilesightVPN-Benutzerhandbuch](#).

Settings

Server

Port

Authentication Code

Device Name

CONNECT

Status

Status Disconnected

Local IP --

Remote IP --

Connection Time --

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

[ENDE]