wieland

wienet v2/v3 Konfiguration

Mobilfunkrouter & LAN-to-LAN Router

Handbuch

Dok.-Nr. BA001038
Stand: 11/2022 (Rev. C)

HINWEISE

Dieses Dokument ist urheberrechtlich geschützt. Alle Rechte liegen bei der Wieland Electric GmbH. Die vollständige oder teilweise Vervielfältigung dieses Dokuments ist nur im Umfang der gesetzlichen Bestimmungen des Urheberrechts zulässig. Änderungen oder Kürzungen ohne vorherige schriftliche Genehmigung der Wieland Electric GmbH sind untersagt.

wienet ist eine Marke der Wieland Electric GmbH. Weitere in dieser Anleitung erwähnte Produkt- und Markennamen sind Marken oder eingetragene Marken der jeweiligen Besitzer. Die Verwendung dieser Namen und Warenzeichen durch Dritte für deren Zwecke kann die Inhaberrechte verletzen.

CE

INHALTSVERZEICHNIS

1 Über dieses Handbuch 6

1.1 Funktion und Aufbau des Handbuchs 6

1.2 Zielgruppen und Qualifikation des Personals 6

1.3 Mitgeltende Dokumente 7

1.4 Darstellung von sicherheitsrelevanten Informationen 7

2 Grundlegende Informationen 8

2.1 Konfigurationsmöglichkeiten 8

2.2 IPv6 Unterstützung 9

2.3 Unterstützung von IEEE 802.1X (RADIUS) 9

3 Zugriff auf die Web-Konfiguration 11

3.1 Vermeidung der Meldung einer Domain-Unstimmigkeit 13

4 Status 14

4.1 Allgemeiner Status 14

4.1.1 Mobile Verbindung 14

4.1.2 Ethernet/LAN Status 15

4.1.3 Systeminformationen 15

4.2 Mobile WAN Status 16

4.3 Wi-Fi-Status 19

4.4 Wi-Fi-Scan 20

4.5 Netzwerkstatus 22

4.6 DHCP-Status 24

4.6.1 Serie v2 24

4.6.2 Serie v3 25

4.7 IPsec-Status 26

4.8 WireGuard Status 27

4.9 DynDNS-Status 28

4.10 System log 29

5 Konfiguration 30

5.1 Ethernet- bzw. LAN-Konfiguration 30

5.1.1 DHCP-Server 32

5.1.2 IPv6-Präfix-Delegierung 33

5.1.3 802.1X-Authentifizierung beim RADIUS-Server 33

5.1.4 Beispiele für LAN-Konfiguration 34

5.2 VRRP-Konfiguration 37

5.3 Mobile WAN Konfiguration 39
5.3.1 Mobilfunkverbindung 39
5.3.2 Konfiguration der DNS-Adressen 40
5.3.3 Konfiguration der Kontrolle der Mobilfunkverbindung 40
5.3.4 Konfiguration des Datenlimits 41
5.3.5 Umschalten der SIM-Kartenkonfiguration 42
5.3.6 Konfiguration des PPPoE-Bridge-Modus 46
5.4 PPPoE-Konfiguration 46
5.5 Wi-Fi-Access-Point-Konfiguration 48
5.6 Wi-Fi-Station-Konfiguration 52
5.7 Backup-Routen 55
5.8 Statische Routen 58
5.9 Firewall-Konfiguration 59
5.10 NAT-Konfiguration 63
5.11 Konfiguration des OpenVPN-Tunnels 68
5.12 Konfiguration des IPSec-Tunnels 74
5.12.1 Konfiguration IPSec für v2 Router 74
5.12.2 Konfiguration IPSec für v3 Router 80
5.13 Konfiguration WireGuard-Tunnel 85
5.14 Konfiguration des GRE-Tunnels 89
5.15 Konfiguration des L2TP-Tunnels 91
5.16 Konfiguration des PPTP-Tunnels 93
5.17 Services 95
5.17.1 DynDNS 95
5.17.2 FTP 96
5.17.3 HTTP 96
5.17.4 NTP 97
5.17.5 PAM 98
5.17.6 SNMP 101
5.17.7 SMTP 104
5.17.8 SMS 105
5.17.9 SSH 111
5.17.10 Syslog 111
5.17.11 Telnet 112
5.18 Erweiterungsport – Konfiguration der seriellen Schnittstellen 112
5.19 Konfiguration des USB-Ports 116
5.20 Skripte 119
5.20.1 Startup-Skript 119
5.20.2 Up/Down-Skript 119

5.21 Konfiguration der automatischen Aktualisierung 120

6 Anwenderanpassung 123

6.1 Benutzermodule 123

7 Administration 125

7.1 Benutzer 125

7.2 Änderung des Profils 126

7.3 Passwort ändern 126

7.4 Zwei-Faktor-Authentifizierung (gilt nur für v2 Router) 127

7.5 Echtzeituhr einstellen 131

7.6 Einstellung des SMS-Service-Centers 131

7.7 SIM-Karte entsperren 132

7.8 SIM-Karte entsperren 132

7.9 Versenden einer SMS-Nachricht 133

7.10 Konfiguration sichern 133

7.11 Konfiguration wiederherstellen 134

7.12 Aktualisierung der Firmware 134

7.13 Reboot (Neustart) 135

7.14 Abmelden 135

8 Konfiguration in typischen Situationen 136

8.1 Internetzugang über LAN 136

8.2 Backup-Zugang zum Internet aus dem LAN 138

8.3 Sichere Netzzusammenschaltung oder mittels VPN 142

8.4 Serielles Gateway 144

9 Entsorgung 146

10 Service und Support 147

11 Anhang 148

11.1 Glossar 148

1 ÜBER DIESES HANDBUCH

Bevor Sie dieses Handbuch und den wienet Router von Wieland verwenden, lesen Sie diesen Abschnitt bitte sorgfältig durch. Hier finden Sie alle notwendigen Informationen zur Inbetriebnahme und Verwendung.

Bitte beachten Sie, dass dieses Handbuch für die v2 und v3 Routerserie verwendet werden kann. Spezifische Unterschiede zwischen den Geräteserien sind im nachfolgenden entsprechend gekennzeichnet.

V2: XR5iv2, LR77 v2, LR140 EMEA, LR240 EMEA, LR241 EMEA

V3: WR-LTE v3, LAN-WR v3, ER300 GLOBAL, LR340 EMEA

1.1 Funktion und Aufbau des Handbuchs

Dieses wienet-Handbuch beschreibt die Konfiguration des Routers.

Dieses Handbuch enthält die erforderlichen Informationen für den bestimmungsgemäßen Gebrauch und technische Daten.

Als Orientierung finden Sie ganz vorne im Handbuch das Gesamtinhaltsverzeichnis.

Dieses Handbuch beschreibt die allgemeinen Informationen zum Produkt. Für weitere Informationen siehe Kapitel 1.3 "Mitgeltende Dokumente", S. 7 oder wenden Sie sich an Wieland Electric GmbH, siehe Rückseite.

Dieses Konfigurationshandbuch beschreibt:

- Konfiguration des Routers Punkt für Punkt gemäß Web-Interface (Kapitel 4 bis 7).
- Beispiele dieser typischen Konfigurationen des Routers (Kapitel 8):
  - Internetzugang über LAN (Local Area Network) per Mobilfunknetz
  - Gesicherter Zugang zum Internet (über LAN)
  - Sichere Netzzusammenschaltung mittels VPN (Virtual Private Network)

1.2 Zielgruppen und Qualifikation des Personals

Die Inbetriebnahme und Installation der Komponenten für derartige Installationen muss berücksichtigt werden.

Daher richtet sich das vorliegende System-Handbuch an:

- Personen, die die entsprechende Schulung nachweisen können und bereits über entsprechende Grundkenntnisse verfügen
- Systemintegratoren
- Elektroinstallateure

1.3 Mitgeltende Dokumente

HINWEIS

Weitere Informationen finden Sie auch auf unserer Internetseite: eshop.wieland-electric.com. Hier können außerdem folgende Dokumente heruntergeladen werden:

- Produktinformationen zu wienet Routern
- Datenblätter zu wienet Routern
- Technische Hinweise zu *vpn01.wienet.cloud* (VPN-Server-Portal)

Tab. 1: Mitgeltende Dokumente

Dokument	Titel	Bestellnummer
Montageanleitung	Montageanleitung wienet WR-LTE v3 SL	BA000774
Handbuch	Handbuch wienet LR77 v2	BA000867
Handbuch	Handbuch wienet WR-LTE v3 SL	BA001034
Montageanleitung	Montageanleitung wienet LTE LR240/241 EMEA	BA001285
Handbuch	Handbuch wienet LTE LR240/241 EMEA	BA001290
Montageanleitung	Montageanleitung wienet LTE LR140 EMEA	BA001309
Handbuch	Handbuch wienet LTE LR140 EMEA	BA001292
Montageanleitung	Montageanleitung wienet LAN ER300 GLOBAL	BA001310
Handbuch	Handbuch wienet LAN ER300 GOBAL	BA001313
Montageanleitung	Montageanleitung wienet LTE LR340 EMEA	BA001311
Handbuch	Handbuch wienet LTE LR340 EMEA	BA001315

1.4 Darstellung von sicherheitsrelevanten Informationen

Informationen, die vor Personen- oder Sachschäden warnen, sind durch Sicherheitshinweise hervorgehoben. Bitte lesen Sie diese Informationen sorgfältig durch.

Diese Bedienungsanleitung verwendet Sicherheitshinweise, die gemäß Schwere einer potentiellen Gefahr zugewiesen werden.



GEFAHR

Das Symbol "GEFAHR" weist auf eine unmittelbare Gefahr hin. Die Nichtbeachtung dieses Symbols kann zu schweren Verletzungen oder zum Tod führen.
"GEFAHR" wird verwendet, um vor Gefahren zu warnen, die zur Zeit der Warnung bereits bestehen (z. B. heiße Oberflächen, scharfe Kanten, Quetschstellen usw.)
Dieses Symbol wird ausschließlich bei Verletzungsgefahr verwendet!



WARNUNG

Das Symbol "WARNUNG" weist auf eine mögliche Gefahr hin. Die Nichtbeachtung dieses Symbols kann zu schweren Verletzungen führen.



VORSICHT

Das Symbol "VORSICHT" weist auf eine mögliche Gefahr hin. Die Nichtbeachtung dieses Symbols kann zu leichten Verletzungen führen.

HINWEIS

Hinweise zu besonderen Funktionen des Geräts.

In den Anweisungen wird auf eine potenziell gefährliche Situation hingewiesen. Die Nichtbeachtung dieses Symbols kann zu Schäden am System oder an der Systemumgebung führen.

Im Falle von "Gefahr" oder "Warnung" ist grundsätzlich Leib oder Leben gefährdet. Sachschäden werden hier nur dann berücksichtigt, wenn auch ein der Gefahrenstufe entsprechendes Risiko von Personenschäden besteht.

2 GRUNDLEGENDE INFORMATIONEN

Die Mobilfunkrouter wienet v2 und v3 sind für die Kommunikation in Mobilfunknetzen mittels LTE-HSPA+, UMTS-, EDGE- oder GPRS-Technologie ausgelegt. Die Datenübertragungsgeschwindigkeit beträgt bis zu 100 Mbit/s bzw. 150 Mbit/s (Download) und bis zu 50 Mbit/s (Upload). Der Router ist eine ideale Lösung für die Drahtlosverbindung von Verkehrs- und Videoüberwachungsanlagen, Einzelrechnern, LANs, Geldautomaten, sonstigen SB-Terminals, Aufzügen und anderen Maschinen.

Die wienet v3-Version des Routers (LAN) ist ein ideales Gerät zur Realisierung einer sicheren Verbindung zweier lokaler Netzwerke (LANs). Die Verbindung erfolgt über zwei ETHERNET 10/100 Schnittstellen und sicheren Tunnel (IPsec, OpenVPN, L2TP).

Die andere ebenso wichtige Möglichkeit, diesen Router zu verwenden, besteht darin, ein beliebiges Gerät mit dem lokalen Netzwerk (LAN) zu verbinden. Zu diesem Zweck ist der wienet-Router mit zwei ETHERNET 10/100-Ports und weiteren Schnittstellen je nach der vom Benutzer gewählten Version des Routers ausgestattet.

Geräte der wienet v2-Reihe können mit einem WLAN-Modul ausgestattet werden. Bitte beachten Sie, dass Router nicht nachträglich mit einer WLAN-Schnittstelle ausgestattet werden können.

2.1 Konfigurationsmöglichkeiten

Eine Benutzername- und Passwort-geschützte Web-Schnittstelle stellt Statistiken über die Router-Aktivitäten, Signalstärke, detailliertes Systemprotokoll usw. zur Verfügung. Der Router unterstützt sowohl IPv4- als auch IPv6-Protokolle und erstellt VPN-Tunnel mit den Technologien IPsec, OpenVPN und L2TP für eine sichere Kommunikation. Der Router unterstützt außerdem DHCP, NAT, NAT-T, DynDNS, NTP, VRRP, Steuerung per SMS, Sicherung der primären Verbindung mehrerer WANs, RADIUS-Authentifizierung über WLAN und viele weitere Funktionen.

Zu den weiteren Diagnosefunktionen, die eine kontinuierliche Kommunikation gewährleisten sollen, gehören die automatische Überprüfung der Mobile WAN-Verbindung mit automatischer Neustartfunktion bei Verbindungsfehlern sowie die Überwachung des Routerstatus durch einen Hardware-Watchdog.

Mithilfe eines Startskriptfensters können Benutzer Linux-Skripte für verschiedene Aktionen einfügen. Benutzer können mehrere Skripte einfügen und der Router kann nach Bedarf zwischen den Konfigurationen wechseln. Beispiele hierfür sind die Verwendung von SMS oder das Überprüfen des Status des Binäreingangs.
wienet-Router können ihre Konfigurationen und Firmware automatisch von einem zentralen Server aktualisieren, was eine Massen-Rekonfiguration mehrerer Router gleichzeitig ermöglicht.

Die Router können per Webbrowser oder Secure Shell (SSH) konfiguriert werden. Die Konfiguration über Webbrowser wird in diesem Konfigurationshandbuch beschrieben. Befehle und Skripte, die bei der Konfiguration über SSH anwendbar sind, werden in Befehle und Skripte für v2- und v3-Router – Anwendungshinweis [1] beschrieben. Die serienmäßige und optionale Ausstattung sowie die technischen Parameter Ihres Routers finden Sie in der Bedienungsanleitung Ihres Routers. Sie können die Zusatzsoftware für die Kommunikation mit einem VPN-Server Wie-Service24 verwenden.

Zulässige Zeichen für die Weboberfläche

Wenn der Router über das Webinterface konfiguriert wird, vermeiden Sie die Eingabe von verbotenen Zeichen in Eingabeformulare (nicht nur für das Passwort). Verbotene Zeichen können in ein Formular geschrieben werden, werden aber bei der Datenspeicherung gelöscht.

Gültige Zeichen sind: `0-9 a-z A-Z * , + - . / : = ? ! # % @ [ ] _ { } ~`

Verbotene Zeichen sind: `" $ & ' ( ) ; < > \ ^ ' | "Leerzeichen"`

2.2 IPv6 Unterstützung

In der Firmware des Routers ist eine unabhängige Ipv4- und Ipv6-Dual-Stack-Konfiguration implementiert. Dies bedeutet, dass Sie den Datenverkehr über beide IP-Protokolle unabhängig konfigurieren können und beide unterstützt werden. Zusätzliche EUI-64 Ipv6-Adressen von Netzwerkschnittstellen werden automatisch durch Standardmethoden generiert. Es gibt eine interne NAT64-Gateway-Netzwerkschnittstelle für die automatische Übersetzung zwischen Ipv6 und Ipv4. Für weitere Informationen siehe Kapitel 4.5 "Netzwerkstatus", S. 22. Dieses Gateway arbeitet nahtlos mit DNS64 zusammen (für die Übersetzung von Domainnamen).

Für Mobilfunkverbindungen über Ipv6-Verbindung siehe Mobile WAN-Konfiguration in Kapitel 5.3.1 "Mobilfunkverbindung", S. 39. Zur Ipv6-LAN-Konfiguration siehe LAN-Konfiguration in Kapitel 5.1 "Ethernet- bzw. LAN-Konfiguration", S. 30. DHCPv6-Server/-Client wird ebenfalls unterstützt. Ipv4 ist die Standardeinstellung, aber Ipv6 kann mit allen Funktionen und Protokollen im Router aktiviert oder verwendet werden, mit Ausnahme der ungesicherten Tunnel GRE, L2TP und PPTP sowie VRRP. Mit den gesicherten Tunneln OpenVPN und Ipsec ist es möglich, Ipv6-Verkehr durch einen Ipv4-Tunnel zu führen und umgekehrt. Die Konfigurationsformulare für NAT, Firewall und Up/Down-Skripte sind für die Ipv4- und Ipv6-Stacks komplett getrennt. Das ICMPv6-Protokoll wird ebenfalls unterstützt. Die Ipv6-Konfiguration wird nach Möglichkeit in jedem der folgenden Kapitel behandelt.

2.3 Unterstützung von IEEE 802.1X (RADIUS)

IEEE 802.1X ist ein IEEE-Standard für portbasierte Netzwerkzugangskontrolle (PNAC). Er ist Teil der IEEE 802.1-Gruppe von Netzwerkprotokollen. Er bietet einen Authentifizierungsmechanismus für Geräte, die sich mit einem LAN oder WLAN verbinden möchten. IEEE 802.1X definiert die Einkapselung des Extensible Authentication Protocol (EAP) über IEEE 802, bekannt als "EAP over LAN" oder EAPoL.

An der 802.1X-Authentifizierung sind drei Parteien beteiligt: ein Client (Supplicant), ein Authentifizierer (Authenticator) und ein Authentifizierungsserver (Authentication Server, siehe Abbildung 1).

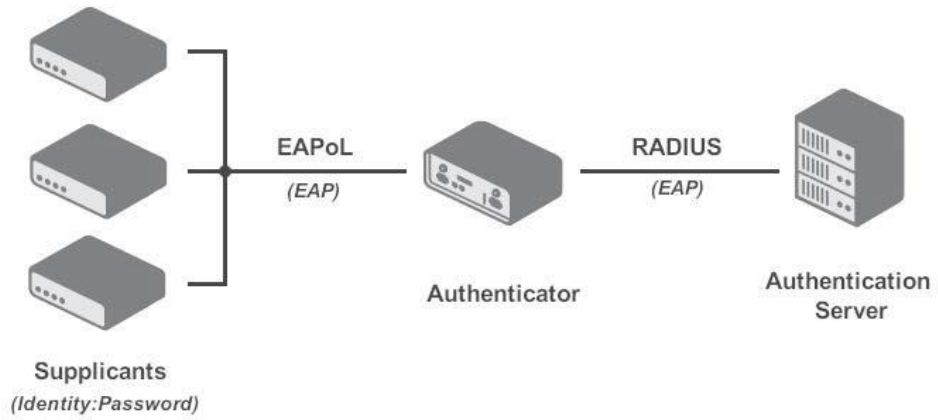


Abb. 1: Funktionsdiagramm IEEE 802.1X

- Der Supplicant ist ein Client-Gerät (z. B. ein Laptop), das sich mit dem LAN/WLAN verbinden möchte. Der Begriff "Supplicant" wird auch synonym für die auf dem Client laufende Software verwendet, die dem Authenticator Anmeldedaten zur Verfügung stellt.
- Der Authenticator ist ein Netzwerkgerät, das eine Datenverbindung zwischen dem Client (Supplicant) und dem Netzwerk (LAN/WAN) herstellt und den Netzwerkverkehr zwischen den beiden zulassen oder blockieren kann, z. B. ein Ethernet-Switch oder ein Wireless Access Point. Der Authenticator kommuniziert mit dem Authentication Server, um festzustellen, ob der Netzzugang für einen Supplicant gewährt wird oder nicht.
- Bei dem Authenticator Server handelt es sich in der Regel um einen vertrauenswürdigen Server, der Anfragen für den Netzzugang empfangen und beantworten und dem Authenticator mitteilen kann, ob die Verbindung zugelassen werden soll und welche Einstellungen für die Verbindung oder die Einstellung des Clients gelten sollen. Auf Authenticator Servern läuft in der Regel Software, die die RADIUS- und EAP-Protokolle unterstützt.

Tabelle 1 fasst alle unterstützten Fälle und Funktionen zusammen, in denen die IEEE 802.1X-Authentifizierung auf wienet Routern verwendet werden kann.

Bitte beachten Sie, dass die Funktion des Authenticator Server von wienet Routern nicht unterstützt wird.

Tab. 2: Unterstützte Funktionen der IEEE 802.1X-Authentifizierung

Interface	Supplicant-Funktion	Authenticator-Funktion
LAN	Eingebaute Funktion, konfigurieren Sie einfach das LAN mit 802.1X-Authentifizierung, siehe Kapitel 5.1.3 "802.1X-Authentifizierung beim RADIUS-Server", S. 33.	Keine eingebaute Funktion, kann aber durch den UM 802.1X Authenticator implementiert werden. Weitere Informationen zu diesem Modul finden Sie in Kapitel 5.1.3 "802.1X-Authentifizierung beim RADIUS-Server", S. 33.
WiFi	Unterstützt für den Stationsmodus (STA), siehe Kapitel 5.6 "Wi-Fi-Station-Konfiguration", S. 52.	Unterstützt für den Access Point (AP) Modus, siehe Kapitel 5.5 "Wi-Fi-Access-Point-Konfiguration", S. 48.

3 ZUGRIFF AUF DIE WEB-KONFIGURATION

VORSICHT

Der Mobilfunkrouter funktioniert nur, wenn der Mobilfunkanbieter korrekt konfiguriert und das Konto aktiviert und für die Datenkommunikation bereitgestellt wurde. Bei Mobilfunkanbietern muss eine SIM-Karte in den Router eingelegt werden. Legen Sie die SIM-Karte nicht ein, während der Router eingeschaltet ist.

Die Überwachung des Status, das Konfigurieren und die Verwaltung des Routers erfolgt über das integrierte Web-Interface. Die Weboberfläche erreichen Sie, indem Sie die IP-Adresse des Routers in den Webbrowser eingeben. Die Standard-IP-Adresse des Routers lautet 192.168.1.1.

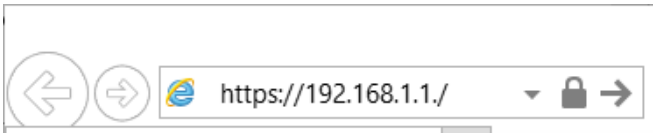


Abb. 2: IP-Adresse

Die Konfiguration kann nur vom Benutzer "root" und seinem Kennwort (Standardkennwort: siehe Etikett "P<letzte 8 Stellen der CSN>h") vorgenommen werden.



Abb. 3: Login

Nachdem die Login-Daten erfolgreich eingegeben wurden, hat der Benutzer Zugriff auf den Router über die Weboberfläche.

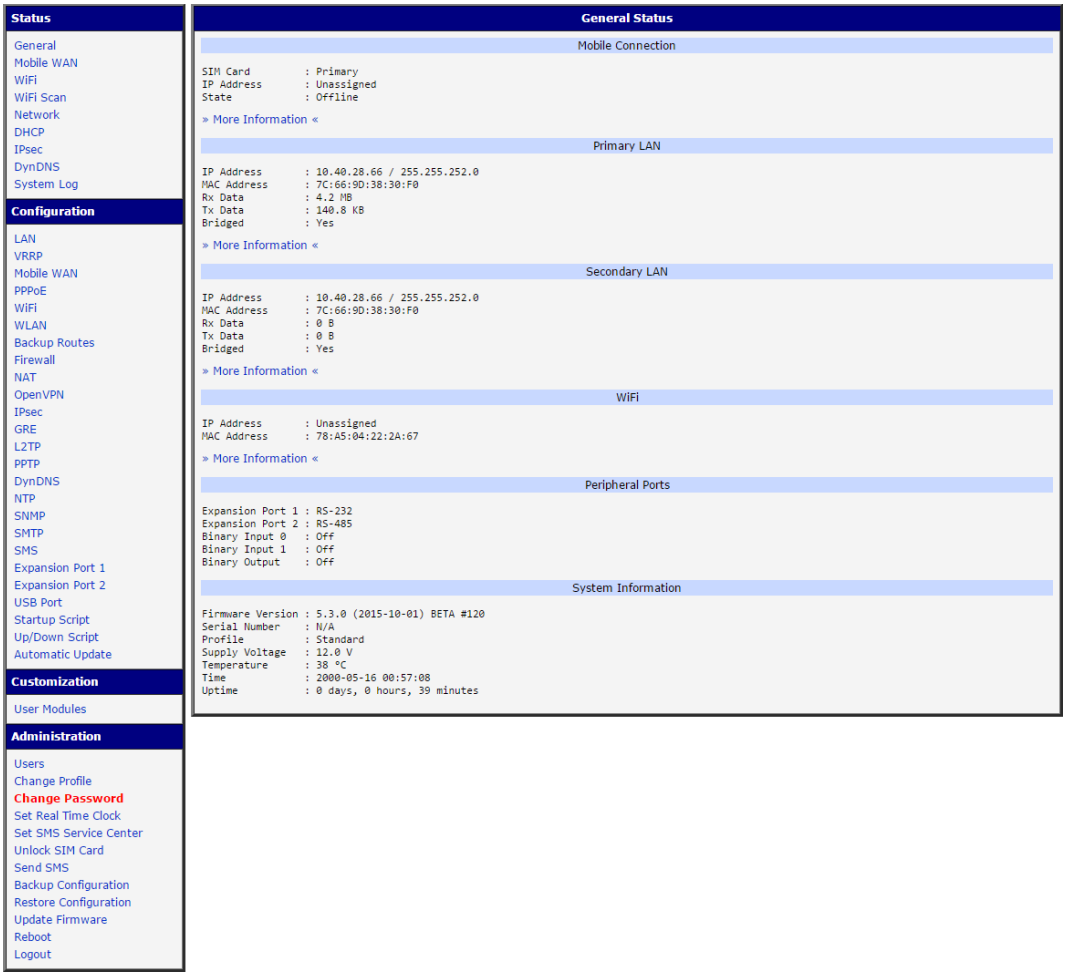


Abb. 4: Beispiel für Web-Konfiguration

Wenn Sie die Anmeldedaten erfolgreich auf der Login-Seite eingeben, wird das Web-Interface angezeigt. Die linke Seite des Web-Interfaces **zeigt** das Menü. Sie finden dort Links für **Status, Konfiguration, Anwenderanpassung und Verwaltung** des Routers. **Bezeichnung und Standort** zeigt die Bezeichnung, den Standort und die SNMP-Konfiguration an (siehe Kapitel 5.17.1 "DynDNS", S. 95). Diese Felder sind für jeden Router benutzerdefiniert.

VORSICHT

Zur Erhöhung der Sicherheit sollten Sie das Standardpasswort ändern. Wenn das Standardpasswort des Routers eingestellt ist, wird der Menüpunkt **Passwort ändern** rot hervorgehoben.

HINWEIS

Nach drei erfolglosen Anmeldeversuchen wird jeder HTTP(S)-Zugriff von einer IP-Adresse für eine Minute gesperrt.

Wenn Sie die Anmeldeinformationen auf der Anmeldeseite erfolgreich eingegeben haben, wird die Weboberfläche angezeigt.
Die linke Seite der Weboberfläche enthält einen Menübaum mit Abschnitten für Überwachung (**Status**), Konfiguration (**Configuration**), Anpassungen (**Customization**) and Administration (**Administration**) des Routers.

Die Elemente **Name** und **Location** in der rechten oberen Ecke zeigen den Namen und den Standort des Routers in der SNMP-Konfiguration an (siehe Kapitel 5.17.1 "DynDNS", S. 95). Diese Felder sind für jeden Router benutzerdefiniert.

Nachdem die grüne LED zu blinken beginnt, können Sie die ursprünglichen Router-Einstellungen wiederherstellen, indem Sie die Reset-Taste (**RST**) auf der Rückseite drücken. Wenn die Reset-Taste gedrückt wird, werden alle Konfigurationen auf die Werkseinstellungen zurückgesetzt und der Router startet neu (die grüne LED leuchtet während des Neustarts).

3.1 Vermeidung der Meldung einer Domain-Unstimmigkeit

wienet **Router Support:**

- CA, Local/Remote Certificate: *.pem, *.crt, *.p12
- Priv. Schlüssel: *.pem, *.key oder *.p12
- Dies gilt für alle Zertifikate im Router (HTTPS, OpenVPN, IPsec, Wi-Fi STA etc.)

Im Router befindet sich das selbstsignierte HTTPS-Zertifikat. Da die Identität dieses Zertifikats nicht validiert werden kann, kann im Webbrowser eine Meldung erscheinen. Um dieses Problem zu lösen, laden Sie Ihr eigenes, von der Zertifizierungsstelle signiertes Zertifikat auf den Router hoch. Wenn Sie Ihr eigenes Zertifikat verwenden möchten (z. B. in Kombination mit dem dynamischen DNS-Dienst), müssen Sie die Dateien **/etc/certs/https_cert** und **/etc/certs/https_key** im Router ersetzen. Dies kann ganz einfach in der GUI auf der Konfigurationsseite **HTTP** erfolgen, siehe Kapitel 5.17.3 "HTTP", S. 96.

HINWEIS Die HTTPS-Zertifikaterstellung im Router wurde seit FW 5.3.5 aktualisiert, um mehr Sicherheit zu bieten. Vorhandene HTTPS-Zertifikate auf bereits hergestellten Routern werden beim Firmware-Upgrade nicht automatisch aktualisiert! Sie können ein HTTPS-Zertifikat aktualisieren oder Ihr eigenes Zertifikat hochladen, für weitere Informationen siehe Kapitel 5.17.3 "HTTP", S. 96.

Wenn Sie sich dafür entscheiden, das selbstsignierte Zertifikat im Router zu verwenden, um zu verhindern, dass bei jeder Anmeldung am Router die Sicherheitsmeldung (Domain Dissens) angezeigt wird, können Sie die folgenden Schritte ausführen:

➡ Fügen Sie den DNS-Eintrag zu Ihrem DNS-System hinzu: **Edit /etc/hosts** (Linux/Unix OS) oder **C:\WINDOWS\system32\drivers\etc\hosts** (Windows OS) oder konfigurieren Sie Ihren eigenen DNS-Server.

➡ Fügen Sie einen neuen Eintrag mit der IP-Adresse Ihres Routers und dem Domänennamen basierend auf der MAC-Adresse des Routers hinzu (MAC-Adresse der ersten Netzwerkschnittstelle, die im **Netzwerkstatus** in der Webschnittstelle des Routers angezeigt wird.) Verwenden Sie Bindestrich-Trennzeichen anstelle von Doppelpunkten.
Beispiel: Ein Router mit der MAC-Adresse 00:11:22:33:44:55 hat den Domänennamen 00-11-22-33-44-55.

➡ Greifen Sie über die neue Domainnamen-Adresse auf den Router zu (z. B. https://00-11-22-33-44-55). Wenn Sie die Sicherheitsmeldung sehen, fügen Sie eine Ausnahme hinzu, damit die Meldung beim nächsten Mal nicht angezeigt wird (z. B. im Firefox-Webbrowser). Wenn es keine Möglichkeit gibt, eine Ausnahme hinzuzufügen, exportieren Sie das Zertifikat in die Datei und importieren Sie es in Ihren Browser oder Ihr Betriebssystem.

HINWEIS Sie müssen den Domainnamen basierend auf der MAC-Adresse des Routers verwenden und es ist nicht garantiert, dass er mit jeder Kombination aus einem Betriebssystem und einem Browser funktioniert.

4 STATUS

4.1 Allgemeiner Status

Eine Zusammenfassung der grundlegenden Informationen zum Router und dessen Aktivitäten kann durch Auswahl des Menüelementes **General** (Allgemeines) aufgerufen werden. Diese Seite wird auch angezeigt, wenn Sie sich im Web-Interface anmelden. Die Informationen werden je nach Art der Routeraktivität oder des Eigenschaftenbereichs in mehrere getrennte Blöcke geteilt – **Mobile Connection** (Mobile Verbindung), Primäres LAN, Sekundäres LAN, Ports für Peripheriegeräte und **System Information**. Handelt es sich beim Router um die SWITCH- oder RS232-RS485-ETH-Version, wird der Block **Tertiary LAN** (Tertiäres LAN) angezeigt. Wenn der Router mit WLAN ausgestattet ist, wird auch ein WLAN-Block angezeigt.

Das **IPv6-Adresselement** kann mehrere verschiedene Adressen für eine Netzwerkschnittstelle anzeigen. Dies ist das Standardverhalten, da eine IPv6-Schnittstelle mehr Adressen verwendet. Die zweite IPv6-Adresse, die nach dem Klicken auf **Weitere Informationen** angezeigt wird, wird automatisch im EUI-64-Format generiert Link-lokale IPv6-Adresse, abgeleitet von der MAC-Adresse der Schnittstelle. Sie wird bei der erstmaligen Nutzung der Schnittstelle (z. B. Kabelanschluss, Mobile WAN-Verbindung, etc.) generiert und zugewiesen.

4.1.1 Mobile Verbindung

Tab. 3: Mobile Verbindung

Element	**Beschreibung**
SIM-Karte	Bestimmung der SIM-Karte *(Primär oder sekundär)*
Übergabebaustein / interface	Legt die Schnittstelle fest
Flags	Zeigt gesetzte Flags für die Schnittstelle an • Keine - Keine Flags • Up - die Schnittstelle ist administrativ aktiviert • Läuft - die Schnittstelle ist im Betriebszustand (Kabel erkannt) • Multicast - die Schnittstelle ist Multicast-fähig
IP Address	IPv4-Adresse der Schnittstelle
IPv6	IPv6-Adresse oder Adressen der Netzwerkschnittstelle – einer Netzwerkschnittstelle können mehrere IPv6-Adressen zugewiesen werden.
MTU	Maximale übertragbare Paketgröße
Rx-Daten	Gesamtanzahl der empfangenen Bytes
Rx-Pakete	Eingehende Pakete
Rx-Fehler	Fehlerhaft eingehende Pakete
Rx Dropped	Verworfene eingehende Pakete
Rx Overruns	Verlorene eingehende Pakete wegen Überlauf
Tx Data	Gesamtzahl der ausgehenden Bytes
Tx Packets	Ausgehende Pakete
Tx Errors	Fehlerhaft ausgehende Pakete
Tx Dropped	Verworfene ausgehende Pakete
Rx Overruns	Verlorene ausgehende Pakete wegen Überlauf
Uptime	Zeigt an, wie lange die Verbindung zum Mobilfunknetz besteht.

4.1.2 Ethernet/LAN Status

Einträge, die in diesem Teil angezeigt werden, haben die gleiche Bedeutung wie Einträge im vorherigen Teil. Darüber hinaus zeigt der Eintrag **MAC Address** die MAC- Adresse der entsprechenden Routerschnittstelle (**Primäres LAN – eth0**, **Sekundäres LAN – eth1**, **Tertiäres LAN – eth2**, **WiFi – wlan0)** im WiFi (AP) Zugangspunktmodus, **WiFi – wlan1** im WiFi (STA) Stationsmodus. Die sichtbaren Informationen hängen von der Konfiguration ab (siehe 5.1 "Ethernet- bzw. LAN-Konfiguration", S. 30 oder Kapitel 5.5 "Wi-Fi-Access-Point-Konfiguration", S. 48).

Tab. 4: Peripherie-Ports

Element	**Beschreibung**
Expansion Port 1	Erweiterung in Position 1 eingebaut (**None** zeigt an, dass keine Erweiterung eingebaut wurde)
Expansion Port 2	Erweiterung in Position 2 eingebaut (**None** zeigt an, dass keine Erweiterung eingebaut wurde)
Binary Input	Status der binären Eingabe
Binary Output	Status der binären Ausgabe

4.1.3 Systeminformationen

Tab. 5: Systeminformationen

Element	**Beschreibung**
Firmware Version	Informationen über die Version der Firmware
Serial Number	Seriennummer des Routers (bei **N/A** nicht verfügbar)
Hardware UUID**	Eindeutige Identifizierung der Geräte-Hardware
Profil	Aktuelles Profil – Standard- oder Alternativprofil (Profile werden z. B. verwendet, um zwischen verschiedenen Betriebsarten umzuschalten)
Supply Voltage*	Versorgungsspannung des Routers
Temperatur*	Betriebstemperatur im Router
Zeit	Aktuelles Datum und Uhrzeit
Uptime	Laufzeit, gibt an, wie lange der Router in Betrieb ist
Licenses	Link zur Liste der Open-Source-Softwarekomponenten der Firmware zusammen mit ihren vollständigen Lizenztexten (GPL-Versionen 2 und 3, LGPL-Version 2, BSD-ähnliche Lizenzen, MIT-ähnliche Lizenzen).
* Nur für v3 ** Nur für v2	

4.2 Mobile WAN Status

HINWEIS Die wienet LAN Router zeigen den Mobilen WAN Status nicht an.

Der Menüpunkt **Mobiles WAN** enthält aktuelle Informationen zu Verbindungen zum Mobilfunknetz. Der erste Teil dieser Seite (**Mobile Network Information**) zeigt grundlegende Informationen über das Mobilfunknetz, in dem der Router betrieben wird, an. Es gibt auch Informationen über das Modul, das im Router montiert ist.

Tab. 6: Informationen zum Mobilfunknetzwerk

Element	**Beschreibung**
Registration	Status der Netzwerkregistrierung
Operator	Gibt das Netzwerk des Betreibers an, in dem der Router operiert
Technik	Art der Übertragungstechnik
PLMN	Code des Netzbetreibers
Cell	Zelle, an die der Router angeschlossen ist
LAC/TAC**	Location Area Code – Netzkennung für 2G/3G Netze Tracking Area Code – Netzkennung für 4G Netze
Channel	Kanal, auf welchem der Router kommuniziert • ARFCN bei GPRS/EDGE-Technologie • UARFCN bei UMTS/HSPA-Technologie, • EARFCN bei LTE-Technologie.
Band**	Abkürzung des Mobilfunkbandes
Signal Strength	Signalstärke (in dBm) der ausgewählten Zelle, für Details siehe Tab. 7, S. 17.
Signal Quality	Qualität des Signals der ausgewählten Zelle • EC/IO für UMTS und CDMA (dies ist das Verhältnis des vom Pilotkanal empfangenen Signals – EC – zum Gesamtpegel der spektralen Dichte, d. h. der Summe der Signale anderer Zellen – IO) • $\frac{N \times RSRP}{RSSI}$RSRQ für LTE-Technologie (als Verhältnis definiert) • Der Wert ist für die EDGE-Technologie nicht verfügbar.
RSSi, RSRP, RSRO, RSCP or Ec/Io**	Parameter, die Informationen über die Signalstärke und Signalqualität liefern
CSQ	Zellsignalqualität, relativer Wert wird durch RSSI (dBm) mit den folgenden Wertebereichen angegeben: • 2 – 9 = Marginal • 10 – 14 = OK • 15 – 19 = Gut • 20 – 30 = Exzellent
Neighbors	Signalstärke benachbarter Hörzellen (nur GPRS)*
Manufacturer	Hersteller des Moduls
Ausführung	Modultyp
Revision	Revision des Moduls
IMEI	IMEI (International Mobile Equipment Identity) Nummer des Moduls
MEID	Mobile Equipment Identifier Anzahl Module
ICCID	Integrated Circuit Card Identifier ist die internationale und individuelle Seriennummer der SIM-Karte.
* Wenn eine benachbarte Zelle für GPRS rot markiert ist, kann der Router wiederholt zwischen der benachbarten und der primären Zelle wechseln, was die Leistung des Routers beeinträchtigt. Um dies zu verhindern, richten Sie die Antenne neu aus oder verwenden Sie eine Richtantenne. ** nur für v2	

Der Wert der Signalstärke wird in unterschiedlichen Farben angezeigt: in Schwarz für gute, in Orange für mittelmäßige und in Rot für schlechte Signalstärke.

Tab. 7: Wertebereiche der Signalstärke für verschiedene Technologien

Signalstärke	GPRS/EDGE/CDMA (RSSI)	UMTS/HSPA (RSCP)	LTE (RSRP)
Gut	> -70 dBm	> -75 dBm	> -90 dBm
Gut	-70 dBm bis -89 dBm	-75 dBm bis -94 dBm	-90 dBm bis -109 dBm
Schlecht	< -89 dBm	< -94 dBm	< -109 dBm

Der mittlere Teil dieser Seite zeigt Informationen über die Qualität des Mobilfunksignals, die übertragenen Daten und die Anzahl der Verbindungen für alle SIM-Karten (für jeden Zeitraum).

Der Router hat Standardintervalle, wie die letzten 24 Stunden und die letzte Woche, sowie einen Zeitraum, der mit **Accounting Start** beginnt, der für das MWAN-Modul definiert ist.

Tab. 8: Beschreibung der Zeiträume

Element	**Beschreibung**
Heute	Der heutige Tag im Zeitintervall von 0:00 bis 23:59
Yesterday	Der gestrige Tag im Zeitintervall von 0:00 bis 23:59
This week	Diese Woche im Zeitintervall von Montag 0:00 Uhr bis Sonntag 23:59 Uhr
Last week	Vorige Woche im Zeitintervall von Montag 0:00 Uhr bis Sonntag 23:59 Uhr
This period	Diese Abrechnungsperiode
Last period	Vorige Abrechnungsperiode

HINWEIS

Tipps für die Tabelle **Mobile Network Statistics**:

- Die Verfügbarkeit der Mobilfunkverbindung (**Availability**) ist eine Prozentangabe, die sich aus dem Verhältnis der Dauer der Mobilfunkverbindung zur Zeit, in der der Router eingeschaltet ist, ergibt.
- Indem man mit dem Cursor auf die Werte der minimalen oder maximalen Signalstärke fährt, wird die Zeit angezeigt, als der Router das letzte Mal diese Signalstärke erreichte.

Der letzte Teil (**Connection Log**) zeigt Informationen über die Mobilfunkverbindungen und eventuell aufgetretene Probleme beim Aufbau an.

Tab. 9: Statistik des Datenverkehrs

Element	**Beschreibung**
RX data	Gesamtumfang der empfangenen Daten
TX data	Gesamtumfang der abgesandten Daten
Verbindungen	Anzahl der hergestellten Mobilfunkverbindungen
Signal Min	Mindestsignalstärke
Signal Avg	Durchschnittliche Signalstärke
Signal Max	Höchste Signalstärke
Cells	Anzahl der Schaltungen zwischen den Zellen
Availability	Verfügbarkeit des Routers über das Mobilfunknetz (Prozentangabe)

Im unteren Teil des Fensters (**Mobile Network Connection Log**) werden die Informationen über den Aufbau der Mobilfunkverbindung

Mobile WAN Status

Mobile Network Information

Registration	: Home Network
Operator	: Vodafone CZ
Technology	: LTE
PLMN	: 23003
Cell	: 10A80C
LAC	: 947C
Channel	: 6400
Signal Strength	: -71 dBm
Signal Quality	: -7 dB

» More Information «

Statistics for 1st SIM card

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	: 0 KB	24 KB	24 KB	0 KB	24 KB	0 KB
Tx Data	: 0 KB	908 KB	908 KB	0 KB	908 KB	0 KB
Connections	: 0	6	6	0	6	0
Signal Min	: -74 dBm	-73 dBm	-74 dBm	?	-74 dBm	?
Signal Avg	: -72 dBm	-71 dBm	-72 dBm	?	-72 dBm	?
Signal Max	: -71 dBm	-71 dBm	-71 dBm	?	-71 dBm	?
Cells	: 1	1	1	0	1	0
Availability	: 100.0%	99.2%	99.8%	0.0%	99.8%	0.0%

Statistics for 2nd SIM card

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	: 0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Tx Data	: 0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Connections	: 0	0	0	0	0	0
Signal Min	: ?	?	?	?	?	?
Signal Avg	: ?	?	?	?	?	?
Signal Max	: ?	?	?	?	?	?
Cells	: 0	0	0	0	0	0
Availability	: 0.0%	0.0%	0.0%	0.0%	0.0%	0.0%

Connection Log

2019-08-21 23:20:07 (1st SIM card) Connection successfully established.

Abb. 5: Mobile WAN Status

4.3 Wi-Fi-Status

HINWEIS Dieses Kapitel trifft nur zu, wenn der Router mit einem Wi-Fi-Modul ausgestattet ist.

Durch Auswahl des Punktes **Status** > **WiFi** > **Status** im Hauptmenü der Weboberfläche werden Informationen über den WLAN-Zugangspunkt (AP) und die WLAN-Station (STA) angezeigt. Informationen zu allen mit dem AP verbundenen Stationen werden ebenfalls aufgelistet. Ein Beispiel für die Ausgabe für den Wi-Fi-Status ist in der folgenden Abbildung dargestellt.

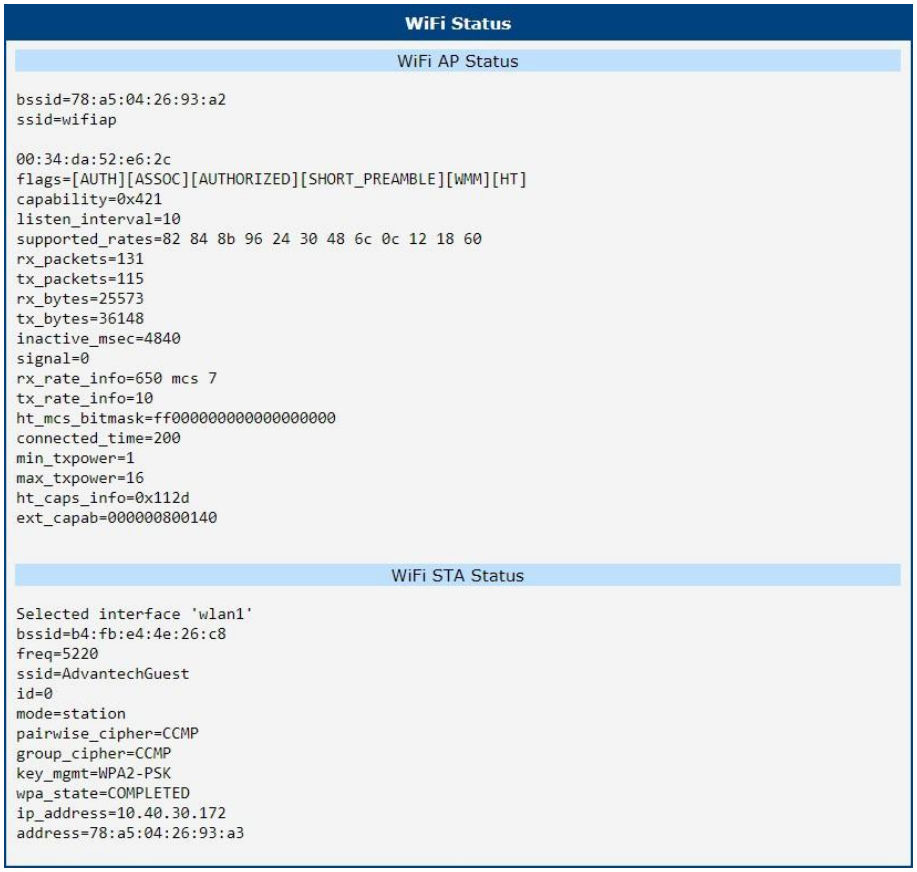


Abb. 6: Wi-Fi-Status

4.4 Wi-Fi-Scan

HINWEIS Dieses Kapitel trifft nur zu, wenn der Router mit einem Wi-Fi-Modul ausgestattet ist.

Wenn Sie das Element **Status** > **WiFi** > **Scan** auswählen, wird nach benachbarten Wi-Fi-Netzwerken gesucht und die Ergebnisse angezeigt. In der folgenden Tabelle finden Sie die Beschreibung einiger Elemente in der Ausgabe des Wi-Fi-Scans.

Tab. 10: Informationen zu den Drahtlos-Netzwerken in der Umgebung

Element	**Beschreibung**
BSS	MAC-Adresse des Zugangspunkts (AP).
TSF	Die Zeitsynchronisierungs-Funktion (TSF) sorgt dafür, dass die Timer sämtlicher Stationen im gleichen Basic Service Set (BSS) synchronisiert werden. Alle Stationen sollen einen lokalen TSF-Timer beibehalten.
freq	Frequenzband des Wi-Fi-Netzwerks [kHz]
Beaconintervall	Dauer der Zeitsynchronisation
Leistungsfähigkeit	Liste der Eigenschaften der Zugangspunkte (AP).
Signal	Signalstärke des Zugangspunkts (AP)
zuletzt online	Letzte Antwortzeit des Zugangspunkts (AP)
SSID	Bezeichner des Zugangspunkts (AP)
Supported rates	Unterstütze Geschwindigkeiten des Zugangspunkts (AP)
DS-Parameter-Set	Kanal, auf dem der Zugriffspunkt (AP) sendet.
ERP	Erweiterte PHY-Rate – Informationselement für Abwärtskompatibilität
Erweiterte unterstütze Geschwindigkeiten	Unterstützte Geschwindigkeiten des Zugangspunkts (AP), die über die acht in der Option Supported rates hinausgehen
RSN	Robust Secure Network – Das Protokoll zur Herstellung einer sicheren Kommunikation über kabellose Datennetzwerke 802.11

Das Ergebnis des Wi-Fi-Scans kann wie folgt aussehen:

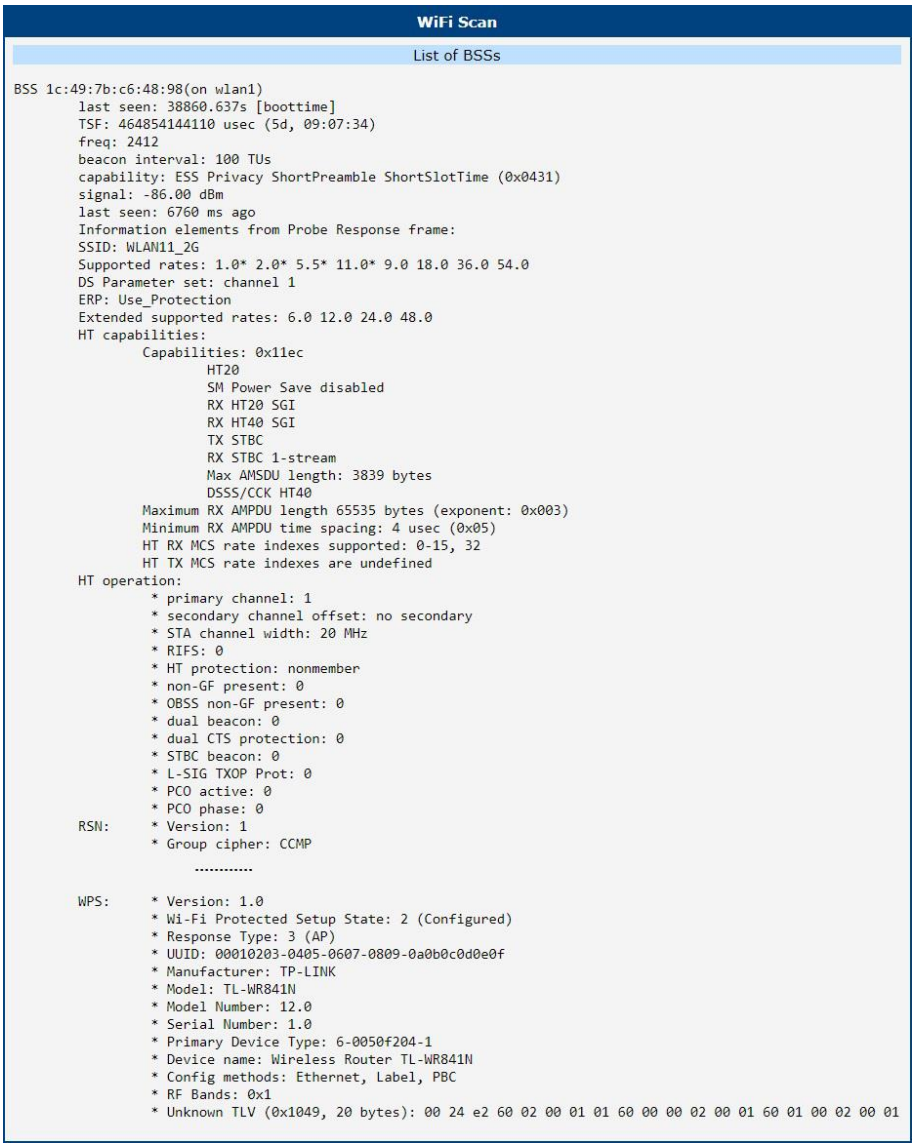


Abb. 7: Wi-Fi-Scan

4.5 Netzwerkstatus

Um Systeminformationen zu den Schnittstellen und der Routing-Tabelle anzuzeigen, wählen Sie den Eintrag **Network** im Menü **Status.** Im oberen Teil des Fensters werden nur Detailinformationen zu aktiven Schnittstellen angezeigt:

Tab. 11: Beschreibung der Schnittstellen im Netzwerk-Status für Serie v3

Element	**Beschreibung**
eth0, eth1, eth2	Netzwerkschnittstellen (Ethernet-Verbindung)
usb0	USB
wlan0	Wi-Fi Interface
ppp0	PPP-Schnittstelle (z. B. PPPoE-Tunnel)
tun0	Schnittstelle OpenVPN-Tunnel
ipsec0	Schnittstelle IPsec-Tunnel
gre1	Schnittstelle GRE-Tunnel
lo	Lokale Schleifenschnittstelle
nat64	Netzwerkschnittstelle des internen Übersetzer-Gateways zwischen IPv6- und IPv4-Adressen.

Tab. 12: Beschreibung der Schnittstellen im Netzwerk-Status für Serie v2

Element	**Beschreibung**
eth0, eth1	Erste und zweite Netzwerkschnittstelle (Ethernet-Verbindung)
usbx	Aktive Schnittstelle in das mobile Netzwerk – das wireless Modul ist über die USB-Schnittstelle angeschlossen
gre1	Schnittstelle GRE-Tunnel (falls konfiguriert)
pppx	PPP-Schnittstelle (z. B. PPPoE-Tunnel)
tunx	Schnittstelle OpenVPN-Tunnel (falls konfiguriert)
ipsecx	Schnittstelle IPsec-Tunnel (falls konfiguriert)
gre1	Schnittstelle GRE-Tunnel (falls konfiguriert)
lo	Lokale Schleifenschnittstelle
nat64	Netzwerkschnittstelle des internen Übersetzer-Gateways zwischen IPv6- und IPv4-Adressen.

Jede der Schnittstellen zeigt folgende Informationen:

Tab. 12: Beschreibung der Netzwerkstatusinformationen

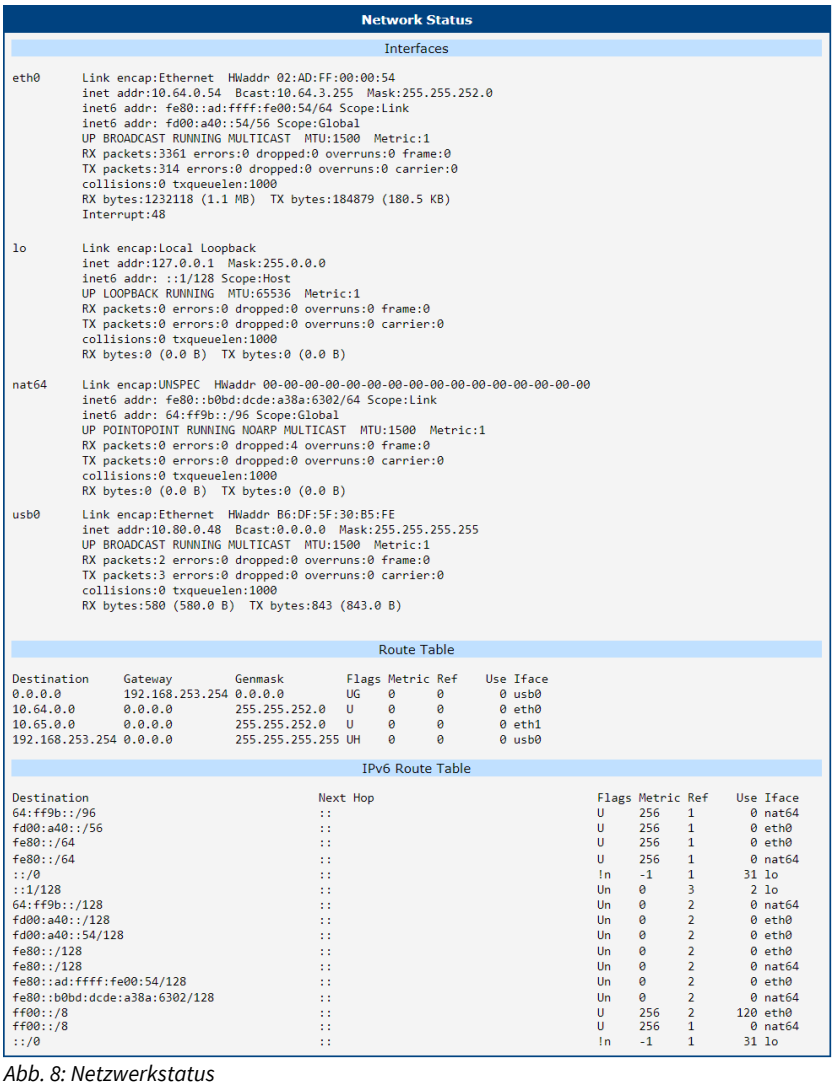
Element	**Beschreibung**
HWaddr	Hardware-Adresse (MAC-Adresse) der Netzwerkschnittstelle
inet addr	IPv4-Adresse der Schnittstelle
inet6 addr	IPV6-Adresse der Schnittstelle. Hier können mehr davon für einzelne Netzwerkschnittstellen sein.
P-t-P	IP-Adresse der Gegenstelle (bei Punkt-zu-Punkt-Verbindung)
Bcast	Adresse in alle Richtungen
Mask	Netzmaske
MTU	Maximale übertragbare Paketgröße
metrisch	Anzahl der Router, über die das Paket durchgehen muss
RX	• **packets** – eingehende Pakete • **errors** – Anzahl der Fehler • **dropped** – verworfene Pakete • **overruns** – verlorene eingehende Pakete wegen Überlauf • **frame** – fehlerhafte eingehende Pakete wegen falscher Größe des Pakets

TX	• **packets** – ausgehende Pakete • **errors** – Anzahl der Fehler • **dropped** – verworfene Pakete • **overruns** – verlorene ausgehende Pakete wegen Überlauf • **carrier** – fehlerhafte ausgehende Pakete mit Fehlern, die auf der physikalischen Schicht entstanden sind
collisions	Anzahl der Kollisionen auf der physikalischen Schicht
txqueuelen	Länge der Front der Netzeinrichtung
RX bytes	Gesamtanzahl der empfangenen Bytes
TX bytes	Gesamtanzahl der abgesandten Bytes

Sie können den Status der Mobilfunknetzverbindung auf dem Netzwerkstatusbildschirm anzeigen. Ist die Verbindung zum Mobilfunknetz aktiv, erscheint sie in den Systeminformationen als usb0-Schnittstelle.

Die **Routing-Tabelle** wird unten auf der Seite **Netzwerk Status** angezeigt. Nachfolgend finden Sie eine **IPv4 Routing-Tabelle** und eine **IPv6 Routing-Tabelle**.

Wenn der Router mit dem Internet verbunden ist (eine Standardroute ist definiert), wird die **nat64**-Netzwerkschnittstelle automatisch erstellt. Dies ist das interne NAT64-Gateway zur Übersetzung der IPv6- und IPv4-Kommunikation. Es wird automatisch verwendet, wenn es über IPv6 verbunden ist und mit einem IPv4-Gerät oder -Netzwerk kommuniziert. Es arbeitet mit DNS64 zusammen, das automatisch im Router läuft (Übersetzung von Domainnamen in IP-Adressen). Das standardmäßige NAT64-Präfix 64:ff9b::/96 wird verwendet, wie Sie in Abb. 8 unten im Abschnitt **IPv6-Routing-Tabelle** sehen können.



Network Status

Interfaces

```
eth0      Link encap:Ethernet  HWaddr 02:AD:FF:00:00:54
          inet addr:10.64.0.54  Bcast:10.64.3.255  Mask:255.255.252.0
          inet6 addr: fe80::ad:ffff:fe00:54/64 Scope:Link
          inet6 addr: fd00:a40::54/56 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3361 errors:0 dropped:0 overruns:0 frame:0
          TX packets:314 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1232118 (1.1 MB)  TX bytes:184879 (180.5 KB)
          Interrupt:48

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

nat64     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet6 addr: fe80::b0bd:dcde:a38a:6302/64 Scope:Link
          inet6 addr: 64:ff9b::/96 Scope:Global
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:4 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

usb0      Link encap:Ethernet  HWaddr B6:DF:5F:30:B5:FE
          inet addr:10.80.0.48  Bcast:0.0.0.0  Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:580 (580.0 B)  TX bytes:843 (843.0 B)
```

Route Table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.253.254 0.0.0.0         UG    0      0        0 usb0
10.64.0.0       0.0.0.0         255.255.252.0   U     0      0        0 eth0
10.65.0.0       0.0.0.0         255.255.252.0   U     0      0        0 eth1
192.168.253.254 0.0.0.0         255.255.255.255 UH    0      0        0 usb0
```

IPv6 Route Table

```
Destination                     Next Hop                        Flags Metric Ref    Use Iface
64:ff9b::/96                    ::                              U     256    1        0 nat64
fd00:a40::/56                   ::                              U     256    1        0 eth0
fe80::/64                       ::                              U     256    1        0 eth0
fe80::/64                       ::                              U     256    1        0 nat64
::/0                            ::                              !n    -1     1       31 lo
::1/128                         ::                              Un    0      3        2 lo
64:ff9b::/128                   ::                              Un    0      2        0 nat64
fd00:a40::/128                  ::                              Un    0      2        0 eth0
fd00:a40::54/128                ::                              Un    0      2        0 eth0
fe80::/128                      ::                              Un    0      2        0 eth0
fe80::/128                      ::                              Un    0      2        0 nat64
fe80::ad:ffff:fe00:54/128       ::                              Un    0      2        0 eth0
fe80::b0bd:dcde:a38a:6302/128   ::                              Un    0      2        0 nat64
ff00::/8                        ::                              U     256    2      120 eth0
ff00::/8                        ::                              U     256    1        0 nat64
::/0                            ::                              !n    -1     1       31 lo
```

Abb. 8: Netzwerkstatus

4.6 DHCP-Status

Die Informationen über die Tätigkeit des DHCP-Servers können durch Anwählen des Menüelements **DHCP** abgerufen werden. Der DHCP-Server gewährleistet die automatische Konfiguration der Einrichtungen, die an das Netz angeschlossen sind, das vom Router verwaltet wird. Der DHCP-Server teilt den einzelnen Einrichtungen die IP-Adresse, die Netzmaske, das Standard-Gateway (IP-Adresse des Routers) und die Adresse des DNS-Servers (IP-Adresse des Routers) zu. Der DHCPv6-Server wird unterstützt.

4.6.1 Serie v2

Die Abbildung zeigt ein Beispiel für einen DHCP-Status. Einträge im Fenster **DHCP-Status** sind gemäß ihren Schnittstellen in separate Teile unterteilt

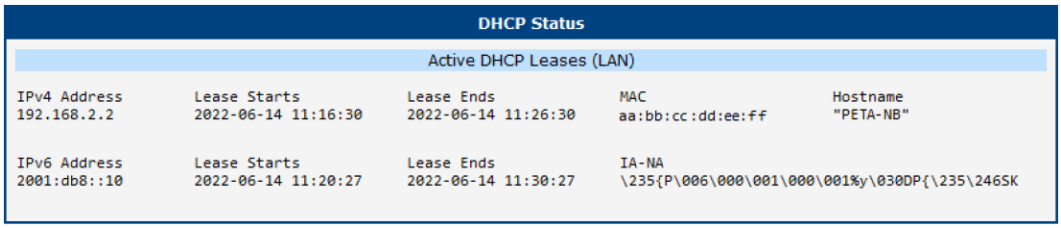


Abb. 9: DHCP-Status Serie v2

Das DHCP Status Fenster zeigt die folgenden Informationen in einer Zeile für jeden Client in der Liste. Die Elemente werden in folgender Tabelle erläutert.

Tab. 13: DHCP Statusbeschreibung

Element	**Beschreibung**
IPv4 Adresse	Zugewiesene IPv4 Adresse
IPv6 Adresse	Zugewiesene IPv6 Adresse
Lease Starts	Zeitpunkt, zu dem der Lease der IP-Adresse startet
Lease Ends	Zeitpunkt, zu dem der Lease, der IP-Adresse abläuft
MAC	MAC-Adresse des Clients
Hostname	Hostname des Clients
IA-NA	Eindeutiger IPv6 Identifikator

Der DHCP-Status kann gelegentlich zwei Datensätze für eine IP-Adresse anzeigen. Dies kann durch das Zurücksetzen der Client-Netzwerkschnittstelle verursacht werden.

4.6.2 Serie v3

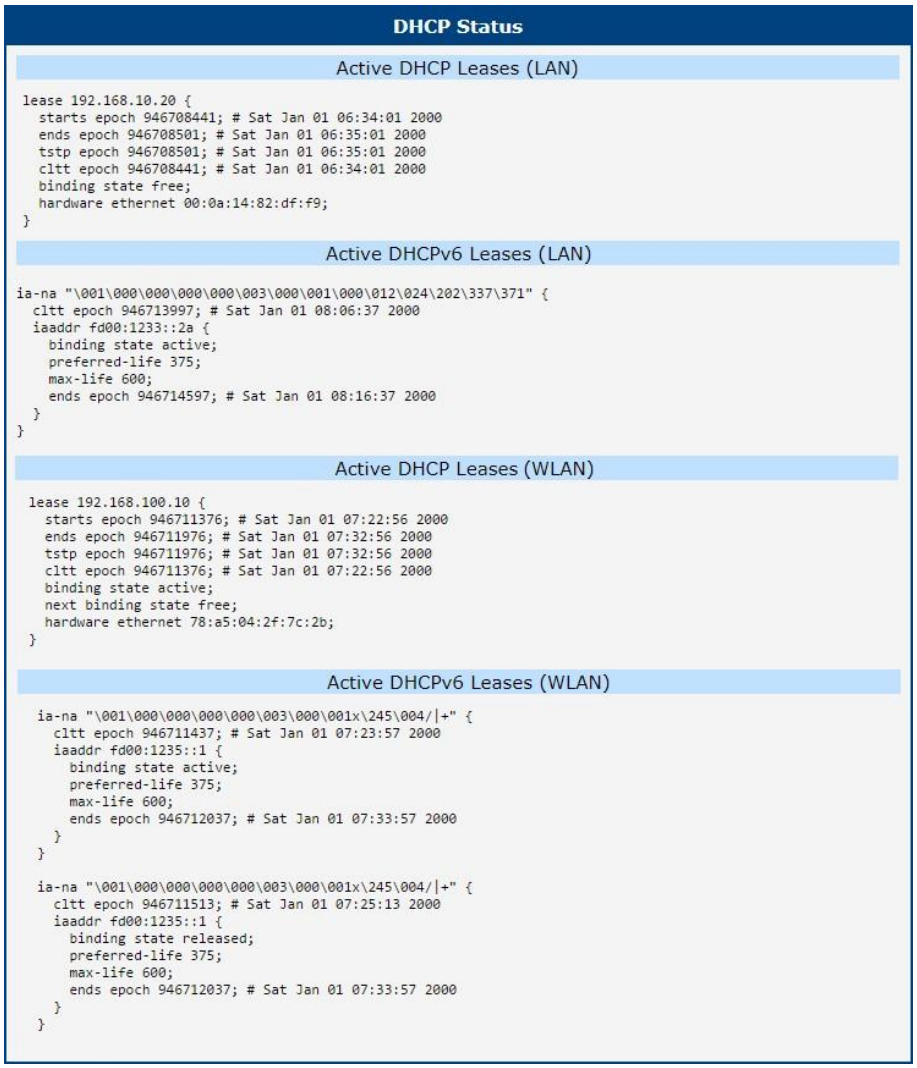


Abb. 10: DHCP-Status Serie v3

Der DHCP-Status kann gelegentlich zwei Datensätze für eine IP-Adresse anzeigen. Dies kann durch das Zurücksetzen der Client-Netzwerkschnittstelle verursacht werden.

Einträge im Fenster **DHCP-Status** sind nach LAN- und WLAN-Schnittstelle und IPv4 (DHCP) und IPv6 (DHCPv6) in separate Teile unterteilt – es gibt Teile **Active DHCP Leases (LAN)**, **Active DHCPv6 Leases (LAN)**, **Active DHCPv6 Leases (WLAN)** und **Active DHCPv6 Leases (WLAN)**, wenn der Router über WLAN verfügt und die WLAN-Netzwerkschnittstelle aktiviert ist. In Abb. 10oben sind sowohl DHCP (IPv4) als auch DHCPv6 (IPv6) Server aktiviert sowie die LAN- und die WLAN-Schnittstelle. Die folgende Tabelle erläutert Informationen aus der Client-Liste:

Tab. 14: DHCP Statusbeschreibung

Element	Beschreibung
lease	Zugewiesene IP-Adresse
iaaddr	(IPv6) Zugewiesene IPv6-Adresse
starts epoch	Zeitpunkt der Vergabe der IP-Adresse
ends epoch	Zeitpunkt, zu dem der Lease der IP-Adresse abläuft
tstp epoch	Zeitpunkt, zu dem Peer mitgeteilt wurde, dass der Lease abläuft
cltt epoch	Zeitpunkt der letzten Transaktion des Clients
binding state	Binding Status des Lease
next binding state	Status, in den die Lease übergeht, wenn der aktuelle Zustand abgelaufen ist.
hardware ethernet	Eindeutige Hardware-/MAC-Adresse
uid	Eindeutige ID
client-hostname	Computername
preferred-life	(IPv6) Dauer der uneingeschränkten Nutzung der Adresse. Wenn die bevorzugte Lebensdauer abläuft, sollte die Adresse nicht für neue Kommunikationen verwendet werden, kann jedoch in bestimmten Fällen weiterhin für bestehende Kommunikationen verwendet werden.
max-life	(IPv6) Maximale Zeit, für die der DHCPv6-Server ein Lease gewähren kann.

4.7 IPsec-Status

Durch Auswahl der Option **IPsec** im Menü **Status** der Webseite werden die Informationen für alle eingerichteten IPsec-Tunnel angezeigt. Wenn der Tunnel korrekt aufgebaut wurde, zeigt der Bildschirm **ESTABLISHED** und die Anzahl der laufenden IPsec-Verbindungen **1 up** an (in der Abbildung unten orange hervorgehoben). Fehlt ein solcher Text im Log (z. B. "0 up"), wurde der Tunnel nicht erstellt!

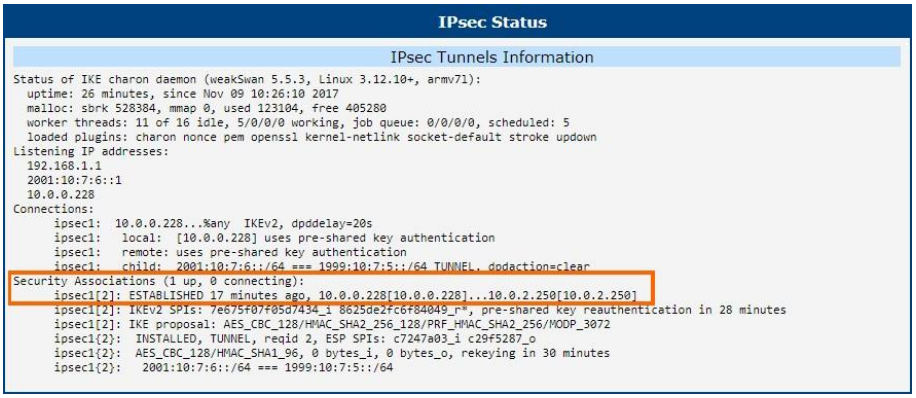
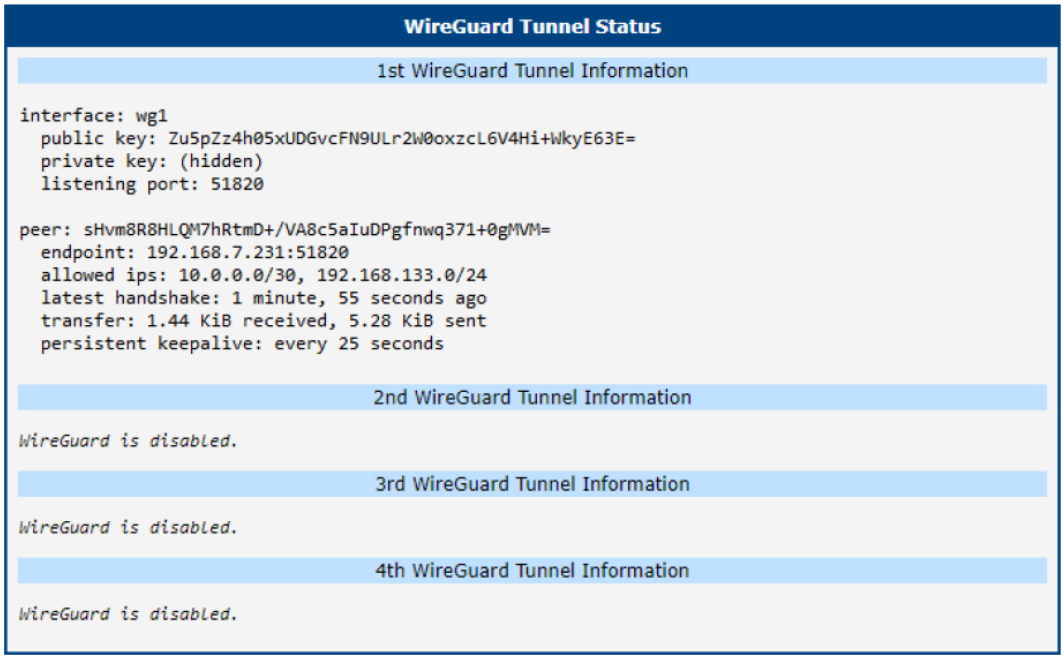


Abb. 11: IPsec-Status

4.8 WireGuard Status

Wenn man die WireGuard Option im Statusmenü der Website auswählt, werden alle Informationen zu bereits erstellten WireGuard-Tunneln angezeigt. In der folgenden Abbildung wird ein Beispiel eines aktiven WireGuard-Tunnels gezeigt.



Die Zeit bei **Latest handshake** gibt an, wann die letzte erfolgreiche Kommunikation mit der anderen Seite des Tunnels erfolgte. Dieses Element wird erst angezeigt, wenn ein Tunnel etabliert wurde.

4.9 DynDNS-Status

Der Router unterstützt DynamicDNS über einen DNS-Server auf www.dyndns.org. Wenn Dynamic DNS konfiguriert ist, kann der Status durch Auswahl des Menüpunkts DynDNS angezeigt werden. Weitere Informationen zum Konfigurieren eines Dynamic DNS-Clients finden Sie unter www.dyndns.org.

Sie können die folgenden aufgelisteten Server für den dynamischen DNS-Dienst verwenden. Es ist möglich, den DynDNSv6-Dienst zu verwenden, wenn der IP-Modus auf der DynDNS-Konfigurationsseite auf IPv6 umgestellt ist.

- www.dyndns.org
- www.spdns.de
- www.dnsdynamic.org
- www.noip.com

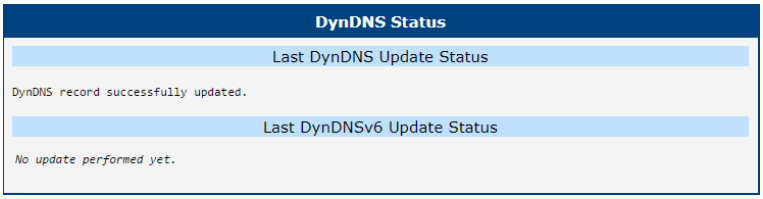


Abb. 12: DynDNS-Status

Wenn der Router eine Aktualisierung des DynDNS-Eintrags erkennt, zeigt der Dialog eine oder mehrere der folgenden Meldungen an:

- DynDNS client is disabled. – DynDNS-Client ausgeschaltet.
- Invalid username or password. – Benutzername oder Passwort ungültig.
- Specified hostname does not exist. – Der angegebene Host-Name existiert nicht.
- Invalid hostname format. – Ungültiges Format für Host-Name.
- Hostname exists, but not under specified username. – Der Host-Name existiert, aber nicht unter dem angegebenen Benutzernamen.
- No update performed yet. – Noch kein Update durchgeführt.
- DynDNS record is already up to date. – DynDNS-Eintrag ist bereits aktuell.
- DynDNS record successfully update. – DynDNS-Eintrag erfolgreich aktualisiert.
- DNS error encountered. – DNS-Fehler aufgetreten.
- DynDNS server failure. – DynDNS-Server-Fehler.



VORSICHT

Der SIM-Karte des Routers muss eine öffentliche IP-Adresse zugewiesen sein, sonst funktioniert DynDNS nicht richtig.

4.10 System log

Im Falle von Problemen beim Aufbau der Verbindung kann das Systemprotokoll durch die Auswahl der Option **System Log** im Menü aufgerufen werden. Ausführliche Meldungen von den einzelnen im Router laufenden Anwendungen werden angezeigt. Über die Schaltfläche **Save Log** ist es möglich, das System-Log auf einem angeschlossenen PC zu speichern (die Textdatei mit der Erweiterung .log wird gespeichert). Über die zweite Schaltfläche – **Save Report** – mit allen notwendigen Informationen zu erstellen. Mit der Schaltfläche – **Save Report** – ist es möglich, einen detaillierten Bericht zu erstellen (erzeugt alle vom Support erforderlichen Informationen in einer Textdatei im Format .txt – statistische Daten, Routing- und Prozesstabellen, Systemprotokoll, Konfiguration).

HINWEIS Sensible Daten aus dem Bericht werden aus Sicherheitsgründen herausgefiltert.

Die Standardgröße des System-Logs (Syslog) beträgt 1.000 Zeilen. Nach dem Erreichen von 1.000 Zeilen wird ein neuer Ordner für das Speichern des Systemprotokolls erstellt. Nach dem Erreichen von 1.000 Zeilen im zweiten Ordner wird der erste Ordner gelöscht und stattdessen ein neuer Ordner erstellt.

Die Erstellung des Systemprotokolls erfolgt durch das Programm **Syslogd**. Es kann auf zwei Arten gestartet werden, die sein Verhalten beeinflussen. Durch die Eingabe von `-S`, gefolgt von einer Dezimalzahl, wird die maximale Anzahl der Zeilen in einer Logdatei eingestellt. Durch die Eingabe von `-R`, gefolgt von einer IP-Adresse, kann man sich im entfernten Syslog Daemon anmelden. (Im Falle von Linux muss der Zielcomputer das entfernte Einloggen erlauben (in der Regel durch `syslogd -R`). Unter Windows muss ein Syslog-Server installiert sein, z. B. **Syslog Watcher**). Damit das Programm **syslogd** durch diese Eingaben gestartet werden kann, ist es notwendig, das Script `/etc/init.d/syslog` über SSH zu ändern oder Zeilen in das **Startup Script** hinzuzufügen (zugänglich in der Sektion **Configuration**) gemäß Abb. 14.

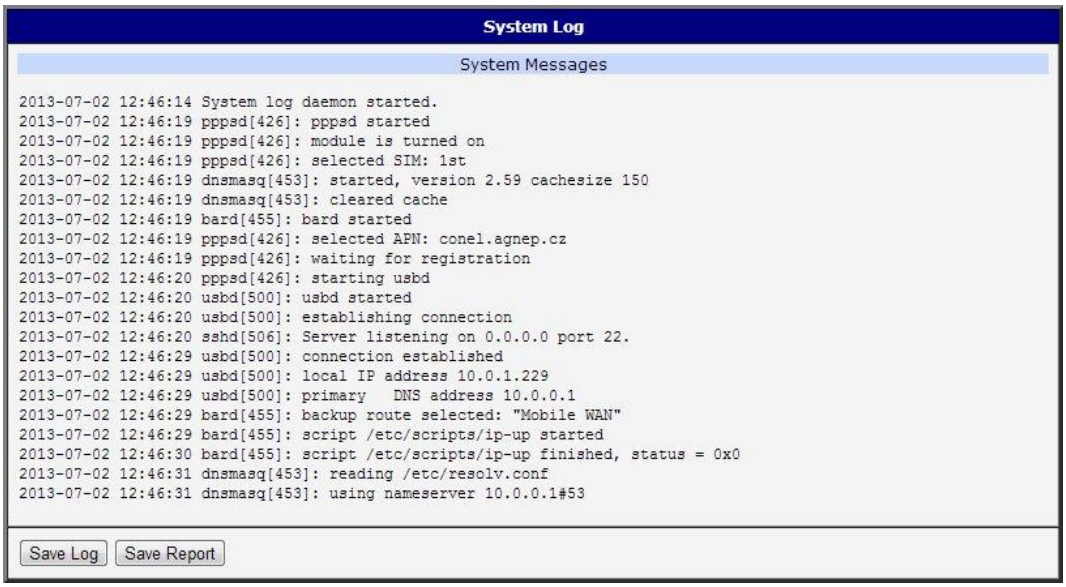


Abb. 13: Systemprotokoll (SysLog)

Das nachfolgende Beispiel (Abbildung) zeigt, wie Syslog-Informationen beim Start zu einem Remote-Server mit der Adresse 192.168.2.115 gesendet werden.

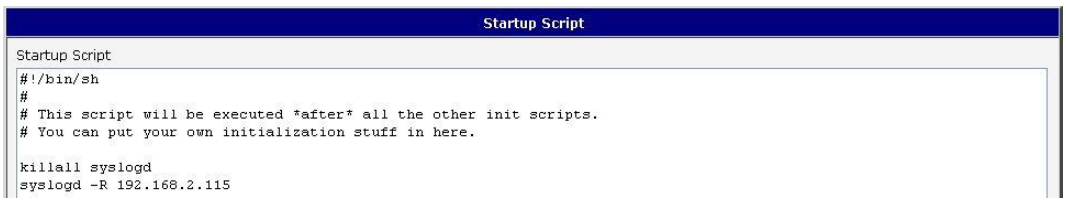


Abb. 14: Beispiel für das Starten des Programms Syslogd mit der Eingabe '-R'

5 KONFIGURATION

5.1 Ethernet- bzw. LAN-Konfiguration

Unterscheidung zwischen den Serien: Für v2 Router wird in der Menüführung der Begriff Ethernet und für v3 Router der Begriff LAN verwendet. Im Folgenden beschränken wir uns auf die Verwendung des Begriffs LAN.

Um die Local Area Network Konfiguration einzugeben, wählen Sie den Menüpunkt **LAN** im Abschnitt **Konfiguration**.
Der Eintrag **LAN** wird im Menü auf der linken Seite erweitert, so dass Sie die richtige Ethernet-Schnittstelle zum Konfigurieren auswählen können: **Primäres LAN** für die erste Ethernet-Schnittstelle des Routers (ETH0), **Sekundäres LAN** für die zweite (ETH1) and **Tertiäres LAN** für die dritte Ethernet-Schnittstelle, falls der Router über 3-Port Ethernet SWITCH oder RS232-RS485-ETH-Schnittstelle verfügt.

Die Seite LAN-Konfiguration ist in IPv4- und Ipv6-Spalten unterteilt, siehe Abbildung unten. Es gibt Dual-Stack-Unterstützung für Ipv4- und Ipv6-Protokolle – sie können parallel laufen; Sie können entweder einen oder beide konfigurieren. Wenn Sie sowohl Ipv4 als auch Ipv6 konfigurieren, wählen andere Netzwerkgeräte das Kommunikationsprotokoll. Konfigurationselemente und Unterschiede zwischen Ipv6 und Ipv4 werden in den folgenden Tabellen beschrieben.

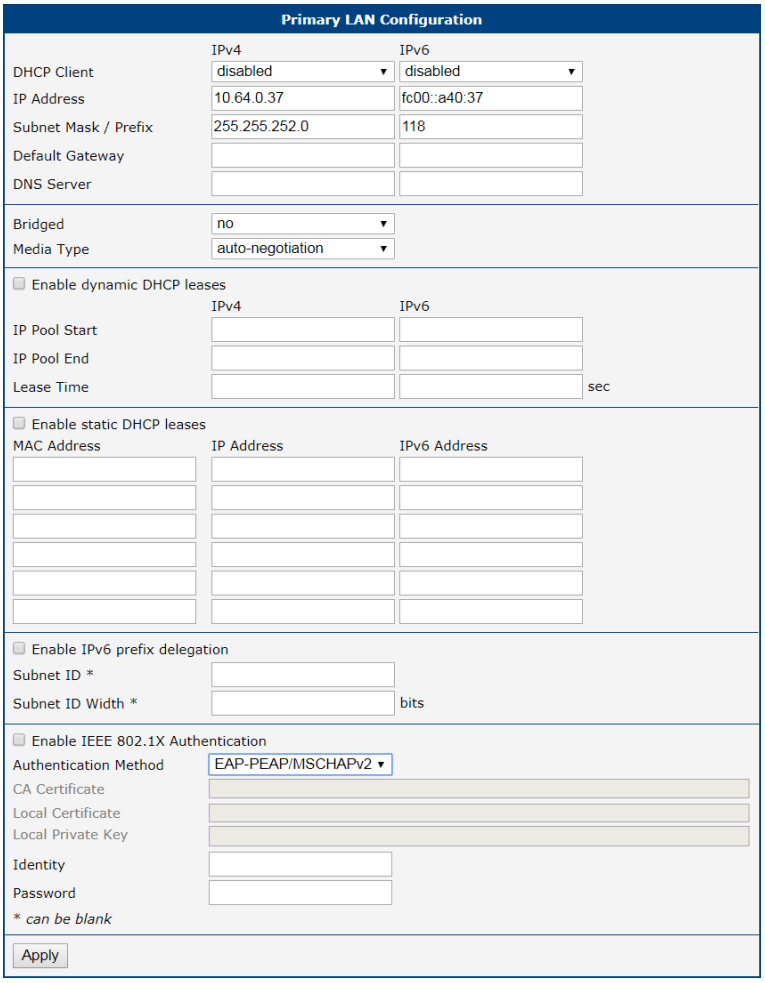


Abb. 15: LAN-Konfigurationsseite

Tab. 15: Konfiguration der Netzwerkschnittstelle

Element	Beschreibung
DHCP-Client	Aktiviert/deaktiviert die DHCP-Client-Funktion. Wenn in der Spalte Ipv6 eingetragen, dann ist der DHCPv6-Client aktiviert. Der DHCPv6-Client unterstützt alle drei Methoden zum Abrufen einer Ipv6-Adresse – SLAAC, zustandsloses DHCPv6 und zustandsbehaftetes DHCPv6. • **deaktiviert** – Der Router lässt keine automatische Zuweisung der IP- Adresse von einem DHCP-Server im LAN-Netzwerk zu. • **aktiviert** – Der Router ermöglicht die automatische Zuweisung der IP- Adresse von einem DHCP-Server im LAN-Netzwerk.
IP-Adresse	Eine feste IP-Adresse der Ethernet-Schnittstelle. Verwenden Sie die Ipv4-Notation in der Spalte Ipv4 und die Ipv6-Notation in der Spalte Ipv6. Die verkürzte Ipv6-Notation wird nicht unterstützt.
Subnetzmaske	Gibt eine Subnetzmaske für die Ipv4-Adresse an. Geben Sie in der Spalte Ipv6 das Präfix für die Ipv6-Adresse ein – Zahl im Bereich 0 bis 128.
Default Gateway	Standard-Gateway gibt die IP-Adresse eines Standard-Gateways an. Wenn ausgefüllt, wird jedes Paket, dessen Ziel nicht in der Routing-Tabelle gefunden wurde, an diese IP-Adresse gesendet. Verwenden Sie die richtige IP-Adressnotation in der Ipv4 bzw. Ipv6-Spalte.
DNS Server	Gibt die IP-Adresse des DNS-Servers an. Wenn die IP-Adresse in der Routing-Tabelle nicht gefunden wird, leitet der Router die Anfrage an den hier angegebenen DNS-Server weiter. Verwenden Sie die richtige IP-Adressnotation in den Spalten Ipv4 und Ipv6.

Die Elemente **Default Gateway** und **DNS Server** werden nur verwendet, wenn das Element **DHCP Client** auf **disabled** gesetzt ist und wenn das primäre (ETH0) oder sekundäre LAN (ETH1) vom Backup Routes-System als Standardroute ausgewählt wurde. (Der Auswahlalgorithmus ist in Abschnitt 4.7 beschrieben). Ab FW 5.3.0 werden Default Gateway und **DNS Server** auch auf Bridged Interfaces (z. B. eth0 + eth1) unterstützt.

Die folgenden Elemente (in der Tabelle unten) gelten global für die konfigurierte Ethernet-Schnittstelle. Es kann immer nur eine Bridge auf dem Router aktiv sein. Die Parameter **DHCP-Client**, **IP-Adresse** und **Subnet Mask / Prefix** der einzigen Schnittstelle werden für die Bridge verwendet. Das primäre LAN (ETH0) hat eine höhere Priorität, wenn beide Schnittstellen (eth0, eth1) zur Bridge hinzugefügt werden. Andere Schnittstellen (wlan0 – wifi) können jederzeit zu einer bestehenden Bridge hinzugefügt oder aus ihr gelöscht werden. Die Bridge kann bei Bedarf für solche Schnittstellen erstellt werden, jedoch nicht, wenn sie durch ihre jeweiligen Parameter konfiguriert wird.

Tab. 16: Konfiguration der Ethernet-Schnittstelle

Element	Beschreibung
Bridged	Aktiviert/deaktiviert die Bridging-Funktion des Routers. • **no** – Router wird nicht als Bridge genutzt (Standard) • **yes** – Router wird als Bridge genutzt
Media type	Gibt den Duplextyp und die Geschwindigkeit an, die im Netzwerk verwendet werden. • **Auto-negation** – Der Router stellt automatisch die beste Geschwindigkeit und den Duplexmodus der Kommunikation gemäß den Möglichkeiten des Netzes ein. • **100 Mbps Full Duplex** – Der Router kommuniziert mit 100 Mbps im Gegenbetrieb. • **100 Mbps Half Duplex** – Der Router kommuniziert mit 100 Mbps im Wechselbetrieb. • **10 Mbps Full Duplex** – Der Router kommuniziert mit 10 Mbps im Gegenbetrieb. • **10 Mbps Half Duplex** – Der Router kommuniziert mit 10 Mbps im Wechselbetrieb.
MTU**	Maximaler Übertragungswert (Standardwert ist 1‘500 Bytes)
** Nur für Serie v2	

5.1.1 DHCP-Server

Der DHCP-Server weist den angeschlossenen DHCP-Clients die IP-Adresse, die Standard-Gateway-IP-Adresse (IP-Adresse des Routers) und die IP-Adresse des DNS-Servers (IP-Adresse des Routers) zu. Wenn diese Werte vom Benutzer im Konfigurationsformular ausgefüllt werden, werden diese bevorzugt.

Der DHCP-Server unterstützt sowohl die statische als auch die dynamische Zuweisung von IP-Adressen. **Dynamic IP address** weist Clients IP-Adressen aus einem definierten Adressraum zu. **Static DHCP** vergibt IP-Adressen, die den MAC-Adressen der angeschlossenen Clients entsprechen.

Wenn die Spalte IPv6 ausgefüllt ist, wird der DHCPv6-Server verwendet. Der DHCPv6-Server bietet den verbundenen Clients eine zustandsorientierte Adresskonfiguration. Nur wenn das **Subnet Prefix** oben auf 64 gesetzt ist, bietet der DHCPv6 Server beides – die Stateful-Adresskonfiguration und SLAAC (Stateless Address Autoconfiguration).

HINWEIS Überlappen Sie die Bereiche statisch zugewiesener IP-Adressen nicht mit Adressen, die vom dynamischen DHCP-Server zugewiesen werden. IP-Adresskonflikte und falsche Netzwerkfunktionen können auftreten, wenn Sie die Bereiche überschneiden.

Tab. 17: Konfiguration des dynamischen DHCP-Servers

Element	**Beschreibung**
Enable dynamic DHCP leases	Wenn diese Option ausgewählt ist, ist der dynamische DHCP-Server aktiviert.
IP Pool Start	Beginn der den DHCP-Clients zugewiesenen IP-Adressen. Verwenden Sie die richtige Notation in den Spalten IPv4 und IPv6.
IP Pool End	Ende der den DHCP-Clients zugewiesenen IP-Adressen. Verwenden Sie die richtige Notation in den Spalten IPv4 und IPv6.
Lease time	Zeit in Sekunden, die die IP-Adresse reserviert wird, bevor sie wiederverwendet werden kann.

Tab. 18: Konfiguration des statischen DHCP-Servers

Element	**Beschreibung**
Enable static DHCP leases	Wenn diese Option ausgewählt ist, ist der statische DHCP-Server aktiviert.
MAC-Adresse	MAC-Adresse eines DHCP-Client.
IPv4-Adresse	Zugewiesene IPv4-Adresse. Verwenden Sie die richtige Notation.
IPv6-Adresse	Zugewiesene IPv6-Adresse. Verwenden Sie die richtige Notation.

5.1.2 IPv6-Präfix-Delegierung

HINWEIS Dies ist eine erweiterte Konfigurationsoption. Die IPv6-Präfix-Delegierung funktioniert automatisch mit DHCPv6 – nur verwenden, wenn eine andere Konfiguration gewünscht wird und Sie die Konsequenzen kennen.

Wenn Sie die automatische IPv6-Präfix-Delegierung überschreiben möchten, können Sie sie in diesem Formular konfigurieren. Sie müssen Ihre Subnet-ID-Breite (Teil der IPv6-Adresse) kennen, siehe Abbildung unten für die Berechnungshilfe – es ist ein Beispiel: 48 Bits sind Site-Präfix, 16 Bits sind Subnet-ID (Subnet-ID-Breite) und 64 Bits ist Interface-ID.

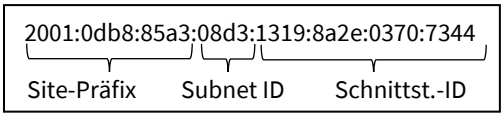


Abb. 16: IPv6-Adresse mit Präfix-Beispiel

Tab. 19: IPv6-Präfix-Delegierung

Element	Beschreibung
Enable IPv6 prefix delegation	Aktiviert die unten ausgefüllte Konfiguration der Präfix-Delegierung.
Subnet ID	Der Dezimalwert der Subnet-ID der Ethernet-Schnittstelle. Der maximale Wert hängt von der Breite der Subnetz-ID ab.
Subnet ID Width	Die maximale Breite der Subnetz-ID hängt von Ihrer Site ab Präfix – es ist der Rest bis 64 Bit.

5.1.3 802.1X-Authentifizierung beim RADIUS-Server

Die Authentifizierung (802.1X) beim RADIUS-Server kann im nächsten Konfigurationsabschnitt aktiviert werden. Der Router kann nur ein RADIUS-Client sein (nicht der Server). Diese Funktionalität erfordert zusätzliche Einstellungen von Identität und Zertifikaten, wie in der folgenden Tabelle beschrieben.

V2 Router unterstützen lediglich die Supplicant Rolle. Die Authentication Rolle wird nicht unterstützt.

Tab. 20: 802.1X-Authentifizierung beim RADIUS-Server

Element	Beschreibung
Enable IEEE 802.1X Authentication	Wählen Sie diese Option, um die 802.1X-Authentifizierung zu aktivieren
Authentication Method	Authentifizierungsmethode auswählen (EAP-PEAPMSCHAPv2 oder EAP-TLS)
CA Certificate	Definition des lokalen Zertifikats für das EAP-TLS-Authentifizierungsprotokoll
Local Certificate	Definition des lokalen Zertifikats für das EAP-TLS-Authentifizierungsprotokoll
Local Private Key	Definition des lokalen privaten Schlüssels für das EAP-TLS-Authentifizierungsprotokoll
Identität	Benutzername – Identität
Passwort	Zugangspasswort. Dieses Element ist nur für das EAP-PEAPMSCHAPv2-Protokoll verfügbar. Nur gültige Zeichen eingeben, siehe Kapitel 2.1 "Konfigurationsmöglichkeiten", S. 8.
Beispiele für LAN-Konfigurationen	Definition des Passworts für den privaten Schlüssel des EAP-TLS-Protokolls. Dieses Element ist nur für das EAP-TLS-Protokoll verfügbar. Nur gültige Zeichen eingeben, siehe Kapitel 2.1 "Konfigurationsmöglichkeiten", S. 8.

5.1.4 Beispiele für LAN-Konfiguration

Beispiel 1: Dynamischer IPv4-DHCP-Server, Standard-Gateway und DNS-Server

- Bereich zugewiesener dynamischen IPv4-Adressen von 192.168.1.2 bis 192.168.1.4.
- Gültigkeit der zugeteilten Adresse: 600 Sekunden (10 Minuten).
- Standardgateway IP-Adresse lautet 192.168.1.20
- DNS-Server IP-Adresse lautet 192.168.1.20

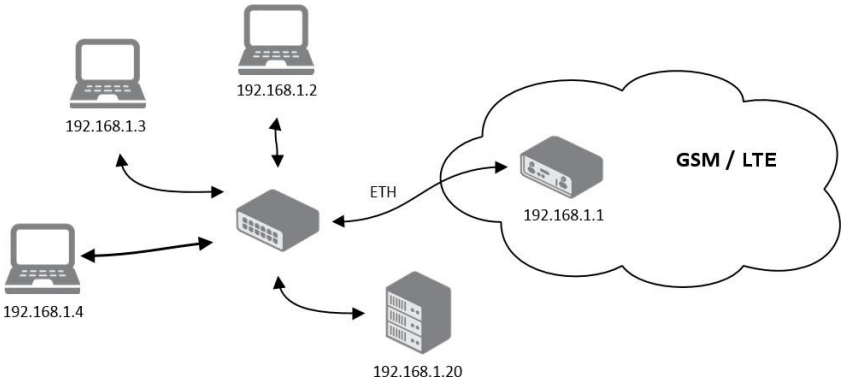


Abb. 17: Beispiel Dynamischer IPv4-DHCP-Server

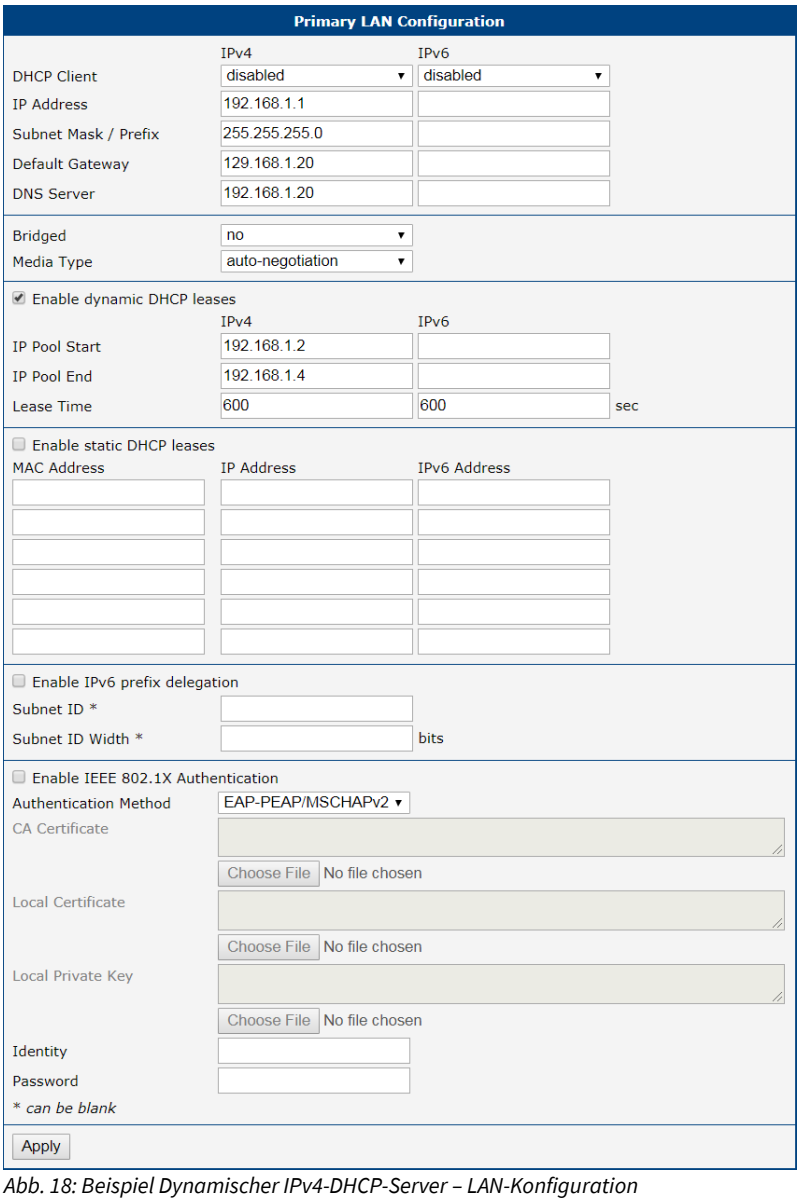


Abb. 18: Beispiel Dynamischer IPv4-DHCP-Server – LAN-Konfiguration

Beispiel 2: Dynamischer und statischer IPv4-DHCP-Server

- Bereich zugewiesener Adressen von 192.168.1.2 bis 192.168.1.4.
- Gültigkeit der zugeteilten Adresse: 600 Sekunden (10 Minuten).
- Client mit MAC-Adresse 01:23:45:67:89:ab hat IP-Adresse 192.168.1.10.
- Client mit MAC-Adresse 01:54:68:18:ba:7e hat IP-Adresse 192.168.1.11.

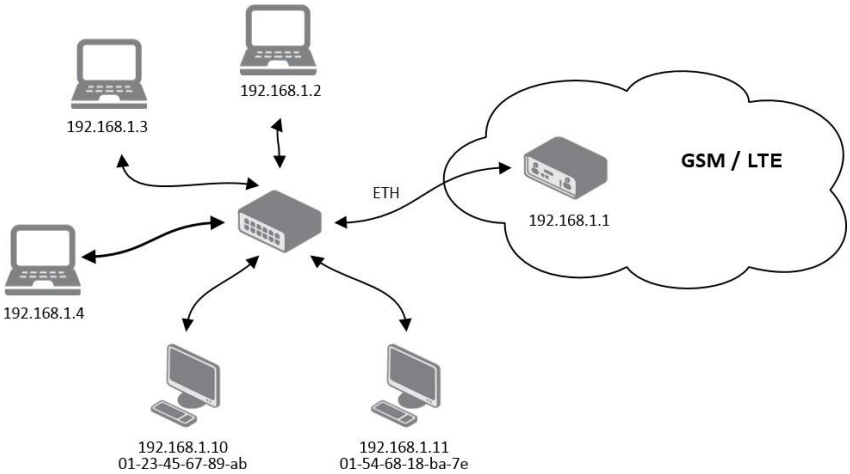


Abb. 19: Beispiel Dynamischer und statischer IPv4-DHCP-Server

Primary LAN Configuration

	IPv4	IPv6	
DHCP Client	disabled	disabled	
IP Address	192.168.1.1		
Subnet Mask / Prefix	255.255.255.0		
Default Gateway			
DNS Server			
Bridged	no		
Media Type	auto-negotiation		

☑ Enable dynamic DHCP leases

	IPv4	IPv6	
IP Pool Start	192.168.1.2		
IP Pool End	192.168.1.4		
Lease Time	600	600	sec

☑ Enable static DHCP leases

MAC Address	IP Address	IPv6 Address
01:23:45:67:89:ab	192.168.1.10	
01:54:68:18:ba:7e	192.168.1.11	

☐ Enable IPv6 prefix delegation

Subnet ID *

Subnet ID Width * bits

☐ Enable IEEE 802.1X Authentication

Authentication Method: EAP-TLS

CA Certificate: Choose File | No file chosen

Local Certificate: Choose File | No file chosen

Local Private Key: Choose File | No file chosen

Identity

Local Private Key Password

* *can be blank*

Apply

Abb. 20: Beispiel Dynamischer und statischer IPv4-DHCP-Server – LAN-Konfiguration

Beispiel 3: Dynamischer IPv6-DHCP-Server

- Der Bereich der dynamisch zugewiesenen IPv6-Adressen reicht von 2001:db8::1 bis 2001:db8::ffff.
- Gültigkeit der zugeteilten Adresse: 600 Sekunden (10 Minuten).
- Der Router ist weiterhin über IPv4 (192.168.1.1) erreichbar.

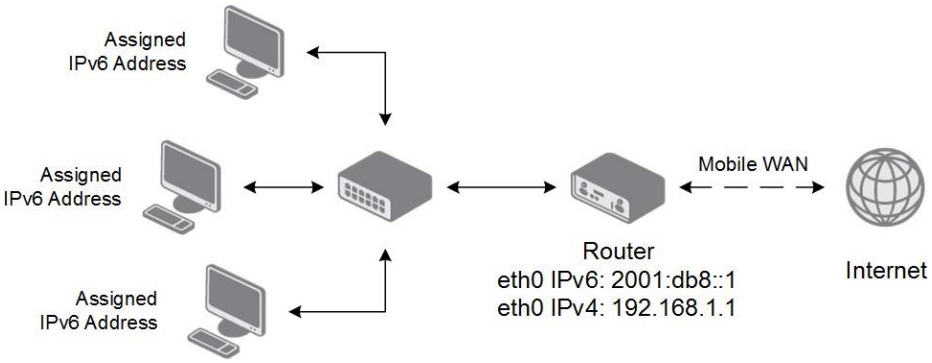


Abb. 21: Beispiel Dynamischer IPv6-DHCP-Server

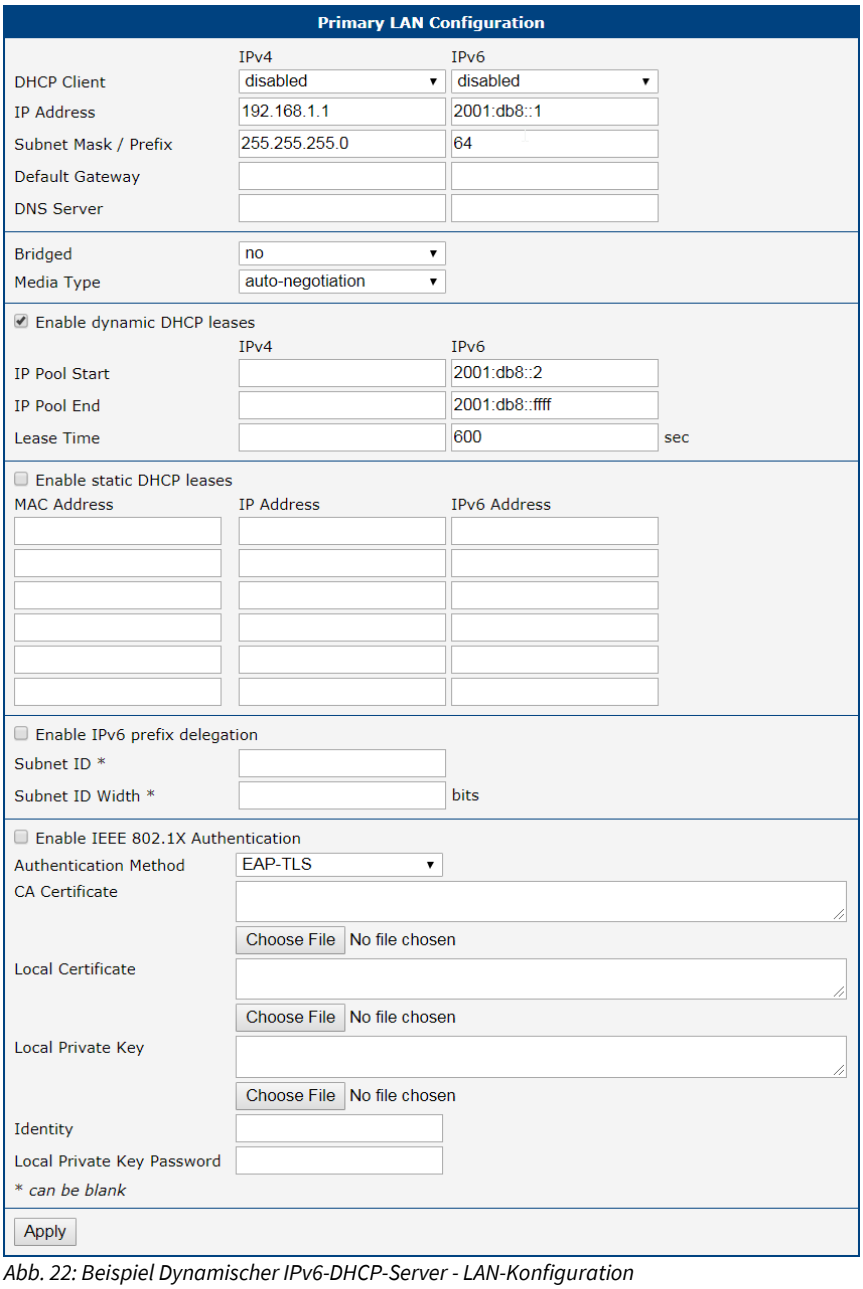


Abb. 22: Beispiel Dynamischer IPv6-DHCP-Server - LAN-Konfiguration

5.2 VRRP-Konfiguration

Wählen Sie den Menüpunkt **VRRP**, um die VRRP-Konfiguration einzugeben. Es gibt zwei Untermenüs, die es ermöglichen, bis zu zwei Instanzen von VRRP zu konfigurieren. Mit dem VRRP-Protokoll (Virtual Router Redundancy Protocol) können Sie das Paket-Routing vom Hauptrouter auf einen Backup-Router übertragen, falls der Hauptrouter ausfällt. (Dies kann verwendet werden, um in kritischen Anwendungen ein drahtloses Mobilfunk-Backup für einen primären kabelgebundenen Router bereitzustellen.) Wenn **Enable VRRP** markiert ist, können Sie die folgenden Parameter einstellen.

Tab. 21: VRRP-Konfiguration

Element	**Beschreibung**
Protokollversion	Wählen Sie die Version des VRRP (VRRPv2 oder VRRPv3).
Virtual Server IP Address	Dieser Parameter legt die IP-Adresse des virtuellen Servers fest. Diese Adresse muss für den primären und den Backup-Router gleich sein. Geräte im LAN verwenden diese Adresse als ihre Standard-Gateway-IP-Adresse.
Virtual Server ID	Dieser Parameter unterscheidet einen virtuellen Router im Netzwerk von einem anderen. Beim Haupt- und beim Backup-Router muss dieser Parameter gleich eingestellt werden.
Host Priority	Zum Hauptrouter wird der Router, der die höhere Priorität dieses Parameters eingestellt hat. In Abhängigkeit von RFC 2338 hat der Hauptrouter die höchstmögliche Priorität, und zwar 255. Der Reserverouter hat die Priorität im Intervall 1– 254 (Ausgangswert ist 100). Der Wert der Priorität gleich 0 ist nicht erlaubt.

Im zweiten Fensterteil kann die Kontrolle des Verbindungsaufbaus durch das Aktvieren der Option **Check connection** gewählt werden, um automatische Testmeldungen für das Mobilfunknetz zu ermöglichen. In einigen Fällen könnte die WAN-Verbindung noch aktiv sein, aber der Router ist nicht in der Lage, Daten über das Mobilfunknetz zu senden. Diese Funktion wird eingesetzt, um zu überprüfen, dass Daten über die PPP-Verbindung gesendet werden können und ergänzt die normale Nachrichtenbehandlung per VRRP. Der derzeit aktive Router (Haupt-/Backup-Router) sendet Testnachrichten an festgelegte Ping-Adressen (**Ping IP Address**) zu periodischen Intervallen (**Ping Interval**) und wartet eine bestimmte Zeit (**Ping Timeout**) auf eine Antwort. Erhält der Router keine Antwort auf den Ping-Befehl, wiederholt er den Vorgang so oft, wie vom Parameter **Ping Probes** vorgegeben. Danach wechselt er zum Backup-Router, bis die PPP-Verbindung wiederhergestellt ist.

HINWEIS Sie können den DNS-Server des Netzbetreibers als Ziel-IP-Adresse für die Testnachrichten (Pings) nutzen.

Die Option **Enable traffic monitoring** kann zur Senkung der Anzahl an Nachrichten, die zur Prüfung der PPP-Verbindung gesendet werden, genutzt werden. Ist dieser Parameter eingestellt, überprüft der Router die Schnittstelle auf Pakete, die sich vom Ping unterscheiden. Geht die Antwort innerhalb des Timeouts ein, das durch den Parameter **Ping Timeout** angegeben wurde, weiß der Router, dass die Verbindung noch aktiv ist. Erhält der Router keine Antwort innerhalb des vordefinierten Zeitraums, versucht er, die mobile WAN-Verbindung mittels Standard-Ping-Befehlen zu prüfen.

Tab. 22: Verbindung prüfen

Element	**Beschreibung**
Ping IP Address	Ziel-IP-Adresse der Ping-Nachrichten. Die IP-Adresse kann nicht als Domain-Name eingegeben werden.
Ping-Intervall	Intervall in Sekunden zwischen den ausgehenden Pings.
Ping Timeout	Zeit in Sekunden für das Warten auf eine Antwort.
Ping Probes	Maximale Anzahl der fehlgeschlagenen Ping-Nachrichten

Beispiel für VRRP-Protokoll

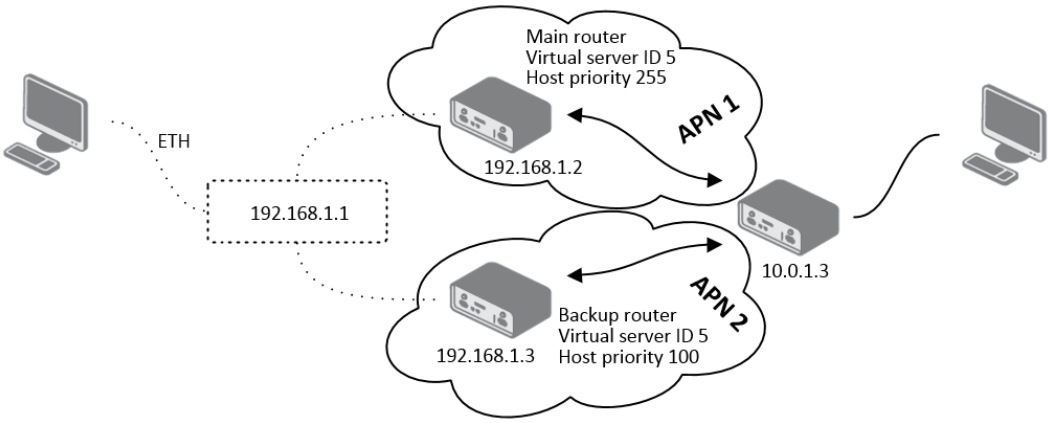


Abb. 23: Topologie des Beispiels für die Einstellung des Protokolls VRRP

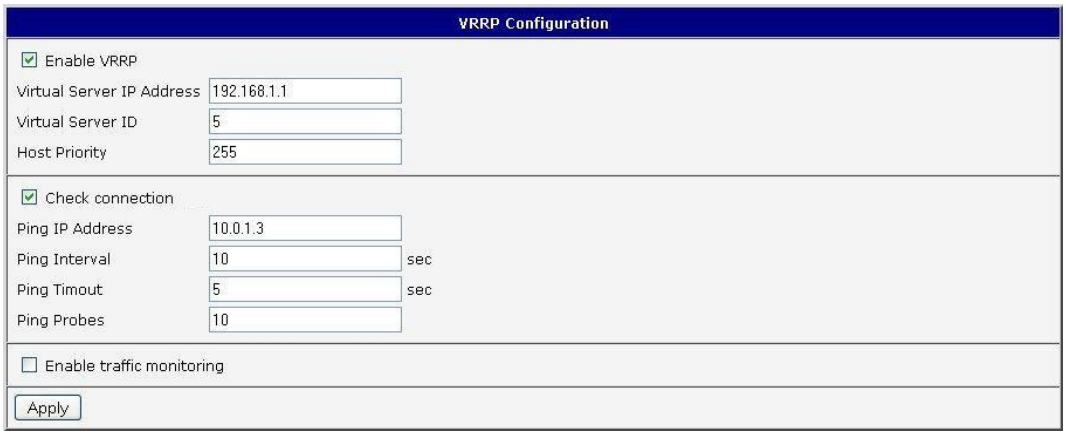


Abb. 24: Beispiel für VRRP-Konfiguration – Hauptrouter

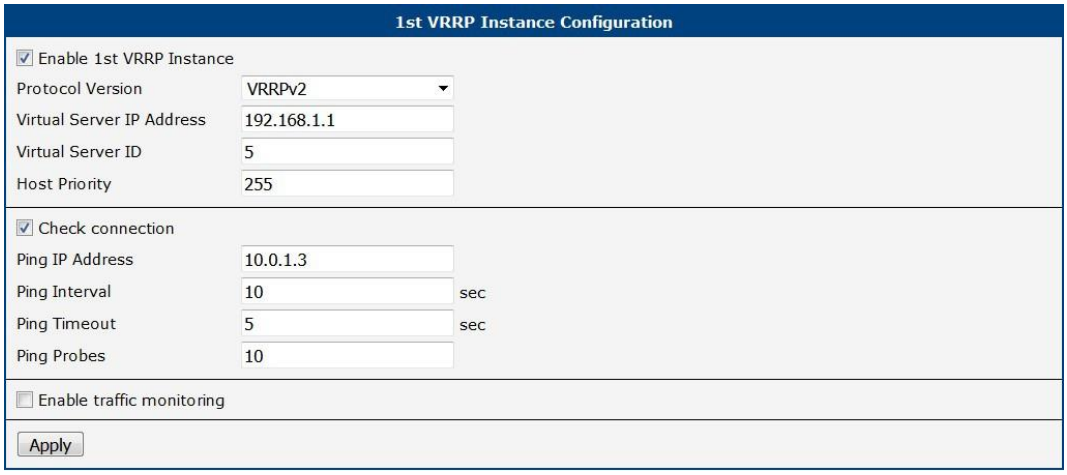


Abb. 25: Beispiel für VRRP-Konfiguration – Backuprouter

5.3 Mobile WAN Konfiguration

HINWEIS Der wienet WR-LAN v3 SL und ER300 Router zeigen die Mobile WAN Konfiguration nicht an

Hinweise für Produktvariante LR140 mit SIM-Karteneinschub:

- Sie können die 2. SIM-Karte, wie in diesem Kapitel beschrieben, in der GUI konfigurieren.
- Sie können auf die 2. SIM-Karte wechseln, was zur Folge hat, dass die Konfiguration der 2. SIM-Karte auf die installierte SIM-Karte übertragen wird.
- Sie können diese Einstellung nutzen um beispielsweise unabhängig einen öffentlichen und privaten APN zu konfigurieren.
- Sie können entweder manuell, per SMS oder automatisch (falls so konfiguriert) zwischen den Konfigurationen wechseln.

Wählen Sie den Punkt **Mobiles WAN** im Menü **Configuration**, um die Konfigurationsseite des Mobilfunknetzes aufzurufen.
Siehe Seite **Mobile WAN Configuration** in Abb. 27.

5.3.1 Mobilfunkverbindung

Ist die Option **Create connection to mobile network** markiert, versucht der Router nach dem Einschalten selbst die Mobilfunkverbindung herzustellen. Die folgenden Optionen können für jede SIM-Karte einzeln oder als zwei getrennte APNs zur Zwischenschaltung einer SIM-Karte eingestellt werden.

Tab. 23: Konfiguration der mobilen WAN-Verbindung

Element	**Beschreibung**
Carrier	Auswahl des Netzbetreibers (nur für wienet WR-LTE v3 SL Router).
APN	Netzzugangspunkt (Access Point Name)
Username	Benutzername für die Anmeldung ins Netz
Passwort	Passwort zum Einloggen in das GSM-Netz. Nur gültige Zeichen eingeben, siehe Kapitel 2.1 "Konfigurationsmöglichkeiten", S. 8.
Authentication	Protokoll der Authentifizierung im GSM-Netz • **PAP oder CHAP** – Authentifizierungsmethode wird vom Router gewählt. • **PAP** – Es wird die PAP-Authentifizierungsmethode genutzt. • **CHAP** – Es wird die CHAP-Authentifizierungsmethode genutzt.
IP Mode	Gibt die Version des verwendeten IP-Protokolls an: • **IPv4** – Nur IPv4 Protokoll wird verwendet (Default). • **IPv6** – Nur IPv6 Protokoll wird verwendet. • **IPv4/IPv6** – IPv4- und IPv6-unabhängiger Dual-Stack ist aktiviert.
IP Address	Nur zur Verwendung im IPv4- und IPv4/IPv6-Modus. Gibt die IPv4-Adresse der SIM-Karte an. Sie geben die IP-Adresse nur dann manuell ein, wenn der Mobilfunkanbieter die IP-Adresse zugewiesen hat.
Phone Number	Gibt die Telefonnummer an, die der Router bei einem GPRS wählt oder CSD-Verbindung. Der Router verwendet die Standardtelefonnummer *99***1 #.
Operator	Gibt den Netzbetreibercode an. Sie können diesen Parameter als PLNM bevorzugten Betreibercode angeben.
Network type	Gibt den im Mobilfunknetz verwendeten Protokolltyp an. • **Automatic selection** – Der Router wählt automatisch die Übertragungsmethode entsprechend der Verfügbarkeit der Übertragungstechnologie. • Es ist auch möglich, eine der folgenden spezifischen Methoden auszuwählen. • für die Datenübertragung: **LTE**, **UMTS/HSPA**, **GPRS/EDGE.**
PIN	Gibt die PIN zum Entsperren der SIM-Karte an. Nur verwenden, wenn dies von einer bestimmten SIM-Karte erforderlich ist. Nach mehreren fehlgeschlagenen Eingabeversuchen der PIN wird die SIM-Karte gesperrt.

MRU	Maximum Receiving Unit – maximale Paketgröße, die der Router über Mobile WAN empfangen kann. Der Standardwert ist 1500 B. Andere Einstellungen können dazu führen, dass der Router Daten falsch empfängt. Minimaler Wert im IPv4- und IPv4/IPv6-Modus: 128 B. Minimaler Wert im IPv6-Modus: 1280 B.
MTU	Maximum Transmission Unit – maximale Paketgröße, die der Router über Mobile WAN übertragen kann. Der Standardwert ist 1500 B. Andere Einstellungen können dazu führen, dass der Router Daten falsch überträgt. Minimaler Wert im IPv4- und IPv4/IPv6-Modus: 128 B. Minimaler Wert im IPv6-Modus: 1280 B.

HINWEIS

Tipps zum Arbeiten mit dem Konfigurationsformular **Mobile WAN**:

- Wenn die MTU-Größe falsch eingestellt ist, überschreitet der Router die Datenübertragung nicht. Ist der MTU-Wert zu niedrig eingestellt, kommt es häufiger zu einer Fragmentierung der Daten. Eine häufigere Fragmentierung bedeutet einen höheren Overhead und auch die Möglichkeit von Paketschäden während der Defragmentierung. Im Gegensatz dazu kann ein höherer MTU-Wert dazu führen, dass das Netzwerk das Paket verwirft.
- **IP address** leer, vergibt der Mobilfunkanbieter beim Verbindungsaufbau automatisch eine IP-Adresse.
  Wenn Sie manuell eine IP-Adresse zuweisen, greift der Router schneller auf das Netzwerk zu.
- Bleibt das Feld **APN** leer, wählt der Router den APN automatisch anhand des IMSI-Codes der SIM-Karte aus.
  Den Namen des gewählten APN finden Sie im Systemprotokoll.
- Wenn das Wort `blank` im Feld **APN** steht, interpretiert der Router die APN als leer.



VORSICHT

Geben Sie die richtige PIN an. Eine falsche PIN kann die SIM-Karte blockieren.

Bei Parametern, die mit einem Sternchen gekennzeichnet sind, müssen Sie nur dann die entsprechenden Informationen eingeben, wenn diese Informationen vom Mobilfunkanbieter gefordert werden.

Wenn der Router keine Verbindung zum Mobilfunknetz herstellen kann, sollten Sie die Richtigkeit der eingegebenen Daten überprüfen. Alternativ können Sie eine andere Authentifizierungsmethode oder einen anderen Netzwerktyp ausprobieren.

5.3.2 Konfiguration der DNS-Adressen

Das Element **DNS** dient der einfacheren Konfiguration auf der Client-Seite. Wenn dieses Element auf den Wert **get from operator** gesetzt ist, versucht der Router, automatisch eine IP-Adresse des primären und sekundären DNS-Servers vom Mobilfunkanbieter abzurufen.
Um die IP-Adressen der primären DNS-Server manuell anzugeben, wählen Sie in der Pulldown-Liste **DNS Server** den Wert **manually** aus.
Sie können auch die IPv4- oder IPv6-Adresse des DNS-Servers (oder beides) basierend auf der Option IP-Modus eingeben.

5.3.3 Konfiguration der Kontrolle der Mobilfunkverbindung

HINWEIS

Die Aktivierung der Funktion "Verbindung prüfen" für Mobilfunknetze ist für einen unterbrechungsfreien und kontinuierlichen Betrieb des Routers erforderlich.

Wenn das Element **Check Connection** auf **enabled** oder **enabled + bind** gesetzt ist, wird die Überprüfung der Verbindung zum Mobilfunknetz aktiviert. Der Router sendet in regelmäßigen Zeitintervallen (**Ping Interval**) automatisch Ping-Anfragen an die angegebene Domäne oder IP-Adresse (**Ping IP Address** oder **Ping IPv6 Address**). Bei erfolglosem Ping wird nach zehn Sekunden ein neuer gesendet. Wenn es dreimal hintereinander fehlschlägt, die IP-Adresse zu pingen, beendet der Router die aktuelle Verbindung und versucht, eine neue aufzubauen. Die Prüfung kann für zwei SIM-Karten separat eingestellt werden. Senden Sie einen ICMP (ICMPv6)-Ping an eine IP-Adresse, von der Sie wissen, dass sie noch funktioniert (Beispielsweise der DNS-Server des Betreibers).

Ist **Check Connection** aktiviert, werden die Ping-Abfragen anhand von Routing-Tabellen gesendet. Dadurch können die Abfragen über jede Schnittstelle gesendet werden. Wenn jede Ping-Nachricht über die Netzwerkschnittstelle gesandt werden muss, die bei der Herstellung einer Verbindung zum Netzbetreiber erstellt wurde, ist es notwendig, die Option **Check Connection** auf **enabled + bind** einzustellen. Die Option **disabled** deaktiviert die Überprüfung der Mobilfunkverbindung.

Tab. 24: Konfiguration der Kontrolle der Mobilfunkverbindung

Element	Beschreibung
Ping IP Address	Gibt die Ziel-IPv4-Adresse oder den Domänennamen der Ping-Abfrage an. Verfügbar im IPv4- und IPv4/IPv6-IP-Modus.
Ping IPv6 Address	Gibt die Ziel-IPv6-Adresse oder den Domänennamen der Ping-Abfrage an. Verfügbar im IPv6- und IPv4/IPv6-IP-Modus.
Ping-Intervall	Zeitintervalle zwischen ausgehenden Pings
Ping Timeout	Wartezeit auf eine Ping-Antwort in Sekunden

Beispiel für eine Verbindung Prüfen Konfiguration

Die folgende Abbildung zeigt das folgende Szenario:
Die Verbindung zum Mobilfunknetz im IPv4 **IP Mode** wird auf der Adresse 8.8.8.8 mit einem Zeitintervall von 60 Sekunden für die erste SIM-Karte und auf der Adresse www.google.com mit dem Zeitintervall 80 Sekunden für die zweite SIM-Karte gesteuert. Bei aktivem Datenstrom auf dem Router werden die Kontroll-Pings nicht gesendet, sondern der Datenstrom überwacht.

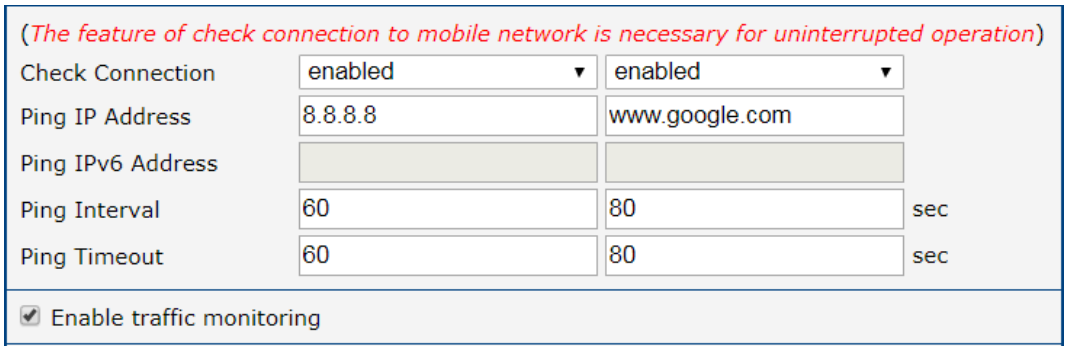


Abb. 26: Beispiel – Verbindung prüfen

5.3.4 Konfiguration des Datenlimits

Tab. 25: Konfiguration des Datenlimits

Element	Beschreibung
Data limit	Gibt die maximal erwartete Datenmenge an, die über GPRS in einem Abrechnungszeitraum (ein Monat) übertragen (gesendet und empfangen) wird. Der Höchstwert beträgt 2 TB (2097152 MB).
Warning Threshold	Gibt einen Prozentsatz des "Datenlimits" im Bereich von 50 % bis 99 % an. Bei Überschreitung des angegebenen prozentualen Datenlimits sendet der Router eine SMS in folgender Form: **Router has exceeded (value of Warning Threshold) of data limit**.
Accounting Start	Gibt den Tag des Monats an, an dem der Abrechnungszeitraum für eine bestimmte SIM-Karte beginnt. Wenn der Diensteanbieter, der die SIM-Karte ausgestellt hat, den Beginn des Abrechnungszeitraums vorgibt, beginnt der Router, die übertragene Datenmenge ab diesem Tag zu zählen.

HINWEIS Wenn der Parameter **Data Limit State** (siehe unten) auf den Wert **not applicable** oder **Send SMS when data limit is exceeded** in **SMS Configuration** nicht ausgewählt ist, wird das hier eingestellte **Data Limit** ignoriert.

5.3.5 Umschalten der SIM-Kartenkonfiguration

Im unteren Teil des Konfigurationsformulars können Sie die Regeln für das Umschalten zwischen den beiden SIM-Karten festlegen.

HINWEIS Abhängig von den hier angegebenen Konfigurationseinstellungen (manuelle Erlaubnis, Roaming, Datenlimit, Zustand der Binäreingänge) wechselt der Router automatisch zwischen den SIM-Karten und deren individuellen Setups. Beachten Sie, dass die für den Verbindungsaufbau ausgewählte SIM-Karte das Ergebnis des logischen Produkts (UND) der Konfiguration hier ist (Tabelle unten).

Tab. 26: Konfiguration des Umschaltens zwischen den SIM-Karten

Element	**Beschreibung**
Roaming State	Konfigurieren Sie die Verwendung von SIM-Karten basierend auf Roaming. Diese Roaming-Funktion muss für die SIM-Karte aktiviert sein, auf der sie aktiviert ist! • **not applicable** – Die SIM-Karte kann überall verwendet werden. • **home network only** – Verwenden Sie die SIM-Karte nur, wenn kein Roaming erkannt wird.
Data Limit State	Konfigurieren Sie die Verwendung von SIM-Karten basierend auf dem oben eingestellten Datenlimit: • **not applicable** –Es ist möglich, die SIM unabhängig vom Limit zu verwenden. • **not exceeded** – Verwenden Sie die SIM-Karte nur, wenn das Datenlimit (oben eingestellt) nicht überschritten wurde.
BIN0 State	Konfigurieren Sie die Verwendung von SIM-Karten basierend auf dem Zustand des Binäreingangs 0: • **not applicable** – Es ist möglich, die SIM unabhängig vom BIN0-Status zu verwenden. • **on** – Verwenden Sie die SIM-Karte nur, wenn der BIN0-Zustand logisch 0 ist – Spannung vorhanden. • **off** – Only use
BIN1 State	Konfigurieren Sie die Verwendung von SIM-Karten basierend auf dem Zustand des Binäreingangs 1: • **not applicable** – Es ist möglich, die SIM unabhängig vom BIN1-Status zu verwenden. • **on** – Verwenden Sie die SIM-Karte nur, wenn der BIN1-Zustand logisch 0 ist – Spannung vorhanden. • **off** – Verwenden Sie die SIM-Karte nur, wenn der BIN1-Zustand logisch 1 ist – keine Spannung.

Verwenden Sie die folgenden Parameter, um die Entscheidungsfindung beim Wechsel der SIM-Karte im Mobilfunkmodul festzulegen.

Tab. 27: Wechseln Sie zwischen SIM-Kartenkonfigurationen

Element	**Beschreibung**
Default SIM Card	Gibt die Standard-SIM-Karte der Module an. Der Router versucht mit dieser Voreinstellung eine Verbindung zum Mobilfunknetz aufzubauen. • **1st** – Die 1. SIM-Karte ist die Standardkarte. • **2nd** – Die 2. SIM-Karte ist die Standardkarte.
Initial State	Legt die Aktion des Mobilfunkmoduls fest, nachdem die SIM-Karte ausgewählt wurde. • **online** – Verbindung zum Mobilfunknetz herstellen, nachdem die SIM-Karte ausgewählt wurde (Default). • **offline** – In den Offline-Modus gehen nach Auswahl der SIM-Karte. **Hinweis:** Wenn Offline, kann dieser Initialstatus nur per SMS geändert werden. – siehe **SMS Configuration**. Das Mobilfunkmodul geht auch in den Offline-Modus, wenn keine der SIM-Karten ausgewählt ist.
Switch to other SIM card when connection fails	Gilt nur, wenn die Verbindung auf der Standard-SIM-Karte hergestellt wird und dann fehlschlägt. Wenn der Verbindungsfehler von der Funktion **Check Connection** oben erkannt wird, wechselt der Router zur Backup-SIM-Karte.
Switch to default SIM card after timeout	Wenn aktiviert, versucht der Router nach dem Timeout, zur Standard-SIM-Karte zurückzukehren. Dies gilt nur, wenn eine Standard-SIM-Karte definiert ist und die Backup-SIM aufgrund eines Ausfalls der Standard-SIM ausgewählt wurde oder wenn Roaming-Einstellungen den Wechsel verursachen. Diese Funktion ist nur verfügbar, wenn **Zu anderer SIM-Karte wechseln, wenn die Verbindung fehlschlägt** aktiviert ist.
Initial timeout	Gibt die Zeitspanne an, die der Router wartet, bevor er zum ersten Mal versucht, zur Standard-SIM-Karte zurückzukehren. Der Bereich dieses Parameters liegt zwischen 1 und 10000 Minuten.
Subsequent Timeout	Gibt die Zeitspanne an, die der Router nach einem erfolglosen Versuch, zur Standard-SIM-Karte zurückzukehren, wartet. Der Bereich liegt zwischen 1 und 10000 Minuten.
Additive constants	Gibt an, wie lange der Router auf weitere Versuche wartet, um zur Standard-SIM-Karte zurückzukehren. Diese Dauer ist die Summe der im Parameter "Nachträglicher Timeout" angegebenen Zeit und der in diesem Parameter angegebenen Zeit. Der Bereich in diesem Parameter reicht von 1 bis 10000 Minuten.

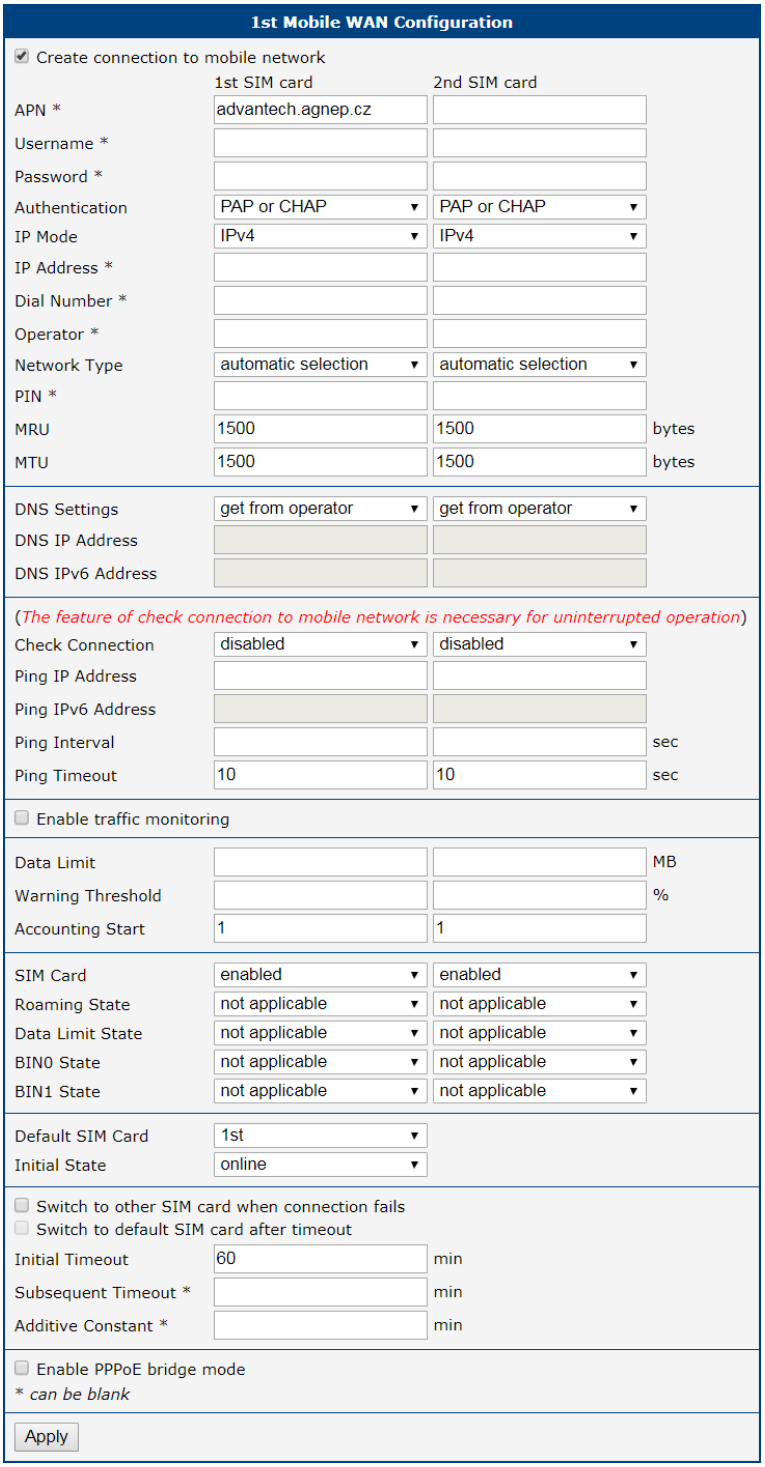


Abb. 27: Konfigurationseite für Mobile WAN

Beispiele für die Konfiguration des Umschaltens zwischen zwei SIM-Karten

Beispiel 1: Timeout-Konfiguration

Aktivieren Sie das Kontrollkästchen Nach Zeitüberschreitung zur Standard-SIM-Karte wechseln und geben Sie die folgenden Werte ein:

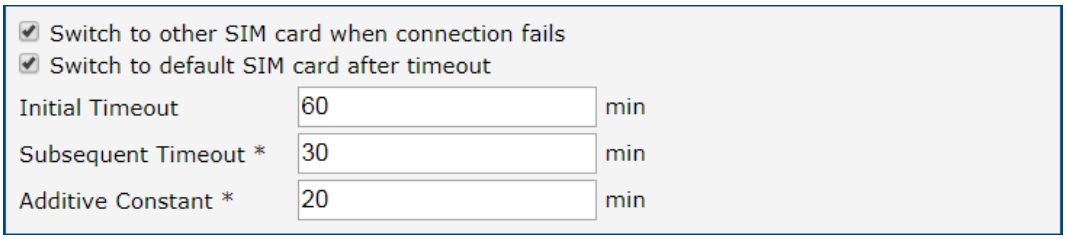


Abb. 28: Beispiel – Timeout-Konfiguration

Der erste Wechsel auf die Standard-SIM-Karte erfolgt nach 60 Minuten. Wenn der erste Versuch fehlschlägt, wird nach 30 Minuten ein zweiter Versuch unternommen. Ein dritter Versuch erfolgt nach 50 Minuten (30+20). Ein vierter Versuch erfolgt nach 70 Minuten (30+20+20).

Beispiel 2: Umschaltung bei Datenbegrenzung

Die folgende Konfiguration veranschaulicht ein Szenario, in dem der Router auf die zweite SIM-Karte wechselt, nachdem das Datenlimit von 800 MB auf der ersten (Standard-) SIM-Karte überschritten wurde. Der Router sendet eine SMS bei Erreichen von 400 MB (diese Einstellung muss auf der SMS-Konfigurationsseite aktiviert werden).
Der Abrechnungszeitraum beginnt am 18. des Monats.

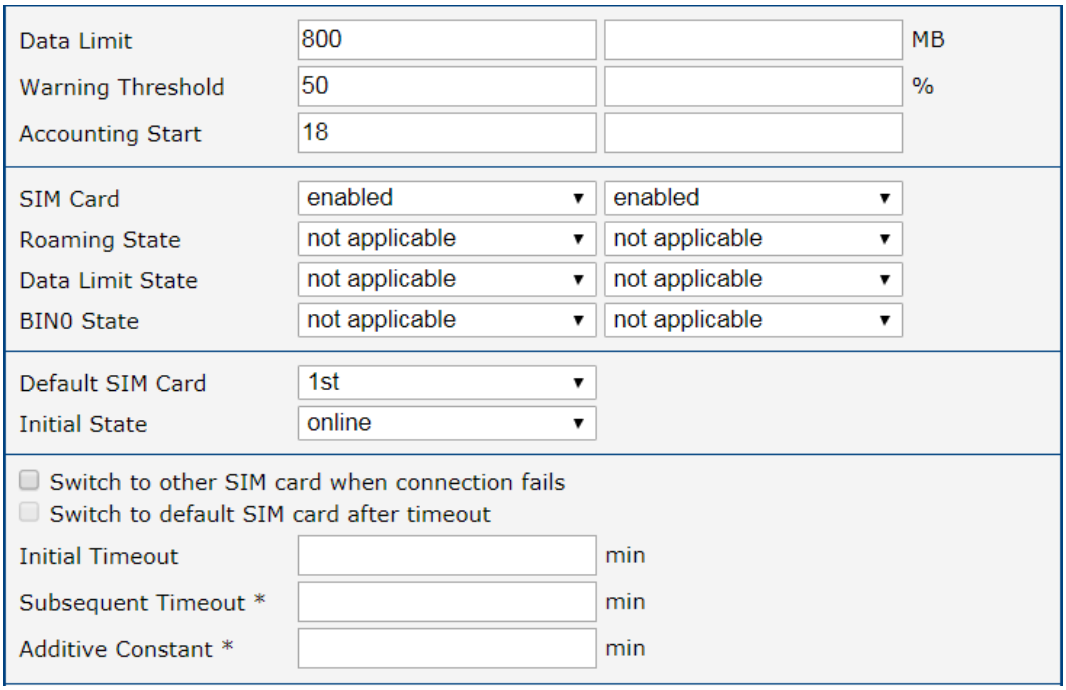


Abb. 29: Beispiel – Datenbegrenzung

5.3.6 Konfiguration des PPPoE-Bridge-Modus

Wenn die Option **Enable PPPoE bridge mode** markiert ist, wird der Modus PPPoE bridge aktiviert. PPPoE (point-to-point over ethernet) ist ein Netzwerkprotokoll, das PPP-Rahmen in Ethernet-Rahmen einrahmt. Dies ermöglicht das Herstellen einer PPPoE-Verbindung von der Einrichtung zum Router. Zum Beispiel von einem PC, der an einen ETH Port Router angeschlossen ist. Dem PC wird die IP-Adresse der SIM-Karte zugeteilt.

VORSICHT

Für wienet v3-Router: Wenn Sie den **PPPoE-Bridge-Modus** aktivieren, können Sie keine **SMS-Konfigurationsfunktionen** nutzen – der Router sendet keine SMS und Sie können den Router nicht per SMS steuern!
Die Funktion **SMS senden** im Abschnitt **Administration** funktioniert nicht. Außerdem werden im '**Mobile WAN-Status**' keine Daten zu Signalstärken angezeigt. Dies wird dadurch verursacht, dass in dieser Version des Routers derselbe Kanal zum Senden von AT-Befehlen im Mobilfunkmodul verwendet wird. Wenn der Kanal durch AT-Befehle für PPPoE-Bridge belegt ist, ist kein Platz für SMS-AT-Befehle.

Die Änderungen der Einstellungen wirken sich nach Betätigung der Schaltfläche **Appl**y aus.

5.4 PPPoE-Konfiguration

PPPoE (Point-to-Point over Ethernet) ist ein Netzwerkprotokoll, das PPP-Frames in Ethernet-Frames kapselt. Der Router verwendet den PPPoE-Client, um eine Verbindung zu Geräten herzustellen, die eine PPPoE-Bridge oder einen PPPoE-Server unterstützen. Die Bridge oder der Server ist normalerweise ein ADSL-Router.

Um die Seite "**PPPoE-Konfiguration"** zu öffnen, wählen Sie den Menüpunkt "**PPPoE"**. Wenn Sie das Kontrollkästchen '**PPPoE-Verbindung erstellen**' markieren, versucht der Router nach dem Booten eine PPPoE-Verbindung aufzubauen. Nach der Verbindung erhält der Router die IP-Adresse des Geräts, mit dem er verbunden ist. Die Kommunikation von einem Gerät hinter dem PPPoE-Server wird an den Router weitergeleitet.

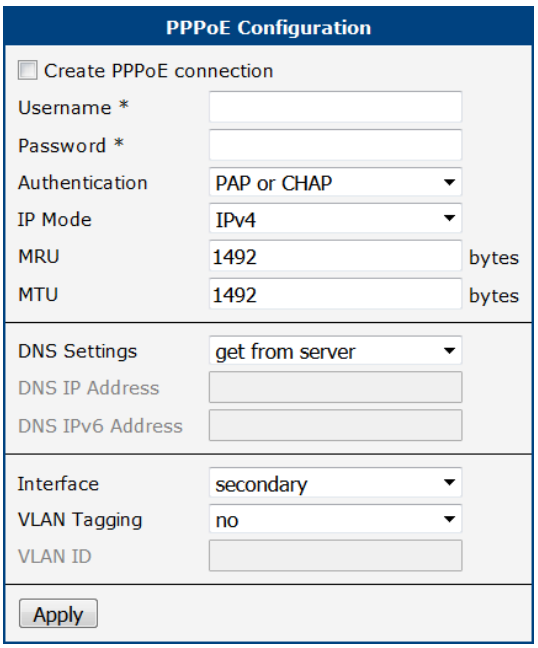


Abb. 30: PPPoE-Konfiguration

Tab. 28: PPPoE-Konfiguration

Element	Beschreibung
Username	Benutzername für sicheren Zugang zu PPPoE
Passwort	Passwort für den sicheren Zugriff auf PPPoE. Nur gültige Zeichen eingeben, siehe Kapitel 2.1 "Konfigurationsmöglichkeiten", S. 8.
Authentication	Protokoll der Authentifizierung im GSM-Netz • **PAP oder CHAP** – Authentifizierungsmethode wird vom Router gewählt • **PAP** – Es wird die PAP-Authentifizierungsmethode genutzt • **CHAP** – Es wird die CHAP-Authentifizierungsmethode genutzt
IP Mode	Spezifiziert die Version des IP-Protokolls: • **IPv4** – Nur IPv4-Protocol wird verwendet (Default) • **IPv6** – Nur IPv6-Protokoll wird verwendet • **IPv4/IPv6** – IPv4 und IPv6 Dual Stack ist aktiviert
MRU	Gibt die maximale Empfangseinheit an. Die MRU identifiziert die maximale Paketgröße, die der Router über PPPoE empfangen kann. Der Defaultwert ist 1492 Byte. Andere Einstellungen können zu einer fehlerhaften Datenübertragung führen. Der Mindestwert im IPv4- und IPv4/IPv6-Modus beträgt 128 Byte. Der kleinste Wert beim IPv6-Protokoll beträgt 1280 Byte.
MTU	Gibt die maximale Übertragungseinheit an. Die MTU identifiziert die maximale Paketgröße, die der Router in einer gegebenen Umgebung übertragen kann. Der Standardwert ist 1492 Byte. Andere Einstellungen können zu einer fehlerhaften Datenübertragung führen. Der Mindestwert im IPv4- und IPv4/IPv6-Modus beträgt 128 Byte. Der Mindestwert im IPv6-Modus beträgt 1280 Byte.
DNS Settings	Kann so eingestellt werden, dass die DNS-Adresse vom Server bezogen oder manuell eingestellt wird
DNS IP Address	Manuelle Einstellung der DNS-Adresse
DNS IP Address	Manuelle Einstellung der IPv6-DNS-Adresse
Übergabebaustein / interface	Eine Ethernet-Schnittstelle auswählen
VLAN Tagging	Tagging Wählen Sie Ja, um das VLAN-Tagging zu aktivieren
VLAN ID	Legen Sie die ID für das VLAN-Tagging fest. Der Bereich reicht von 1 bis 1000

HINWEIS Das Festlegen eines falschen Paketgrößenwerts (MRU, MTU) kann zu einer fehlgeschlagenen Übertragung führen.

5.5 Wi-Fi-Access-Point-Konfiguration

HINWEIS Dieses Kapitel trifft nur zu, wenn der Router mit einem Wi-Fi-Modul ausgestattet ist.

Das Wi-Fi-Modul unterstützt den Multi-Role-Modus, der es ermöglicht, gleichzeitig als Access Point (AP) und Station (STA) zu arbeiten. Der Mehrkanalmodus wird ebenfalls unterstützt, sodass der AP und die STA auf unterschiedlichen Kanälen arbeiten können.

Aktivieren Sie den WLAN-Zugangspunktmodus, indem Sie das Kontrollkästchen **WLAN-AP aktivieren** oben auf der Konfigurationsseite **Konfiguration > WLAN > Zugangspunkt** aktivieren. In diesem Modus wird der Router zu einem Access Point, mit dem sich andere Geräte im **Stationsmodus (STA)** verbinden können. Sie können die folgenden Eigenschaften einstellen, die in der folgenden Tabelle aufgeführt sind.

RADIUS-Netzwerkprotokoll (Remote Authentication Dial-In User Service), das eine zentralisierte Authentifizierung, Autorisierung und Abrechnung (AAA) bietet. Die Verwaltung für Benutzer wird über Wi-Fi unterstützt. Der Router kann nur ein RADIUS-Client sein (nicht der Server) – normalerweise als Wi-Fi-AP (Access Point), der mit dem RADIUS-Server verhandelt.

Tab. 29: Konfiguration des Wi-Fi-Access-Point

Element	**Beschreibung**
Enable WiFi AP	Wi-Fi Access Point (AP) aktivieren.
IP Address	Eine feste IP-Adresse der WiFi-Schnittstelle. Verwenden Sie die IPv4-Notation in der IPv4-Spalte und die IPv6-Notation in der IPv6-Spalte. Gekürzte IPv6-Notation wird unterstützt.
Subnet Mask / Prefix	Gibt eine Subnetzmaske für die IPv4-Adresse an. Geben Sie in der Spalte IPv6 das Präfix für die IPv6-Adresse ein – Zahl im Bereich 0 bis 128.
Bridged	Bridgemodus aktivieren • **no** – Bridgemodus ist nicht zulässig (Standardwert). Das WLAN-Netzwerk ist nicht mit dem LAN-Netzwerk des Routers verbunden. • **yes** – Bridgemodus ist zulässig. Das WLAN-Netzwerk ist mit einem oder mehreren LAN-Netzwerken über den Router verbunden. In diesem Fall werden die meisten Einstellungen dieser Tabelle ignoriert. Stattdessen werden die Einstellungen der ausgewählten Netzwerkschnittstelle (LAN) übernommen.
Enable dynamic DHCP leases	Aktivieren Sie die dynamische Zuweisung von IP-Adressen mithilfe des DHCP-Servers (DHCPv6).
IP Pool Start	Anfang des IP-Adressbereichs, der DHCP-Clients zugewiesen wird. Verwenden Sie die richtige Notation in den Spalten IPv4 und IPv6.
IP Pool End	Ende des IP-Adressbereichs, der DHCP-Clients zugewiesen wird. Verwenden Sie die richtige Notation in den Spalten IPv4 und IPv6.
Lease Time	Zeit in Sekunden, die der Client die IP-Adresse verwenden darf.
Enable IPv6 prefix delegation	Aktiviert die unten ausgefüllte Konfiguration der Präfix-Delegierung.
Subnet ID	Der Dezimalwert der Subnet-ID der Ethernet-Schnittstelle. Der maximale Wert hängt von der Breite der Subnetz-ID ab.
Subnet ID Width	Die maximale Breite der Subnetz-ID hängt von Ihrer Site ab. Präfix – es ist der Rest bis 64 Bit.
SSID	Eindeutige Kennung des Wi-Fi-Netzwerks

SSID-Netzwerkbezeichnung	Methode, bei der dem Netzwerk eine eindeutige Bezeichnung (SSID) im Signalrahmen zugewiesen wird. • **Aktiviert** – SSID wird im Signalrahmen gesendet. • **Null-Länge** – Der Signalrahmen bietet keine SSID. An den Signalrahmen gesendete Anforderungen werden ignoriert. • **Deaktiviert** – Jedes SSID-Zeichen im Signalrahmen wird durch 0 ersetzt. Die ursprüngliche Länge wird beibehalten. An den Signalrahmen gesendete Anforderungen werden ignoriert.
Client Isolation	Wenn diese Option aktiviert ist, isoliert der Access Point alle verbundenen Clients, sodass sie sich nicht sehen (sie befinden sich in verschiedenen Netzwerken, sie können untereinander keinen PING durchführen). Wenn deaktiviert, verhält sich das Access Point wie ein Switch, aber drahtlos – die Clients befinden sich im selben LAN und können sich gegenseitig sehen.
Country Code	Code des Landes, in dem der Router mit WLAN verwendet wird. Dieser Code muss im Format ISO 3166-1 alpha-2 eingegeben werden. Wenn kein Ländercode angegeben ist und der Router kein System implementiert hat, um diesen Code zu ermitteln, wird "US" als Standard-Ländercode verwendet. Wird kein Ländercode angegeben oder ein falscher Ländercode eingegeben, kann es zu einem Verstoß gegen die Regulierungsvorschriften für die Nutzung von Frequenzbändern im jeweiligen Land kommen.
HW-Modus	HW-Modus des Wi-Fi-Standards, der vom Access Point (AP) unterstützt wird • IEE 802.11b (2,4 GHz) • IEE 802.11b+g (2,4 GHz) • IEE 802.11b+g+n (2,4 GHz) • IEE 802.11a (5 GHz) • IEE 802.11a+n (5 GHz)
Channel	Kanal, auf dem der Wi-Fi-AP sendet. Unterstützte 2,4-GHz-Kanäle: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13. Auf wienet v3-Router werden nur die Kanäle 1 bis 11 unterstützt! Unterstützte 5-GHz-Kanäle: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165.
BW 40 MHz	Option für den HW-Modus 802.11n, der die gleichzeitige Übertragung auf zwei standardmäßigen 20 MHz-Kanälen ermöglicht. Wenn dieser Kanal belegt ist, wird stattdessen der BW 20 MHz-Kanal verwendet.
WMM	Aktiviert grundlegende QoS für Wi-Fi-Netzwerke. Diese Version garantiert keinen Netzwerkdurchsatz. Es eignet sich für einfache Anwendungen, die QoS erfordern.
Authentication	Stellt Zugangskontrolle für autorisierte Nutzer in Drahtlos-Netzwerken bereit: • **Open** – Keine Authentifizierung erforderlich (freier Zugangspunkt) • **Shared** (Freigegeben) – Basisauthentifizierung mittels eines WEP-Schlüssels. • **WPA-PSK** – Authentifizierung mit besserer Authentifizierungsmethode PSK-PSK • **WPA2-PSK** – Authentifizierung mit AES-Verschlüsselung • **WPA-Enterprise** – RADIUS-Authentifizierung durch externen Server über Benutzername und Passwort • **WPA2-Enterprise** – RADIUS-Authentifizierung mit besserer Verschlüsselung • **802.1X** – RADIUS-Authentifizierung mit portbasierter Network Access Control (PNAC) unter Verwendung der Kapselung des Extensible Authentication Protocol (EAP) über LAN – EAPOL

Verschlüsselung	Datenverschlüsselungstyp in Wi-Fi-Netzwerken: • **None** – Keine Datenverschlüsselung • **WEP** – Verschlüsselung mit statischen WEP-Schlüsseln. Diese Verschlüsselung kann für die freigegebene Authentifizierung (Shared) verwendet werden. • **TKIP** – Dynamische Verschlüsselung, die sowohl für *WPA-PSK*- als auch *WPA2-PSK*- Authentifizierung verwendet werden kann. • **AES** – Verbesserte Verschlüsselung für *WPA2-PSK*- Authentifizierung
WEP Key Type	Typ des WEP-Schlüssels für WEP-Verschlüsselung: • **ASCII** – WEP-Schlüssel wird im ASCII-Format eingegeben • **HEX** – WEP-Schlüssel wird im Hexadezimal-Format eingegeben
WEP Default Key	Gibt WEP-Standardschlüssel an
WEP Key 1 – 4	Menüelemente für vier verschiedene WEP-Schlüssel • Der WEP-Schlüssel im ASCII-Format muss zwischen Anführungszeichen eingegeben werden und muss folgende Längen aufweisen: – 5 ASCII-Zeichen (40b WEP-Schlüssel) – 13 ASCII-Zeichen (104b WEP-Schlüssel) – 16 ASCII-Zeichen (128b WEP-Schlüssel) • Der WEP-Schlüssel im Hexadezimal-Format darf nur mit hexadezimalen Zahlen eingegeben werden. Dieser Schlüssel kann mit folgenden Längen festgelegt werden. – 10 Hexadezimalzahlen (40b WEP-Schlüssel) – 26 Hexadezimalzahlen (104b WEP-Schlüssel) – 32 Hexadezimalzahlen (128b WEP-Schlüssel)
WPA-PSK-Typ	Die möglichen Schlüsseloptionen für die WPA-PSK-Authentifizierung: • 256-Bit-Schlüssel • ASCII-Passphrase • PSK-Datei
WPA PSK	Schlüssel für WPA-PSK-Authentifizierung. Dieser Schlüssel muss wie folgt gemäß dem ausgewählten WPA-PSK-Typ eingegeben werden: • **256-bit secret** – 64 Hexadezimalzahlen • **ASCII passphrase** – von 8 bis 63 Zeichen • **PSK File** – absoluter Pfad zur Datei, die die Liste der Paare enthält (PSK-Schlüssel, MAC-Adresse)
RADIUS Auth Server IP	IPv4- oder IPv6-Adresse des RADIUS-Servers. Nur wenn eine der RADIUS-Authentifizierungen ausgewählt ist.
RADIUS Auth Password	Passwort für den Zugriff auf den RADIUS-Server. Nur wenn eine der RADIUS-Authentifizierungen ausgewählt ist.
RADIUS Auth Port	RADIUS-Server-Port. Der Standardwert ist 1812. Nur wenn eine der RADIUS-Authentifizierungen ausgewählt ist.
RADIUS Acct Server IP	IPv4- oder IPv6-Adresse des RADIUS-Accounting-Servers. Nur definieren, wenn vom Authentifizierungs- und Autorisierungsserver abweichend. Nur wenn eine der RADIUS-Authentifizierungen ausgewählt ist.
RADIUS Acct Password	Zugangspasswort des RADIUS-Accounting-Servers. Nur definieren, wenn vom Authentifizierungs- und Autorisierungsserver abweichend. Nur wenn eine der RADIUS-Authentifizierungen ausgewählt ist.
RADIUS Acct Port	RADIUS-Accounting-Server-Port. Der Standardwert ist 1813. Nur definieren, wenn er sich vom Authentifizierungs- und Autorisierungsserver unterscheidet. Nur wenn eine der RADIUS-Authentifizierungen ausgewählt ist.

Zugriffsliste	Bestimmt eine Zugangsart/Verweigerungsliste: • **Disabled** – Deaktiviert – Annahme-/Verweigerungsliste wird nicht verwendet • **Accept** – Nur Optionen, die in der Annahme-/Verweigerungsliste Zugang zum Netzwerk haben • **Deny** – Optionen, die in der Zugangs-/Verweigerungsliste erwähnt werden, haben keinen Zugang zum Netzwerk
Accept/Deny List	Annahme-/Verweigerungsliste der MAC-Adressen von Clients, die sich mit dem Netzwerk verbinden wollen. Jede MAC-Adresse wird separat in einer Zeile aufgeführt.
Syslog Level	Kommunikationslevel, wenn das System in das Systemprotokoll schreibt • **Verbose debugging** – Höchste Log-Stufe • **Debugging** • **Informational** – Standard-Log-Stufe • **Meldung** • **Warning** – Tiefste Log-Stufe
Weitere Optionen	Ermöglicht dem Benutzer, zusätzliche Parameter zu definieren

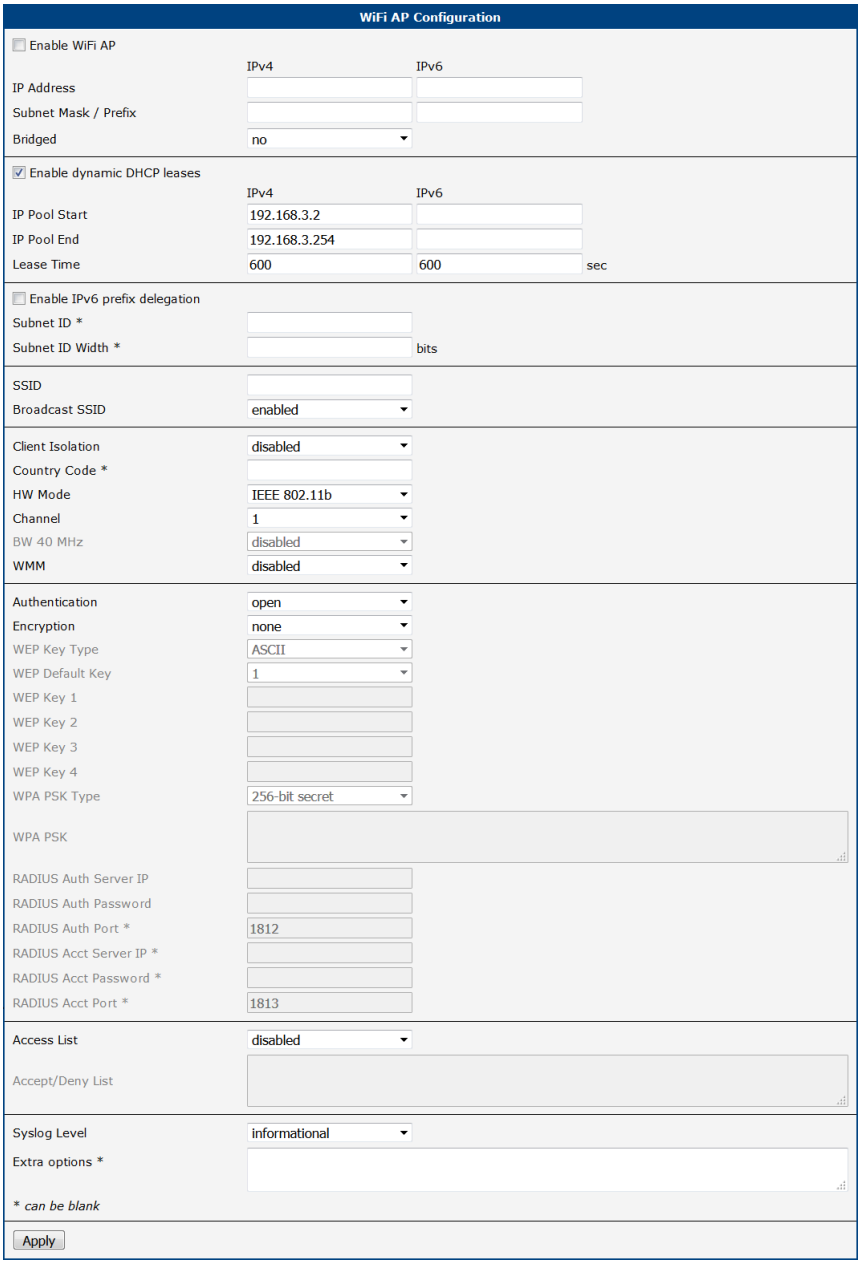


Abb. 31: Konfigurationsseite des Wi-Fi-Access-Points

5.6 Wi-Fi-Station-Konfiguration

HINWEIS Dieses Kapitel trifft nur zu, wenn der Router mit einem Wi-Fi-Modul ausgestattet ist.

Das Wi-Fi-Modul unterstützt den Multi-Role-Modus, der es ermöglicht, gleichzeitig als Access Point (AP) und Station (STA) zu arbeiten. Der Mehrkanalmodus wird ebenfalls unterstützt, sodass der AP und die STA auf unterschiedlichen Kanälen arbeiten können.

Aktivieren Sie den WLAN-Stationsmodus, indem Sie das Kontrollkästchen "**WiFi STA aktivieren"** oben auf der Konfigurationsseite "**Konfiguration > WLAN > Station"** aktivieren. In diesem Modus wird der Router zu einer Client-Station.
Er empfängt Datenpakete vom verfügbaren Access Point (AP) und sendet Daten per Kabelverbindung über das Wi-Fi-Netzwerk.
Sie können die folgenden Eigenschaften einstellen, die in der folgenden Tabelle aufgeführt sind.

Im Wi-Fi STA-Modus werden nur die Authentifizierungsmethoden EAP-PEAP/MSCHAPv2 (sowohl PEAPv0 als auch PEAPv1) und EAP-TLS unterstützt.

Tab. 30: Konfiguration der Wi-Fi-Station

Element	**Beschreibung**
Enable WiFi STA	WLAN-Station (STA) aktivieren.
DHCP-Client	Aktiviert/deaktiviert den DHCP-Client. In der Spalte IPv6 ist der DHCPv6-Client aktiviert.
IP Address	Eine feste IP-Adresse der Wi-Fi-Schnittstelle. Verwenden Sie die IPv4-Notation in der IPv4-Spalte und die IPv6-Notation in der IPv6-Spalte. Gekürzte IPv6-Notation wird unterstützt.
Subnet Mask / Prefix	Gibt eine Subnetzmaske für die IPv4-Adresse an. Geben Sie in der Spalte IPv6 das Präfix für die IPv6-Adresse ein – Zahl im Bereich 0 bis 128.
Default Gateway	Gibt die IP-Adresse eines Standardgateways an. Wenn ausgefüllt, wird jedes Paket, dessen Ziel nicht in der Routing-Tabelle gefunden wurde, dorthin gesendet. Verwenden Sie die richtige IP-Adressnotation in den Spalten IPv4 und IPv6.
DNS Server	Gibt die IP-Adresse des DNS-Servers an. Wenn die IP-Adresse in der Routing-Tabelle nicht gefunden wird, wird der DNS-Server angefordert. Verwenden Sie die richtige IP-Adressnotation in den Spalten IPv4 und IPv6.
SSID	Eindeutige Kennung des Wi-Fi-Netzwerks
Probe Hidden SSID	Prüft versteckte SSID
Country Code	Code des Landes, in dem der Router mit WLAN verwendet wird. Dieser Code muss im Format ISO 3166-1 alpha-2 eingegeben werden. Wenn kein Ländercode angegeben ist und der Router kein System implementiert hat, um diesen Code zu ermitteln, wird "US" als Standard-Ländercode verwendet. Wird kein Ländercode angegeben oder ein falscher Ländercode eingegeben, kann es zu einem Verstoß gegen die Regulierungsvorschriften für die Nutzung von Frequenzbändern im jeweiligen Land kommen.

Authentication	Stellt Zugangskontrolle für autorisierte Nutzer in Drahtlos-Netzwerken bereit: • **Open** – Keine Authentifizierung erforderlich (freier Zugangspunkt) • **Shared** (Freigegeben) – Basisauthentifizierung mittels eines WEP-Schlüssels. • **WPA-PSK** – Authentifizierung mit besserer Authentifizierungsmethode PSK-PSK • **WPA2-PSK** – Authentifizierung mit AES-Verschlüsselung • **WPA-Enterprise** – RADIUS-Authentifizierung durch externen Server über Benutzername und Passwort • **WPA2-Enterprise** – RADIUS-Authentifizierung mit besserer Verschlüsselung • **802.1X** – RADIUS-Authentifizierung mit portbasierter Network Access Control (PNAC) unter Verwendung der Kapselung des Extensible Authentication Protocol (EAP) über LAN – EAPOL
Verschlüsselung	Datenverschlüsselungstyp in Wi-Fi-Netzwerken: • **None** – Keine Datenverschlüsselung • **WEP** – Verschlüsselung mit statischen WEP-Schlüsseln. Diese Verschlüsselung kann für die freigegebene Authentifizierung (Shared) verwendet werden. • **TKIP** – Dynamische Verschlüsselung, die sowohl für *WPA-PSK*- als auch *WPA2-PSK*- Authentifizierung verwendet werden kann. • **AES** – Verbesserte Verschlüsselung für *WPA2-PSK*- Authentifizierung
WEP-Schlüsseltyp	Typ des WEP-Schlüssels für WEP-Verschlüsselung: • **ASCII** – WEP-Schlüssel wird im ASCII-Format eingegeben • **HEX** – WEP-Schlüssel wird im Hexadezimal-Format eingegeben
WEP Default Key	Gibt WEP-Standardschlüssel an
WEP Key 1 – 4	Menüelemente für vier verschiedene WEP-Schlüssel • Der WEP-Schlüssel im ASCII-Format muss zwischen Anführungszeichen eingegeben werden und muss folgende Längen aufweisen: – 5 ASCII-Zeichen (40b WEP-Schlüssel) – 13 ASCII-Zeichen (104b WEP-Schlüssel) – 16 ASCII-Zeichen (128b WEP-Schlüssel) • Der WEP-Schlüssel im Hexadezimal-Format darf nur mit hexadezimalen Zahlen eingegeben werden. Dieser Schlüssel kann mit folgenden Längen festgelegt werden. – 10 Hexadezimalzahlen (40b WEP-Schlüssel) – 26 Hexadezimalzahlen (104b WEP-Schlüssel) – 32 Hexadezimalzahlen (128b WEP-Schlüssel)
WPA-PSK-Typ	Die möglichen Schlüsseloptionen für die WPA-PSK-Authentifizierung: • 256-Bit-Schlüssel • ASCII-Passphrase • PSK-Datei
WPA PSK	Schlüssel für WPA-PSK-Authentifizierung. Dieser Schlüssel muss wie folgt gemäß dem ausgewählten WPA-PSK-Typ eingegeben werden: • **256-bit secret** – 64 Hexadezimalzahlen • **ASCII passphrase** – von 8 bis 63 Zeichen • **PSK File** – absoluter Pfad zur Datei, die die Liste der Paare enthält (PSK-Schlüssel, MAC-Adresse)
RADIUS EAP Authentication	Art des Authentifizierungsprotokolls (EAP-PEAP/MSCHAPv2 oder EAP-TLS).
RADIUS CA Certificate	Definition des CA-Zertifikats für das EAP-TLS-Authentifizierungsprotokoll.
RADIUS Local Certificate	Definition des lokalen Zertifikats für das EAP-TLS-Authentifizierungsprotokoll.

RADIUS Local Private Key	Definition des lokalen privaten Schlüssels für das EAP-TLS-Authentifizierungsprotokoll.
RADIUS Identity	RADIUS-Benutzername – Identität. Nur wenn eine der RADIUS-Authentifizierungen ausgewählt ist.
RADIUS Password	Passwort für den RADIUS-Zugang. Nur wenn eine der RADIUS-Authentifizierungen ausgewählt ist.
Syslog Level	Kommunikationslevel, wenn das System in das Systemprotokoll schreibt • **Verbose debugging** – Höchste Log-Stufe • **Debugging** • **Informational** – Standard-Log-Stufe • **Meldung** • **Warning** – Tiefste Log-Stufe
Weitere Optionen	Ermöglicht dem Benutzer, zusätzliche Parameter zu definieren

Die Änderungen der Einstellungen wirken sich nach Betätigung der Schaltfläche **Apply** aus.

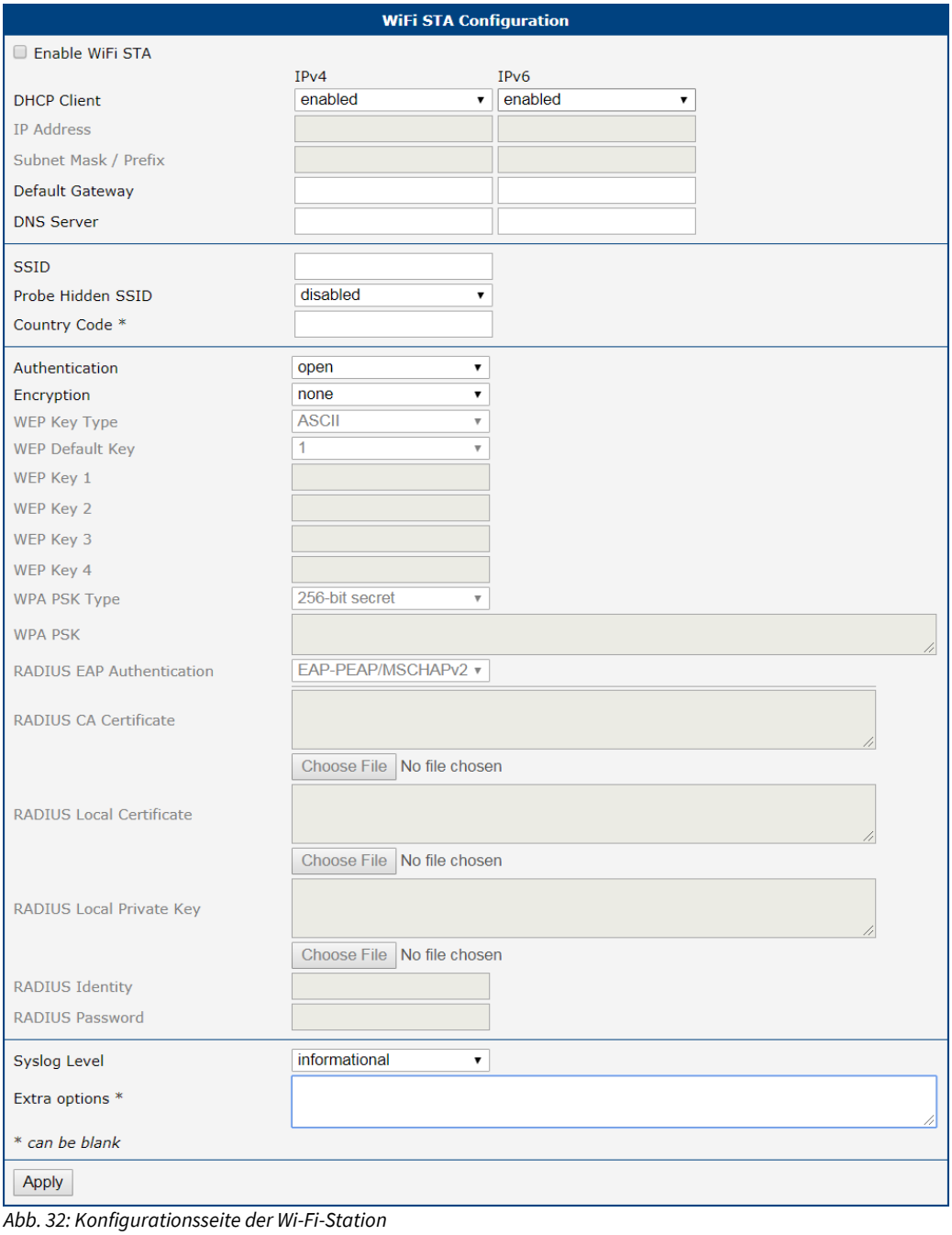


Abb. 32: Konfigurationsseite der Wi-Fi-Station

5.7 Backup-Routen

Mithilfe des Konfigurationsformulars auf der Seite **Backup Routen** können Sie die primäre Verbindung mit alternativen Verbindungen zum Internet (mobiles Netzwerk) sichern oder den Modus **Mehrere WANs** aktivieren. Es ist auch möglich, jede Backup-Verbindungsoption zu priorisieren. Die Umschaltung zwischen Verbindungen erfolgt nach Priorität und Status der Verbindungen.

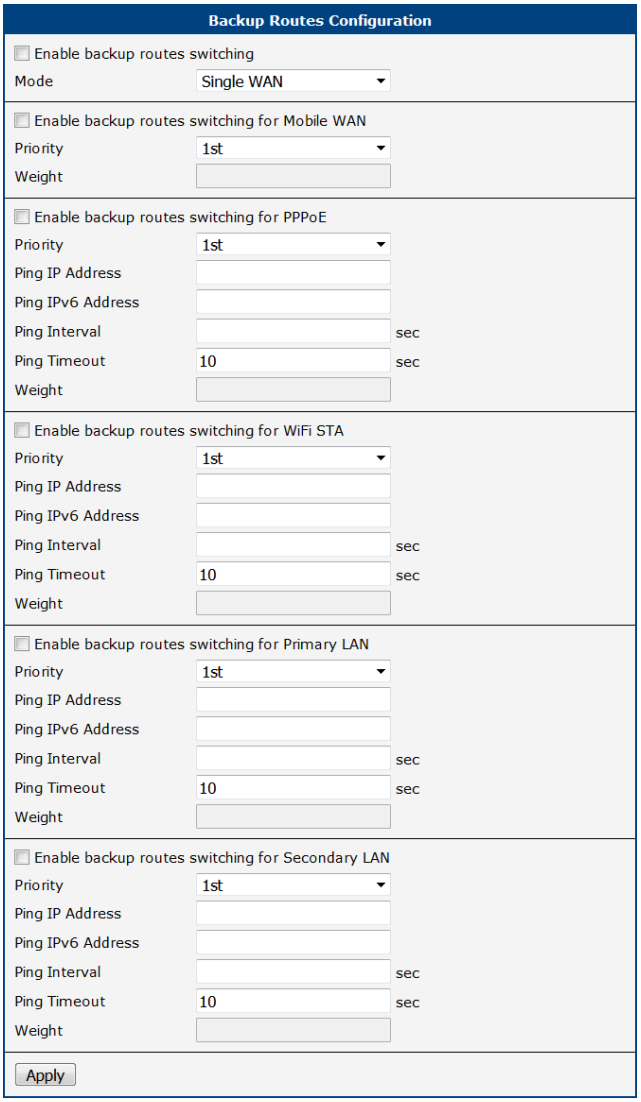


Abb. 33: Konfigurationsseite der Backup-Routen

Tab. 31: Bestimmung der Backup-Routen

Element	Beschreibung
Enable backup routes switching	Die Standardroute wird gemäß den folgenden Einstellungen ausgewählt. Wenn deaktiviert (nicht markiert), arbeitet das Backup-Routen-System im Abwärtskompatibilitätsmodus basierend auf den Standardprioritäten der Netzwerkschnittstellen (unten aufgelistet).
Mode	• **Single WAN** – Der Standardmodus. Es wird immer nur eine Schnittstelle für die WAN-Kommunikation verwendet. Andere Schnittstellen werden für WAN verwendet, wenn die bevorzugte Schnittstelle ausfällt, basierend auf den festgelegten Prioritäten. • **Mehrere WANs** – Mehrere Schnittstellen können für die WAN-Verbindung verwendet werden. Wenn WAN-Kommunikation über mehrere Schnittstellen empfangen wird, wird daher dieselbe Schnittstelle als Antwort verwendet; der Verkehr bleibt auf der angegebenen Schnittstelle. Die eingestellten Prioritäten werden bei der Datenübertragung vom Router oder aus dem Netzwerk hinter dem Router verwendet. Für diese Übertragungen wird die Schnittstelle mit der höchsten Priorität verwendet. • **Load Balancing** – In diesem Modus kann die Gewichtung für jede Schnittstelle eingestellt werden. Diese Einstellung bestimmt die relative Anzahl der Datenströme, die durch die Schnittstellen gehen. Bitte beachten Sie, dass dies möglicherweise nicht genau der Datenmenge entspricht, es hängt stark von der Anzahl der Streams und der Struktur der Daten ab

Um die Netzwerkschnittstellen zum Backup-Routen-System hinzuzufügen, markieren Sie die Checkbox(en) der folgenden Schnittstellenoptionen:
Enable backup routes switching for Mobile WAN, **Enable backup routes switching for PPPoE**, **Enable backup routes switching for WiFi STA**, **Enable backup routes switching for Primary LAN**, **Enable backup routes switching for Secondary LAN** oder **Enable backup routes switching for Tertiary LAN**. Aktivierte Schnittstellen werden dann für den WAN-Zugriff entweder im Modus **Single WAN** (nur eine Schnittstelle gleichzeitig) oder im Modus **Multiple WANs** (mehrere Schnittstellen gleichzeitig) verwendet, basierend auf gesetzten Prioritäten:



Wenn Sie die Verbindung zum mobilen WAN als eine der Backup-Routen verwenden möchten, müssen Sie die Option **enable + bind** im Element **Check Connection** auf der Seite **Mobile WAN** auswählen und die Ping-Adresse eingeben, siehe Kapitel 5.3.1 "Mobilfunkverbindung", S. 39.

Netzwerkschnittstellen, die zu einzelnen Backup-Routen gehören, werden auch vor der Verwendung auf Flags überprüft, die den Zustand der Schnittstelle anzeigen (z. B. RUNNING auf der Seite **Network Status**). Dadurch wird beispielsweise das Abziehen eines Ethernet-Kabels verhindert. Sie können eine oder beide Ping-IP-Adressen (IPv4 und IPv6) eingeben – basierend auf dem IP-Protokoll, das für eine bestimmte Netzwerkschnittstelle und WAN-Verbindungseinstellungen verwendet wird. IPv4 und IPv6 sind als Dual-Stack im Router implementiert.

Die Änderungen der Einstellungen wirken sich nach Betätigung der Schaltfläche **Apply** aus.

Tab. 32: Konfiguration der Backup-Routen

Element	Beschreibung
Priorität	Priorität für die Verbindungsart (Netzwerkschnittstelle)
Ping IP Address	Ziel-IPv4-Adresse oder Domänenname von Ping-Anfragen, zur Überprüfung der Verbindung.
Ping IPv6 Address	Ziel-IPv6-Adresse oder Domänenname von Ping-Anfragen zur Überprüfung der Verbindung.
Ping-Intervall	Die Zeitintervalle zwischen aufeinanderfolgenden Ping-Anfragen
Ping Timeout	Zeit in Sekunden für das Warten auf eine Antwort.
Gewicht	Gewichtung nur für den Load-Balancing-Modus. Die Zahl von 1 bis 256 bestimmt das Verhältnis für den Lastausgleich der Schnittstelle. Wenn beispielsweise zwei Schnittstellen die Gewichtung auf 1 eingestellt haben, beträgt das Verhältnis 50% zu 50%. Wenn sie das Gewicht auf 1 und 4 eingestellt haben, beträgt das Verhältnis 20% zu 80%.

Standardprioritäten für Backup-Routen

Wenn das Kontrollkästchen **Enable backup routes switching** deaktiviert ist, arbeitet das Backup-Routen-System im Abwärtskompatibilitätsmodus. Der Router wählt die Route basierend auf den Standardprioritäten der aktivierten Einstellungen für jede der Netzwerkschnittstellen aus, wodurch geeignete Dienste aktiviert werden, die diesen Netzwerkschnittstellen entsprechen. Die folgende Liste enthält die Namen der Backup-Routen und der entsprechenden Netzwerkschnittstellen in der Reihenfolge der Standardprioritäten:

- Mobile WAN (pppX, usbX)
- PPPoE (ppp0)
- WiFi STA (wlan0)
- Sekundäres LAN bzw. ETH1 (eth1)
- Tertiäres LAN (eth2)
- Primäres LAN bzw. ETH0 (eth0)

Beispiel für Standardprioritäten:

Die Funktion **Backup-Routen** ist deaktiviert. Der Router wählt das **Secondary LAN/ETH1** nur dann als Standardroute aus, wenn Sie das Kontrollkästchen **Create connection to mobile network** auf der Seite **Mobile WAN** deaktivieren, das Kontrollkästchen **Create PPPoE connection** auf der Seite **PPPoE** deaktivieren und **Enable WiFi STA** auf der Seite **WiFi > Station** ebenfalls deaktivieren. Um das **Primary LAN/ETH0** auszuwählen, löschen Sie die IP-Adresse auf der Seite **Secondary LAN/ETH1** und deaktivieren Sie den **DHCP-Client** für das **Secondary LAN/ETH1**.

HINWEIS Bedenken Sie, dass es ein Konzept variabler WAN- und LAN-Schnittstellen gibt, auch wenn die Backup-Routen nicht aktiviert sind. Es kann vorkommen, dass die vom LAN vorgesehene Schnittstelle zur WAN-Schnittstelle wird (aufgrund von festgelegten oder voreingestellten Prioritäten). Die Kommunikation von WAN-Schnittstelle zu LAN-Schnittstelle kann dann je nach **NAT** und **Firewall Configuration** blockiert werden.

5.8 Statische Routen

Statische Routen können auf der Konfigurationsseite **Static Routes** angegeben werden. Eine statische Route bietet einen festen Routing-Pfad durch das Netzwerk. Sie wird manuell auf dem Router konfiguriert und muss aktualisiert werden, wenn die Netzwerktopologie kürzlich geändert wurde. Statische Routen sind private Router, es sei denn, sie werden durch ein Routing-Protokoll neu verteilt. Das Konfigurationsformular für statische Routen ist in der folgenden Abbildung dargestellt.

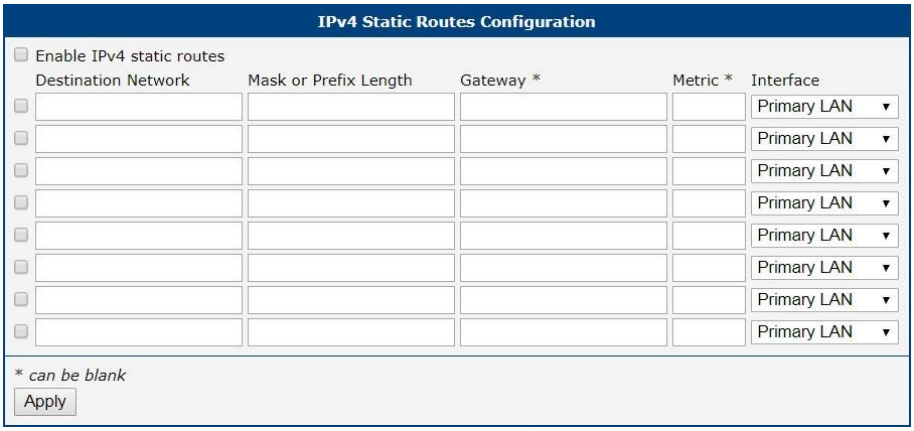


Abb. 34: Konfiguration der statischen Routen

Tab. 33: Konfiguration statischer Routen

Element	**Beschreibung**
Enable IP static routes	Wenn diese Option aktiviert ist, wird die statische Routing-Funktionalität aktiviert. Aktiv sind nur Routen, die durch das Kontrollkästchen in der ersten Spalte der Tabelle aktiviert sind.
Destination Network	Die Ziel-IP-Adresse des entfernten Netzwerks oder Hosts, dem Sie eine statische Route zuweisen möchten.
Mask or Prefix Length	Die Subnetzmaske des Remote-Netzwerks oder die Host-IP-Adresse.
Gateway	IP-Adresse des Gateway-Geräts, das den Kontakt zwischen dem Router und dem entfernten Netzwerk oder Host ermöglicht.
Metric	Metrik-Definition, bedeutet Nummernbewertung der Priorität für die Route in der Routingtabelle. Routen mit niedrigeren Metriken haben eine höhere Priorität.
Interface	Wählen Sie eine Schnittstelle aus, auf der sich das Remote-Netzwerk oder der Host befindet.

5.9 Firewall-Konfiguration

Das erste Sicherheitselement für eingehende Pakete ist eine Überprüfung der aktivierten Quell-IP-Adressen und Zielports.
Es gibt eine unabhängige IPv4- und IPv6-Firewall, da im Router Dual-Stack-IPv4 und IPv6 implementiert sind. Wenn Sie links im Menü **Konfiguration** auf das Element **Firewall** klicken, werden die Optionen **IPv4** und **IPv6** erweitert und Sie können auf **IPv6** klicken, um die IPv6-Firewall zu aktivieren und zu konfigurieren – siehe Abbildung unten. Die Konfigurationsfelder haben in den Formularen **IPv4-Firewall-Konfiguration** und **IPv6-Firewall-Konfiguration** dieselbe Bedeutung.

Sie können die Regeln für IP-Adressen, Protokolle und Ports festlegen, um den Zugriff auf den Router und das hinter dem Router angeschlossene interne Netzwerk zuzulassen oder zu verweigern. Um diese Funktion zu aktivieren, aktivieren Sie das Kontrollkästchen **Filterung eingehender Pakete aktivieren** oben auf der Seite **IPv4 (IPv6) Firewall Configuration**. Die Erreichbarkeit wird anhand der IP-Adresstabelle geprüft.
Das bedeutet, dass nur auf die in der Tabelle erlaubten Adressen zugegriffen werden darf. Es ist möglich, bis zu acht Remote-IP-Adressen für Zugriff/Verweigerung anzugeben.
Sie können die folgenden Parameter angeben:

Tab. 34: Filtern der eingehenden Pakete

Element	**Beschreibung**
Source	IP-Adresse, für die die Regel gilt. Verwenden Sie die IPv4-Adresse in der **IPv4-Firewall-Konfiguration** und die IPv6-Adresse in der **IPv6-Firewall-Konfiguration**.
Protokoll	Gibt das Protokoll an, für das die Regel gilt: • **all** – Regeln gelten für alle Protokolle • **TCP** – Regeln gelten für TCP-Protokoll • **UDP** – Regeln gelten für UDP-Protokoll • **ICMP/ICMPv6** – Regeln gelten für ICMP-Protokoll. Bei IPv6 Firewall-Konfiguration gibt es die ICMPv6-Option.
Target Port(s)	Der Portnummernbereich, der den Zugriff auf den Router ermöglicht. Geben Sie die niedrigste und die höchste Portnummer getrennt durch den Bindestrich ein. Ein statischer Port ist ebenfalls zulässig.
Action	Gibt die Regel an – die Art der Aktion, die der Router ausführt: • **allow** – Der Router lässt die Pakete in das Netzwerk eintreten. • **deny** – Der Router verweigert den Paketen den Zugang zum Netzwerk.
Description	Beschreibung der Regel

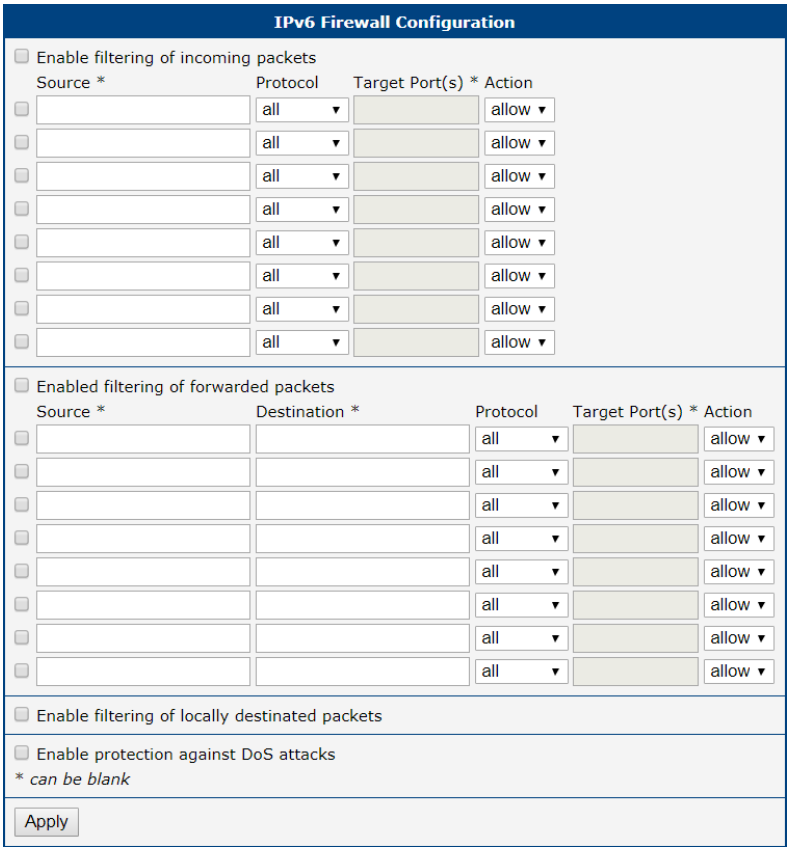


Abb. 35: Firewall-Konfiguration – IPv6 Firewall

Der folgende Teil des Konfigurationsformulars definiert die Weiterleitungsrichtlinie. Wenn das Element **Enabled filtering of forwarded packets** nicht aktiviert ist, werden Pakete automatisch akzeptiert.

Wenn Sie diese Funktion aktivieren und ein Paket an eine andere Netzwerkschnittstelle adressiert ist, sendet der Router das Paket an die FORWARD-Kette. Wenn die FORWARD-Kette das Paket akzeptiert und es eine Regel für die Weiterleitung gibt, sendet der Router das Paket. Wenn eine Weiterleitungsregel nicht verfügbar ist, verwirft der Router das Paket.

Dieses Konfigurationsformular enthält auch eine Tabelle zur Angabe der Filterregeln. Sie können eine Regel erstellen, um Daten mit dem ausgewählten Protokoll zuzulassen, indem Sie nur das Protokoll angeben, oder strengere Regeln erstellen, indem Sie Werte für Quell-IP-Adressen, Ziel-IP-Adressen und Ports angeben.

Tab. 35: Forward-Filterung

Element	Beschreibung
Source	IP-Adresse, für die die Regel gilt. Verwenden Sie die IPv4-Adresse in der **IPv4-Firewall-Konfiguration** und die IPv6-Adresse in der **IPv6-Firewall-Konfiguration**.
Destination	Ziel-IP-Adresse, für die die Regel gilt. Verwenden Sie die IPv4-Adresse in der **IPv4-Firewall-Konfiguration** und die IPv6-Adresse in der **IPv6-Firewall-Konfiguration**.
Protokoll	Gibt das Protokoll an, für das die Regel gilt: • **all** – Regeln gelten für alle Protokolle • **TCP** – Regeln gelten für TCP-Protokoll • **UDP** – Regeln gelten für UDP-Protokoll • **ICMP/ICMPv6** – Regeln gelten für ICMP-Protokoll. Bei IPv6 Firewall-Konfiguration gibt es die ICMPv6-Option.
Target Port(s)	Die Ziel-Portnummern. Geben Sie die niedrigste und die höchste Portnummer getrennt durch den Bindestrich ein. Ein statischer Port ist ebenfalls zulässig.
Action	Gibt die Regel an – die Art der Aktion, die der Router ausführt: • **allow** – Der Router lässt die Pakete in das Netzwerk eintreten. • **deny** – Der Router verweigert den Paketen den Zugang zum Netzwerk.
Description	Beschreibung der Regel

Wenn Sie die Funktion **Enable filtering of locally destined packets** aktivieren, verwirft der Router die Pakete, die einen nicht unterstützten Dienst anfordern. Das Paket wird automatisch ohne Informationen verworfen.

Als Schutz vor DoS-Angriffen begrenzt **Enable protection against DoS attacks** die Anzahl der zulässigen Verbindungen pro Sekunde auf fünf. Der DoS-Angriff überflutet das Zielsystem mit sinnlosen Anforderungen.

Beispiel der Firewall-Konfiguration

Der Router hat folgenden Zugang erlaubt:

- von der Adresse 171.92.5.45 mittels eines jeglichen Protokolls
- von der Adresse 10.0.2.123 mit Hilfe des Protokolls TCP an Port 1000
- von der Adresse 142.2.26.54 mit Hilfe des Protokolls ICMP
- von IP-Adresse 14.2.2.6.54 unter Verwendung des TCPP-Protokolls auf Zielports von 1020 bis 1040

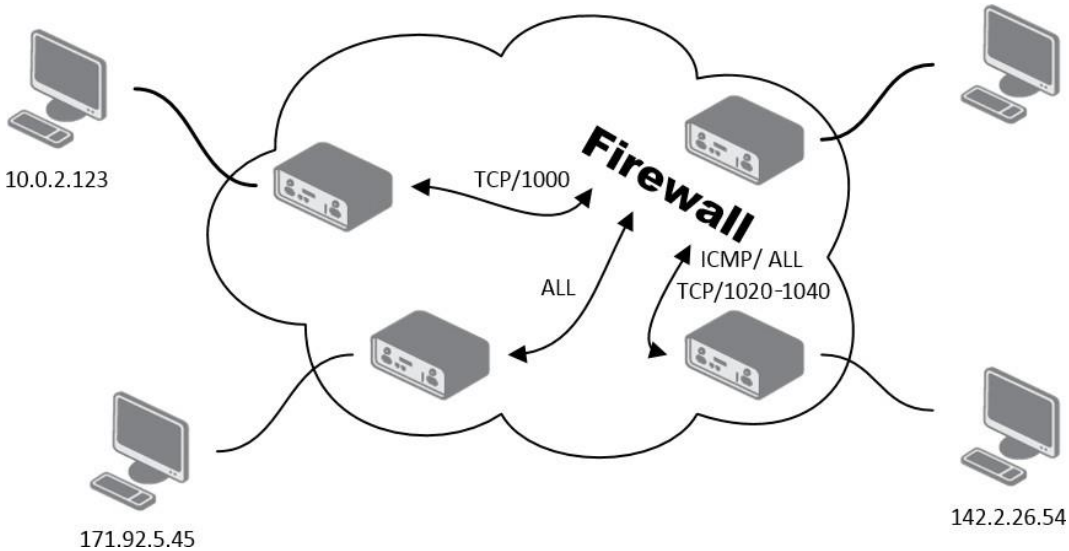


Abb. 36: Beispiel für die Topologie einer IPv4-Firewall-Konfiguration

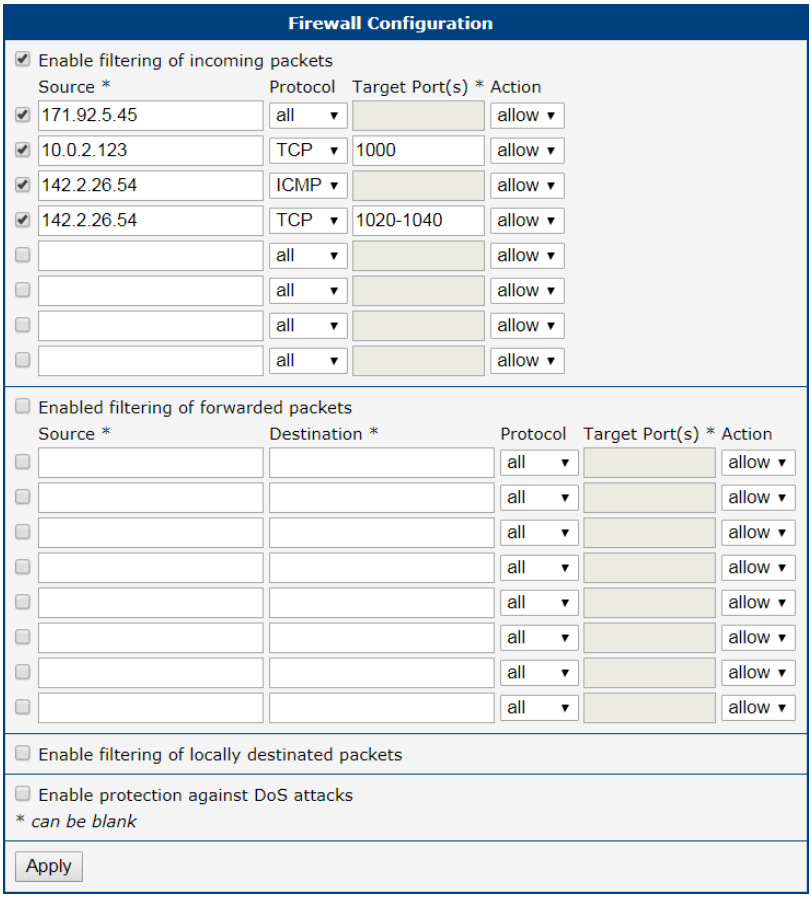


Abb. 37: Beispiel für die IPv4-Firewall-Konfiguration

5.10 NAT-Konfiguration

Um die Adressübersetzungsfunktion zu konfigurieren, klicken Sie im Hauptmenü im Abschnitt **Konfiguration** auf **NAT**. Es gibt eine unabhängige IPv4- und IPv6-NAT-Konfigurationen, da im Router Dual-Stack-IPv4 und IPv6 implementiert sind. Das Element **NAT** im Menü auf der linken Seite erweitert sich zu IPv4- und IPv6-Optionen und Sie können auf IPv6 klicken, um IPv6-NAT zu aktivieren und zu konfigurieren – siehe Abbildung unten.
Die Konfigurationsfelder haben in den Formularen **IPv4 NAT Configuration** und **IPv6 NAT Configuration** dieselbe Bedeutung.

Der Router verwendet tatsächlich Port Address Translation (PAT), eine Methode zum Zuordnen eines TCP/UDP-Ports zu einem anderen TCP/UDP-Port. Der Router modifiziert die Informationen im Paket-Header, wenn die Pakete einen Router durchlaufen. In diesem Konfigurationsformular können Sie bis zu 16 PAT-Regeln angeben.

Tab. 36: NAT-Konfiguration

Element	**Beschreibung**
Public Port(s)	Der öffentliche Portnummernbereich für NAT. Geben Sie die niedrigste und höchste Portnummer, getrennt durch Bindestrich ein. Ein statischer Port ist ebenfalls zulässig.
Private Port(s)	Der private Portnummernbereich für NAT. Geben Sie die niedrigste und höchste Portnummer, getrennt durch Bindestrich ein. Ein statischer Port ist ebenfalls zulässig.
Type	Protokolltyp – TCP oder UDP.
Server IPv4 address	Nur in **IPv4-NAT-Konfiguration**. IPv4-Adresse, an die der Router eingehende Daten weiterleitet.
Server IPv6 Adresse	Nur in **IPv6-NAT-Konfiguration**. IPv6-Adresse, an die der Router eingehende Daten weiterleitet.
Description	Beschreibung der Regel

Wenn Sie mehr als sechzehn NAT-Regeln benötigen, fügen Sie die restlichen Regeln in das Startup-Skript ein. Das Dialogfeld **Startskript** befindet sich auf der Seite **Skripte** im Abschnitt **Konfiguration** des Menüs.
Verwenden Sie beim Erstellen Ihrer Regeln im Startup-Skript diesen Befehl für IPv4 NAT::

```
iptables -t nat -A pre_nat -p tcp --dport [PORT_PUBLIC] -j DNAT --to-
destination [IPADDR]:[PORT_PRIVATE]
```

Geben Sie die IP-Adresse [IPADDR], die öffentlichen Portnummern [PORT_PUBLIC] und den privaten [PORT_PRIVATE] anstelle von eckigen Klammern ein.
Verwenden Sie für IPv6-NAT den Befehl `ip6tables` mit denselben Optionen.

```
ip6tables -t nat -A napt -p tcp --dport [PORT_PUBLIC] -j DNAT --to-
destination [IP6ADDR]:[PORT_PRIVATE]
```

Wenn Sie die folgenden Optionen aktivieren und die Portnummer eingeben, ermöglicht Ihnen der Router den Fernzugriff auf den Router über die WAN-Schnittstelle (Mobiles WAN).

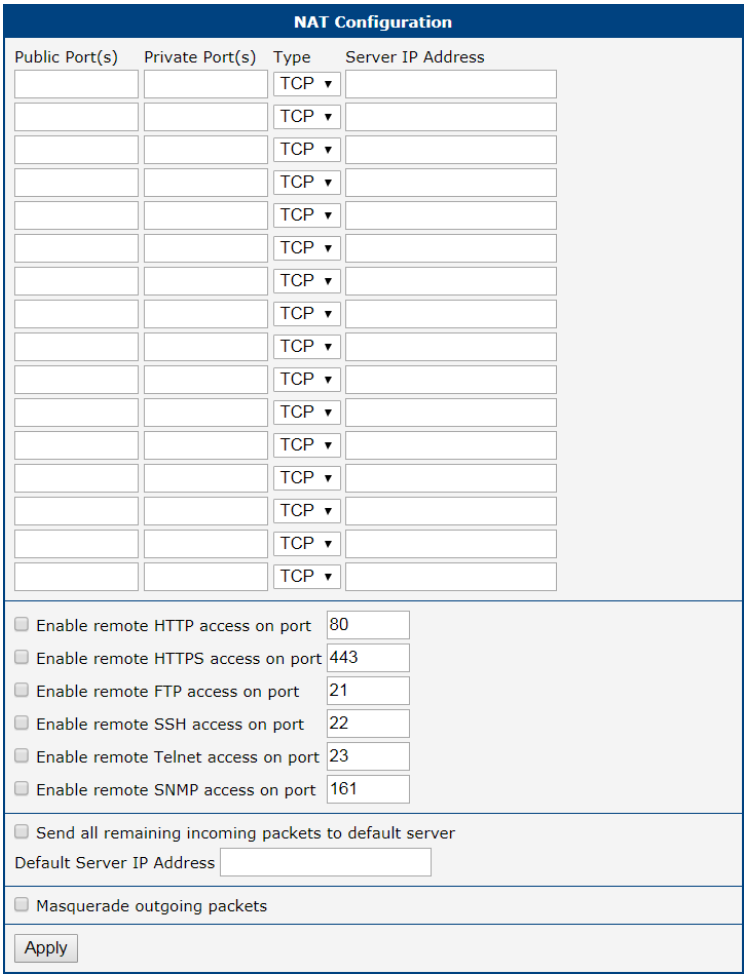


Abb. 38: Konfigurationsseite für IPv6 NAT

Tab. 37: Konfiguration des Remotezugriffs

Element	Beschreibung
Enable remote HTTP access on port	Diese Option legt die Umleitung von HTTP nur auf HTTPS fest (in der Standardkonfiguration deaktiviert).
Enable remote HTTPS access on port	Wenn Feld und Portnummer ausgefüllt sind, ist die Konfiguration des Routers über das Webinterface erlaubt (in der Standardkonfiguration deaktiviert).
Enable remote FTP access on port	Wählen Sie diese Option, um den Zugriff auf den Router über FTP zuzulassen (in der Standardkonfiguration deaktiviert).
Enable remote SSH access on port	Wählen Sie diese Option, um den Zugriff auf den Router über SSH zuzulassen (in der Standardkonfiguration deaktiviert).
Enable remote Telnet access on port	Wählen Sie diese Option, um den Zugriff auf den Router über Telnet zuzulassen (in der Standardkonfiguration deaktiviert).
Enable remote SNMP access on port	Wählen Sie diese Option, um den Zugriff auf den Router über SNMP zuzulassen (in der Standardkonfiguration deaktiviert).
Masquerade outgoing packets	Aktiviert/deaktiviert die Funktion zur Übersetzung von Netzwerkadressen.



Enable remote HTTP access on port aktiviert nur die Weiterleitung von HTTP- zu HTTPS-Protokoll. Der Router erlaubt kein ungesichertes HTTP-Protokoll, um Zugang zur Webkonfiguration zu erhalten. Um Zugang zur Webkonfiguration zu erhalten, stets die Option **Enable remote HTTPS access on port** überprüfen. Niemals die Option HTTP aktivieren, nur um Zugang zur Webkonfiguration aus dem Internet zu erhalten (Konfiguration wäre vom Internet nicht zugänglich). Stets die Option HTTPS und die Option HTTP zusammen prüfen (um die Weiterleitung von HTTP einzustellen).

Verwenden Sie die folgenden Parameter, um das Routing eingehender Daten aus dem WAN (Mobile WAN) zu einem angeschlossenen Computer einzustellen.

Tab. 38: Konfiguration aller eingehenden Pakete

Element	**Beschreibung**
Send all remaining incoming packets to default server	Aktiviert/deaktiviert die Weiterleitung nicht übereinstimmender eingehender Pakete an den Standardserver. Voraussetzung für die Funktion ist, dass Sie im Feld Default Server IPv4/IPv6 Address einen Standardserver angeben. Der Router kann eingehende Daten von einem GPRS an einen Computer mit der zugewiesenen IP-Adresse weiterleiten.
Default Server IP Address	Nur in **IPv4-NAT-Konfiguration**; IPv4-Adresse.
Default Server IPv6 Address	Nur in **IPv6-NAT-Konfiguration**; IPv6-Adresse.

Durch die Aktivierung der nachfolgenden Optionen und die Eingabe der Nummer des Ports wird der entfernte Zugang zum Router vom Internet erlaubt.

Beispiel 1: Konfiguration mit einem an den Router angeschlossenen Gerät

Es ist wichtig, das Kontrollkästchen **Alle verbleibenden eingehenden Pakete an Standardserver senden** für diese Konfiguration zu markieren. Die IP-Adresse in diesem Beispiel ist die Adresse des Geräts hinter dem Router. Das Standard-Gateway der Geräte im Subnetzwerk, die mit dem Router verbunden sind, ist dieselbe IP-Adresse, die im Feld **IPv4-Standardadresse des Servers** angezeigt wird. Das verbundene Gerät antwortet, wenn ein Ping an die IP-Adresse der SIM-Karte gesendet wird.

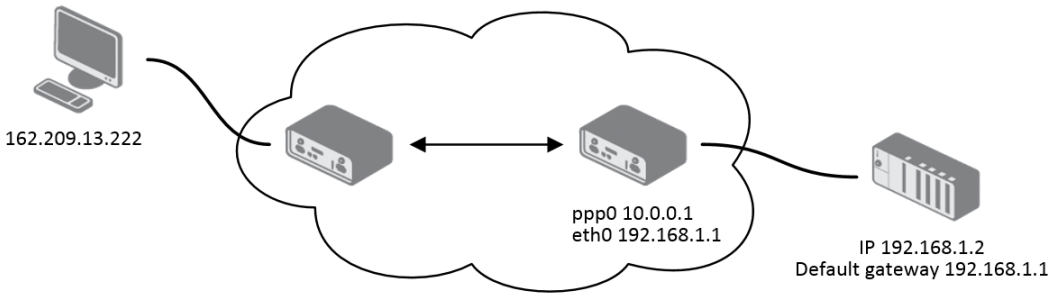


Abb. 39: Beispiel 1 – Topologie für die Konfiguration von NAT

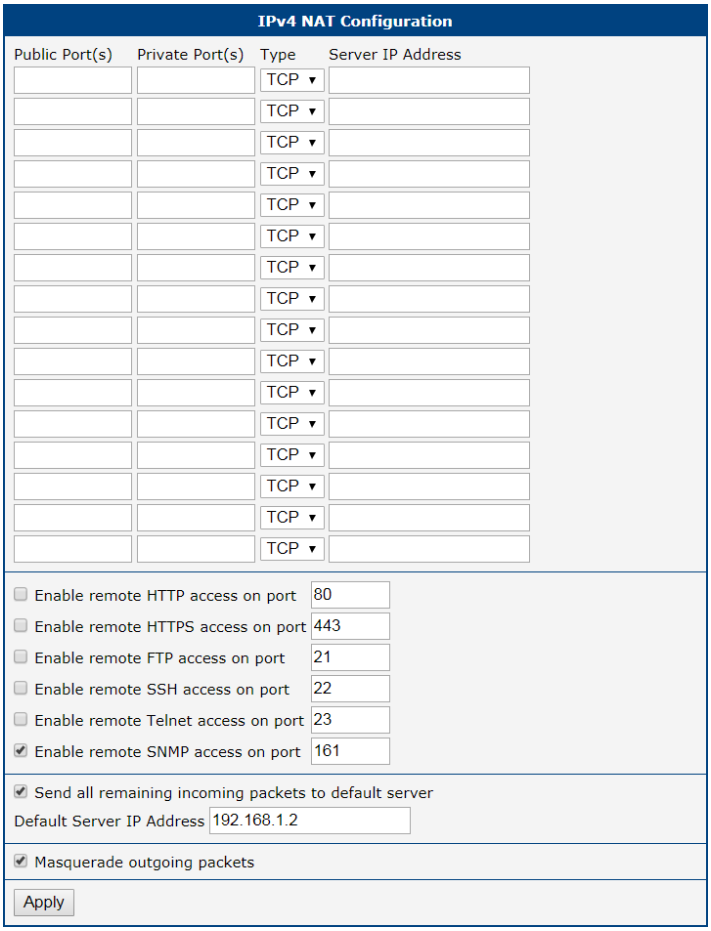


Abb. 40: Beispiel 1 – Konfigurationsseite für IPv4 NAT

Beispiel 2: Konfiguration mit mehreren Geräten am Router

In diesem Beispiel können Sie mit dem Switch weitere Geräte hinter dem Router anschließen. Jedes hinter dem Router angeschlossene Gerät hat eine eigene IP-Adresse. Geben Sie die Adresse in das Feld **Server IP Address** im NAT-Dialogfeld ein. Die Geräte kommunizieren über Port 80, aber Sie können die Portweiterleitung mit den Feldern **Public Port** und **Private Port** im NAT-Dialog einstellen. Sie haben den Router nun so konfiguriert, dass er beim Zugriff auf die IP-Adresse 10.0.0.1:81 aus dem Internet auf die 192.168.1.2:80-Socket hinter dem Router zugreift. Wenn Sie eine Ping-Anfrage an die öffentliche IP-Adresse des Routers (10.0.0.1) senden, antwortet der Router wie gewohnt (keine Weiterleitung).
Und da **Alle verbleibenden eingehenden Pakete an den Standardserver senden** inaktiv ist, verweigert der Router Verbindungsversuche.

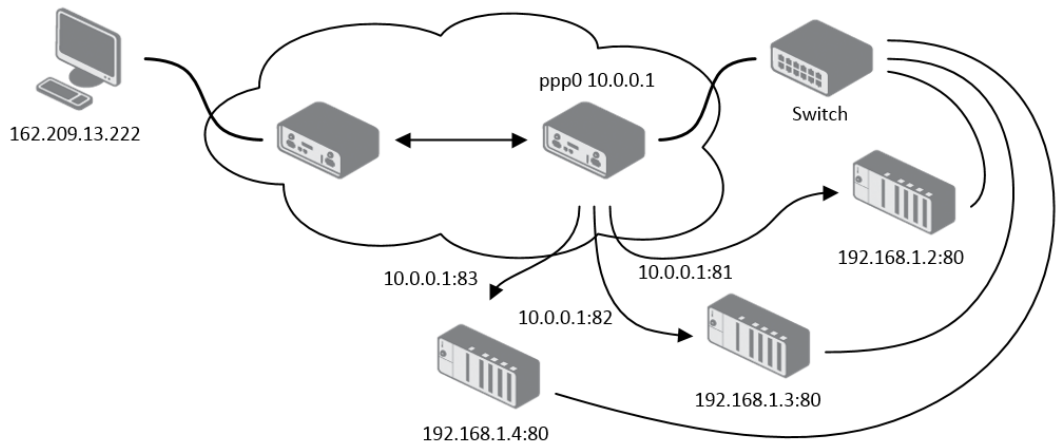


Abb. 41: Beispiel 2 – Topologie für die Konfiguration von NAT

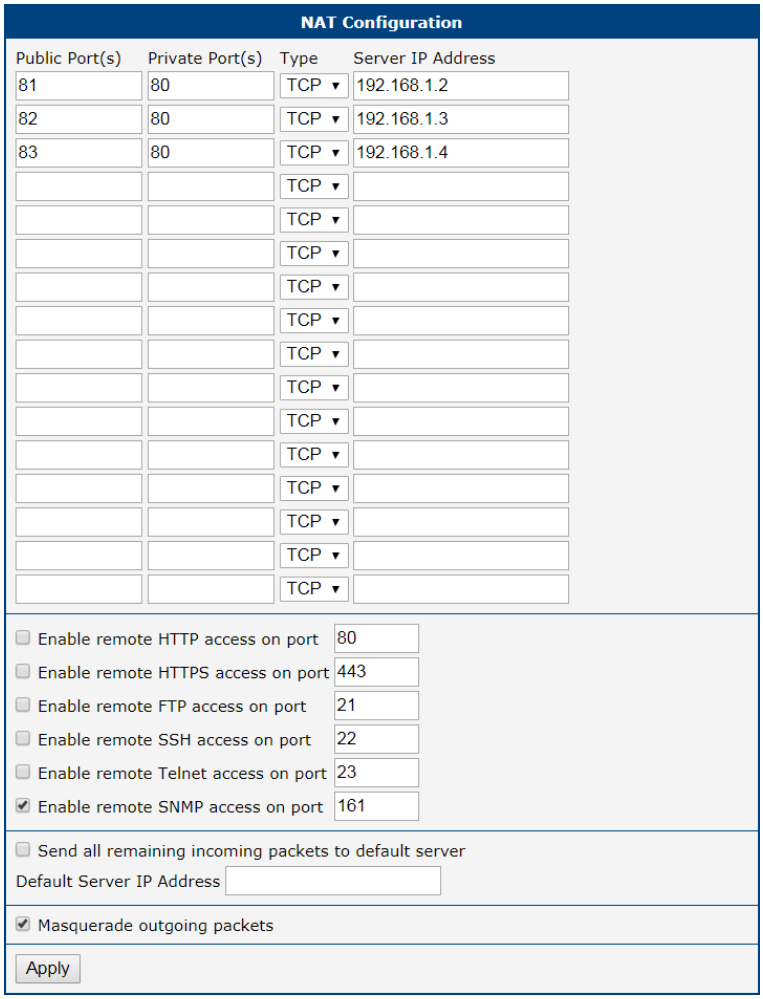


Abb. 42: Beispiel 2 – Konfiguration der Adressenübersetzung (NAT)

5.11 Konfiguration des OpenVPN-Tunnels

Wählen Sie das Element **OpenVPN** aus, um einen OpenVPN-Tunnel zu konfigurieren.
Das Menüelement wird erweitert und Sie können vier separate Konfigurationsseiten sehen: **1. Tunnel**, **2. Tunnel**, **3. Tunnel** und **4. Tunnel**. Mit der OpenVPN-Tunnelfunktion können Sie eine sichere Verbindung zwischen zwei getrennten LAN-Netzwerken herstellen. Mit dem Router können Sie bis zu vier OpenVPN-Tunnel erstellen. IPv4- und IPv6-Dual-Stack wird unterstützt.

Tab. 39: Konfiguration des OpenVPN-Tunnels für v2 Router

Element	**Beschreibung**
Description	Beschreibung (oder Bezeichnung) des Tunnels
Interface Type	TAP befindet sich auf dem Ethernetebene (Schicht 2) und agiert als ein Switch, wohingegen TUN auf der Netzwerkebene (Schicht 3) arbeitet und das Routing von Paketen im VPN übernimmt. TAP fungiert also als Bridge und TUN als Router. • **TUN** – Wählen des TUN Modus • **TAP** – Wählen des TAP Modus, aber davor muss erst die Bridge an der Ethernetschnittstelle konfiguriert werden
Protocol	Protokoll, über das der Tunnel kommuniziert: • **UDP** – OpenVPN kommuniziert mit UDP • **TCP server** – OpenVPN kommuniziert mittels TCP im Server-Modus • **TCP client** – OpenVPN kommuniziert mittels TCP im Client-Modus • **UDPv6** – Das OpenVPN kommuniziert mit UDP über IPv6 • **TCPv6-Server** – Das OpenVPN kommuniziert mit TCP über IPv6 im Servermodus • **TCPv6-Client** – Das OpenVPN kommuniziert mit TCP über IPv6 im Client-Modus
UDP/TCP port	Port des entsprechenden Protokolls (UDP oder TCP).
1st Remote IP Address	Erste IPv4/IPV6-Adresse der gegenüberliegenden Tunnelseite (Domainname kann verwendet werden).
2nd Remote IP Address	Zweite IPv4/IPV6-Adresse der gegenüberliegenden Tunnelseite (Domainname kann verwendet werden).
Remote Subnet	Netzwerk-IPv4-Adresse der gegenüberliegenden Seite des Tunnels.
Remote Subnet Mask	IPv4 Subnetzmaske der gegenüberliegenden Seite des Tunnels.
Redirect Gateway	Fügt das Standard-Gateway hinzu (überschreibt es). Alle Pakete werden dann über einen Tunnel an dieses Gateway gesendet, wenn sich darin kein anderes festgelegtes Standard-Gateway befindet.
Local Interface IP Address	IPv4-Adresse einer lokalen Schnittstelle. Für ein korrektes Routing wird empfohlen, eine beliebige IPv4-Adresse aus dem lokalen Bereich einzugeben, auch wenn Sie nur IPv6-Tunnel verwenden
Remote Interface IP Address	IPv4-Adresse der Schnittstelle der gegenüberliegenden Seite des Tunnels. Für ein korrektes Routing wird empfohlen, eine beliebige IPv4-Adresse aus dem lokalen Bereich einzugeben, auch wenn Sie nur IPv6-Tunnel verwenden.
Remote IPv6 Subnet	IPv6-Adresse des entfernten IPv6-Netzwerks. Äquivalent des Remote-Subnetzes im Abschnitt IPv4.
Remote IPv6 Prefix	IPv6-Präfix des entfernten IPv6-Netzwerks. Äquivalent der Remote-Subnetzmaske im Abschnitt IPv4.
Local Interface IPv6 Address	Gibt die IPv6-Adresse einer lokalen Schnittstelle an.
Remote Interface IPv6 Address	Gibt die IPv6-Adresse der Schnittstelle der gegenüberliegenden Seite des Tunnels an.

Ping Interval	Parameter (in Sekunden) definiert, wie oft der Router eine Nachricht an die Gegenstelle sendet, um zu überprüfen, ob der Tunnel noch verbunden ist.
Ping Timeout	Gibt das Zeitintervall an, in dem der Router auf eine Nachricht wartet, die von der Gegenseite gesendet wird. Stellen Sie für eine ordnungsgemäße Überprüfung des OpenVPN-Tunnels das Ping-Timeout auf einen größeren Wert als das Ping-Intervall ein.
Renegotiate Interval	Legt den Neuverhandlungszeitraum (Neuautorisierung) des OpenVPN-Tunnels fest. Sie können diesen Parameter nur festlegen, wenn der **Authenticate Mode** auf **username/password or X.509 certificate** eingestellt ist. Nach diesem Zeitraum ändert der Router die Tunnelverschlüsselung, um den Tunnel sicher zu halten.
Max Fragment Size	Maximale Größe eines gesendeten Pakets
Compression	Komprimierung der gesendeten Daten: • **none** – Es wird keine Kompression verwendet. • **LZO** – Es wird eine drahtlose Kompression verwendet. Die Kompression muss an beiden Seiten des Tunnels ausgewählt werden.
NAT Rules	NAT-Regeln gelten für OpenVPN Tunnel: • **not applied** – NAT-Regeln werden nicht auf den OpenVPN-Tunnel angewendet. • **applied** – NAT-Regeln werden auf den OpenVPN-Tunnel angewendet.
Authenticate Mode	Mit diesem Parameter wird die Authentifizierung eingestellt • **none** – es ist keine Authentifizierung eingestellt • **Pre-shared secret** – damit wird der geteilte Schlüssel für beide Tunnelseiten eingestellt • **Username/password** – ermöglicht die Authentifizierung mittels CA Certificate, Username and Password • **X.509 Certificate (multiclient)** – ermöglicht die Authentifizierung von X.509 im Multiclient-Modus • **X.509 Certificate (client)** – ermöglicht die Authentifizierung von X.509 im Client-Modus • **X.509 Certificate (server)** – ermöglicht die Authentifizierung von X.509 im Server-Modus
Security Mode	Wählen des Sicherheitsmodus, tls-auth oder tls-crypt. Es wird empfohlen den tls-crypt Modus zu verwenden. In diesem Modus werden alle Daten mit einem vorab geteilten Schlüssel codiert. Außerdem ist dieser Modus resistenter gegenüber TLS Denial-of-service Attacken.
Pre-shared Secret	Spezifiziert den vorab geteilten Schlüssel, der im Authenticate Mode verwendet werden kann.
CA Certificate	Die Authentifizierung mittels CA Certificate kann in den Authentifizierungen Username/password und X.509 Certificate verwendet werden.
DH Parameters	Protokoll für den Austausch von DH-Parametern; kann für die X.509-Zertifikatsauthentifizierung im Servermodus verwendet werden.
Local Certificate	Im lokalen Gerät verwendetes Zertifikat; Sie können dieses Authentifizierungszertifikat für den Authentifizierungsmodus X.509-Zertifikat verwenden.
Local Private Key	Der lokale private Schlüssel Local Private Key kann in der Authentifizierung X.509 Certificate verwendet werden.
Local Passphrase	Passphrase, die während der Generierung von privaten Schlüsseln verwendet wird.
Username	Die Authentisierung mittels des Benutzernamens und Passwortes kann in der Authentifizierung Username/Password verwendet werden.

Passwort	Für den Benutzername/Passwort-Modus kann die Authentifizierung mit einem Login-Namen und die Passwort-Authentifizierung verwendet werden. Nur gültige Zeichen eingeben, siehe Kapitel 2.1 "Konfigurationsmöglichkeiten", S. 8.
User's Up Script	Kundenspezifisches Skript, welches ausgeführt wird, wenn der OpenVPN Tunnel aufgebaut ist.
User's Down Script	Kundenspezifisches Skript, welches ausgeführt wird, wenn der OpenVPN Tunnel geschlossen wird.
Extra Options	Mit Hilfe des Parameters Extra Options ist es möglich, zusätzliche Parameter des OpenVPN-Tunnels, wie z. B. DHCP options usw. durch zwei Bindestriche zu definieren. Für mögliche Parameter siehe Befehl Help in the router via SSH – run the `openvpnd --help`.

Tab. 40: Konfiguration des OpenVPN-Tunnels für v3 Router

Element	**Beschreibung**
Description	Beschreibung (oder Bezeichnung) des Tunnels
Protocol	Protokoll, über das der Tunnel kommuniziert: • **UDP** – OpenVPN kommuniziert mit UDP • **TCP server** – OpenVPN kommuniziert mittels TCP im Server-Modus • **TCP client** – OpenVPN kommuniziert mittels TCP im Client-Modus • **UDPv6** – Das OpenVPN kommuniziert mit UDP über IPv6 • **TCPv6-Server** – Das OpenVPN kommuniziert mit TCP über IPv6 im Servermodus • **TCPv6-Client** – Das OpenVPN kommuniziert mit TCP über IPv6 im Client-Modus
UDP/TCP port	Port des entsprechenden Protokolls (UDP oder TCP).
Remote IP Address	IPv4/IPV6-Adresse der gegenüberliegenden Tunnelseite (Domainname kann verwendet werden).
Remote Subnet	Netzwerk-IPv4-Adresse der gegenüberliegenden Seite des Tunnels.
Remote Subnet Mask	IPv4 Subnetzmaske der gegenüberliegenden Seite des Tunnels.
Redirect Gateway	Fügt das Standard-Gateway hinzu (überschreibt es). Alle Pakete werden dann über einen Tunnel an dieses Gateway gesendet, wenn sich darin kein anderes festgelegtes Standard-Gateway befindet.
Local Interface IP Address	IPv4-Adresse einer lokalen Schnittstelle. Für ein korrektes Routing wird empfohlen, eine beliebige IPv4-Adresse aus dem lokalen Bereich einzugeben, auch wenn Sie nur IPv6-Tunnel verwenden
Remote Interface IP Address	IPv4-Adresse der Schnittstelle der gegenüberliegenden Seite des Tunnels. Für ein korrektes Routing wird empfohlen, eine beliebige IPv4-Adresse aus dem lokalen Bereich einzugeben, auch wenn Sie nur IPv6-Tunnel verwenden.
Remote IPv6 Subnet	IPv6-Adresse des entfernten IPv6-Netzwerks. Äquivalent des Remote-Subnetzes im Abschnitt IPv4.
Remote IPv6 Prefix	IPv6-Präfix des entfernten IPv6-Netzwerks. Äquivalent der Remote-Subnetzmaske im Abschnitt IPv4.
Local Interface IPv6 Address	Gibt die IPv6-Adresse einer lokalen Schnittstelle an.
Remote Interface IPv6 Address	Gibt die IPv6-Adresse der Schnittstelle der gegenüberliegenden Seite des Tunnels an.
Ping Interval	Parameter (in Sekunden) definiert, wie oft der Router eine Nachricht an die Gegenstelle sendet, um zu überprüfen, ob der Tunnel noch verbunden ist.

Ping Timeout	Gibt das Zeitintervall an, in dem der Router auf eine Nachricht wartet, die von der Gegenseite gesendet wird. Stellen Sie für eine ordnungsgemäße Überprüfung des OpenVPN-Tunnels das Ping-Timeout auf einen größeren Wert als das Ping-Intervall ein.
Renegotiate Interval	Legt den Neuverhandlungszeitraum (Neuautorisierung) des OpenVPN-Tunnels fest. Sie können diesen Parameter nur festlegen, wenn der **Authenticate Mode** auf **username/password or X.509 certificate** eingestellt ist. Nach diesem Zeitraum ändert der Router die Tunnelverschlüsselung, um den Tunnel sicher zu halten.
Max Fragment Size	Maximale Größe eines gesendeten Pakets
Compression	Komprimierung der gesendeten Daten: • **none** – Es wird keine Kompression verwendet. • **LZO** – Es wird eine drahtlose Kompression verwendet. Die Kompression muss an beiden Seiten des Tunnels ausgewählt werden.
NAT Rules	NAT-Regeln gelten für OpenVPN Tunnel: • **not applied** – NAT-Regeln werden nicht auf den OpenVPN-Tunnel angewendet. • **applied** – NAT-Regeln werden auf den OpenVPN-Tunnel angewendet.
Authenticate Mode	Mit diesem Parameter wird die Authentifizierung eingestellt • **none** – es ist keine Authentifizierung eingestellt • **Pre-shared secret** – damit wird der geteilte Schlüssel für beide Tunnelseiten eingestellt • **Username/password** – ermöglicht die Authentifizierung mittels CA Certificate, Username and Password • **X.509 Certificate (multiclient)** – ermöglicht die Authentifizierung von X.509 im Multiclient-Modus • **X.509 Certificate (client)** – ermöglicht die Authentifizierung von X.509 im Client-Modus • **X.509 Certificate (server)** – ermöglicht die Authentifizierung von X.509 im Server-Modus
Pre-shared Secret	Authentifizierung mit Pre-Shared Secret; kann für jeden angebotenen Authentifizierungsmodus verwendet werden.
CA Certificate	Die Authentifizierung mittels CA Certificate kann in den Authentifizierungen Username/password und X.509 Certificate verwendet werden.
DH Parameters	Protokoll für den Austausch von DH-Parametern; kann für die X.509-Zertifikatsauthentifizierung im Servermodus verwendet werden.
Local Certificate	Im lokalen Gerät verwendetes Zertifikat; Sie können dieses Authentifizierungszertifikat für den Authentifizierungsmodus X.509-Zertifikat verwenden.
Local Private Key	Der lokale private Schlüssel Local Private Key kann in der Authentifizierung X.509 Certificate verwendet werden.
Username	Die Authentisierung mittels des Benutzernamens und Passwortes kann in der Authentifizierung Username/Password verwendet werden.
Passwort	Für den Benutzername/Passwort-Modus kann die Authentifizierung mit einem Login-Namen und die Passwort-Authentifizierung verwendet werden. Nur gültige Zeichen eingeben, siehe Kapitel 2.1 "Konfigurationsmöglichkeiten", S. 8.
Extra Options	Mit Hilfe des Parameters Extra Options ist es möglich, zusätzliche Parameter des OpenVPN-Tunnels, wie z. B. DHCP options usw. durch zwei Bindestriche zu definieren. Für mögliche Parameter siehe Befehl Help in the router via SSH – run the `openvpnd --help`.

Voraussetzung für den Tunnelaufbau ist: WAN-Route muss aktiv sein (z. B. Mobilfunkverbindung aufgebaut), auch wenn der Tunnel nicht durch das WAN geht.

Die Änderungen der Einstellungen wirken sich nach Betätigung der Schaltfläche **Apply** aus.

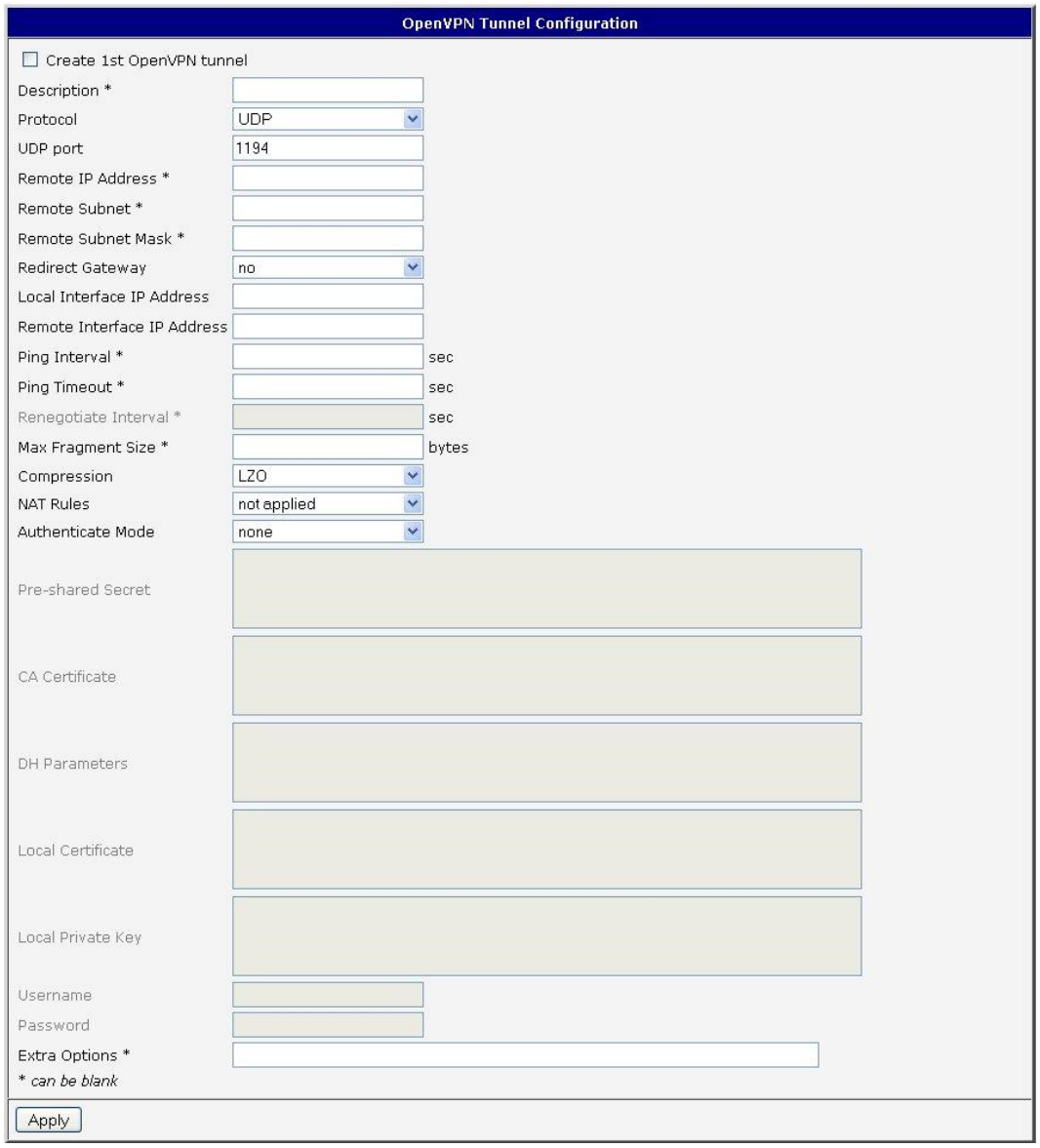


Abb. 43: Konfiguration des OpenVPN-Tunnels

Beispiel für die OpenVPN-Tunnelkonfiguration im IPv4-Netzwerk

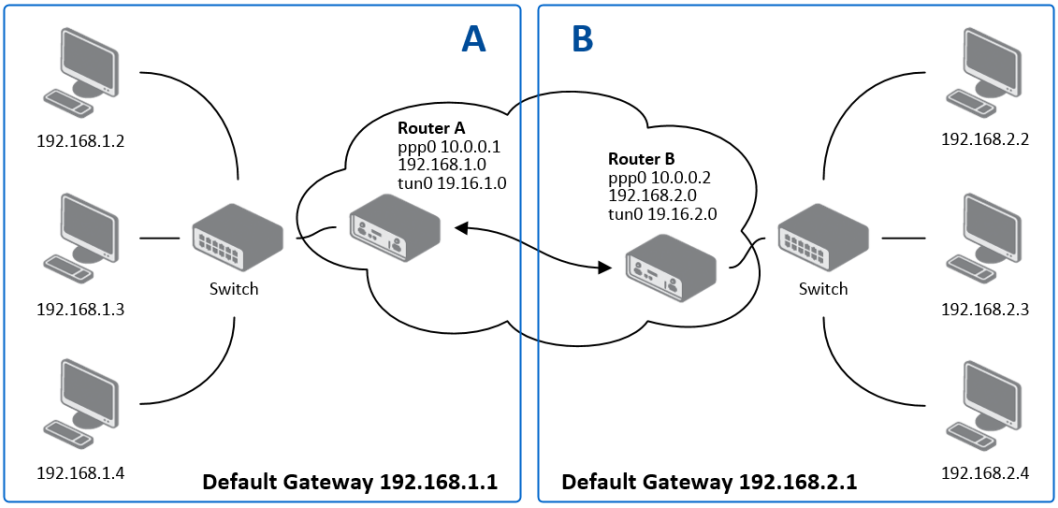


Abb. 44: Topologie des Beispiels für die Konfiguration eines OpenVPN-Tunnels

Tab. 41: Beispiel der Konfiguration des OpenVPN-Tunnels

Konfiguration	**A**	**B**
Protokoll	UDP	UDP
UDP-Port	1194	1194
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Interface IP Address	19.16.1.0	19.16.2.0
Remote Interface IP Address	19.16.2.0	19.18.1.0
Compression	LZO	LZO
Authenticate mode	Keine	Keine

5.12 Konfiguration des IPSec-Tunnels

Um die Seite **IPsec-Tunnelkonfiguration** zu öffnen, klicken Sie im Hauptmenü im Abschnitt **Konfiguration** auf **IPsec**. Das Menüelement wird erweitert und Sie sehen vier separate Konfigurationsseiten: **1st Tunnel**, **2nd Tunnel**, **3rd Tunnel** und **4th Tunnel**. Mit der IPsec-Tunnelfunktion können Sie eine gesicherte Verbindung zwischen zwei getrennten LAN-Netzwerken herstellen. Mit dem Router können Sie bis zu vier IPsec-Tunnel erstellen.
IPv4- und IPv6-Tunnel werden unterstützt (Dual-Stack), Sie können IPv6-Datenverkehr durch den IPv4-Tunnel transportieren und umgekehrt.



- Um Daten zwischen dem lokalen und dem entfernten Subnetz zu verschlüsseln, geben Sie die entsprechenden Werte in den Subnetzfeldern auf beiden Routern an. Um den Datenstrom nur zwischen den Routern zu verschlüsseln, lassen Sie die Felder für lokale und entfernte Subnetze leer.
- Wenn Sie die Protokoll- und Portinformationen im Feld **Lokales Protokoll/Port** angeben, kapselt der Router nur die Pakete ein, die den Einstellungen entsprechen.
- Für eine optimale Einrichtung empfehlen wir, den Anweisungen auf der Webseite zu folgen: https://wiki.strongswan.org/projects/strongswan/wiki/SecurityRecommendations

5.12.1 Konfiguration IPSec für v2 Router

Szenarios für eine routenbasierte Konfiguration

Es gibt weitere Möglichkeiten routenbasierte Konfigurationen im Router zu verwenden. Nachfolgend werden die gebräuchlichsten Konfigurationen gelistet:

1. Enabled Installing Routes
   - Remote (lokale) Subnetze werden als Verkehrsselektoren (Routen) verwendet
   - Das Ergebnis ist identisch zu einem richtlinienbasierten VPN
   - Ein Vorteil dieses Ansatzes ist die Möglichkeit unverschlüsselten Datenverkehr, der durch den IPsec Tunnel Nummer X läuft, mit dem tcdump Werkzeug zu verifizieren: `tcpdump -i ipsecX`.
   - Die Option **Install Routes** muss auf **yes** gesetzt werden
2. Statische Routen
   - Sobald der IPsec Tunnel aufgebaut ist, werden die Routen von einer Applikation statisch installiert
   - Als Applikation für statische Routen kann z. B. FRR/STATICD verwendet werden
   - Die Option **Install Routes** muss auf **no** gesetzt werden
3. Dynamische Routen
   - Routen werden dynamisch von einer Applikation, die ein dynamisches Protokoll verwendet, installiert
   - Als Applikation für dynamische Routen kann z. B. FRR/BGP oder FRR/OSPF verwendet werden. Die Applikation erhält die Routen von einem (BGP/OSPF) Server.
   - Die Option **Install Routes** muss auf **no** gesetzt werden
4. Multiple Clients
   - Erlaubt den Aufbau eines VPN -Netzwerks mit einer Vielzahl an Clients. Ein Router agiert als Server und weist den anderen Clients im Netzwerk IP Adressen zu
   - Der Server hat die Elemente **Remote Virtual Network** und **Remote Virtual Mask** konfiguriert, während der Client das Element **Local Virtual Address** konfiguriert hat
   - Die Option **Install Routes** muss auf **yes** gesetzt werden

IPSec Authentifizierungsszenarien

Es gibt vier grundlegende Authentifizierungsoptionen, welche konfiguriert und verwendet werden können.

1. Pre-shared Key
   - Wählen Sie im **Authenticate Mode** die **X.509 certificate** Option.
   - Geben Sie den geteilten Schlüssel im Feld **Pre-shared key** ein.
2. Öffentlicher Schlüssel
   - Wählen Sie im **Authenticate Mode** die **X.509 certificate** Option.
   - Geben Sie den öffentlichen Schlüssel im Feld **Local Certificate / PubKey** ein.
3. Peer Zertifikat
   - Wählen Sie im **Authenticate Mode** die **X.509 certificate** Option.
   - Geben Sie den remote Schlüssel im Feld **Remote Certificate / PubKey** ein. Benutzer mit diesem Zertifikat sind dann berechtigt.
     - Ein CA-Zertifikat wird nicht benötigt.
4. CA-Zertifikat
   - Wählen Sie im **Authenticate Mode** die **X.509 certificate** Option.
   - Geben Sie das CA-Zertifikat oder eine Liste von CA-Zertifikaten in das Feld **CA Certificate** ein. Jedes durch CA signierte Zertifikat wird akzeptiert.
     - Ein Remote Zertifikat wird nicht benötigt.

HINWEIS

- Die Peer- und CA-Zertifikate können parallel konfiguriert und genutzt werden. Die Authentifizierung erfolgt durch eine der beiden Methoden.
- Die Local ID ist entscheidend. Wenn man die Zertifikatsauthentifizierung verwendet, muss die IKE-Identität im Zertifikat enthalten sein, entweder als ein subject oder als `subjectAltName`.

Beschreibung der Elemente der Konfiguration

Die Oberfläche der IPsec Konfiguration sehen Sie in der untenstehenden Abbildung. Eine Beschreibung aller gezeigten Elemente, die für einen IPsec Tunnel konfiguriert werden können, finden Sie in Tab. 42.

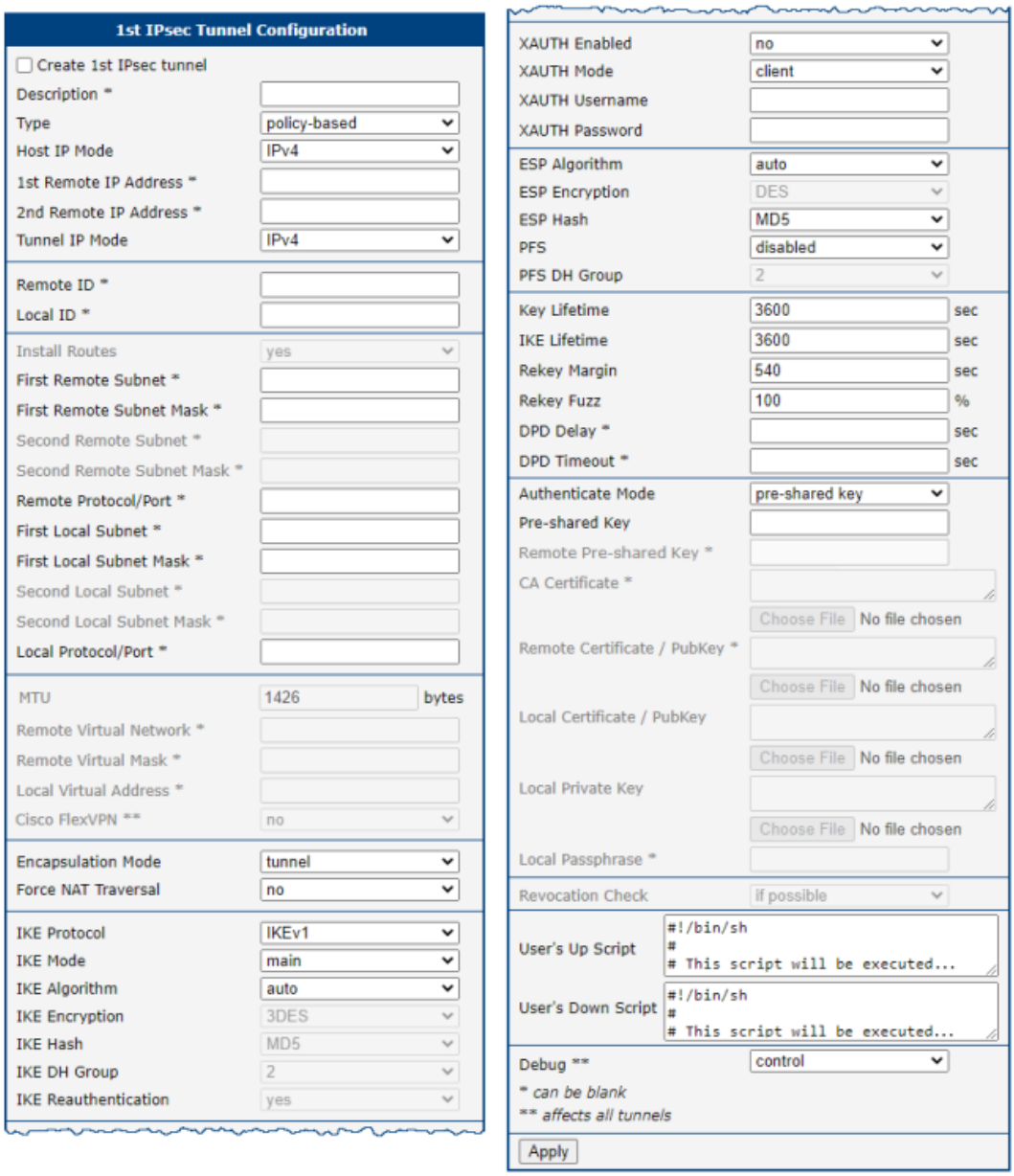


Abb. 45: Konfiguration eines IPsec Tunnels

Tab. 42: Konfiguration eines IPsec Tunnels

Element	**Beschreibung**
Description	Name (Beschreibung) des Tunnels
Host IP Mode	• **IPv4** – Der Router kommuniziert über IPv4 mit der gegenüberliegenden Seite des Tunnels. • **IPv6** – Der Router kommuniziert über IPv4 mit der gegenüberliegenden Seite des Tunnels.
Remote IP Address	IPv4/IPv6-Adresse oder Domänenname der Remote-Seite des Tunnels, basierend auf dem obigen Host-IP-Modus.
Remote ID	Bezeichner (ID) der Gegenstelle des Tunnels. Die ID bestehen aus zwei Teilen: *Host-Name* und *Domain-Name* (mehr Informationen gemäß Tabelle).
First Remote Subnet	IPv4- oder IPv6-Adresse eines Netzwerks hinter der Remote-Seite des Tunnels, basierend auf dem obigen Tunnel-IP-Modus.
First Remote Subnet Mask/ Prefix	IPv4-Subnetzmaske eines Netzwerks hinter der Gegenseite des Tunnels oder IPv6-Präfix (einzelne Zahl 0 bis 128).
Second Remote Subnet	IPv4- oder IPv6-Adresse des zweiten Netzwerks hinter der Remote-Seite des Tunnels, basierend auf dem obigen Tunnel-IP-Modus. Nur für IKE-Protokoll = IKEv2.
Second Remote Subnet Mask/Prefix	IPv4-Subnetzmaske des zweiten Netzwerks hinter der Gegenseite des Tunnels oder IPv6-Präfix (einzelne Zahl 0 bis 128). Nur für IKE-Protokoll = IKEv2.
Remote Protocol/Port	Gibt Protokoll/Port der entfernten Seite des Tunnels an. Die allgemeine Form ist Protokoll/Port, zum Beispiel 17/1701 für UDP (Protokoll 17) und Port 1701. Es ist nur die Eingabe der Protokollnummer möglich, obiges Format wird bevorzugt.
Local ID	Bezeichner (ID) der lokalen Seite des Tunnels. Die ID bestehen aus zwei Teilen: *Host-Name* und *Domain-Name* (mehr Informationen gemäß Tabelle).
First Local Subnet	IPv4- oder IPv6-Adresse eines lokalen Netzwerks, basierend auf dem obigen Tunnel-IP-Modus.
First Local Subnet Mask	IPv4-Subnetzmaske eines lokalen Netzwerks oder IPv6-Präfix (einzelne Zahl 0 bis 128).
Second Local Subnet	IPv4- oder IPv6-Adresse des zweiten lokalen Netzwerks, basierend auf dem obigen Tunnel-IP-Modus. Nur für IKE-Protokoll = IKEv2.
Second Local Subnet Mask/Prefix	IPv4-Subnetzmaske des zweiten lokalen Netzwerks oder IPv6-Präfix (Einzelnummer 0 bis 128). Für IKE-Protokoll = nur IKEv2.
Local Protocol/Port	Gibt Protokoll/Port eines lokalen Netzwerks an. Die allgemeine Form ist Protokoll/Port, zum Beispiel 17/1701 für UDP (Protokoll 17) und Port 1701. Es ist nur die Eingabe der Protokollnummer möglich, obiges Format wird bevorzugt.
Encapsulation Mode	Gibt den IPsec-Modus gemäß der Kapselungsmethode an. Sie können den Tunnelmodus auswählen, in dem das gesamte IP-Datagramm gekapselt wird, oder den Transportmodus, in dem nur der IP-Header gekapselt wird.
Force NAT traversal	NAT-Traversal-Erzwingung aktivieren (UDP-Kapselung von ESP-Paketen) (**Enabled**).
IKE Protocol	Gibt die IKE-Version an (IKEv1/IKEv2, IKEv1 oder IKEv2).
IKE Mode	Definiert den Modus für den Verbindungsaufbau (**main** oder **aggressive**). Wenn der Aggressive-Modus ausgewählt ist, ist der Aufbau des IPsec-Tunnels schneller, aber die Verschlüsselung ist dauerhaft auf 3DES-MD5 eingestellt. **Wir empfehlen, aufgrund einer geringeren Sicherheit keinen aggressiven Modus zu verwenden!**

IKE Algorithm	Art der Auswahl des Algorithmus: • **auto** – Verschlüsselung und Hash-Algorithmus werden automatisch ausgewählt • **manual** – Verschlüsselung und Hash-Algorithmus werden vom Benutzer ausgewählt
IKE Encryption	Verschlüsselungsalgorithmus – 3DES, AES128, AES192, AES256, AES128GCM128, AES192GCM128, AES256GCM128
IKE Hash	Hash-Algorithmen – MD5, SHA1, SHA256, SHA384 oder SHA512
IKE DH Group	Diffie-Hellman-Gruppen bestimmen die Stärke des Schlüssels, der im Schlüsselaustauschprozess verwendet wird. Höhere Gruppennummern sind sicherer, erfordern jedoch zusätzliche Zeit zum Berechnen des Schlüssels.
IKE Reauthentication	KE-Neuauthentifizierung aktivieren oder deaktivieren (nur IKEv2).
XAUTH Enabled	Erweiterte Authentifizierung aktivieren (nur für IKEv1).
XAUTH Mode	Wählen Sie den XAUTH-Modus (Client oder Server).
XAUTH Username	XAUTH-Benutzername
XAUTH Password	XAUTH-Passwort
ESP Algorithm	Art der Auswahl des Algorithmus: • **auto** – Verschlüsselung und Hash-Algorithmus werden automatisch ausgewählt • **manual** – Verschlüsselung und Hash-Algorithmus werden vom Benutzer ausgewählt
ESP Encryption	Verschlüsselungsalgorithmus – DES, 3DES, AES128, AES192, AES256, AES128GCM128, AES192GCM128, AES256GCM128
ESP Hash	Hash-Algorithmen – MD5, SHA1, SHA256, SHA384 oder SHA512
PFS	Perfect Forward Secrecy; Stellt sicher, dass abgeleitete Sitzungsschlüssel nicht kompromittiert werden, wenn einer der privaten Schlüssel in Zukunft kompromittiert wird.
PFS DH Group	Diffie-Hellman Gruppennummer (siehe *IKE DH Group*)
Key Lifetime	Lebenslanger Schlüssel-Datenteil des Tunnels. Der Mindestwert dieses Parameters beträgt 60 s. Der Maximalwert beträgt 86400 s.
IKE Lifetime	Lebenslanger Schlüssel-Serviceteil des Tunnels. Der Mindestwert dieses Parameters beträgt 60 s. Der Maximalwert beträgt 86400 s.
Rekey Margin	Zeit vor dem Ablauf der Gültigkeit der Schlüssel, wenn neue Schlüssel erzeugt werden. Der Höchstwert muss kleiner sein als die Hälfte der Parameter IKE und Key Lifetime.
Rekey Fuzz	Prozentuelle Verlängerung der Zeit Rekey Margin.
DPD Delay	Das Zeitintervall, während dessen die Funktionsfähigkeit des IPsec-Tunnels getestet wird.
DPD Timeout	Das Zeitintervall, während dessen die Antwort abgewartet wird.
Authenticate Mode	Gibt die Mittel an, mit denen sich der Router authentifiziert: • **Pre-shared key** – damit wird der geteilte Schlüssel für beide Tunnelseiten eingestellt • **X.509 Certificate** – ermöglicht die Authentifizierung von X.509 im Multiclient-Modus
Pre-shared Key	Geteilter Schlüssel für beide Tunnelseiten für die Authentifizierung Pre-shared key.
CA Certificate	Zertifikat für die Authentifizierung X.509
Remote Certificate / PubKey	Zertifikat für die X.509-Authentifizierung oder PubKey für die Authentifizierung mit öffentlichen Schlüsselsignaturen
Local Certificate / PubKey	Zertifikat für die X.509-Authentifizierung oder PubKey für die Authentifizierung mit öffentlichen Schlüsselsignaturen
Local Private Key	Privater Schlüssel für die Authentifizierung X.509

Local Passphrase	Passphrase, die während der Generierung des privaten Schlüssels verwendet wird
Debug	Wählen Sie die Stufe der Ausführlichkeit für das Systemprotokoll. Silent (Default), audit, control, control-more, raw, private (am ausführlichsten, einschließlich der privaten Schlüssel).

Wir empfehlen, die Standardeinstellungen beizubehalten. Wenn Sie die Schlüsselwechselzeiten höher einstellen, verursacht der Tunnel zwar niedrigere Betriebskosten, aber die Einstellung bietet auch weniger Sicherheit. Umgekehrt verursacht der Tunnel bei einer Reduzierung der Zeit höhere Betriebskosten, sorgt aber für mehr Sicherheit. Die Änderungen in den Einstellungen werden übernommen, nachdem Sie auf die Schaltfläche **Apply** geklickt haben.



- Wenn lokale und entfernte Subnetze nicht konfiguriert sind, werden nur Pakete zwischen lokaler und entfernter IP-Adresse gekapselt, sodass nur die Kommunikation zwischen zwei Routern verschlüsselt wird.
- Wenn Protokoll-/Portfelder konfiguriert sind, werden nur Pakete, die diesen Einstellungen entsprechen, gekapselt.

Beispiel für die grundlegende Konfiguration eines IPSec-Tunnels

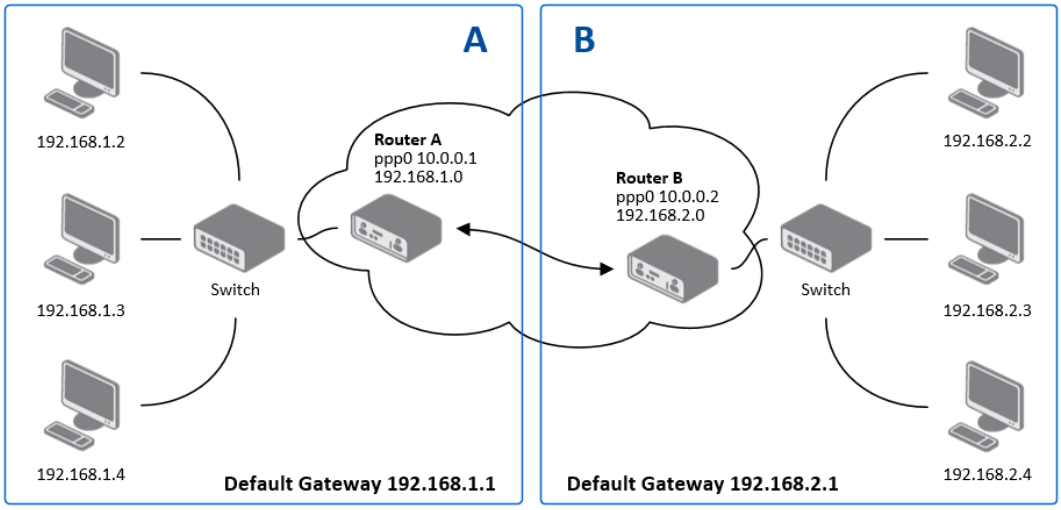


Abb. 46: Topologie des Beispiels für die grundlegende Konfiguration eines IPsec-Tunnels

Die Konfiguration des IPSec-Tunnels für Router A und B ist wie folgt:

Tab. 43: Beispiel für IPsec-Konfiguration

Konfiguration	**A**	**B**
Host IP Mode	IPv4	IPv4
Remote IP Address	10.0.0.2	10.0.0.1
Tunnel IP Mode	IPv4	IPv4
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Subnet	192.168.1.0	192.168.2.0
Local Subnet Mask:	255.255.255.0	255.255.255.0
Authenticate mode	Pre-shared Key	Pre-shared Key
Pre-shared Key	Test	Test

5.12.2 Konfiguration IPSec für v3 Router

Tab. 44: Konfiguration des IPsec-Tunnels

Element	**Beschreibung**
Description	Name (Beschreibung) des Tunnels
Host IP Mode	• **IPv4** – Der Router kommuniziert über IPv4 mit der gegenüberliegenden Seite des Tunnels. • **IPv6** – Der Router kommuniziert über IPv4 mit der gegenüberliegenden Seite des Tunnels.
Remote IP Address	IPv4/IPv6-Adresse oder Domänenname der Remote-Seite des Tunnels, basierend auf dem obigen Host-IP-Modus.
Remote ID	Bezeichner (ID) der Gegenstelle des Tunnels. Die ID bestehen aus zwei Teilen: *Host-Name* und *Domain-Name* (mehr Informationen gemäß Tabelle).
First Remote Subnet	IPv4- oder IPv6-Adresse eines Netzwerks hinter der Remote-Seite des Tunnels, basierend auf dem obigen Tunnel-IP-Modus.
First Remote Subnet Mask/ Prefix	IPv4-Subnetzmaske eines Netzwerks hinter der Gegenseite des Tunnels oder IPv6-Präfix (einzelne Zahl 0 bis 128).
Second Remote Subnet	IPv4- oder IPv6-Adresse des zweiten Netzwerks hinter der Remote-Seite des Tunnels, basierend auf dem obigen Tunnel-IP-Modus. Nur für IKE-Protokoll = IKEv2.
Second Remote Subnet Mask/Prefix	IPv4-Subnetzmaske des zweiten Netzwerks hinter der Gegenseite des Tunnels oder IPv6-Präfix (einzelne Zahl 0 bis 128). Nur für IKE-Protokoll = IKEv2.
Remote Protocol/Port	Gibt Protokoll/Port der entfernten Seite des Tunnels an. Die allgemeine Form ist Protokoll/Port, zum Beispiel 17/1701 für UDP (Protokoll 17) und Port 1701. Es ist nur die Eingabe der Protokollnummer möglich, obiges Format wird bevorzugt.
Local ID	Bezeichner (ID) der lokalen Seite des Tunnels. Die ID bestehen aus zwei Teilen: *Host-Name* und *Domain-Name* (mehr Informationen gemäß Tabelle).
First Local Subnet	IPv4- oder IPv6-Adresse eines lokalen Netzwerks, basierend auf dem obigen Tunnel-IP-Modus.
First Local Subnet Mask	IPv4-Subnetzmaske eines lokalen Netzwerks oder IPv6-Präfix (einzelne Zahl 0 bis 128).
Second Local Subnet	IPv4- oder IPv6-Adresse des zweiten lokalen Netzwerks, basierend auf dem obigen Tunnel-IP-Modus. Nur für IKE-Protokoll = IKEv2.
Second Local Subnet Mask/Prefix	IPv4-Subnetzmaske des zweiten lokalen Netzwerks oder IPv6-Präfix (Einzelnummer 0 bis 128). Für IKE-Protokoll = nur IKEv2
Local Protocol/Port	Gibt Protokoll/Port eines lokalen Netzwerks an. Die allgemeine Form ist Protokoll/Port, zum Beispiel 17/1701 für UDP (Protokoll 17) und Port 1701. Es ist nur die Eingabe der Protokollnummer möglich, obiges Format wird bevorzugt.
Encapsulation Mode	Gibt den IPsec-Modus gemäß der Kapselungsmethode an. Sie können den Tunnelmodus auswählen, in dem das gesamte IP-Datagramm gekapselt wird, oder den Transportmodus, in dem nur der IP-Header gekapselt wird.
Force NAT traversal	NAT-Traversal-Erzwingung aktivieren (UDP-Kapselung von ESP-Paketen) (**Enabled**)
IKE Protocol	Gibt die IKE-Version an (IKEv1/IKEv2, IKEv1 oder IKEv2).
IKE Mode	Definiert den Modus für den Verbindungsaufbau (**main** oder **aggressive**). Wenn der Aggressive-Modus ausgewählt ist, ist der Aufbau des IPsec-Tunnels schneller, aber die Verschlüsselung ist dauerhaft auf 3DES-MD5 eingestellt. **Wir empfehlen, aufgrund einer geringeren Sicherheit keinen aggressiven Modus zu verwenden!**

IKE Algorithm	Art der Auswahl des Algorithmus: • **auto** – Verschlüsselung und Hash-Algorithmus werden automatisch ausgewählt • **manual** – Verschlüsselung und Hash-Algorithmus werden vom Benutzer ausgewählt
IKE Encryption	Verschlüsselungsalgorithmus – 3DES, AES128, AES192, AES256, AES128GCM128, AES192GCM128, AES256GCM128
IKE Hash	Hash-Algorithmen – MD5, SHA1, SHA256, SHA384 oder SHA512
IKE DH Group	Diffie-Hellman-Gruppen bestimmen die Stärke des Schlüssels, der im Schlüsselaustauschprozess verwendet wird. Höhere Gruppennummern sind sicherer, erfordern jedoch zusätzliche Zeit zum Berechnen des Schlüssels.
IKE Reauthentication	KE-Neuauthentifizierung aktivieren oder deaktivieren (nur IKEv2)
XAUTH Enabled	Erweiterte Authentifizierung aktivieren (nur für IKEv1)
XAUTH Mode	Wählen Sie den XAUTH-Modus (Client oder Server)
XAUTH Username	XAUTH-Benutzername
XAUTH Password	XAUTH-Passwort
ESP Algorithm	Art der Auswahl des Algorithmus: • **auto** – Verschlüsselung und Hash-Algorithmus werden automatisch ausgewählt • **manual** – Verschlüsselung und Hash-Algorithmus werden vom Benutzer ausgewählt
ESP Encryption	Verschlüsselungsalgorithmus – DES, 3DES, AES128, AES192, AES256, AES128GCM128, AES192GCM128, AES256GCM128
ESP Hash	Hash-Algorithmen – MD5, SHA1, SHA256, SHA384 oder SHA512
PFS	Perfect Forward Secrecy; Stellt sicher, dass abgeleitete Sitzungsschlüssel nicht kompromittiert werden, wenn einer der privaten Schlüssel in Zukunft kompromittiert wird
PFS DH Group	Diffie-Hellman Gruppennummer (siehe *IKE DH Group*)
Key Lifetime	Lebenslanger Schlüssel-Datenteil des Tunnels. Der Mindestwert dieses Parameters beträgt 60 s. Der Maximalwert beträgt 86400 s.
IKE Lifetime	Lebenslanger Schlüssel-Serviceteil des Tunnels. Der Mindestwert dieses Parameters beträgt 60 s. Der Maximalwert beträgt 86400 s.
Rekey Margin	Zeit vor dem Ablauf der Gültigkeit der Schlüssel, wenn neue Schlüssel erzeugt werden. Der Höchstwert muss kleiner sein als die Hälfte der Parameter IKE und Key Lifetime.
Rekey Fuzz	Prozentuelle Verlängerung der Zeit Rekey Margin.
DPD Delay	Das Zeitintervall, während dessen die Funktionsfähigkeit des IPsec-Tunnels getestet wird.
DPD Timeout	Das Zeitintervall, während dessen die Antwort abgewartet wird.
Authenticate Mode	Gibt die Mittel an, mit denen sich der Router authentifiziert: • **Pre-shared key** – damit wird der geteilte Schlüssel für beide Tunnelseiten eingestellt • **X.509 Certificate** – ermöglicht die Authentifizierung von X.509 im Multiclient-Modus
Pre-shared Key	Geteilter Schlüssel für beide Tunnelseiten für die Authentifizierung Pre-shared key.
CA Certificate	Zertifikat für die Authentifizierung X.509
Remote Certificate / PubKey	Zertifikat für die X.509-Authentifizierung oder PubKey für die Authentifizierung mit öffentlichen Schlüsselsignaturen
Local Certificate / PubKey	Zertifikat für die X.509-Authentifizierung oder PubKey für die Authentifizierung mit öffentlichen Schlüsselsignaturen
Local Private Key	Privater Schlüssel für die Authentifizierung X.509

Local Passphrase	Passphrase, die während der Generierung des privaten Schlüssels verwendet wird
Debug	Wählen Sie die Stufe der Ausführlichkeit für das Systemprotokoll. Silent (Default), audit, control, control-more, raw, private (am ausführlichsten, einschließlich der privaten Schlüssel).



- Wenn lokale und entfernte Subnetze nicht konfiguriert sind, werden nur Pakete zwischen lokaler und entfernter IP-Adresse gekapselt, sodass nur die Kommunikation zwischen zwei Routern verschlüsselt wird.
- Wenn Protokoll-/Portfelder konfiguriert sind, werden nur Pakete, die diesen Einstellungen entsprechen, gekapselt.

Das folgende Verfahren beschreibt, wie Sie Zertifikate und Schlüssel ohne Kennwortphrase generieren:

```
******************** certification authority ************************
openssl rand -out private/.rand 1024
openssl genrsa -des3 -out private/ca.key 2048
openssl req -new -key private/ca.key -out tmp/myrootca.req
openssl x509 -req -days 7305 -sha1 -extensions v3_ca -signkey
private/ca.key -in tmp/myrootca.req -out ca.crt
******************** server cert
***********************************
openssl genrsa -out private/server.key 2048
openssl req -new -key private/server.key -out tmp/server.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -
CAkey
private/ca.key -in tmp/server.req -CAserial ca.srl -CAcreateserial
-out server.crt
******************** client cert
***********************************
openssl genrsa -out private/client.key 2048
openssl req -new -key private/client.key -out tmp/client.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -
CAkey
private/ca.key -in tmp/client.req -CAserial ca.srl -CAcreateserial
-out client.crt
```

Nachfolgend sind die Zertifikate mit der Passwortphrase "router" aufgeführt (Zertifizierungsstelle bleibt unverändert):

```
******************** server cert
***********************************
openssl genrsa -des3 -passout pass:router -out private/server.pem
2048
openssl req -new -key private/server.pem -out tmp/server.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -
CAkey
private/ca.key -in tmp/server.req -CAserial ca.srl -CAcreateserial
-out server.crt
******************** client cert
***********************************
openssl genrsa -des3 -passout pass:router -out private/client.pem
2048
openssl req -new -key private/client.pem -out tmp/client.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -
CAkey
private/ca.key -in tmp/client.req -CAserial ca.srl -CAcreateserial
-out client.crt
```

IPsec unterstützt die folgenden Typen von Identifikatoren (IDs) beider Tunnelseiten (Elemente **Remote ID** und **Local ID**):

- IP-Adresse (z. B. 192.168.1.1)
- DN (z. B. D=DE, W=Wieland, OU=TP, CN=A)
- FQDN (z. B. @director.wieland.com) – **vor FQDN muss immer @ stehen**
- User FQDN (z. B. director@wieland.com)

HINWEIS

Die Zertifikate und privaten Schlüssel müssen im PEM-Format vorliegen. Als Zertifikat kann nur ein solches verwendet werden, das durch den Beginn und das Ende des Zertifikats eingeleitet wird.

Die zufällige Zeit, nach der die neuen Schlüssel wieder ausgetauscht werden, wird so definiert: **Lebensdauer – (Rekey margin + Zufallswert im Bereich (von 0 bis Rekey margin * Rekey Fuzz/100))**
Standardmäßig wird der wiederholte Schlüsselaustausch im Zeitbereich gehalten:

- Minimale Zeit: 1 h – (9 m + 9 m) = 42 m
- Maximale Zeit: 1 h – (9 m + 0 m) = 51 m

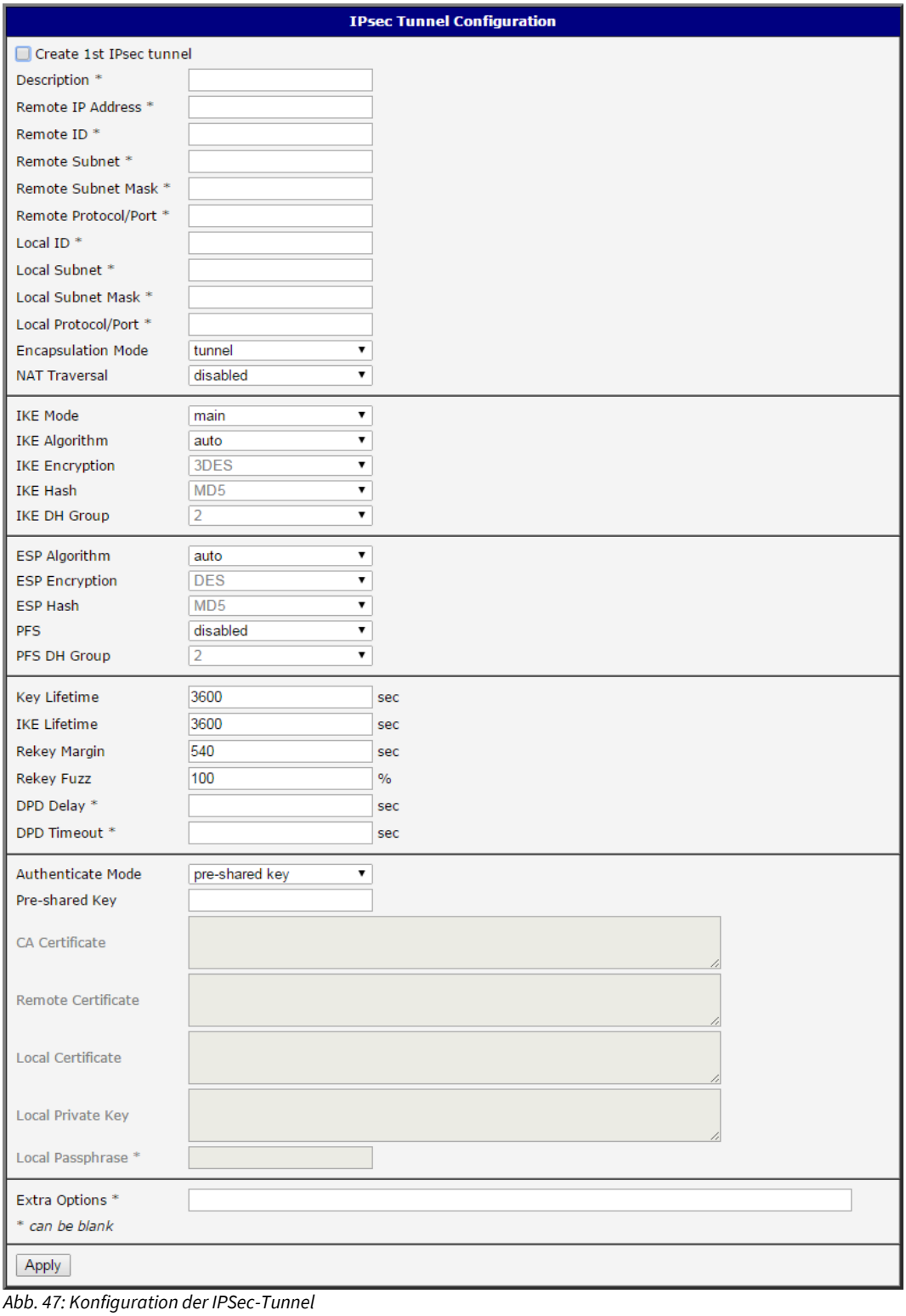


Abb. 47: Konfiguration der IPSec-Tunnel

Wir empfehlen, die Standardeinstellungen beizubehalten. Wenn Sie die Schlüsselwechselzeiten höher einstellen, verursacht der Tunnel zwar niedrigere Betriebskosten, aber die Einstellung bietet auch weniger Sicherheit. Umgekehrt verursacht der Tunnel bei einer Reduzierung der Zeit höhere Betriebskosten, sorgt aber für mehr Sicherheit. Die Änderungen in den Einstellungen werden übernommen, nachdem Sie auf die Schaltfläche **Apply** geklickt haben.

5.13 Konfiguration WireGuard-Tunnel

HINWEIS WireGuard ist nur bei v2 Routern verfügbar.

WireGuard ist ein auf einer open source Software basiertes Kommunikationsprotokoll, welches verschlüsselte virtuelle private Netzwerke (VPNs) implementiert. Die Vorteile dieses Protokolls sind die einfache Handhabung, eine hohe Leistungsgeschwindigkeit und eine geringe Angriffsfläche. Es bietet damit eine höhere Leistungsfähigkeit als IPsec und OpenVPN. Das WireGuard Protokoll nutzt UDP für die Datenweiterleitung. Die v2 Router ermöglichen den Aufbau von bis zu vier WireGuard-Tunneln.

Um die Konfigurationsseite für den WireGuard-Tunnel zu öffnen, klicken Sie bitte in der Sektion **Configuration** des Hauptmenüs auf **WireGuard.** Das Menü wird dann vier separate Konfigurationsseiten anzeigen: **1st Tunnel, 2nd Tunnel, 3rd Tunnel** and **4th Tunnel.**

IPv4 und IPv6 Tunnel werden unterstützt (dual stack). Man kann IPv6 Verkehr durch einen IPv4 Tunnel übertragen und umgekehrt.

Die Ansicht der WireGuard-Konfiguration wird in der folgenden Abbildung angezeigt und die Tab. 45 beschreibt alle Elemente, die man für einen WireGuard-Tunnel konfigurieren kann.

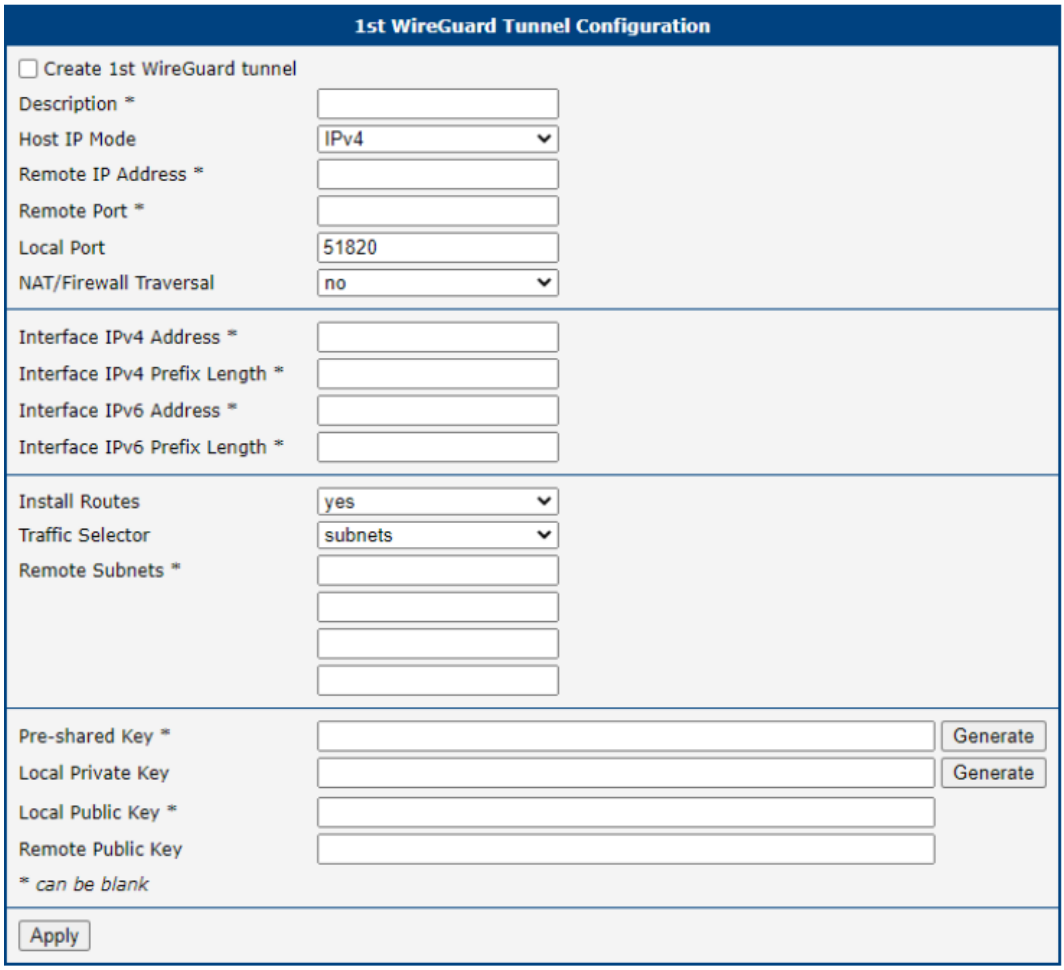


Abb. 48: WireGuard-Tunnel-Konfiguration

Tab. 45: WireGuard-Tunnel-Konfiguration

Element	**Beschreibung**
Description	Name (Beschreibung) des Tunnels
Host IP Mode	• **IPv4** – Der Router kommuniziert über IPv4 mit der gegenüberliegenden Seite des Tunnels. • **IPv6** – Der Router kommuniziert über IPv4 mit der gegenüberliegenden Seite des Tunnels.
Remote IP Address	IPv4/IPv6-Adresse oder Domänenname der Remote-Seite des Tunnels, basierend auf dem obigen Host-IP-Modus.
Remote Port	Port auf der Remote-Seite des Tunnels.
Local Port	Port auf der lokalen Seite des Tunnels (Standardport ist 51820).
NAT/Firewall Traversal	Falls Einstellung = *yes*, läuft die keepalive Kommunikation (alle 25 Sekunden), um den aufgebauten Tunnel zu erhalten. Dies ist hilfreich, wenn der Client hinter dem NAT läuft.
Interface IPv4 Address	Adresse des lokalen IPv4 Tunnels
Interface IPv4 Prefix Length	Prefix des lokalen IPv4 Tunnels
Interface IPv6 Address	Adresse des lokalen IPv6 Tunnels
Interface IPv6 Prefix Length	Prefix des lokalen IPv6 Tunnels
Install Routes	• **no** – Installiert keine Routen. Anzuwenden, wenn ein dynamisches Routing Protokoll konfiguriert ist. • **yes** – Installiert Routen.
Traffic Selector	• **all traffic** – Leitet alle Pakete durch den WIreGuard-Tunnel. • **subnets** – Route abhängig von den gelisteten Subnetzen.
Remote Subnets	Falls der *Traffic Selector* auf *Subnets* eingestellt ist, können andere Subnetze (Routen) durch den WIreGuard-Tunnel geroutet werden.
Pre-shared Key	Optionaler Schlüssel für eine zusätzliche Verschlüsselungsschicht und ein höheres Sicherheitslevel. Man kann die Schaltfläche *Generate* drücken, um einen zufälligen Code zu generieren.
Local Private Key	Privater Schlüssel der lokalen Seite. Man kann die Schaltfläche *Generate* drücken, um einen zufälligen Code zu generieren.
Local Public Key	Der öffentliche Schlüssel der lokalen Tunnelseite.
Remote Public Key	Der öffentliche Schlüssel der Remote-Tunnelseite.

Die Änderungen werden übernommen, wenn die Schaltfläche **Apply** gedrückt wird.

Beispiel für eine WireGuard-IPv4-Tunnel-Konfiguration

Im Beispiel besteht eine WireGuard-IPv4-Tunnel-Konfiguration zwischen Router A und Router B.

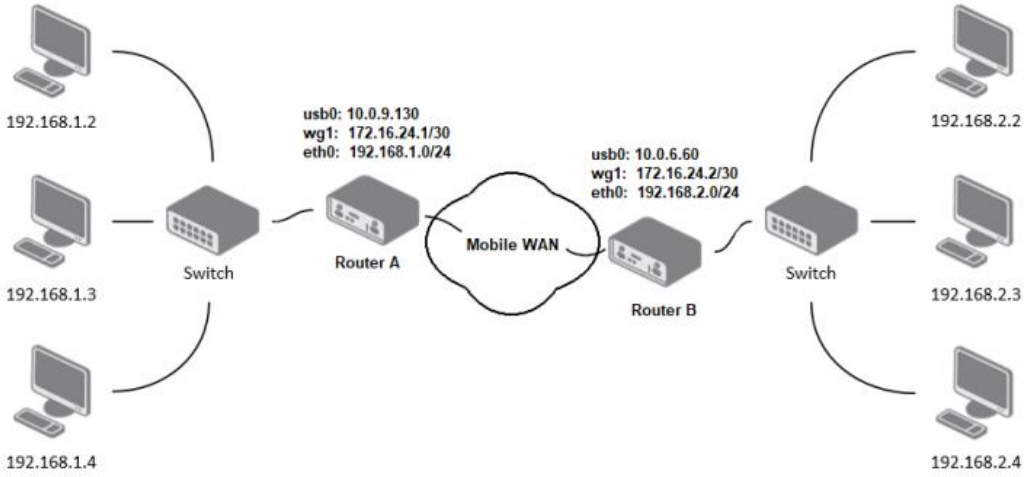


Abb. 49: Beispiel einer Topologie einer WIreGuard-Konfiguration

Router B ist so konfiguriert, dass er hört und Router A stellt die Seite dar, die den Tunnel initiiert. Die Konfiguration von Router A und Router B der vorgehenden Topologie ist wie folgt:

Tab. 46: Beispiel für WireGuard-IPv4-Tunnel-Konfiguration

Configuration	**Router A**	**Router B**
Host IP Mode	IPv4	IPv4
Remote IP Address	10.0.6.60	-
Remote port	51820	-
Local port	51820	51820
NAT/Firewall Traversal	Yes	No
Interface IPv4 Address	172.16.24.1	172.16.24.2
Interface IPv4 Prefix Length	30	30
Install Routes	Yes	Yes
Traffic Selector	Subnets	Subnets
Remote Subnets	192.168.2.0/24	192.168.1.0/24
Local Private Key	Ein lokaler privater Schlüssel	Ein lokaler privater Schlüssel
Local Public Key	Ein lokaler öffentlicher Schlüssel	Ein lokaler öffentlicher Schlüssel
Remote Public Key	Ein öffentlicher Schlüssel der Gegenseite	Ein öffentlicher Schlüssel der Gegenseite

In der nachfolgenden Abbildung findet sich die WireGuard Statusseite von Router A. Falls der Tunnel erfolgreich aufgebaut wurde, wird die **latest handshake** Zeit angezeigt. Der Wert gibt die Zeit seit der letzten erfolgreichen Kommunikation mit der Gegenseite des Tunnels an. Dieses Feld wird nicht angezeigt bis eine Kommunikation durch den Tunnel erfolgt ist (gesendete Daten durch Router A oder das Senden von keepalive Daten, wenn **NAT/Firewall Traversal** auf **yes** gesetzt ist).

1st WireGuard Tunnel Information

```
interface: wg1
  public key: jYlVmPwwlmzoC3y6xUX7dbXeDfvrRJxL42f4xOA4FkA=
  private key: (hidden)
  listening port: 51820

peer: 3/L9L9REE6BM1zO3CgET4r2N3QPKPTK/9yAj1hOq0n4=
  endpoint: 10.0.6.60:51820
  allowed ips: 172.16.24.0/30, 192.168.2.0/24
  latest handshake: 1 minute, 17 seconds ago
  transfer: 644 B received, 2.26 KiB sent
  persistent keepalive: every 25 seconds
```

Route Table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.253.254	0.0.0.0	UG	0	0	0	usb0
172.16.24.0	0.0.0.0	255.255.255.252	U	0	0	0	wg1
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	wg1
192.168.7.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
192.168.11.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.253.254	0.0.0.0	255.255.255.255	UH	0	0	0	usb0

Abb. 50: Router A . WireGuard Statusseite und Route Tabelle

1st WireGuard Tunnel Information

```
interface: wg1
  public key: 3/L9L9REE6BM1zO3CgET4r2N3QPKPTK/9yAj1hOq0n4=
  private key: (hidden)
  listening port: 51820

peer: jYlVmPwwlmzoC3y6xUX7dbXeDfvrRJxL42f4xOA4FkA=
  endpoint: 10.0.9.130:51820
  allowed ips: 172.16.24.0/30, 192.168.1.0/24
  latest handshake: 1 minute, 22 seconds ago
  transfer: 2.59 KiB received, 736 B sent
```

Route Table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.253.254	0.0.0.0	UG	0	0	0	usb0
10.1.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eth2
172.16.24.0	0.0.0.0	255.255.255.252	U	0	0	0	wg1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	wg1
192.168.7.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
192.168.100.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.253.254	0.0.0.0	255.255.255.255	UH	0	0	0	usb0

Abb. 51: Router B - WireGuard Statusseite und Route Tabelle

5.14 Konfiguration des GRE-Tunnels

HINWEIS GRE ist ein unverschlüsseltes Protokoll. GRE über IPv6 wird nicht unterstützt.

Um die **GRE tunnels configuration** zu öffnen, klicken Sie im Konfigurationsabschnitt des Hauptmenüs auf **GRE**. Der Menüpunkt wird erweitert und Sie sehen vier separate Konfigurationsseiten: 1. Tunnel, 2. Tunnel, 3. Tunnel und 4. Tunnel. Mit der GRE-Tunnelfunktion können Sie eine unverschlüsselte Verbindung zwischen zwei getrennten LAN-Netzwerken herstellen. Mit dem Router können Sie vier GRE-Tunnel erstellen.

Tab. 47: Konfiguration des GRE-Tunnels

Element	Beschreibung
Beschreibung	Beschreibung des Tunnels
Remote IP Address	IP-Adresse der Gegenstelle des Tunnels
Remote Subnet	IP-Netzadresse hinter der Gegenstelle des Tunnels
Remote Subnet Mask	Netzmaske hinter der Gegenstelle des Tunnels
Local Interface IP Address	IP-Adresse der lokalen Seite des Tunnels
Remote Interface IP Address	IP-Adresse der Gegenstelle des Tunnels
Multicasts	Aktiviert/deaktiviert das Senden von Multicast: • **disabled** – Multicast gesperrt • **enabled** – Multicast aktiviert
Pre-shared Key	Ein optionaler Wert, der den gemeinsamen 32-Bit-Schlüssel im numerischen Format definiert, durch den die gefilterten Daten durch den Tunnel gelangen. Dieser Schlüssel muss auf beiden Routern gleich definiert sein, sonst verwirft der Router empfangene Pakete.



VORSICHT Der GRE-Tunnel kann das NAT nicht passieren.

Die Änderungen der Einstellungen wirken sich nach Betätigung der Schaltfläche **Apply** aus.

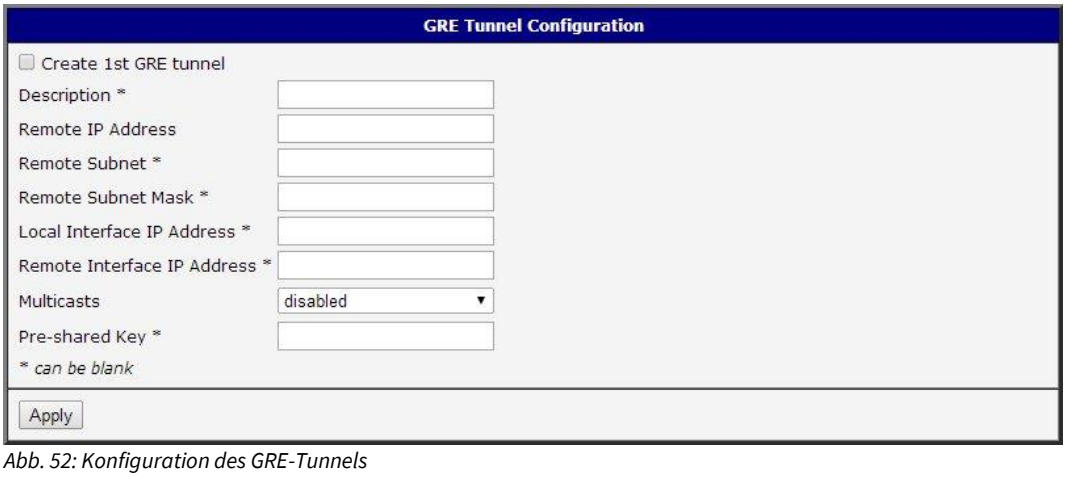


Abb. 52: Konfiguration des GRE-Tunnels

Beispiel für die Konfiguration eines GRE-Tunnels

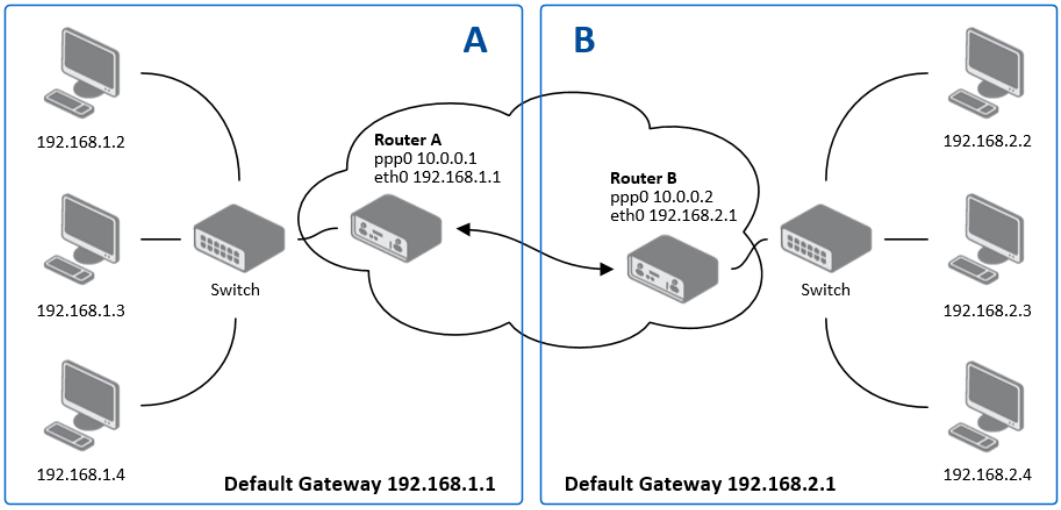


Abb. 53: Topologie für die Konfiguration eines GRE-Tunnels

Tab. 48: Beispiel für die Konfiguration eines GRE-Tunnels

Konfiguration	**A**	**B**
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0

5.15 Konfiguration des L2TP-Tunnels

HINWEIS L2TP ist ein unverschlüsseltes Protokoll. L2TP über IPv6 wird nicht unterstützt.

Um die Seite **L2TP Tunnel Configuration** zu öffnen, klicken Sie auf **L2TP** im Abschnitt **Configuration** des Hauptmenüs. Mit der L2TP-Tunnelfunktion können Sie eine passwortgeschützte Verbindung zwischen zwei LAN-Netzwerken herstellen. Aktivieren Sie das Kontrollkästchen **Create L2TP tunnel**, um den Tunnel zu aktivieren.

Tab. 49: Konfiguration des L2TP-Tunnels

Element	**Beschreibung**
Andere Betriebsart	Modus des L2TP.Tunnels auf der Seite des Routers: • **L2TP server** – definiert den IP-Adressbereichs, die vom Server angeboten wird • **L2TP client** – definiert die IP-Adresse des Servers
Server IP Address	IP-Adresse des Servers
Client Start IP Address	Erste IP-Adresse innerhalb des Adressbereichs. Der Bereich wird den Clients vom Server angeboten.
Client End IP Address	Letzte IP-Adresse innerhalb des Adressbereichs. Der Bereich wird den Clients vom Server angeboten.
Local IP Address	IP-Adresse der lokalen Seite des Tunnels
Remote IP Address	IP-Adresse der Gegenstelle des Tunnels
Remote Subnet	IP-Adresse des Netzes hinter der Gegenstelle des Tunnels
Remote Subnet Mask	Netzmaske hinter der Gegenstelle des Tunnels
MRU**	Maximaler Empfangswert. Standardwert ist 1‘400 Bytes.
MTU**	Maximaler Sendewert. Standardwert ist 1‘400 Bytes.
Username	Anmeldename für das Einloggen in den L2TP-Tunnel
Passwort	Passwort für die Anmeldung beim L2TP-Tunnel. Nur gültige Zeichen eingeben, siehe Kapitel 2.1 "Konfigurationsmöglichkeiten", S. 8.
** Gilt nur für v2	

Die Änderungen der Einstellungen wirken sich nach Betätigung der Schaltfläche **Apply** aus.

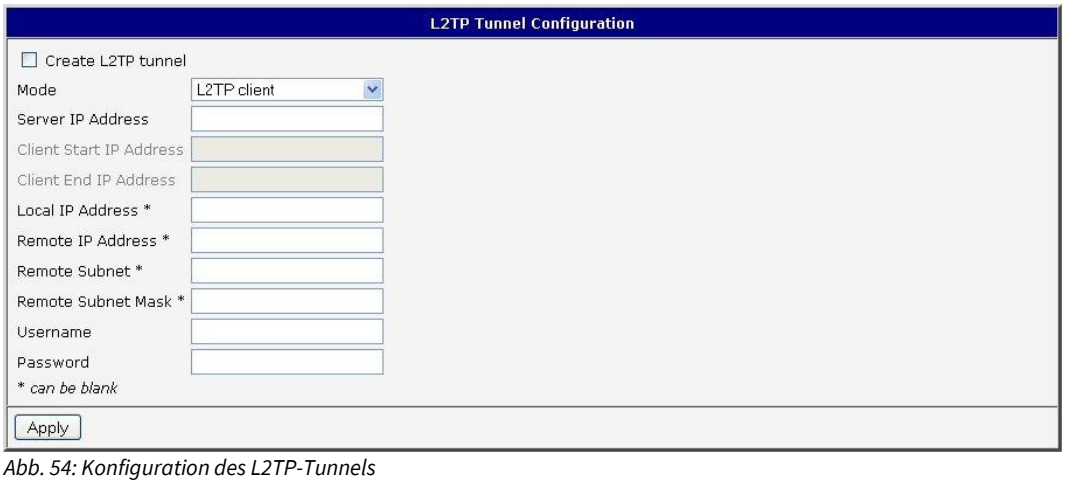


Abb. 54: Konfiguration des L2TP-Tunnels

Beispiel für die Konfiguration eines L2TP-Tunnels

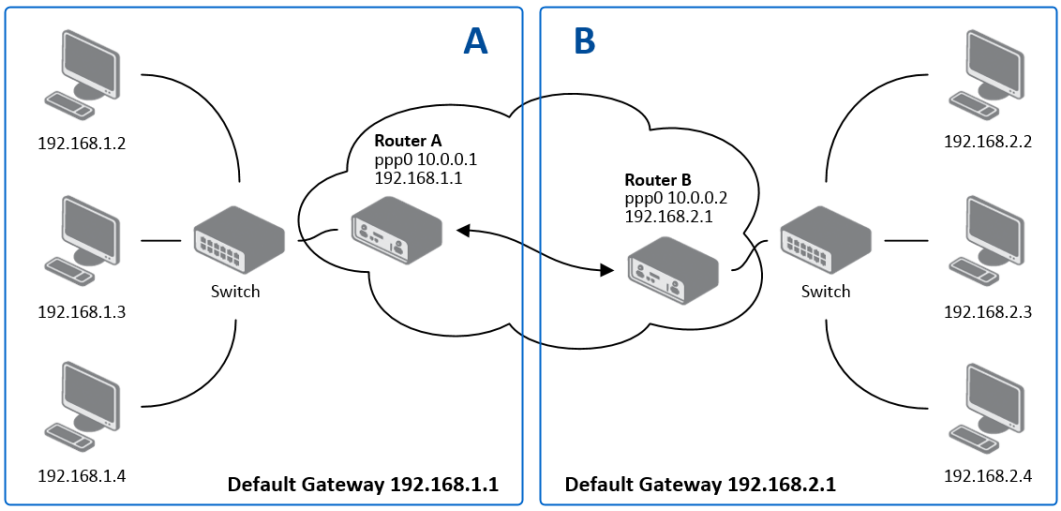


Abb. 55: Topologie für die Konfiguration eines L2TP-Tunnels

Tab. 50: Beispiel für die Konfiguration eines L2TP-Tunnels

Konfiguration	**A**	**B**
Andere Betriebsart	L2TP Server	L2TP Client
Server IP Address	—	10.0.0.1
Client Start IP Address	192.168.1.2	—
Client End IP Address	192.168.1.254	—
Local IP Address	192.168.1.	—
Remote IP Address	—	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	Benutzername	Benutzername
Passwort	Passwort	Passwort

5.16 Konfiguration des PPTP-Tunnels

HINWEIS PPTP ist ein unverschlüsseltes Protokoll. PPTP über IPv6 wird nicht unterstützt.

Wählen Sie im Menü den Eintrag **PPTP**, um einen PPTP-Tunnel zu konfigurieren. PPTP-Tunnel ermöglicht passwortgeschützte Verbindungen zwischen zwei LANs. Es ist ähnlich wie L2TP. Die Tunnel sind aktiv, nachdem Sie **Create PPTP tunnel** ausgewählt haben.

Tab. 51: PPTP-Tunnelkonfiguration

Element	Beschreibung
Andere Betriebsart	PPTP-Tunnelmodus auf der Seite des Routers: • **PPTP server** – im Falle des Servers muss die IP-Adresse des Adressbereichs definiert werden, die vom Server angeboten wird • **PPTP client** – im Falle des Clients muss die IP-Adresse des Servers definiert werden
Server IP Address	IP-Adresse des Servers
Local IP Address	IP-Adresse der lokalen Seite des Tunnels
Remote IP Address	IP-Adresse der Gegenstelle des Tunnels
Remote Subnet	IP-Adresse des Netzes hinter der Gegenstelle des Tunnels
Remote Subnet Mask	Netzmaske hinter der Gegenstelle des Tunnels
MRU**	Maximaler Empfangswert. Standardwert ist 1‘460 Bytes, um fragmentierte Pakete zu vermeiden.
MTU**	Maximaler Sendewert. Standardwert ist 1‘460 Bytes, um fragmentierte Pakete zu vermeiden.
Username	Anmeldename für das Einloggen in den PPTP-Tunnel
Passwort	Passwort für die Anmeldung beim PPTP-Tunnel. Nur gültige Zeichen eingeben, siehe Kapitel 2.1 "Konfigurationsmöglichkeiten", S. 8.
** Nur für v2	

Die Änderungen der Einstellungen wirken sich nach Betätigung der Schaltfläche **Appl**y aus.

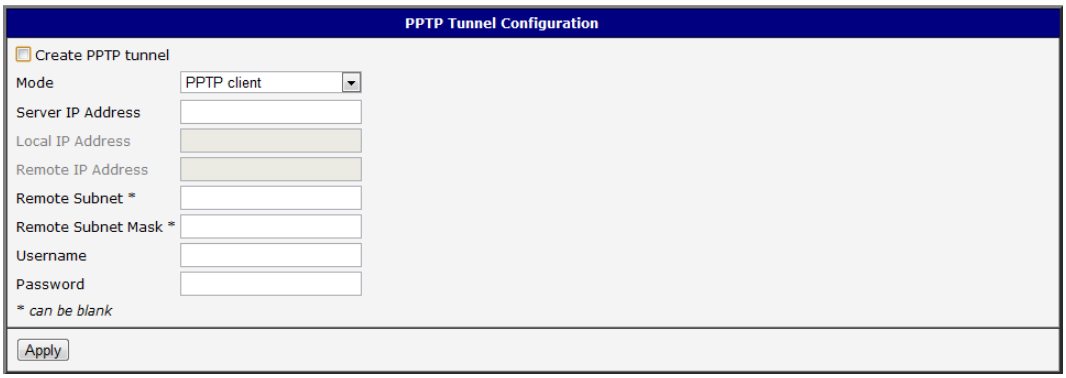


Abb. 56: Konfiguration des PPTP-Tunnels

HINWEIS Die Firmware unterstützt auch für PPTP Passthrough, was bedeutet, dass es möglich ist, einen Tunnel durch den Router einzurichten.

Beispiel für die Konfiguration eines PPTP-Tunnels

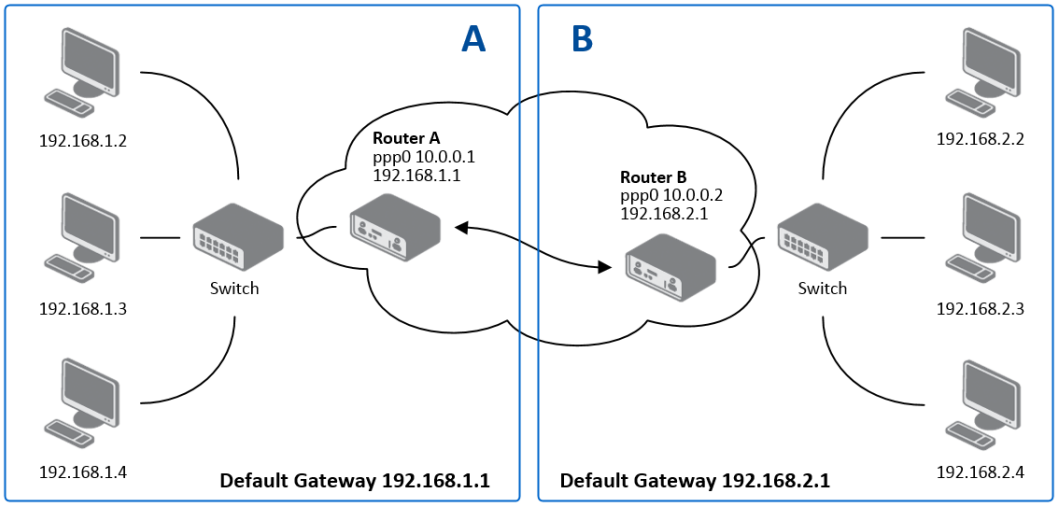


Abb. 57: Topologie des Beispiels für die Konfiguration eines PPTP-Tunnels

Tab. 52: Beispiel für die Konfiguration eines PPTP -Tunnels

Konfiguration	**A**	**B**
Andere Betriebsart	PPTP-Server	PPTP-Client
Server IP Address	—	10.0.0.1
Local IP Address	192.168.1.1	—
Remote IP Address	—	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	Benutzername	Benutzername
Passwort	Passwort	Passwort

5.17 Services

5.17.1 DynDNS

Mit dem DynDNS-Dienst können Sie mit einem leicht zu merkenden benutzerdefinierten Hostnamen aus der Ferne auf den Router zugreifen. Dieser Client überwacht die IP-Adresse des Routers und aktualisiert sie bei jeder Änderung. Damit DynDNS funktioniert, ist eine öffentliche IP-Adresse (statisch oder dynamisch) und ein aktives Konto bei www.dyndns.org (Remote Access Service) erforderlich. Registrieren Sie die benutzerdefinierte Domäne (dritte Ebene) und die Kontoinformationen, die im Konfigurationsformular angegeben sind. Sie können auch andere Dienste nutzen – siehe Tabelle unten, Punkt Server. Um die DynDNS-Konfigurationsseite zu öffnen, klicken Sie im Hauptmenü auf DynDNS.

Tab. 53: Konfiguration von DynDNS

Element	Beschreibung
Hostname	Third Level Domain, die am Server www.dyndns.org registriert ist
Username	Anmeldename für das Einloggen in den DynDNS-Server
Passwort	Passwort für die Anmeldung am DynDNS-Server. Nur gültige Zeichen eingeben, siehe Kapitel 2.1 "Konfigurationsmöglichkeiten", S. 8.
IP Mode	Spezifiziert die Version des IP-Protokolls: • **IPv4** – Nur IPv4 Protokoll wird verwendet (Default). • **IPv6** – Nur IPv6 Protokoll wird verwendet. • **IPv4/IPv6** – IPv4 und IPv6 Dual Stack ist aktiviert.
Server	Gibt einen anderen DynDNS-Dienst als www.dyndns.org an. Mögliche weitere Dienste: www.spdns.de, www.dnsdynamic.org, www.noip.com Geben Sie in dieses Feld die Serviceinformationen des Update-Servers ein. Wenn Sie dieses Feld leer lassen, wird der Standardserver Members.dyndns.org verwendet.

Beispiel für die Konfiguration des DynDNS-Clients mit der Domain wieland.dyndns.org

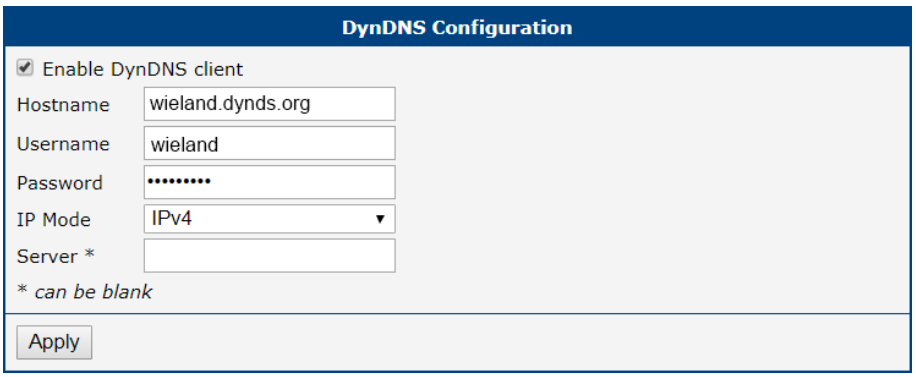


Abb. 58: Beispiel der Konfiguration von DynDNS

HINWEIS Um auf die Konfiguration des Routers ferngesteuert zuzugreifen, ist es notwendig, dies in der NAT-Konfiguration zu aktivieren (unterer Teil des Formulars), siehe Kapitel 5.10 "NAT-Konfiguration", S. 63.

5.17.2 FTP

Das FTP-Protokoll (File Transfer Protocol) kann verwendet werden, um Dateien zwischen dem Router und einem anderen Gerät im Computernetzwerk zu übertragen. Die Konfiguration des FTP-Servers kann auf der Seite **FTP Configuration** unter dem Menüpunkt **Services** durchgeführt werden.

Tab. 54: FTP-Konfiguration

Element	Beschreibung
Enable FTP	Dienst zum Aktivieren des FTP-Servers
Maximum Sessions	Gibt an, wie viele gleichzeitige Verbindungen der FTP-Server akzeptieren soll. Sobald das Maximum erreicht ist, werden zusätzliche Verbindungen zurückgewiesen, bis einige der bestehenden Verbindungen beendet werden. Der Bereich reicht von 1 bis 500.
Session Timeout	Wird verwendet, um inaktive Sitzungen zu schließen. Der Server beendet eine FTP-Sitzung, nachdem sie für die angegebene Anzahl von Sekunden nicht verwendet wurde. Die Bandbreite reicht von 60 bis 7200.

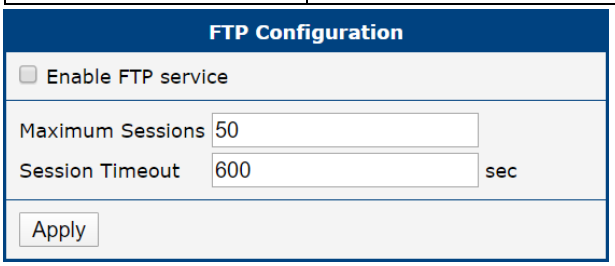


Abb. 59: Konfiguration des FTP-Servers

5.17.3 HTTP

Das HTTP-Protokoll (Hypertext Transfer Protocol) ist ein Internetprotokoll, das für den Austausch von Hypertextdokumenten im HTML-Format verwendet wird. Dieses Protokoll wird für den Zugriff auf den Webserver verwendet, der für die Benutzerkonfiguration des Routers verwendet wird. Empfohlen wird jedoch das HTTPS-Protokoll, das eine Verschlüsselung für den sicheren Austausch der übertragenen Daten verwendet. Die Konfiguration des HTTP- und HTTPS-Dienstes kann auf der Seite **HTTP Configuration** unter dem Menüpunkt **Services** erfolgen. Standardmäßig ist der HTTP-Dienst deaktiviert, und bevorzugt wird der HTTPS-Dienst verwendet. Bei dieser Standardeinstellung wird eine Anfrage zur Kommunikation mit dem HTTP-Protokoll automatisch auf das HTTPS-Protokoll umgeleitet.

Tab. 55: HTTP and HTTPS services configuration

Element	Beschreibung
Enable HTTP service	Aktivierung des HTTP-Dienstes
Enable HTTPS service	Aktivierung des HTTPS-Dienstes
Minimum TLS Version	Falls angegeben, deaktiviert der Router TLS-Versionen, die niedriger als das angegebene Minimum sind. Wählen Sie aus Sicherheitsgründen die höchste Version des TLS-Protokolls, es sei denn, Sie benötigen einen älteren Webbrowser.
Session-Timeout	Inaktivitäts-Timeout, wenn die Sitzung geschlossen wird.
Keep the current certificate	Aktuelles Zertifikat im Router hinterlassen.
Generate a new certificate	Generieren Sie ein neues selbstsigniertes Zertifikat für den Router
Upload a new certificate	Laden Sie ein benutzerdefiniertes PEM-Zertifikat hoch, das von der Zertifizierungsstelle signiert werden kann
Certificate	Wählen Sie eine Datei mit dem PEM-Zertifikat
Private Key	Wählen Sie eine Datei mit dem privaten Schlüssel des Zertifikats

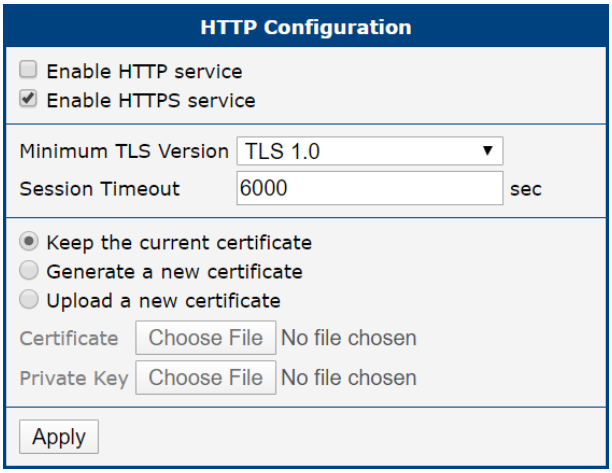


Abb. 60: Konfiguration von HTTP- und HTTPS-Diensten

5.17.4 NTP

Mit dem Konfigurationsformular **NTP** können Sie den NTP-Client konfigurieren.
Um die Seite **NTP** zu öffnen, klicken Sie im Hauptmenü im Abschnitt **Configuration** auf **NTP**. Mit NTP (Network Time Protocol) können Sie die interne Uhr des Routers regelmäßig einstellen. Die Uhrzeit wird von Servern eingestellt, die den Netzwerkgeräten die genaue Uhrzeit zur Verfügung stellen. IPv6-Zeitserver werden unterstützt.

- Wenn Sie das Kontrollkästchen **Enable local NTP service** markieren, fungiert der Router als NTP-Server für andere Geräte im lokalen Netzwerk (LAN).
- Wenn Sie das Kontrollkästchen **Synchronize clock with NTP server** markieren, fungiert der Router als NTP-Client. Das bedeutet, dass der Router die interne Uhr alle 24 Stunden automatisch anpasst.

Tab. 56: NTP-Konfiguration

Element	Beschreibung
Primary NTP Server Address	IPv4-Adresse, IPv6-Adresse oder Domänenname des primären NTP-Servers.
Secondary NTP Server Address	IPv4-Adresse, IPv6-Adresse oder Domänenname des sekundären NTP-Servers.
Timezone	Gibt die Zeitzone an, in der Sie den Router installiert haben.
Daylight Saving Time	• Aktiviert/deaktiviert den DST shift. **No** – Time Shift ist ausgeschaltet • **Yes** – Die Zeitumstellung erfolgt.

Die folgende Abbildung zeigt ein Beispiel für eine NTP-Konfiguration, bei der der primäre Server auf ntp.cesnet.cz und der sekundäre Server auf tik.cesnet.cz eingestellt ist und die automatische Sommerzeitumstellung aktiviert ist.

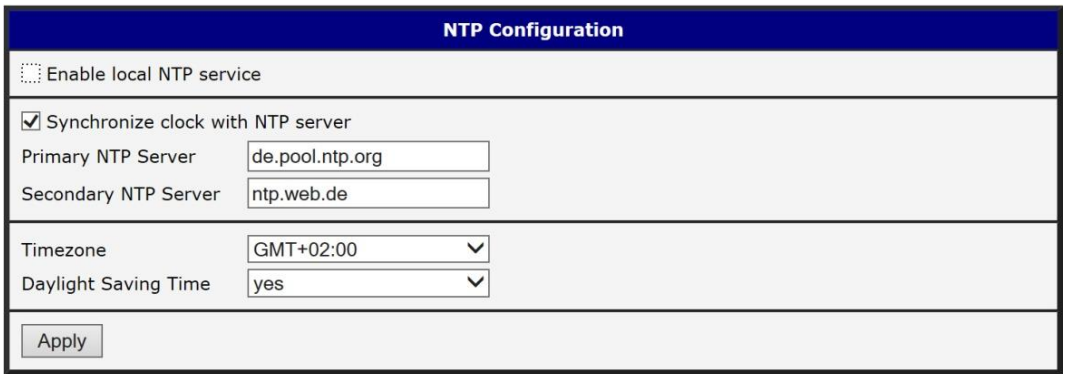


Abb. 61: Beispiel der NTP-Konfiguration

5.17.5 PAM

Ein Pluggable Authentication Module (PAM) ist ein Mechanismus zur Integration mehrerer Low-Level-Authentifizierungsschemata in eine High-Level-Application Programming Interface (API). Die auf dieser Konfigurationsseite vorgenommene Konfiguration wirkt sich auf alle Authentifizierungsmechanismen des Routers aus. Die für die PAM-Authentifizierung verfügbaren Modi sind in der folgenden Tabelle aufgeführt.

Tab. 57: Options for PAM Mode

Element	Beschreibung
local user database	Authentifizieren Sie sich nur gegen die lokale Benutzerdatenbank.
RADIUS with fallback	Authentifizieren Sie sich beim RADIUS-Server und dann bei der lokalen Datenbank, falls der RADIUS-Server nicht erreichbar ist.
RADIUS only	Authentifizieren Sie sich nur beim RADIUS-Server. Beachten Sie, dass Sie sich beim Router nicht authentifizieren können, wenn der RADIUS-Server nicht erreichbar ist!
TACACS+ with fallback	Authentifizieren Sie sich beim TACACS+-Server und dann bei der lokalen Datenbank, falls der TACACS+-Server nicht erreichbar ist.
TACACS+ only	Authentifizieren Sie sich nur beim TACACS+-Server. Beachten Sie, dass Sie sich beim Router nicht authentifizieren können, wenn der TACACS+-Server nicht erreichbar ist!

Um die Authentifizierung gegen einen RADIUS-Server zu konfigurieren, wählen Sie ab dem PAM-Modus RADIUS mit Fallback oder RADIUS only und richten Sie alle erforderlichen Elemente ein.

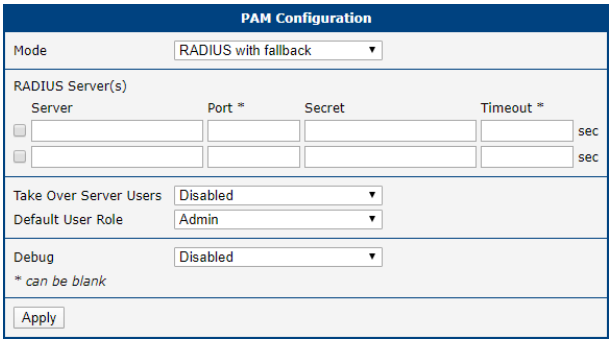


Abb. 62: Konfiguration von RADIUS

Tab. 58: Konfiguration von RADIUS

Element	Beschreibung
Server	Adresse des RADIUS-Servers. Es können bis zu zwei Server konfiguriert werden.
Port	Port des RADIUS-Servers.
Secret	Der geheime Schlüssel zum Überprüfen der Identität des Benutzers.
Timeout	Timeout für die Authentifizierung beim RADIUS-Server.
Take Over Server Users	Wenn aktiviert, wird bei der Anmeldung ein neues Benutzerkonto erstellt, falls die RADIUS-Authentifizierung erfolgreich ist und kein entsprechendes lokales Konto vorhanden ist. Neue Konten werden ohne Passwort erstellt. Ein vorhandenes Benutzerkonto mit Passwort wird durch diese Funktion nie geändert.
Default User Role	Wählen Sie die Standardbenutzerrolle (Admin oder Benutzer).
Debug*	Aktiviert oder deaktiviert die Protokollierung der RADIUS-Debug-Informationen im Systemprotokoll.
* nur für v3	

Um die Authentifizierung gegen einen TACACS+-Server zu konfigurieren, wählen Sie ab dem PAM-Modus TACACS+ mit Fallback oder TACACS+ nur aus und richten Sie alle erforderlichen Elemente ein.

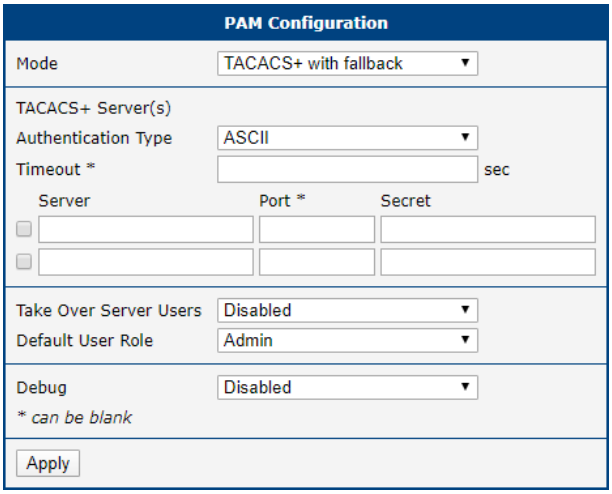


Abb. 63: Konfiguration von TACACS+

Tab. 59: Konfiguration von TACACS+

Element	Beschreibung
Authentication Type	Wählen Sie als Authentifizierungstyp ASCII, PAP oder CHAP aus.
Timeout	Zeitüberschreitung für die Authentifizierung beim TACACS+-Server.
Server	Adresse des TACACS+-Servers. Es können bis zu zwei Server konfiguriert werden.
Port	Port des TACACS+ Servers.
Secret	Der geheime Schlüssel zum Überprüfen der Identität des Benutzers.
Take Over Server Users	Wenn aktiviert, wird bei der Anmeldung ein neues Benutzerkonto erstellt, falls die RADIUS-Authentifizierung erfolgreich ist und kein entsprechendes lokales Konto vorhanden ist. Neue Konten werden ohne Passwort erstellt. Ein vorhandenes Benutzerkonto mit Passwort wird durch diese Funktion nie geändert.
Default User Role	Wählen Sie die Standardbenutzerrolle (Admin oder Benutzer).
Debug*	Aktiviert oder deaktiviert die Protokollierung der TACACS+-Debug-Informationen im Systemlog.
*nur für v3	

Zwei-Faktor-Authentifizierungsservice (nur verfügbar in v2 Routern)

Um den Zwei-Faktor-Authentifizierungsservice zu aktivieren, müssen Sie in der Zwei-Faktor-Authentifizierungsbox wählen zwischen Google Authenticator oder dem OATH-Toolkit und auf **Apply** drücken.

Siehe Kapitel 7.4 "Zwei-Faktor-Authentifizierung (gilt nur für v2 Router)", S. 127, um die Zwei-Faktor-Authentifizierung für einen Benutzer zu konfigurieren.

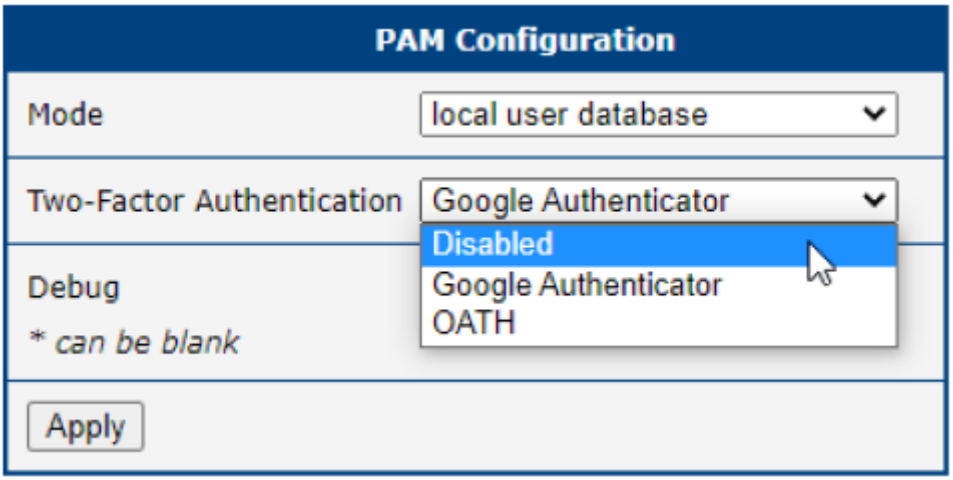


Abb. 64: Aktivierung der Zwei-Faktor-Authentifizierung

5.17.6 SNMP

Auf der Seite **SNMP** können Sie den SNMP v1/v2- oder v3-Agenten konfigurieren, der Informationen über den Router (und eventuell über seine Erweiterungsports) an eine Managementstation sendet.
Um die Seite **SNMP** zu öffnen, klicken Sie im Hauptmenü im Abschnitt **Configuration** auf **SNMP**.
SNMP (Simple Network Management Protocol) liefert Statusinformationen über die Netzwerkelemente wie Router oder Endpoint-Computer. In der Version v3 ist die Kommunikation gesichert (verschlüsselt).
Um den SNMP-Dienst zu aktivieren, markieren Sie das Kontrollkästchen **Enable the SNMP agent**.
Das Senden von SNMP-Traps an eine IPv6-Adresse wird unterstützt.

Tab. 60: Konfiguration des SNMP-Agenten

Element	**Beschreibung**
Bezeichnung	Benennung des Routers.
Location	Ort, an dem Sie den Router installiert haben.
Kontakt	Identifiziert die Person, die den Router verwaltet, zusammen mit den Informationen, wie man diese Person kontaktieren kann.

Um die SNMPv1/v2-Funktion zu aktivieren, markieren Sie das Kontrollkästchen **Enable SNMPv1/v2**.
Für den Zugriff auf den **Community** SNMP-Agenten ist außerdem die Angabe eines Passworts erforderlich. Die Standardeinstellung ist **public**.

Sie können für die Community **Read** (nur lesen) und die Community **Write** (lesen und schreiben) für SNMPv1/v2 ein unterschiedliches Passwort definieren.
Sie können auch 2 SNMP-Benutzer für SNMPv3 definieren. Sie können einen Benutzer als schreibgeschützt (**Read**) und einen anderen als lesend und schreibend (**Write**) definieren. Der Router bietet Ihnen die Möglichkeit, die Parameter in der folgenden Tabelle für jeden Benutzer separat zu konfigurieren. Der Router verwendet die Parameter nur für den SNMP-Zugriff.

Um die SNMPv3-Funktion zu aktivieren, markieren Sie das Kontrollkästchen **Enable SNMPv3 access** und geben Sie dann die folgenden Parameter an:

Tab. 61: SNMPv3-Konfiguration

Element	**Beschreibung**
Username	Benutzername
Authentication	Algorithmus für die Passwortverschlüsselung / Benutzeridentität
Authentication Password	Kennwort zum Generieren des Schlüssels, der für die Authentifizierung verwendet wird. Nur gültige Zeichen eingeben, siehe Kapitel 2.1 "Konfigurationsmöglichkeiten", S. 8.
Privacy	Algorithmus für die Passwortverschlüsselung / Datensicherheit
Privacy Password	Passwort für die Verschlüsselung im Privacy Protocol. Nur gültige Zeichen eingeben, siehe Kapitel 2.1 "Konfigurationsmöglichkeiten", S. 8.

Durch Auswahl der Erweiterung **Enable I/O** ist es möglich, die E/A-Binäreingänge des Routers zu überwachen.

Durch Auswahl von **Enable M-BUS extension** und Eingabe von **Baudrate**, **Parity** und **Stop Bits** können Sie den Status des über MBUS verbundenen Geräts beobachten. Der MBUS-Erweiterungsport wird derzeit nicht unterstützt, es ist jedoch möglich, einen externen RS232/MBUS-Konverter zu verwenden.

Durch Auswahl von **Enable reporting to supervisory system** und Eingabe der **IP Address** und **Period** können Sie statistische Informationen an das Überwachungssystem R-SeeNet senden.

Tab. 62: SNMP-Konfiguration (R-SeeNet)

Element	**Beschreibung**
IP Address	IP-Adresse
Periode	Zeitraum für das Senden statistischer Daten (in Minuten)

Jeder überwachte Wert wird durch einen numerischen Bezeichner **OID – Object Identifier** eindeutig identifiziert. Dieser Bezeichner besteht aus einer Reihe von Zahlen, die durch einen Punkt getrennt sind. Die Form jeder OID wird durch den Bezeichnerwert des Elternelements bestimmt und dieser Wert wird dann durch einen Punkt und eine aktuelle Nummer ergänzt. Es liegt also auf der Hand, dass es sich um eine Baumstruktur handelt. Die folgende Abbildung zeigt die grundlegende Baumstruktur, die zum Erstellen der OIDs verwendet wird.

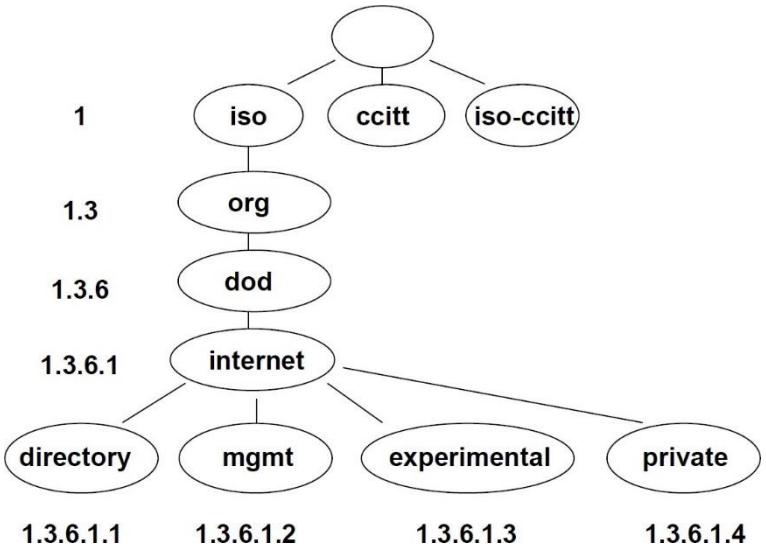


Abb. 65: Konfiguration von TACACS+

Die für Conel-Router spezifischen SNMP-Werte erstellen den Baum beginnend bei OID = .1.3.6.1.4.1.30140. Sie interpretieren die OID wie folgt:

iso.org.dod.internet.private.enterprises.conel

Das bedeutet, dass der Router beispielsweise Informationen über die interne Temperatur (OID 1.3.6.1.4.1.30140.3.3) oder über die Netzspannung (OID 1.3.6.1.4.1.30140.3.4) liefert. Für binäre Ein- und Ausgänge wird der folgende OID-Bereich verwendet:

Tab. 63: Objektbezeichner für binären Eingang und Ausgang

OID	Beschreibung
.1.3.6.1.4.1.30140.2.3.1.0	Binärer Eingang BIN0 (Werte 0,1)
.1.3.6.1.4.1.30140.2.3.2.0	Binärer Ausgang OUT0 (Werte 0,1)
.1.3.6.1.4.1.30140.2.3.3.0	Binärer Eingang BIN1 (Werte 0,1)

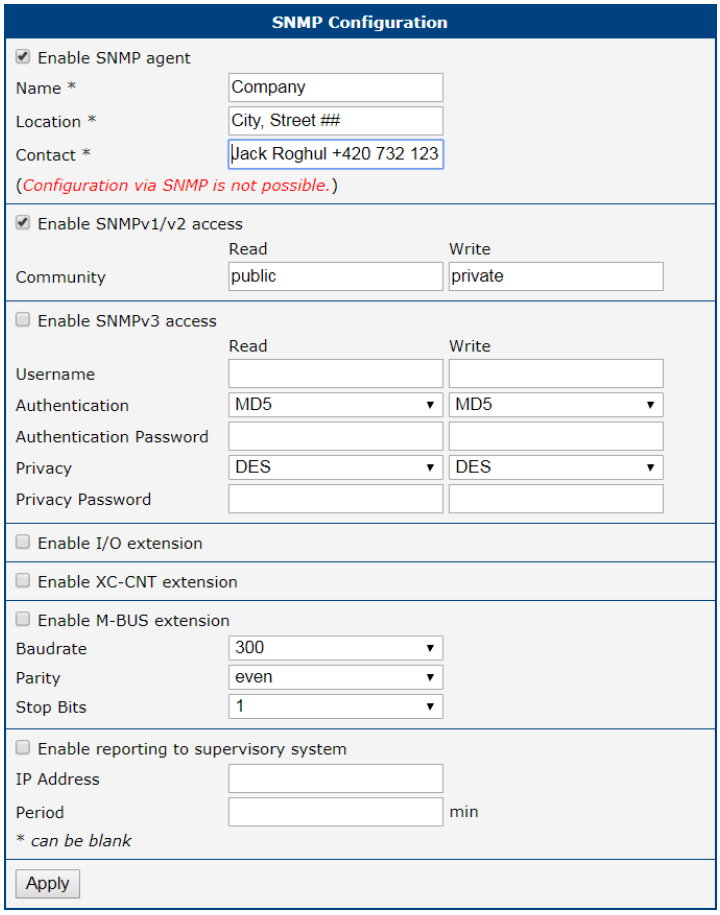


Abb. 66: Beispiel der SNMP-Konfiguration

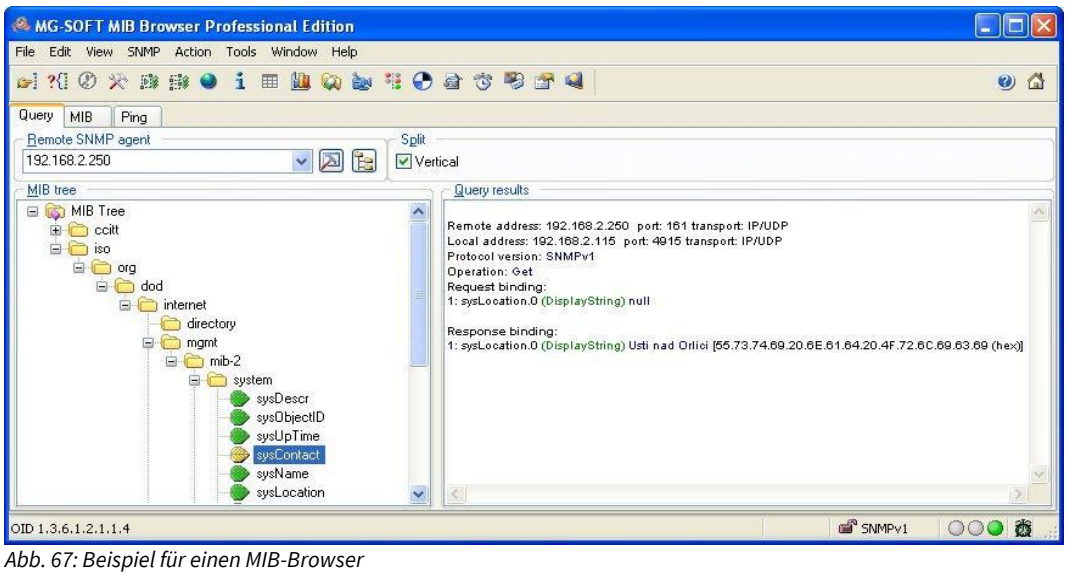


Abb. 67: Beispiel für einen MIB-Browser

Um auf ein bestimmtes Gerät zuzugreifen, geben Sie im Feld Remote SNMP agent die IP-Adresse des SNMP-Agenten, der der Router ist, ein. Der Dialog zeigt nach Eingabe der IP-Adresse die internen Variablen im MIB-Baum an. Außerdem können Sie den Status der internen Variablen durch Eingabe ihrer OID ermitteln.

Der Pfad zu den Variablen ist:

iso → org → dod → internet → private → enterprises → wieland → protocols

Der Pfad zu den Grundangaben des Routers ist:

iso → org → dod → internet → mgmt → mib-2 → system

5.17.7 SMTP

Der Punkt **SMTP** dient zur Konfiguration des SMTP-Clients (Simple Mail Transfer Protocol) zum Versenden von E-Mails. IPv6-E-Mail-Server werden unterstützt.

Tab. 64: Konfiguration des SMTP-Clients

Element	Beschreibung
SMTP Server Address	IPv4/IPv6 oder Domänenadresse des Mailservers.
SMTP Port	Port, auf den der SMTP-Server hört
Sichere Methode	none, SSL/TLS, oder STARTTLS. Die sichere Methode muss durch den SMTP-Server unterstützt werden.
Username	Benutzername zum E-Mail-Konto.
Passwort	Passwort für E-Mail-Konto. Nur gültige Zeichen eingeben, siehe Kapitel 2.1 "Konfigurationsmöglichkeiten", S. 8.
Own E-mail Address	E-Mail-Adresse des Absenders

HINWEIS

Der Mobilfunkanbieter kann andere SMTP-Server blockieren, dann können Sie nur den SMTP-Server des Betreibers verwenden.

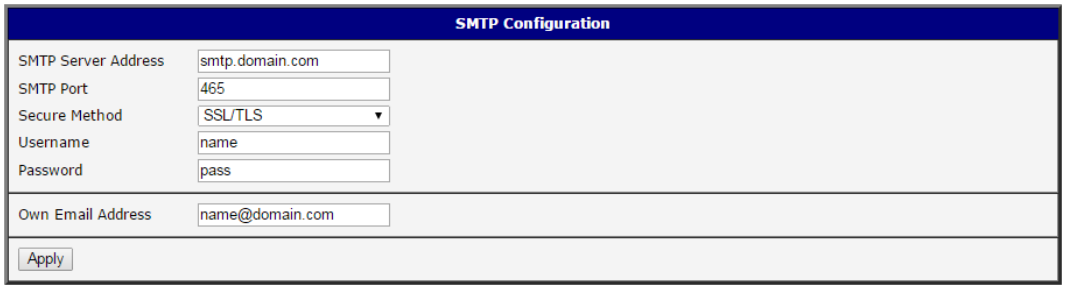


Abb. 68: Beispiel für die Konfiguration des SMTP-Clients

Sie können E-Mails über das Startup-Skript senden. Das Dialogfeld **Startup Script** befindet sich unter **Scripts** im Abschnitt **Configuration** des Hauptmenüs. Der Router ermöglicht auch das Versenden von E-Mails über eine SSH-Verbindung. Verwenden Sie den Befehl `email` mit den folgenden Parametern:

Tab. 65: Parameter für das Versenden von E-Mails

Parameter	Beschreibung
`-t`	E-Mail-Adresse des Empfängers
`-s`	Betreff der Nachricht (muss in Anführungszeichen stehen)
`-m`	Nachricht (muss in Anführungszeichen stehen)
`-a`	Anlage
`-r`	Anzahl der Sendeversuche (Standard: 2 Versuche)

VORSICHT

Befehle und Parameter können nur in Kleinbuchstaben eingegeben werden.

Beispiel zum Versenden einer E-Mail: `email -t name@domain.com -s "subject" -m "message" -a c:\directory\abc.doc -r 5`

Dieser Befehl verschickt eine E-Mail an die E-Mail-Adresse **name@domain.com** mit dem Betreff der Nachricht "subject", der eigentlichen Nachricht "**message**" und der Anlage "abc.doc" aus dem Verzeichnis "c:\directory\" und 5 Versuchen, die Nachricht zuzustellen.

5.17.8 SMS

HINWEIS Die wienet LAN Router zeigen keine SMS-Konfiguration an.

Öffnen Sie die Seite **SMS** im Untermenü **Services** des Abschnitts **Configuration** des Hauptmenüs. Der Router kann bei bestimmten Ereignissen automatisch SMS-Nachrichten an ein Mobiltelefon oder einen SMS-Nachrichtenserver senden. Im Formular können Sie auswählen, welche Ereignisse eine SMS-Nachricht generieren.

Tab. 66: Konfiguration Versenden von SMS

Element	Beschreibung
Send SMS on power up	Aktiviert/deaktiviert das automatische Senden einer SMS-Nachricht beim Einschalten.
Send SMS on connect to mobile network	Aktiviert/deaktiviert das automatische Versenden einer SMS-Nachricht, wenn der Router mit einem Mobilfunknetz verbunden ist.
Send SMS on disconnect to mobile network	Aktiviert/deaktiviert das automatische Versenden einer SMS-Nachricht, wenn der Router vom Mobilfunknetz getrennt wird.
Send SMS when datalimit exceeded	Aktiviert/deaktiviert den automatischen Versand einer SMS-Nachricht bei Überschreitung des Datenlimits.
Send SMS when binary input on I/O port (BIN0) is active	Automatischer SMS-Versand bei aktivem Binärausgang des Routers, deren Text durch den Parameter BIN0 festgelegt wird.
Add timestamp to SMS	Aktiviert/deaktiviert das Hinzufügen eines Zeitstempels zu den SMS-Nachrichten. Dieser Zeitstempel hat ein festes Format YYYY-MM-DD hh:mm:ss.
Phone Number 1	Telefonnummer für das Versenden der automatisch generierten SMS.
Phone Number 2	Telefonnummer für das Versenden der automatisch generierten SMS.
Phone Number 3	Telefonnummer für das Versenden der automatisch generierten SMS.
Unit ID	Der Name des Routers. Der Router sendet den Namen in der SMS.
BIN0 – SMS	Text der SMS-Nachricht, wenn der Binäreingang aktiviert ist.

Fernsteuerung durch SMS

Nachdem Sie eine Telefonnummer in das Feld Telefonnummer 1 eingegeben haben, ermöglicht Ihnen der Router, die Steuerung des Geräts mithilfe einer SMS-Nachricht zu konfigurieren. Sie können bis zu drei Nummern für eingehende SMS-Nachrichten konfigurieren. Um die Funktion zu aktivieren, markieren Sie das Kontrollkästchen **Enable Remote Control via SMS**. Die Standardeinstellung der Funktion Fernbedienung ist aktiv.

Tab. 67: Steuerung über SMS-Konfiguration

Element	Beschreibung
Phone Number 1	Gibt die erste Telefonnummer an, die per SMS auf den Router zugreifen darf.
Phone Number 2	Gibt die zweite Telefonnummer an, die per SMS auf den Router zugreifen darf.
Phone Number 3	Gibt die dritte Telefonnummer an, die per SMS auf den Router zugreifen darf.

HINWEIS
- Wenn Sie eine oder mehrere Telefonnummern eingeben, können Sie den Router mit SMS-Nachrichten steuern, die nur von den angegebenen Telefonnummern gesendet werden.
- Wenn Sie das Wildcard-Zeichen * eingeben, können Sie den Router mit SMS-Nachrichten steuern, die von einer beliebigen Telefonnummer gesendet werden.

Die meisten Kontroll-SMS ändern die Router-Konfiguration nicht. Wird der Router beispielsweise per SMS in den Offline-Modus versetzt, verbleibt der Router in diesem Modus, kehrt aber nach dem Neustart in den Online-Modus zurück. Die einzige Ausnahme ist der Befehl set profile, der die Konfiguration dauerhaft ändert, siehe Tabelle unten.

Um den Router per SMS zu steuern, senden Sie nur den Nachrichtentext, der den Steuerbefehl enthält. Sie können Kontroll-SMS-Nachrichten in der folgenden Form senden:

Tab. 68: Control SMS

SMS	Beschreibung
go online sim 1	Wechseln zu Karte SIM1
go online sim 2	Wechseln zu Karte SIM2
go online	Der Router wird in den Online-Modus umgeschaltet
go offline	Der Router wird in den Offline-Modus umgeschaltet
set out0=0	Binärausgang auf 0 setzen
set out0=1	Binärausgang auf 1 setzen
set profile std	Standardprofil einstellen, diese Änderung ist dauerhaft.
set profile alt1	Alternatives Profil 1 einstellen, diese Änderung ist dauerhaft.
set profile alt2	Alternatives Profil 2 einstellen, diese Änderung ist dauerhaft.
set profile alt3	Alternatives Profil 3 einstellen, diese Änderung ist dauerhaft.
reboot	Reboot des Routers
get ip	Der Router antwortet mit der IP-Adresse der SIM-Karte



Jede empfangene Kontroll-SMS wird verarbeitet und anschließend vom Router gelöscht! Dies kann zu Verwirrung führen, wenn Sie das AT-SMS-Protokoll zum Lesen empfangener SMS verwenden möchten (siehe Abschnitt unten).

Erweiterte SMS-Steuerung:

Wenn in empfangenen SMS ein unbekannter Befehl vorhanden ist und die Fernsteuerung per SMS aktiviert ist, wird das Skript in "/var/scripts/sms" ausgeführt, bevor die SMS gelöscht wird. Mit diesem Skript ist es möglich, eigene zusätzliche SMS-Befehle zu definieren. In solchen SMS können maximal 7 Wörter verwendet werden. Da sich die Skriptdatei im RAM des Routers befindet, ist es möglich, die Erstellung einer solchen Datei zum Startskript hinzuzufügen.

AT-SMS-Protokoll

Das AT-SMS-Protokoll ist ein privater Satz von AT-Befehlen, die von den Routern unterstützt werden. Es kann verwendet werden, um über häufig verwendete AT-Befehle direkt auf das Mobilfunkmodul im Router zuzugreifen, mit Kurznachrichten (SMS senden) und Statusinformationen und Einstellungen des Mobilfunkmoduls zu arbeiten.

Durch Auswahl von **Enable AT-SMS protocol on expansion port 1** bzw. **Enable AT-SMS protocol on expansion port 2** und **Baudrate** ist es möglich, eine SMS über den seriellen Port 1 bzw. 2 zu senden/empfangen.

Tab. 69: AT-SMS-Protokoll über serielle Ports

Element	Beschreibung
Baudrate	Übertragungsgeschwindigkeit am Erweiterungsport 1
	Übertragungsgeschwindigkeit am Erweiterungsport 2

Durch die Auswahl der Option **Enable AT-SMS protocol on TCP port** und Eingabe des TCP-Ports (bei **TCP port**) ist es möglich, das Versenden/Empfangen von SMS-Nachrichten am TCP-Port freizugeben. SMS-Nachrichten werden mittels der bekannten AT-Befehle versandt.

Tab. 70: AT-SMS-Protokoll am TCP-Port

Element	Beschreibung
TCP Port	TCP-Port, der das Senden/Empfangen von SMS-Nachrichten erlaubt.

Wenn Sie über eine serielle Schnittstelle oder Ethernet (TCP) eine Verbindung zum Router aufbauen, können Sie mit AT-Befehlen SMS-Nachrichten verwalten.

In der folgenden Tabelle sind nur die von den Routern unterstützten Befehle aufgeführt. Bei anderen AT-Befehlen wird immer die OK-Antwort gesendet. Es gibt keine Unterstützung für die Behandlung komplexer AT-Befehle, daher sendet der Router in einem solchen Fall eine ERROR-Antwort.

Tab. 71: Liste der AT-Befehle

AT-Befehl	**Beschreibung**
AT+CGMI	Fragt den Hersteller ab
AT+CGMM	Fragt das Modell ab
AT+CGMR	Fragt Revisionsinformationen des Modells ab
AT+CGPADDR	Fragt die IP-Adresse der ppp0-Schnittstelle ab
AT+CGSN	Fragt die Seriennummer des Produktes ab
AT+CIMI	Fragt die International Mobile Subscriber Identity Number (IMSI) ab
AT+CMGD	Löscht eine SMS-Nachricht
AT+CMGF	Stellt das Format für die Anzeige von SMS ein
AT+CMGL	Listet Nachrichten aus dem Nachrichtenspeicher zu einem bestimmten Status auf
AT+CMGR	Liest eine Nachricht aus dem Nachrichtenspeicher
AT+CMGS	Sendet eine SMS vom Gerät an die eingegebene Telefonnummer
AT+CMGW	Schreibt eine SMS in den SIM-Speicher
AT+CMSS	Sendet eine Nachricht vom SIM-Speicher
AT+COPS?	Identifiziert alle verfügbaren Mobilfunknetze
AT+CPIN	Wird verwendet um den PIN-Code abzufragen und einzugeben
AT+CPMS	Wählt den SMS-Nachrichtenspeichertyp, der für den SMS-Betrieb verwendet wird
AT+CREG	Zeigt den Status der Netzwerkregistrierung an
AT+CSCA	Legt die Nummer des Kurznachrichtendienstzentrums (SMSC) fest
AT+CSCS	Wählt den Zeichensatz
AT+CSQ	Gibt die Signalstärke des registrierten Netzwerks aus
AT+GMI	Fragt den Hersteller ab
AT+GMM	Fragt das Modell ab
AT+GMR	Fragt Revisionsinformationen des Modells ab
AT+GSN	Fragt die Seriennummer des Produktes ab
ATE	Bestimmt, ob das Gerät die empfangenen Zeichen wiederholt oder nicht (Echo)
ATI	Überträgt die herstellerspezifischen Informationen über das Gerät

SMS vom Router senden

Es gibt weitere Möglichkeiten, um eigene SMS vom Router zu senden:

- Verwendung des oben beschriebenen AT-SMS-Protokolls – Wenn Sie eine Verbindung zum Router über eine serielle Schnittstelle oder Ethernet (TCP) herstellen, können Sie mit AT-Befehlen SMS-Nachrichten senden und verwalten.
- Verwenden der HTTP POST-Methode für eine Remote-Ausführung, Aufrufen von CGI-Skripten im Router. Weitere Informationen und Beispiele finden Sie in der Anwendungsnotiz Befehle und Skripte [1].
- Über die Weboberfläche des Routers im Abschnitt **Administration**, SMS-Element senden, siehe Kapitel 7.9 "Versenden einer SMS-Nachricht", S. 133.
- Mit dem Befehl `gsmsms` z. B. im Terminal, wenn über SSH mit dem Router verbunden.

Beispiele: Konfiguration des SMS-Versands

Nach dem Einschalten des Routers wird eine SMS an die definierte Rufnummer im folgenden Format gesendet: Router (Unit ID) has been powered up. Signal strength –xx dBm.

Nach der Verbindung mit dem Mobilfunknetz wird eine SMS an die definierte Telefonnummer im folgenden Format gesendet: Router (Unit ID) has established connection to mobile network. IP address xxx.xxx.xxx.xxx

Nach dem Trennen zum Mobilfunknetz wird eine SMS im folgenden Format an die definierte Telefonnummer gesendet: Router (Unit ID) has lost connection to mobile network. IP address xxx.xxx.xxx.xxx

Beispiel 1: SMS-Konfiguration

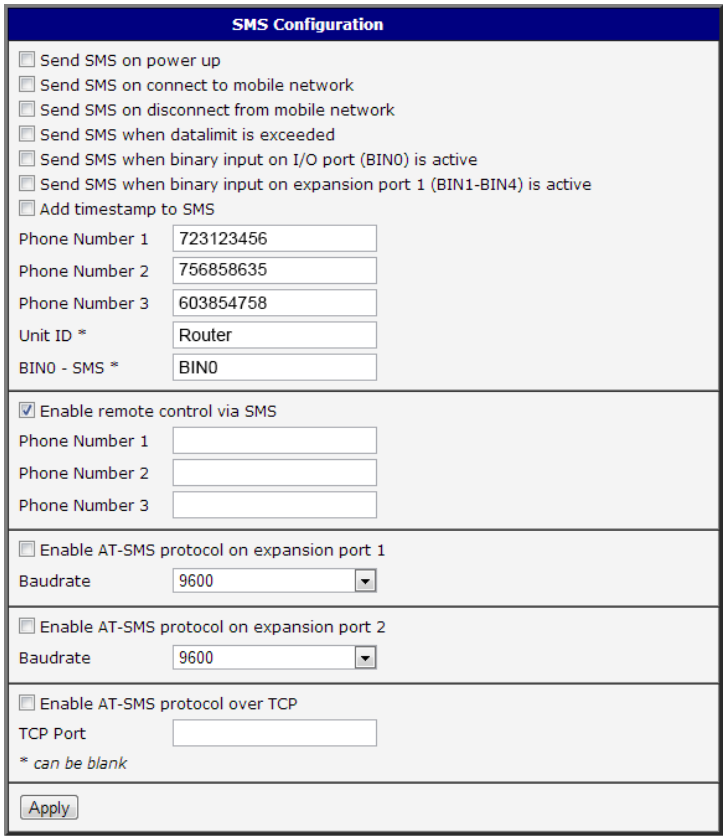


Abb. 69: Beispiel 1 – SMS-Konfiguration

Beispiel 2: Einstellung des Routers zum Versand von SMS-Nachrichten über die serielle Schnittstelle (PORT 1)

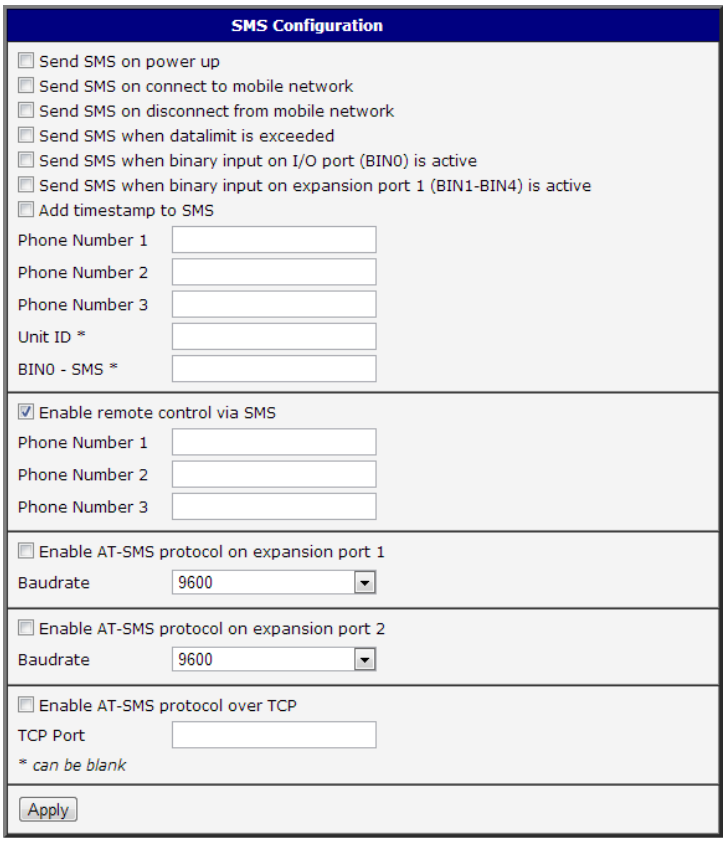


Abb. 70: Beispiel 2 – Versand von SMS über serielle Schnittstelle

Beispiel 3: Einstellung des Routers für die Steuerung mittels SMS-Nachrichten von einer beliebigen Telefonnummer aus

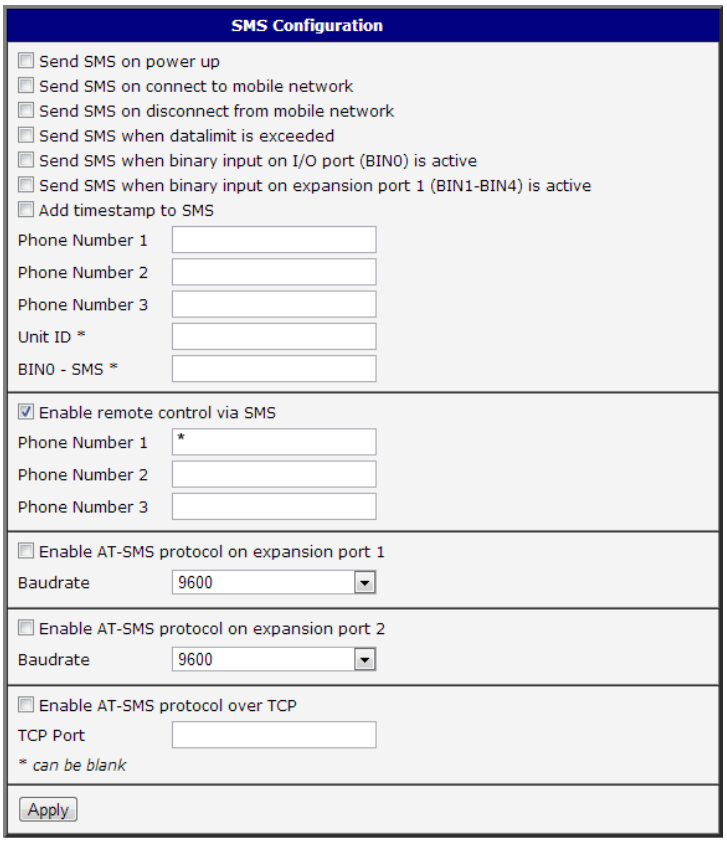


Abb. 71: Beispiel 3 – Steuerung per SMS von einer beliebigen Telefonnummer

Beispiel 4: Konfiguration der Steuerung des Routers per SMS von den beiden Telefonnummern

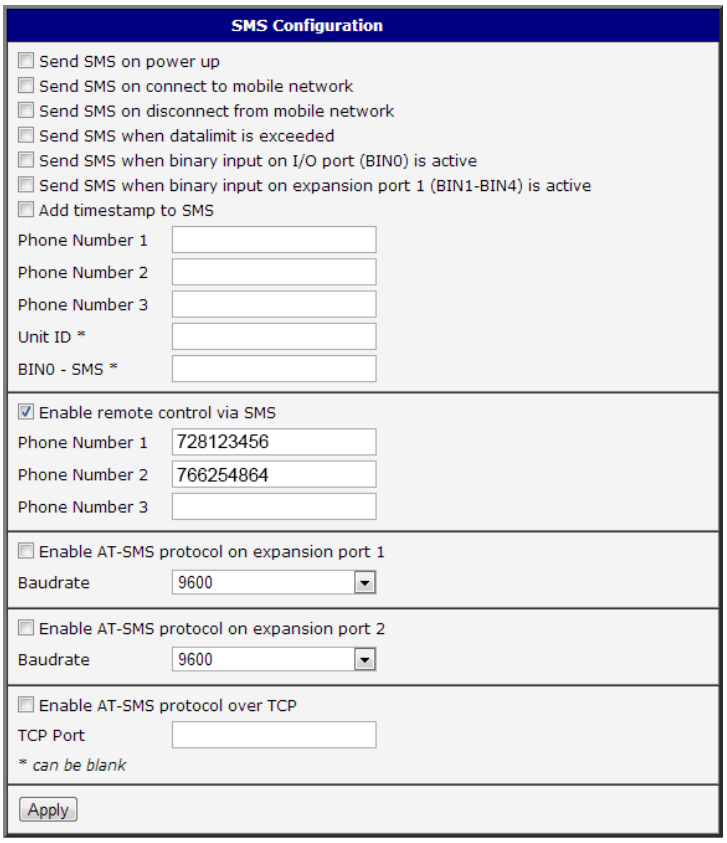


Abb. 72: Beispiel 4 – Steuerung per SMS von beiden Telefonnummern

5.17.9 SSH

Das SSH-Protokoll (Secure Shell) ermöglicht eine sichere Remote-Anmeldung am Router. Die Konfiguration des SSH-Dienstes kann auf der Konfigurationsseite **SSH** unter dem Menüpunkt **Services** erfolgen. Durch Ankreuzen des Elements **Enable SSH service** wird der SSH-Server auf dem Router aktiviert.

Tab. 72: SSH Service Konfiguration

Element	**Beschreibung**
Enable SSH service	Aktivieren des SSH-Dienstes.
Session-Timeout	Inaktivitäts-Timeout, wenn die Sitzung geschlossen wird.
Keep the current SSH key**	Aktuellen SSH-Schlüssel beibehalten.
Generate a new SSH key**	Generierung eines neuen SSH-Schlüssels.
Key Length**	Länge des zu generierenden SSH-Schlüssels.
** nur für v2	

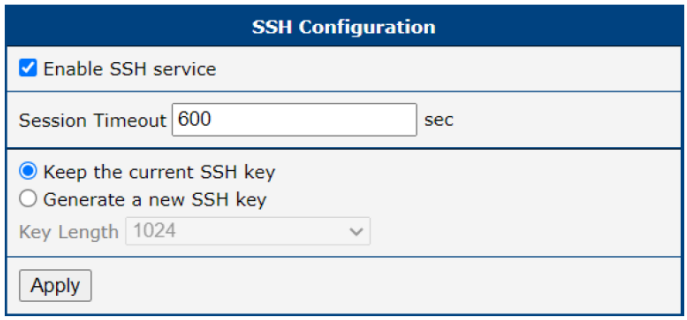


Abb. 73: Konfiguration des HTTP-Dienstes

5.17.10 Syslog

Die Konfiguration des Systemprotokolls, genannt syslog, kann auf dieser Konfigurationsseite vorgenommen werden. Die Größe dieses Protokolls kann durch die maximale Anzahl seiner Zeilen eingeschränkt werden. Optional können die IP-Adresse und der UDP-Port für die Echtzeit-Logverteilung konfiguriert werden.

Tab. 73: SSH Service Konfiguration

Element	**Beschreibung**
Log Size	Beschränkung der Protokollgröße durch die maximale Anzahl seiner Zeilen.
Remote IP Address	Optionale Einstellungen der IP-Adresse für die Echtzeit-Logverteilung.
Remote UDP Port	Optionale Einstellungen des UDP-Ports für die Echtzeit-Logverteilung.
Device ID**	Optionale Einstellungen der Routeridentifikation zur Fernprotokollierung. Falls das Feld leer bleibt, wird *Router* verwendet.
** nur für v2	

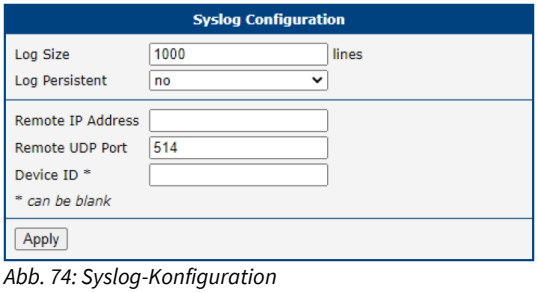


Abb. 74: Syslog-Konfiguration

5.17.11 Telnet

Telnet ist ein Protokoll, das verwendet wird, um eine bidirektionale interaktive textorientierte Kommunikationseinrichtung mit dem Router bereitzustellen. Die Konfiguration des Telnet-Dienstes kann auf der Telnet-Konfigurationsseite unter dem Menüpunkt **Dienste** vorgenommen werden.

Tab. 74: SSH Service Konfiguration

Element	Beschreibung
Enable Telnet service	Aktivierung des Telnet-Dienstes
Maximum Sessions	Wird verwendet, um inaktive Sitzungen zu schließen. Der Server beendet eine Telnet-Sitzung, nachdem sie für die angegebene Anzahl von Sekunden nicht verwendet wurde. Der Bereich reicht von 1 bis 500.

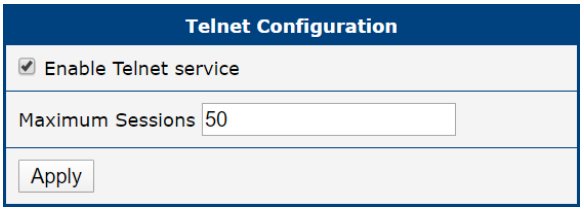
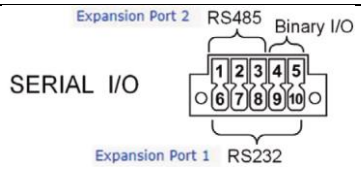
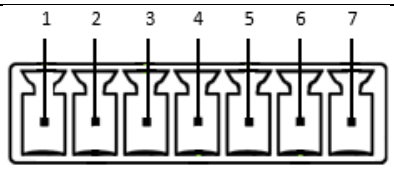


Abb. 75: Syslog-Konfiguration

5.18 Erweiterungsport – Konfiguration der seriellen Schnittstellen

Die Konfiguration der seriellen bzw. der RS232- und RS485-Schnittstelle kann über die Elemente **Expansion Port 1** bzw. **Expansion Port 2** im Menü erfolgen.

Tab. 75: Unterschiede der seriellen Schnittstellen bei v2 und v3 Routern

Router	v3	v2
	 *Abb. 76: Konfiguration der seriellen I/Os*	 *Abb. 77: RS232 und RS485 Pinbelegung*
Binäre I/Os	Die binären in- und Outputs können auf verschiedene Arten verwendet werden • Versenden von SMS über den binären Input • Setzen des binären Outputs via SMS • Lesen des Status der binären I/Os durch SNMP • Umschalten von SIM-Karten über den binären Input • Die binären I/Os können gelesen oder via *Scripts* durch Befehle gesetzt werden	-

Im oberen Teil des Konfigurationsfensters kann der Port aktiviert werden und der Typ des angeschlossenen Ports wird im Element **Port Type** angezeigt. Weitere Elemente sind in der folgenden Tabelle beschrieben. IPv6 TCP/UDP-Client/Server werden unterstützt.

Tab. 76: Konfiguration des wählbaren Ports – serielle Schnittstelle

Element	Beschreibung
Baudrate	Angewandte Geschwindigkeit der Kommunikation.
Data Bits	Anzahl der Datenbits
Parity	Kontroll-Paritätsbit • **none** – es wird keine Parität versandt • **even** – es wird eine gerade Parität versandt • **odd** – es wird eine ungerade Parität versandt
Stop Bits	Anzahl der Stoppbits
Flow Control	Setzen Sie die Flusssteuerung auf **none** oder **Hardware**.
Split Timeout	Zeit bis zum Abbrechen von Reports. Wenn die Lücke zwischen zwei Zeichen den Wert des Parameters in Millisekunden überschreitet, werden alle gepufferten Zeichen gesendet über den Ethernet-Port.
Protokoll	Protokoll: • **TCP** – Kommunikation über das Protokoll TCP (verbindungsorientiert) • **UDP** – Kommunikation über das Protokoll UDP (verbindungslos)
Andere Betriebsart	Kommunikationsmodus: • **TCP server** – der Router hört die eingehenden Anfragen über die TCP-Verbindung ab • **TCP** client – der Router verbindet sich zum TCP-Server an der angegebenen IP-Adresse und am TCP-Port
Server Adresse	Wenn oben TCP-Client eingestellt ist, müssen die Serveradresse und der TCP-Port eingegeben werden. IPv4- und IPv6-Adressen sind zulässig.
TCP Port	TCP/UDP-Port, der für die Kommunikation verwendet wird. Der Router verwendet den Wert sowohl für den Server- als auch für den Client-Modus.
Inactivity Timeout	Zeitraum, nach dem die TCP/UDP-Verbindung bei Inaktivität unterbrochen wird

Wenn Sie das Kontrollkästchen **Reject new connections** markieren, weist der Router alle anderen Verbindungsversuche zurück. Das bedeutet, dass der Router keine Mehrfachverbindungen mehr unterstützt.

Wenn Sie das Kontrollkästchen **Check TCP connection** markieren, überprüft der Router die TCP-Verbindung.

Tab. 77: Konfiguration des Erweiterungsports – check TCP connection

Element	Beschreibung
Keepalive Time	Zeit, nach der der Router eine Überprüfung der Verbindung durchführt
Keepalive Interval	Wartezeit des Routers auf eine Antwort
Keepalive Probes	Anzahl der Tests, die der Router durchführt

Wenn Sie das Kontrollkästchen **Use CD as indicator of the TCP connection** markieren, verwendet der Router das Trägererkennungssignal (CD), um den Status der TCP-Verbindung zu überprüfen. Das CD-Signal überprüft, ob ein anderes Gerät an der anderen Seite des Kabels angeschlossen ist.

Tab. 78: Beschreibung des CD-Signals

CD	Beschreibung
Aktiv	TCP-Verbindung ist aktiviert
Nonactive	TCP-Verbindung ist deaktiviert

Wenn Sie das Kontrollkästchen **Use DTR as control of TCP connection** markieren, verwendet der Router das Data Terminal Ready (DTR) Signal, um die TCP-Verbindung zu kontrollieren. Das Remote-Gerät sendet ein DTR-Signal an den Router, das anzeigt, dass das entfernte Gerät für die Kommunikation bereit ist.

Tab. 79: Beschreibung des DTR-Signals

DTR	Verhalten des Servers	Verhalten des Clients
Aktiv	Der Router ermöglicht den Aufbau von TCP-Verbindungen.	Der Router baut die TCP-Verbindung auf.
Nonactive	Der Router verweigert den Aufbau von TCP-Verbindungen.	Der Router trennt die TCP-Verbindung.

Die Änderungen der Einstellungen wirken sich nach Betätigung der Schaltfläche **Apply** aus.

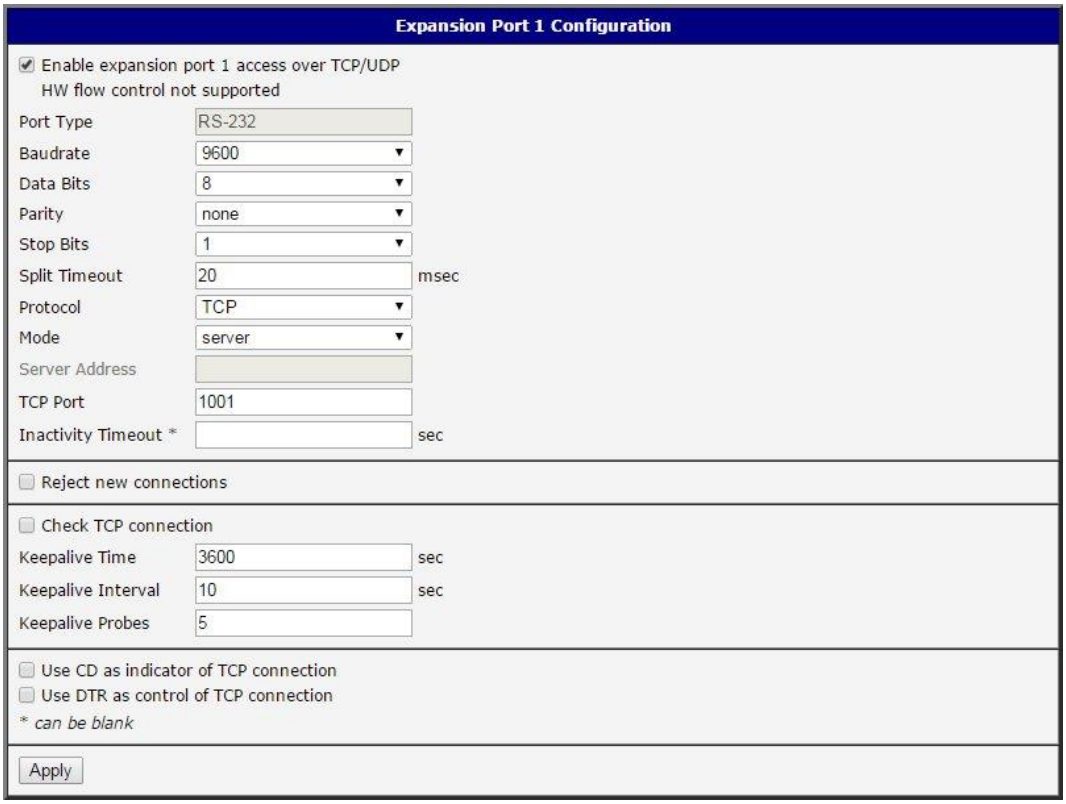


Abb. 78: Konfiguration des Erweiterungsports

Beispiele für die Konfiguration des Erweiterungsports:

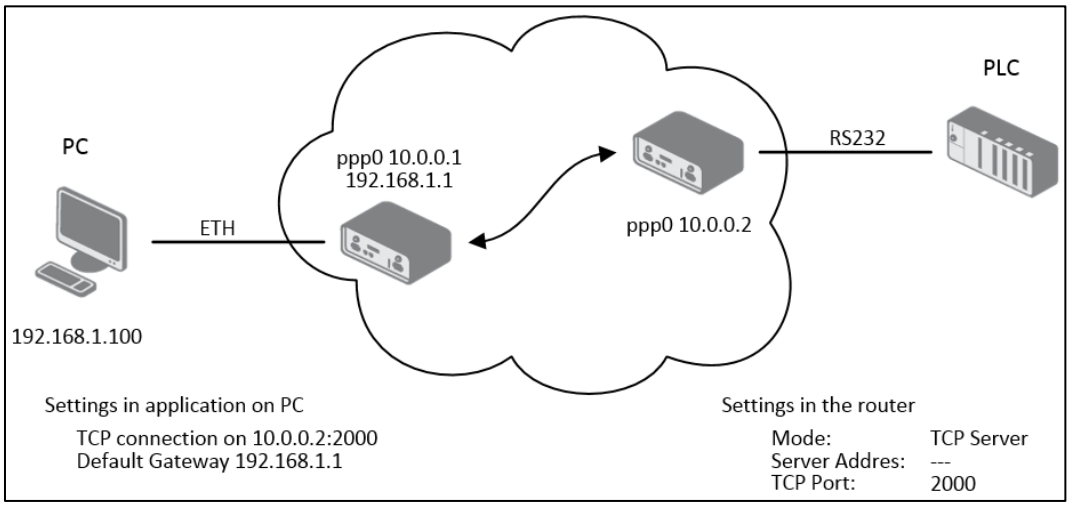


Abb. 79: Beispiel 1 – Konfiguration des Erweiterungsports

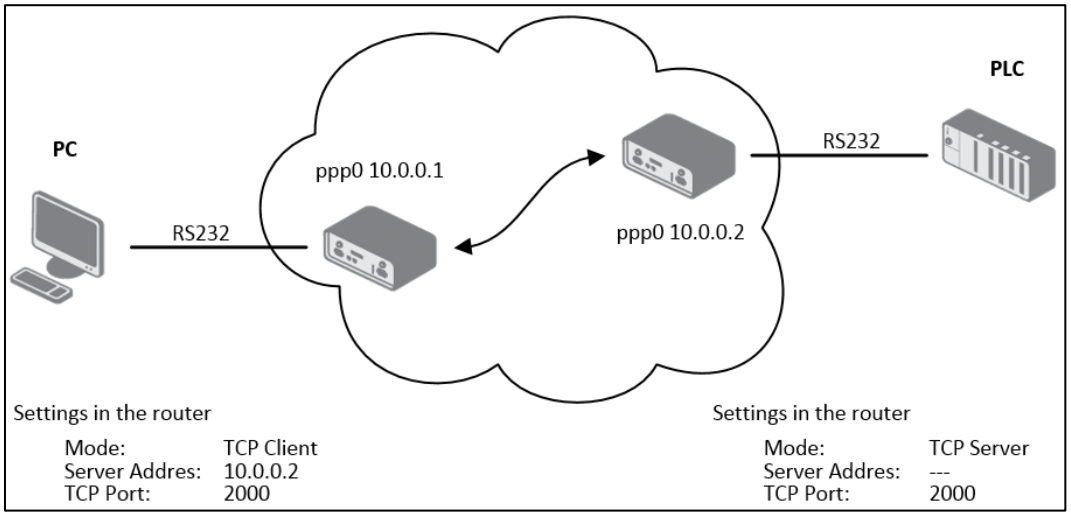


Abb. 80: Beispiel 2 – Konfiguration des Erweiterungsports

5.19 Konfiguration des USB-Ports

HINWEIS Gilt nur, falls der Router über einen USB-Port verfügt.

Sie können einen USB-zu-RS232-Konverter verwenden, um Daten vom seriellen Port aus dem Ethernet-Netzwerk auf die gleiche Weise wie die RS232-Erweiterungsportfunktion zu senden. Um die Werte für die USB-Port-Parameter festzulegen, klicken Sie im Hauptmenü im Abschnitt **Configuration** auf den Eintrag **USB-Port**. Die folgenden Tabellen beschreiben die im Konfigurationsformular verfügbaren Parameter. IPv6 TCP/UDP-Client/Server werden unterstützt.

Tab. 80: Konfiguration des USB-Ports 1

Element	Beschreibung
Baudrate	Angewandte Geschwindigkeit der Kommunikation.
Data Bits	Anzahl der Datenbits
Parity	Kontroll-Paritätsbit: • **none** – es wird keine Parität versandt • **even** – es wird eine gerade Parität versandt • **odd** – es wird eine ungerade Parität versandt
Stop Bits	Anzahl der Stoppbits
Split Timeout	Zeit, bis Berichte abgebrochen werden. Wenn die Lücke zwischen zwei Zeichen den Parameter in Millisekunden überschreitet, werden alle gepufferten Zeichen über den Ethernet-Port gesendet.
Protocol	Kommunikationsprotokoll: • **TCP** – Kommunikation über das Protokoll TCP (verbindungsorientiert) • **UDP** – Kommunikation über das Protokoll UDP (verbindungslos)
Mode	Kommunikationsmodus: • **TCP server** – Der Router hört auf eingehende TCP-Verbindungsanfragen • **TCP client** – der Router verbindet sich zum TCP-Server an der angegebenen IP-Adresse und am TCP-Port
Server Address	Wenn **TCP-Client** eingestellt ist, müssen die Serveradresse und der TCP-Port eingegeben werden. IPv4- und IPv6-Adressen sind zulässig.
TCP Port	TCP/UDP-Port, der für die Kommunikation verwendet wird. Der Router verwendet den Wert sowohl für den Server- als auch für den Client-Modus
Inactivity Timeout	Zeitraum, nach dem die TCP/UDP-Verbindung bei Inaktivität unterbrochen wird

Wenn das Element **Reject new connections** aktiviert ist, werden alle anderen Verbindungen abgelehnt. Das heißt, es ist nicht möglich, mehrere Verbindungen aufzubauen.

Wenn der Punkt **Check TCP connection** aktiviert ist, wird die Überprüfung der aufgebauten TCP-Verbindung aktiviert.

Tab. 81: USB PORT Konfiguration 2

Element	Beschreibung
Keepalive Time	Zeit, nach der die Überprüfung der Verbindung durchgeführt wird
Keepalive Interval	Zeitdauer, während der auf eine Antwort gewartet wird
Keepalive Probes	Anzahl der Versuche

Wenn Sie das Kontrollkästchen **Use CD as indicator of the TCP connection** markieren, verwendet der Router das Trägererkennungssignal (CD), um den Status der TCP-Verbindung zu überprüfen. Das CD-Signal überprüft, ob ein anderes Gerät an der anderen Seite des Kabels angeschlossen ist.

Tab. 82: Beschreibung des CD-Signals

CD	Beschreibung
Aktiv	TCP-Verbindung ist aktiviert
Nonactive	TCP-Verbindung ist deaktiviert

Wenn Sie das Kontrollkästchen **Use DTR as control of TCP connection** markieren, verwendet der Router den Data Terminal Ready (DTR) Single, um die TCP-Verbindung zu kontrollieren. Das Remote-Gerät sendet eine DTR-Single an den Router, die anzeigt, dass das entfernte Gerät für die Kommunikation bereit ist.

Tab. 83: Beschreibung des DTR-Signals

DTR	Verhalten des Servers	Verhalten des Clients
Aktiv	Der Router ermöglicht die Einrichtung von TCP-Verbindungen.	Der Router baut die TCP-Verbindung auf.
Nonactive	Der Router verweigert die Einrichtung von TCP-Verbindungen.	Der Router trennt die TCP-Verbindung.

HINWEIS

Der Router unterstützt die folgenden USB/RS232-Konverter:

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210×

Die Änderungen der Einstellungen wirken sich nach Betätigung der Schaltfläche **Apply** aus.

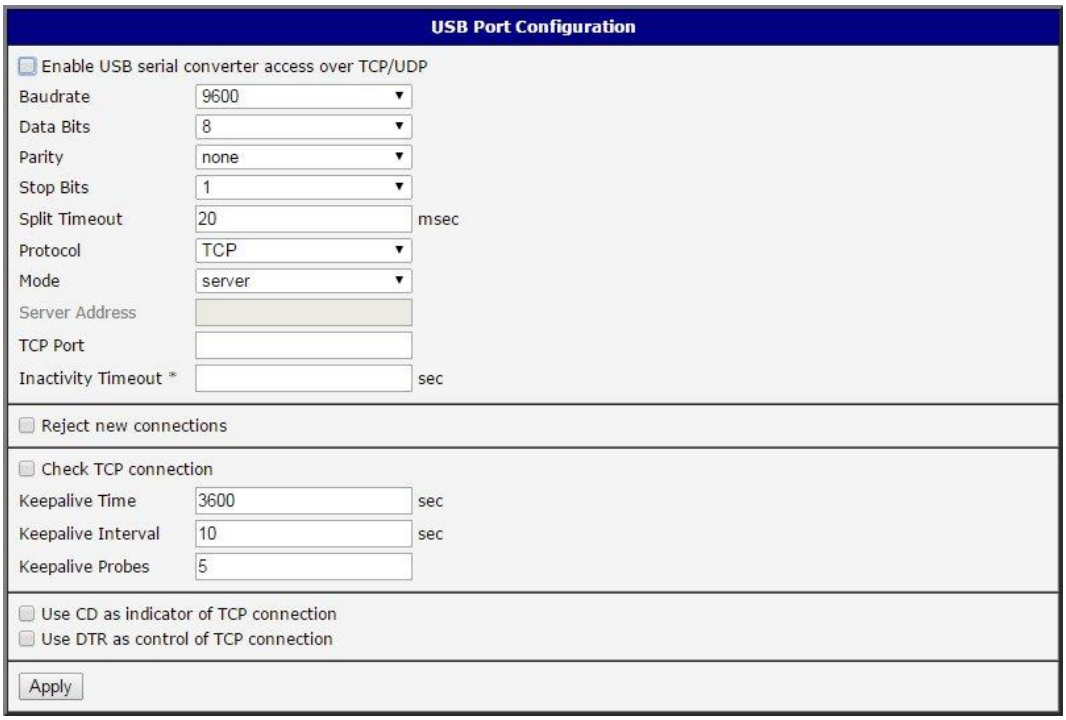


Abb. 81: USB-Konfiguration

Beispiele für die Konfiguration des USB-Ports

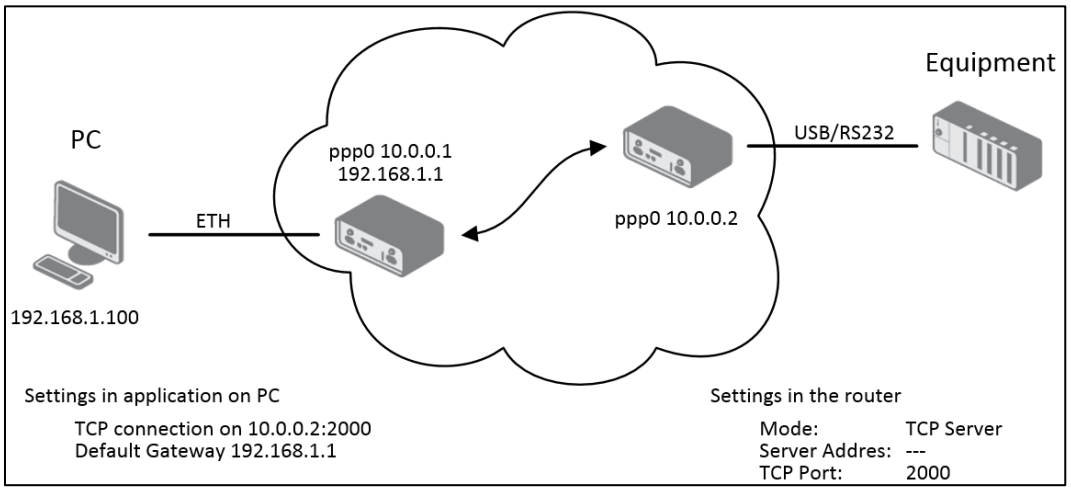


Abb. 82: Beispiel 1 – Konfiguration des USB-Ports

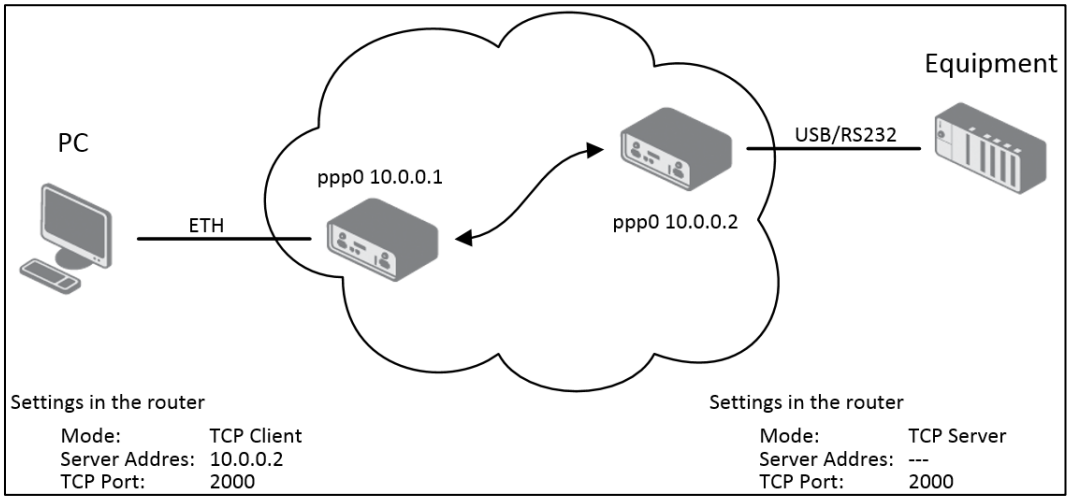


Abb. 83: Beispiel 2 – Konfiguration des USB-Ports

5.20 Skripte

Es besteht die Möglichkeit, eigene Shell-Skripte zu erstellen, die in bestimmten Situationen ausgeführt werden. Rufen Sie die Seite Scripts im Abschnitt Configuration im Menü auf. Der Menüpunkt wird erweitert und es gibt Startup Script, Up/Down IPv4 und Up/Down IPv6 Skripte, die Sie verwenden können – es gibt IPv4 und IPv6 unabhängige Dual-Stack.

5.20.1 Startup-Skript

Verwenden Sie das Fenster **Startup Script**, um Ihre eigenen Skripte zu erstellen, die ausgeführt werden, nachdem alle Initialisierungsskripts ausgeführt wurden – direkt nach dem Einschalten oder Neustarten des Routers.

Die Änderungen der Einstellungen wirken sich nach Betätigung der Schaltfläche **Apply** aus.

HINWEIS Die Änderungen sind wirksam nach dem Herunterfahren und Einschalten des Routers. Dies kann in der Option **Reboot** im Bereich **Administration** erfolgen oder durch SMS-Nachricht (siehe **SMS Konfiguration**).

Beispiel für Startup-Skript

Wenn Sie den Router starten, stoppen Sie das syslogd-Programm und starten Sie syslogd mit Remote-Logging an der Adresse 192.168.2.115 und einer auf 100 Einträge beschränkten Auflistung. Fügen Sie diese Zeilen zum Startskript hinzu:

```
killall syslogd
syslogd -R 192.168.2.115 -S 100
```

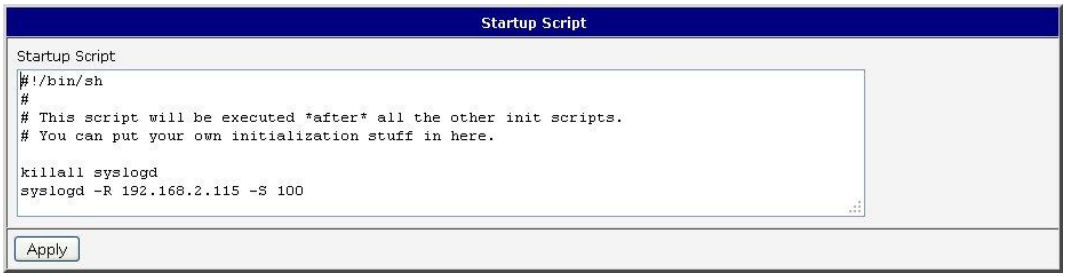


Abb. 84: Beispiel für Startup-Skript

5.20.2 Up/Down-Skript

Verwenden Sie die Seiten **Up/Down IPv4** und **Up/Down IPv6**, um Skripte zu erstellen, die ausgeführt werden, wenn die Mobile WAN-Verbindung hergestellt (up) oder unterbrochen wird (down). Im Router ist ein unabhängiger IPv4- und IPv6-Dual-Stack implementiert, sodass unabhängige IPv4- und IPv6-Up/Down-Skripte vorhanden sind. **IPv4 Up/Down Script** läuft nur bei der aufgebauten/unterbrochenen IPv4 WAN Verbindungen, **IPv6 Up/Down Script** läuft nur bei der aufgebauten/unterbrochenen IPv6 WAN Verbindungen. Alle Skripte, die in das Up Script-Fenster eingegeben werden, werden ausgeführt, nachdem eine WAN-Verbindung hergestellt wurde. In das Fenster **Down Script** eingegebene Skriptbefehle werden ausgeführt, wenn die WAN-Verbindung unterbrochen wird.

Die Änderungen in den Einstellungen werden wirksam, nachdem Sie auf die Schaltfläche **Apply** geklickt und den Router neu gestartet haben.

Beispiel für ein IPv6-Up/Down-Skript

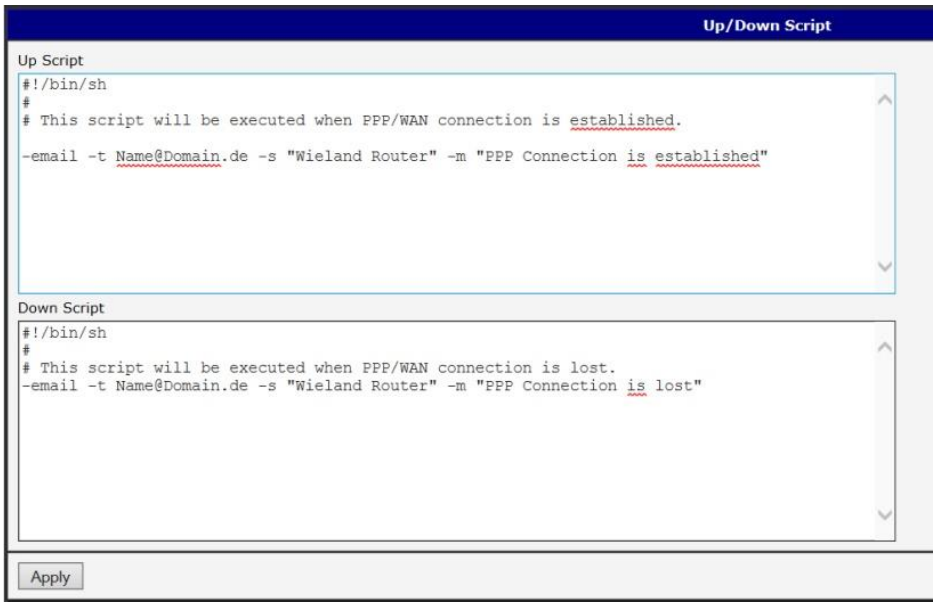


Abb. 85: Beispiel für ein Up/Down-Skript

Nach Aufbau oder Verlust einer IPv6-Verbindung (Verbindung zum Mobilfunknetz) sendet der Router eine E-Mail mit Informationen zum Verbindungsstatus. Vorher muss **SMTP** konfiguriert werden.

Fügen Sie diese Zeile zum Feld Up Script hinzu:

```
email -t name@domain.com -s "Router" -m "Connection up."
```

Fügen Sie diese Zeile zum Feld Down Script hinzu:

```
email -t name@domain.com -s "Router" -m "Connection down."
```

5.21 Konfiguration der automatischen Aktualisierung

Der Router kann so konfiguriert werden, dass er automatisch von einer FTP-Site oder einem Webserver nach Firmware-Updates sucht und seine Firmware- oder Konfigurationsinformationen aktualisiert. IPv6-Sites/Server werden unterstützt. Verwenden Sie das Menü **Automatic Update**, um die Einstellungen für das automatische Update zu konfigurieren. Es ist auch möglich, die Konfiguration und Firmware über den USB-Hostanschluss des Routers zu aktualisieren. Um eine mögliche ungewollte Manipulation der Dateien zu verhindern, überprüft der Router, ob die heruntergeladene Datei im Format tar.gz vorliegt. Zunächst wird das Format der heruntergeladenen Datei überprüft.
Dann wird der Architekturtyp und jede Datei im Archiv (tar.gz-Datei) überprüft.

Wenn die Option **Enable automatic update of configuration** ausgewählt ist, prüft der Router, ob eine Konfigurationsdatei auf dem Remote-Server vorhanden ist, und wenn die Konfiguration in der Datei von der aktuellen Konfiguration abweicht, aktualisiert er seine Konfiguration auf die neuen Einstellungen und führt einen Neustart durch.

Wenn die Option **Enable automatic update of firmware** aktiviert ist, sucht der Router nach einer neuen Firmware-Datei und aktualisiert gegebenenfalls seine Firmware.

Der Name der Konfigurationsdatei besteht aus Basis-URL, Hardware-MAC-Adresse der ETH0-Schnittstelle und cfg-Erweiterung.
Die Hardware-MAC-Adresse und cfg-Erweiterung werden dem Dateinamen automatisch hinzugefügt und müssen nicht eingegeben werden.
Wenn der Parameter **Unit ID** aktiviert ist, definiert er den konkreten Konfigurationsnamen, der auf den Router heruntergeladen wird, und die Hardware-MAC-Adresse im Konfigurationsnamen wird nicht verwendet.

Der Name der Firmware-Datei besteht aus Basis-URL, Routertyp und Bin-Erweiterung. Den richtigen Firmware-Dateinamen finden Sie auf der Seite 'Update Firmware ' im Abschnitt 'Administration'" – er wird dort geschrieben. Siehe Kapitel 7.12 "Aktualisierung der Firmware", S. 134.



- Auf den HTTP(S)/FTP(S) Server müssen immer zwei Dateien (.bin und .ver) hochgeladen werden. Falls auf den HTTP-Server nur die Datei mit dem Suffix .bin hochgeladen werden sollte, würde die falsche Antwort "200 OK" (anstelle der erwarteten "404 Not Found") beim Versuch, die nicht existierende Datei .ver herunterzuladen, versendet. Dies führt zu dem hohen Risiko, dass der Router unablässig versucht die .bin-Datei herunterzuladen.
- Die Aktualisierung von Firmware kann Inkompatibilität mit den Benutzermodulen verursachen. Es wird empfohlen, die Benutzermodule auf die neueste Version zu aktualisieren. Informationen zu den Benutzermodulen und die Kompatibilität der Firmware entnehmen Sie am Anfang des Anwendungshinweises der Benutzermodule.
- Die automatische Update-Funktion wird auch fünf Minuten nach dem Firmware-Upgrade ausgeführt, unabhängig von der geplanten Zeit.

Tab. 84: Konfiguration der automatischen Aktualisierung

Element	**Beschreibung**
Source	Woher der Router die Firmware und Konfiguration herunterlädt: • **HTTP(S)/FTP(S) Server** – Updates werden von der unten angegebenen Basis-URL-Adresse heruntergeladen. Das verwendete Protokoll wird durch diese Adresse angegeben: HTTP, HTTPS, FTP oder FTPS (nur impliziter Modus wird unterstützt). • **USB flash drive** – Der Router sucht die aktuelle Firmware im Wurzelverzeichnis des Geräts, das an den USB-Port angeschlossen ist. • **Both** – der Router sucht die aktuelle Firmware in beiden Quellen.
Base URL	Basis-URL, IPv4- oder IPv6-Adresse, von der die Konfigurationsdatei heruntergeladen wird. Diese Option gibt auch das Kommunikationsprotokoll (HTTP, HTTPS, FTP oder FTPS) an, siehe Beispiele unten.
Unit ID	Bezeichnung der herunterzuladenden Konfiguration (Name der Datei ohne Erweiterung). Falls die Unit ID nicht angegeben ist, wird die MAC-Adresse des Routers als Dateiname verwendet (als Trennzeichen wird ein Punkt anstelle eines Doppelpunkts benutzt).
Decryption Password	Passwort für die Entschlüsselung der verschlüsselten Konfigurationsdatei. Dies ist nur erforderlich, wenn die Konfiguration verschlüsselt ist.
Update Window Start	Wählen Sie eine Stunde (Bereich von 1 bis 24) aus, in der die automatische Aktualisierung täglich durchgeführt wird. Wird die Zeit nicht angegeben (auf dynamisch gesetzt), erfolgt das automatische Update fünf Minuten nach dem Hochfahren des Routers und dann regelmäßig alle 24 Stunden.
Update Window Length	Dieser Wert definiert den Zeitraum, innerhalb dessen das Update durchgeführt wird. Dieser Zeitraum beginnt zu dem Zeitpunkt, der im Feld **Update Window Start** festgelegt wurde. Der genaue Zeitpunkt, zu dem das Update durchgeführt wird, wird zufällig generiert.

Beispiel für die automatische Aktualisierung

Die folgenden Beispiele zeigen, ob eine neue Firmware oder Konfiguration jeden Tag um 1:00 Uhr morgens zur Verfügung steht. Ein Beispiel dafür ist der Routertyp wienet WR-LTE v3 SL.

- Firmware: http://wieland-electric.com/wienet-v3-LTE.bin (keine reale Adresse!)
- Konfigurationsdatei: http://wieland-electric.com/bamberg.cfg (keine reale Adresse!)

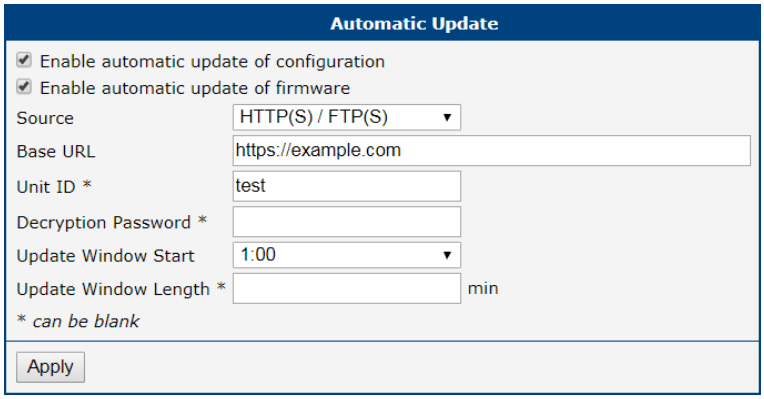


Abb. 86: Beispiel für die automatische Aktualisierung 1

Beispiel für automatisches Update basierend auf MAC

Die folgenden Beispiele zeigen, ob eine neue Firmware oder Konfiguration jeden Tag um 1:00 Uhr morgens zur Verfügung steht. Die Konfigurationsdatei ist verschlüsselt; deshalb wurde das Entschlüsselungspasswort konfiguriert. Ein Beispiel dafür ist der Routertyp wienet WR-LTE v3 SL mit MAC-Adresse 00:11:22:33:44:55.

- Firmware: www.wieland-electric.com
- Konfigurationsdatei: www.wieland-electric.com

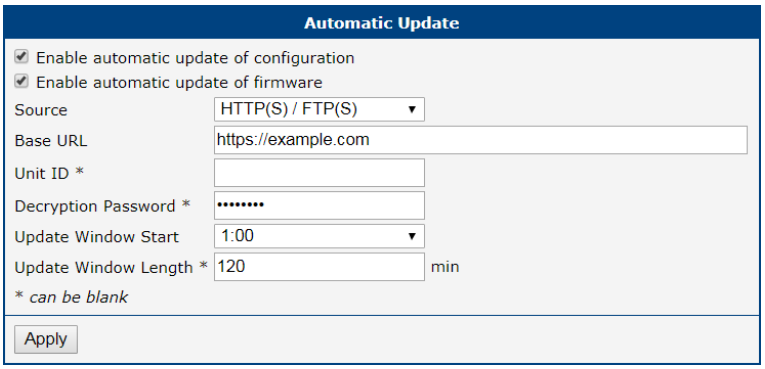


Abb. 87: Beispiel für die automatische Aktualisierung 1

6 ANWENDERANPASSUNG

6.1 Benutzermodule

Sie können benutzerdefinierte Softwareprogramme im Router ausführen, um die Funktionen des Routers zu erweitern. Über den Menüpunkt User Modules können Sie dem Router neue Softwaremodule hinzufügen, diese entfernen oder ihre Konfiguration ändern. Verwenden Sie die Schaltfläche Durchsuchen, um das Arbeitsplatzmodul auszuwählen (das kompilierte Modul hat die Erweiterung tgz). Verwenden Sie die Schaltfläche **Add**, um ein Benutzermodul hinzuzufügen.

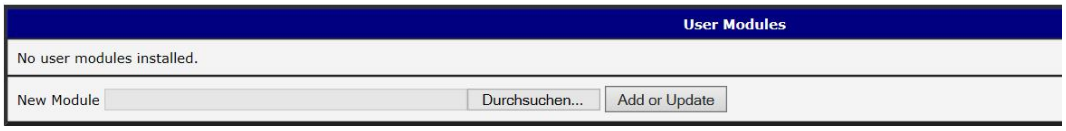


Abb. 88: Benutzermodul hinzufügen (1)

Das neue Modul erscheint in der Modulliste auf derselben Seite. Wenn das Modul eine index.html- oder index.cgi-Seite enthält, dient der Modulname als Link zu dieser Seite. Das Modul kann über die Schaltfläche **Delete** gelöscht werden.

Das Aktualisieren eines Moduls erfolgt auf die gleiche Weise. Klicken Sie auf die Schaltfläche **Add** und das Modul mit der höheren (neueren) Version ersetzt das vorhandene Modul. Die aktuelle Modulkonfiguration wird im gleichen Zustand belassen.

Die Programmierung und Zusammenstellung der Module erfolgt durch den Wieland-Support.

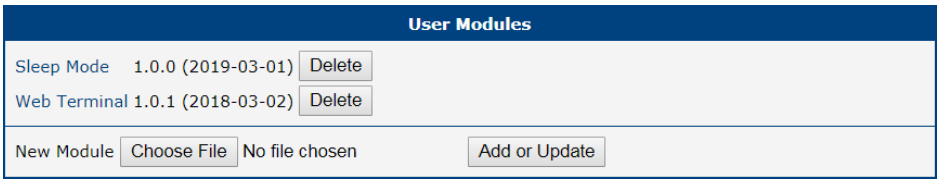


Abb. 89: Benutzermodul hinzufügen (2)

Benutzermodule können kundenspezifisch programmiert werden. Wenden Sie sich für nähere Informationen an den Wieland Support.

Tab. 85: Benutzermodule

Modulname	Beschreibung
MODBUS TCP2RTU	Bietet eine Protokollumsetzung von MODBUS TCP/IP nach MDBUS RTU für die serielle Schnittstelle.
Easy VPN client	Bietet eine sichere Verbindung von Netzwerken hinter dem Router zu Netzwerken hinter einem CISCO Router.
NMAP	Aktiviert TCP- und UDP-Scan.
Daily Reboot	Aktiviert den täglichen Neustart des Routers zur angegebenen Zeit.
HTTP Authentication	Fügt den Authentifizierungsprozess zu einem Server hinzu, der diesen Dienst nicht bereitstellt.
BGP, RIP, OSPF	Bietet Unterstützung für dynamische Protokolle.
PIM SM	Bietet Unterstützung für das Multicast-Routing-Protokoll PIMSM.
WMBUS Concentrator	Ermöglicht den Empfang von Nachrichten von WMBUS-Zählern und speichert den Inhalt dieser Nachrichten in einer XML-Datei.
pduSMS	Sendet Kurznachrichten (short messages/SMS) an bestimmte Rufnummern.
GPS	Erlaubt dem Router das Feststellen von Positions- und Zeitinformationen bei jedem Wetter überall auf oder in der Nähe der Erde, solange eine uneingeschränkte direkte Sichtlinie zu wenigstens vier GPS-Satelliten besteht.
Pinger	Ermöglicht die manuelle oder automatische Überprüfung der Funktionsfähigkeit der Verbindung zwischen zwei Netzwerkschnittstellen (Ping).
IS-IS	Bietet Unterstützung für das Protokoll IS-IS.
Webterminal	Erlaubt durch die Web Administrations-GUI den Zugriff auf die Benutzerkonsole des Routers.
Node.js	Erlaubt die Ausführung von JavaScript-Code außerhalb eines Webbrowsers.
Node-RED	Erlaubt die Erstellung einer Applikation über eine Weboberfläche.
Node-RED Dashboard	Ermöglicht die einfache und schnelle Erstellung eines Dashboards mit live Daten.
Node-RED Modbus	Ermöglicht das Lesen und Schreiben einer Vielzahl von Registern von SPS/PLCs mit Modbus.



VORSICHT

In einigen Fällen kann das Firmware-Update zu Inkompatibilitäten mit verwendeten Modulen führen. Einige davon sind abhängig von der Version des Linux-Kernels (z. B. SmsBE und PoS-Konfiguration). Es wird empfohlen, Benutzermodule auf die neueste Version zu aktualisieren.

7 ADMINISTRATION

7.1 Benutzer

HINWEIS Dieses Konfigurationsmenü ist nur für Benutzer mit der Rolle **Admin** verfügbar!

Verwenden Sie die Option **Users** im Teil **Administration** des Hauptmenüs zur Verwaltung der Benutzerkonten. Der erste Block dieser Form enthält eine Übersicht der hinzugefügten Benutzer. Die nachfolgende Tabelle beschreibt die Bedeutung aller Schaltflächen in diesem Block.

Tab. 86: Benutzerübersicht

Element	Beschreibung
Lock	Sperrt Benutzerkonten. Dieser Benutzer darf sich nicht im Router anmelden (weder Webinterface noch SSH)
Change Password	Ermöglicht das Ändern des Passworts für den entsprechenden Benutzer. Gültige Zeichen sind nicht eingeschränkt.
Delete	Löscht entsprechendes Benutzerkonto

VORSICHT Achten Sie darauf, nicht alle Benutzer der Rolle **Admin** zu sperren. In diesem Zustand hat jeder Benutzer Zugriffsrechte, um die Benutzer zu konfigurieren!

Der zweite Block enthält Konfigurationsformen, die Ihnen das Hinzufügen eines neuen Benutzers ermöglicht. Alle Optionen werden in der nachfolgenden Tabelle beschrieben.

Tab. 87: Benutzer hinzufügen

Element	Beschreibung
Role	Definiert die Art des Benutzerkontos • **User** – Benutzer mit grundlegenden Berechtigungen – hat nur Lesezugriff auf die Web-GUI, ein paar Menüpunkte der Web-GUI sind versteckt, vollen Zugang zur GUI der Router Apps, kein Zugriff auf den Router über Telnet, SSH oder SFTP, nur Lesezugriff auf den FTP-Server. • **Admin** – Benutzer mit erweiterten Berechtigungen – hat vollen Zugriff auf die Web-GUI, Zugriff auf den Router über Telnet, SSH oder SFTP. Dieser Benutzer hat nicht die gleichen Rechte wie der Superuser auf Linux-basierten Systemen.
Username	Name des Benutzers, der Zugriff hat, um sich am Gerät anzumelden.
Passwort	Passwort für den Benutzer. Gültige Zeichen sind nicht eingeschränkt.
Confirm Password	Bestätigt das Passwort, das Sie oben angegeben haben.

HINWEIS Benutzer mit der Rolle **User** können nicht auf den Router über Telnet, SSH oder SFTP zugreifen. Read-only FTP-Zugang ist für diese Benutzer erlaubt.

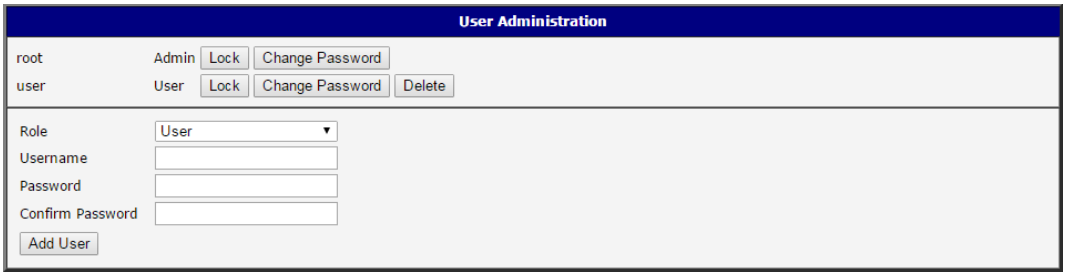


Abb. 90: Benutzer

7.2 Änderung des Profils

Bis zu drei alternative Routerkonfigurationen oder Profile können im nichtflüchtigen Speicher des Routers gespeichert werden. Sie können die aktuelle Konfiguration zu einem Routerprofil über die Menüoption **Change Profile** speichern. Wählen Sie das alternative Profil aus zur Speicherung der Einstellungen und um zu gewährleisten, dass das Kästchen **Copy settings from current profile to selected profile** markiert ist. Die aktuellen Einstellungen werden im alternativen Profil gespeichert, nachdem die Schaltfläche **Apply** betätigt wurde. Alle Änderungen wirken erst nach einem Neustart des Routers über das Menü **Reboot** im Webadministrator oder mit einer entsprechenden SMS-Nachricht.

Beispiele für Benutzerprofile

Die Profile können für das Umschalten zwischen den verschiedenen Modi des Router-Betriebs benutzt werden wie beispielsweise PPP-Verbindung, VPN-Tunnel usw. Das Umschalten zwischen diesen Einstellungen kann danach mit Hilfe des Binäreingangs, einer SMS-Nachricht oder von der Web-Schnittstelle des Routers durchgeführt werden.

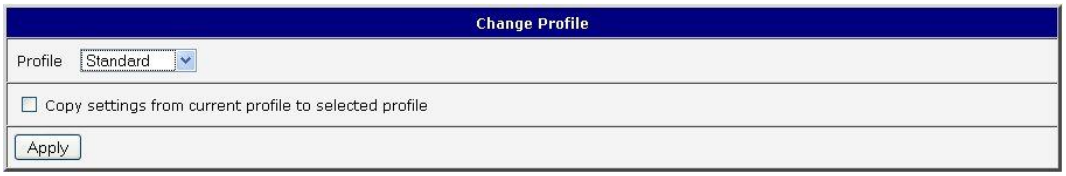


Abb. 91: Änderung des Profils

7.3 Passwort ändern

Kennwort bestätigen und klicken Sie auf die Schaltfläche Übernehmen. Verwenden Sie das Konfigurationsformular Passwort ändern im Abschnitt **Administration** des Hauptmenüs, um Ihr Passwort für die Anmeldung am Gerät zu ändern. Geben Sie das neue Kennwort in das Feld **New Password** ein, bestätigen Sie das Kennwort mit dem Feld **Confirm Password** und klicken Sie auf die Schaltfläche **Apply**. Zeichen für das Passwort sind nicht eingeschränkt.



VORSICHT

Das Standardpasswort ist P<letzte 8 Ziffern von CSN>h. Es wird dringend empfohlen, das Kennwort während der Ersteinrichtung zu ändern, um die Sicherheit zu erhöhen. Sie können den Fernzugriff auf den Router beispielsweise in NAT erst aktivieren, wenn Sie das Kennwort ändern.

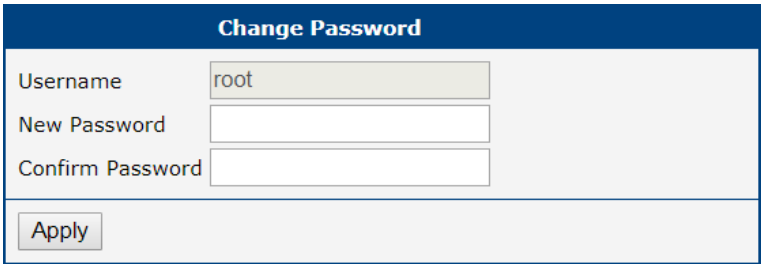


Abb. 92: Passwort ändern

7.4 Zwei-Faktor-Authentifizierung (gilt nur für v2 Router)

HINWEIS Falls die Konfiguration der Zwei-Faktor-Authentifizierung fehlschlägt oder nicht vollständig abgeschlossen wird, kann man sich nicht mehr unter dem Benutzernamen auf dem Router anmelden. Die einzige Lösung hierfür ist ein Zurücksetzen auf Werkseinstellungen. Um das Zurücksetzen zu vermeiden, wird empfohlen einen Backup Account anzulegen, um im Falle von Problemen bei der Konfiguration ein Aufschalten auf den Router zu ermöglichen. Dieser Backup Account kann bei erfolgreicher Konfiguration der Zwei-Faktor-Authentifizierung gelöscht werden.

HINWEIS Für eine erfolgreiche Anmeldung mit der Zwei-Faktor Authentifizierung ist es notwendig, dass die korrekte Systemzeit auf dem Router eingestellt ist. Daher wird dringend empfohlen die Option **Synchronize clock with NTP server** zu aktivieren (siehe Kapitel 5.17.4 "NTP", S. 97).

Hinweise zur Implementierung:

- Zwei verschiedene Zwei-Faktor Implementationen werden unterstützt:
  - Google Authenticator
  - OATH Toolkit
- Diese können für folgende Dienste verwendet werden:
  - Protokollierung des Web Servers des Routers
  - SSH Protokollierung
  - TLENET Protokollierung
- Die Zwei-Faktor-Authentifizierung ist standardmäßig deaktiviert.
- Die Daten der Zwei-Faktor-Authentifizierung werden während des Benutzer backup/restore Prozesses gespeichert und wiederhergestellt.
- Alle privaten Zwei-Faktor-Authentifizierungsdaten werden gelöscht, wenn der entsprechende Benutzer gelöscht wird.
- Für die Zwei-Faktor-Authentifizierung braucht es keine Internet- oder Mobilfunkverbindung. Es muss lediglich die Systemzeit synchronisiert sein.

Konfigurationsschritte:

1. Aktivieren Sie den Zwei-Faktor-Authentifizierungsdienst (siehe Kapitel 5.17.5 "PAM", S. 98, Zwei-Faktor-Authentifizierungsdienst)
2. Aktivieren Sie die Zwei-Faktor-Authentifizierung für den aktuell angemeldeten Benutzer wie in diesem Kapitel unter Benutzerkonfiguration beschrieben.
3. Verwenden Sie eine Applikation oder einen Dienst, um die Zwei-Faktor-Authentifizierung, wie in diesem Kapitel unter Authenticator beschrieben, auszuführen.

Benutzerkonfiguration:

HINWEIS Die in diesem Kapitel beschriebene Konfiguration der Zwei-Faktor-Authentifizierung gilt für den eingeloggten Benutzer. Falls sich dieser Benutzer dann abmeldet, wird bei der nächsten Anmeldung bereits die Zwei-Faktor-Authentifizierung angewendet.

Falls Sie einen der beiden oben erwähnten Zwei-Faktor-Authentifizierungsdienste aktiviert haben, werden Sie folgende Abbildung für den Google Authenticator sehen, welche den Status "aktiviert" haben wird.

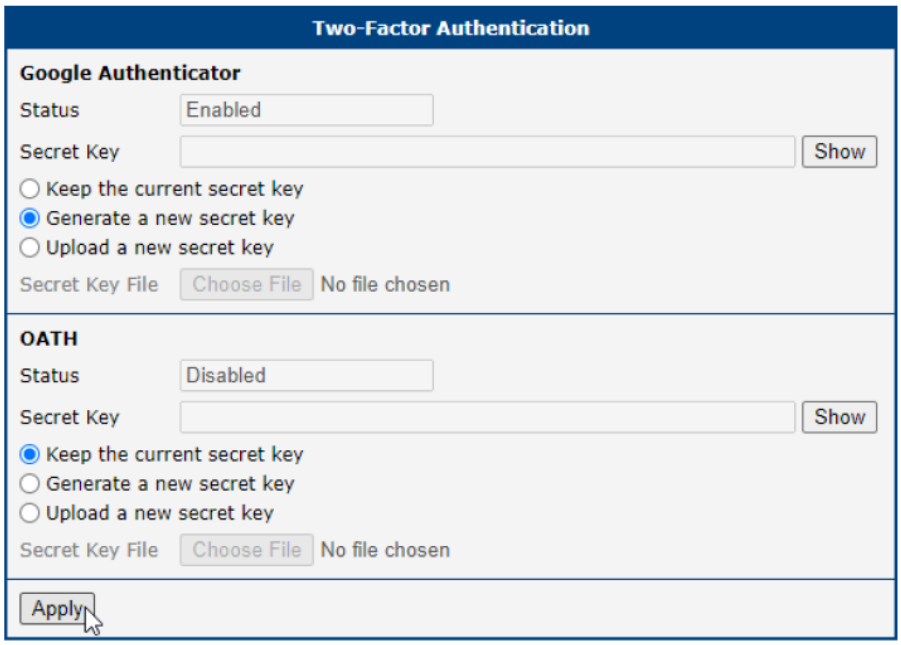


Abb. 93: Zwei-Faktor Benutzerkonfiguration

Es wird ein geheimer Schlüssel für die Zwei-Faktor-Authentifizierung benötigt. Sie können den Schlüssel durch anwählen der **Generate a new secret key** Option wie in Abb. 93 gezeigt, generieren lassen. Alternativ können Sie einen geheimen Schlüssel auch aus einer Datei hochladen. Wählen Sie hierzu **Upload a new secret key** und wählen Sie die entsprechende Datei aus. Beim Drücken der **Apply** Schaltfläche wird der geheime Schlüssel gespeichert. Klicken Sie dann auf die Schaltfläche **Show**, welche rechts vom Schlüssel angezeigt wird und notieren Sie sich den Schlüssel.

HINWEIS Notieren Sie sich den Schlüssel bevor Sie sich ausloggen. Sonst können Sie sich nicht wieder anmelden.

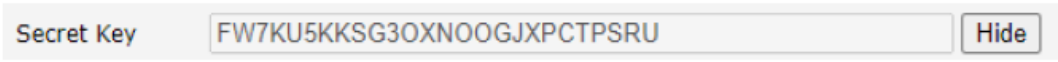


Abb. 94: Geheimer Schlüssel

Analog dazu können Sie den Schlüssel für den OATH-Dienst konfigurieren.

Authenticator

Um sich per Zwei-Faktor-Authentifizierung anzumelden, benötigt man eine Authenticator Applikation. Sowohl Google Authenticator als auch OATH benutzen standardmäßig TOTP (Time-based one-time password, RFC 2038). Sie können jeden kompatiblen Authenticator verwenden. Für weiterführende Informationen beachten Sie die entsprechenden Handbücher.

Sie können den Google Authenticator verwenden. In der folgenden Abbildung finden Sie die Downloadlinks.



Abb. 95: Links für die Google Authenticator Applikation

Die Authenticator-Extension ist als Erweiterung für bekannte Browser verfügbar. In Abb. 96 finden Sie die Downloadlinks.



Abb. 96: Links zur Authenticator Erweiterung

Sie nehmen in einer Authenticator Applikation einen neuen Eintrag vor und tragen den geheimen Schlüssel ein, den Sie sich notiert haben.

Router Web Login

Wenn Sie sich über das Web beim Router anmelden, müssen Sie wie gewohnt den Benutzernamen und das Passwort eingeben.

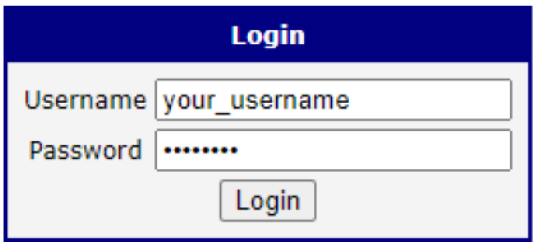


Abb. 97: Standard Anmeldung

Nun werden Sie aufgefordert den Verifizierungscode einzugeben, siehe Abb. 98. Diesen Code erhalten Sie vom Authenticator. Beachten Sie, dass der Code nur für eine beschränkte Zeit nutzbar ist. Das Zeitlimit beträgt etwa fünf Minuten, gesetzt dem Fall, dass die Systemzeit korrekt ist.

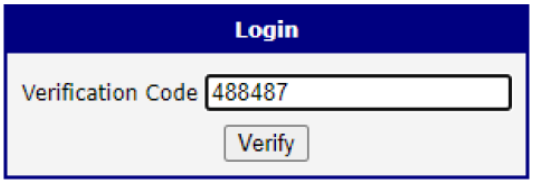


Abb. 98: Verifizierungsschlüssel

Nach dem korrekten Eingeben des Schlüssels sind Sie erfolgreich auf der Weboberfläche des Routers angemeldet.

SSH und Telnet Anmeldung

Die Anmeldung via SSH und Telnet mittels Zwei-Faktor-Authentifizierung verläuft ähnlich. Geben Sie Ihren Benutzernamen, das Passwort und den generierten Verifikationscode ein. Ein Beispiel einer SSH Anmeldung finden Sie in folgender Abbildung.

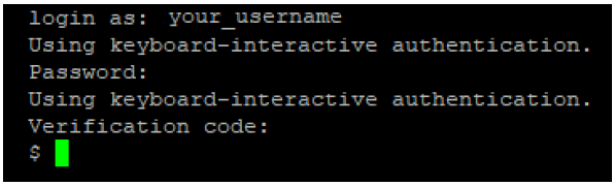


Abb. 99: SSH Anmeldung

7.5 Echtzeituhr einstellen

Sie können die interne Uhr direkt über den Dialog **Set Real Time Clock** im Abschnitt **Administration** des Hauptmenüs einstellen. Sie können **Date** und **Time** manuell einstellen. Verwenden Sie bei der manuellen Eingabe der Werte das Format jjjj-mm-tt, wie in der Abbildung unten gezeigt. Sie können die Uhr auch über den angegebenen NTP-Server einstellen.
IPv4, IPv6-Adresse oder Domänenname wird unterstützt. Nachdem Sie die entsprechenden Werte eingegeben haben, klicken Sie auf die Schaltfläche **Apply**.

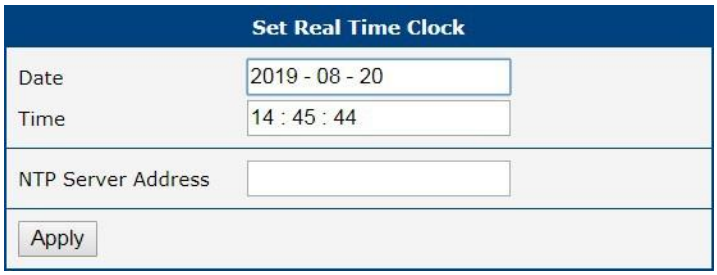


Abb. 100: Echtzeituhr einstellen

7.6 Einstellung des SMS-Service-Centers



Die wienet LAN-Router unterstützen die Option **Set SMS service center address** nicht.

Die Funktion erfordert die Eingabe der Telefonnummer des SMS-Service-Centers, um SMS-Nachrichten zu versenden.
Um die Telefonnummer des SMS-Servicecenters anzugeben, verwenden Sie das Konfigurationsformular **Set SMS Service Center** im Abschnitt **Administration** des Hauptmenüs. Sie können das Feld leer lassen, wenn Ihre SIM-Karte standardmäßig die Rufnummer des SMS-Service-Centers enthält. Diese Telefonnummer kann einen Wert ohne internationale Vorwahl (xxx-xxx-xxx) oder mit internationaler Vorwahl (+420-xxx-xxx-xxx) haben. Wenn Sie keine SMS-Nachrichten senden oder empfangen können, wenden Sie sich an Ihren Mobilfunkanbieter, um herauszufinden, ob dieser Parameter erforderlich ist.

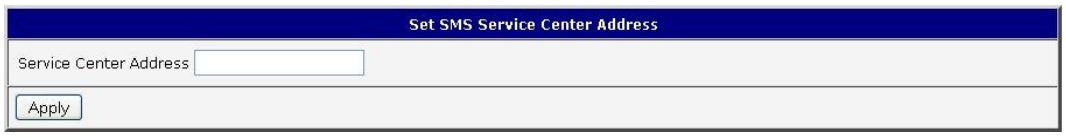


Abb. 101: Einstellung des SMS-Service-Centers

7.7 SIM-Karte entsperren

VORSICHT

Die wienet LAN-Router unterstützen die Kartenoption **Unlock SIM** nicht.

Es ist möglich, die PIN-geschützte SIM-Karte im Router zu verwenden – geben Sie einfach die PIN auf der Seite **Mobile WAN Configuration** ein. Hier können Sie den PIN-Schutz (4–8-stellige Personal Identification Number) von der SIM-Karte entfernen, falls Ihre SIM-Karte durch eine solche geschützt ist. Öffnen Sie das Formular **Unlock SIM Card** im Abschnitt **Administration** des Hauptmenüs und geben Sie die PIN-Nummer in das Feld **SIM PIN** ein und klicken Sie dann auf die Schaltfläche **Apply**. Es wird auf die aktuell aktivierte SIM-Karte angewendet, oder auf die erste SIM-Karte, wenn momentan keine SIM-Karte aktiviert ist.

VORSICHT

Der Zugriff auf die SIM-Karte wird gesperrt, wenn der PIN-Code 3 mal falsch eingegeben wird. Die Entsperrung der SIM-Karte durch die PUK-Nummer wird im nächsten Kapitel beschrieben.

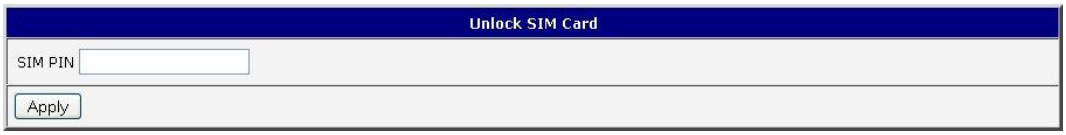


Abb. 102: SIM-Karte entsperren

7.8 SIM-Karte entsperren

VORSICHT

Die wienet LAN-Router unterstützen die Option **Unblock SIM Card** nicht.

Auf dieser Seite können Sie die SIM-Karte nach 3 falschen PIN-Versuchen entsperren oder den PIN-Code der SIM-Karte ändern.
Um die SIM-Karte zu entsperren, gehen Sie zur Verwaltungsseite **Unblock SIM Card**. Geben Sie in beiden Fällen den PUK-Code in das Feld **SIM PUK** und den neuen SIM-PIN-Code in das Feld **New SIM PIN** ein. Um fortzufahren, klicken Sie auf die Schaltfläche **Apply**.
Es wird auf die aktuell aktivierte SIM-Karte angewendet, oder auf die erste SIM-Karte, wenn momentan keine SIM-Karte aktiviert ist.

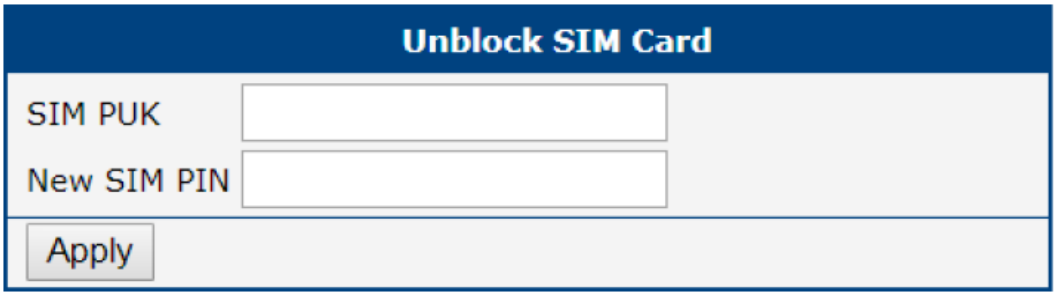


Abb. 103: Entsperren der SIM-Karte

VORSICHT

Nach drei erfolglosen Eingabeversuchen des PUK-Codes wird die SIM-Karte dauerhaft gesperrt.

7.9 Versenden einer SMS-Nachricht

VORSICHT

Die wienet LAN-Router unterstützen die Option **Send SMS** nicht.

Sie können eine SMS-Nachricht vom Router senden, um das Mobilfunknetz zu testen.
Verwenden Sie das Dialogfeld **Send SMS** im Abschnitt **Administration** des Hauptmenüs, um SMS-Nachrichten zu senden. Geben Sie die Telefonnummer und den Text der Nachricht in die Textfelder ein und klicken Sie auf die Schaltfläche **Send**.

Die maximale Länge der SMS beträgt 160 Zeichen. (Um längere Nachrichten zu senden, installieren Sie das pduSMS-Benutzermodul).

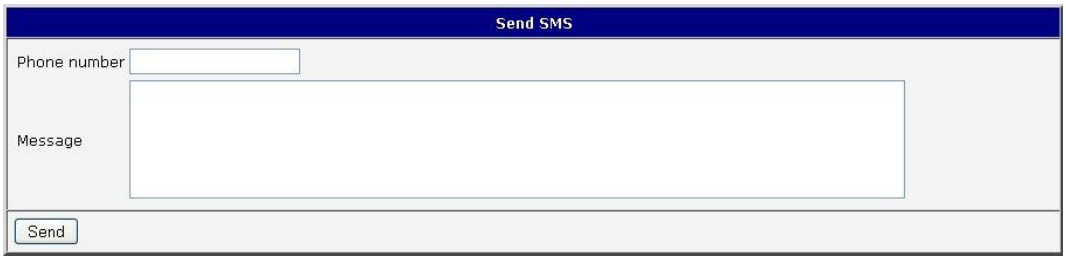


Abb. 104: SMS-Nachricht versenden

Es ist auch möglich, eine SMS-Nachricht mit CGI-Skript zu senden.

7.10 Konfiguration sichern

VORSICHT

Denken Sie beim Erstellen von Backups an potenzielle Sicherheitsprobleme, insbesondere für Benutzerkonten. Es sollte eine verschlüsselte Konfiguration oder eine gesicherte Verbindung zum Router verwendet werden.

Sie können die aktuelle Konfiguration des Routers mit dem Element **Backup Configuration** im Menüabschnitt **Administration** speichern. Wenn Sie auf dieses Element klicken, öffnet sich ein Konfigurationsfenster, siehe Abbildung unten. Hier können Sie auswählen, was gesichert wird.
Sie können die Konfiguration des Routers (Element **Configuration**) oder die Konfiguration aller Benutzerkonten (Element **Users**) sichern. Beide Arten der Konfiguration können separat oder gleichzeitig in einer Konfigurationsdatei gesichert werden.

VORSICHT

Es wird empfohlen, die Konfiguration in einer verschlüsselten Datei zu speichern.
Wenn das Verschlüsselungskennwort nicht konfiguriert ist, wird die Konfiguration in einer unverschlüsselten Datei gespeichert.

Klicken Sie auf die Schaltfläche Übernehmen und die Konfiguration wird in einer Konfigurationsdatei (Datei mit der Erweiterung cfg) in einem Verzeichnis gemäß den Einstellungen des Webbrowsers gespeichert. Die gespeicherte Konfiguration kann später für ihre Wiederherstellung verwendet werden.
Für weitere Informationen siehe Kapitel 7.11 "Konfiguration wiederherstellen", S. 134.

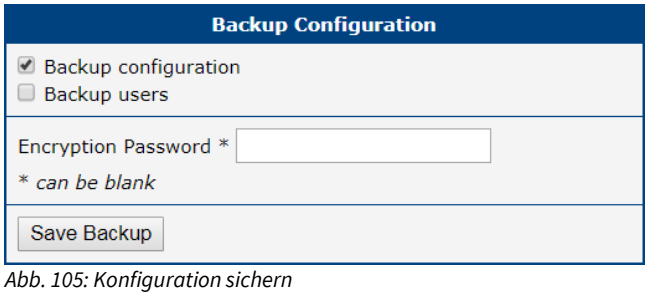


Abb. 105: Konfiguration sichern

7.11 Konfiguration wiederherstellen

VORSICHT

Aufgrund des unterschiedlichen Formats ist es nicht möglich, Benutzerkonten, die auf einem Router der Produktlinie v1 (und älter) gesichert wurden, auf einen Router der Produktlinie v2 (und neuer) zu importieren. Die gleiche Einschränkung gilt für die entgegengesetzte Richtung.

Sie können eine in einer Datei gespeicherte Konfiguration des Routers wiederherstellen, indem Sie das Formular **Restore Configuration** verwenden. Klicken Sie auf die Schaltfläche **Browse**, um zu dem Verzeichnis zu navigieren, das die in den Router zu ladende Konfigurationsdatei enthält.
Wenn die Konfiguration in einer verschlüsselten Datei gespeichert wurde, muss das Entschlüsselungskennwort festgelegt werden, um die Datei erfolgreich zu entschlüsseln.
Um den Wiederherstellungsprozess zu starten, klicken Sie auf die Schaltfläche **Apply**.

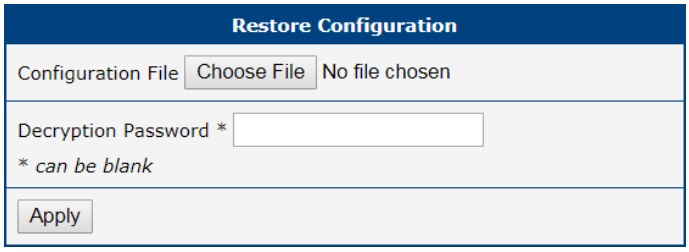


Abb. 106: Konfiguration wiederherstellen

7.12 Aktualisierung der Firmware

Wählen Sie die Menüoption **Update Firmware** aus, um die aktuelle Version der Router-Firmware einzusehen und die neue Firmware in den Router zu laden. Um die neue Firmware zu laden, durchsuchen Sie die neue Firmware-Datei und betätigen die Schaltfläche **Update** zur Aktualisierung.

VORSICHT

- Aus Sicherheitsgründen wird dringend empfohlen, die Firmware des Routers regelmäßig auf die neueste Version zu aktualisieren. Ein Downgrade der Firmware auf eine ältere Version als die Produktionsversion oder das Hochladen einer Firmware, die für ein anderes Gerät bestimmt ist, kann zu Fehlfunktionen des Geräts führen.
- Das Firmware-Update kann ein Inkompatibilitätsproblem mit einem Arbeitsplatzmodul verursachen. Es wird empfohlen, alle Arbeitsplatzmodule zusammen mit der Firmware des Routers auf die neueste Version zu aktualisieren.

Die Firmware für die Router erhalten Sie auf der Produktseite des Engineering Portals, die unter e-shop.wieland-electric.com verfügbar ist.

Die Seite **Update Firmware** zeigt die aktuelle Firmware-Version des Routers und den aktuellen Firmware-Namen an, siehe Abbildung unten. Auf dieser Seite kann auch die Firmware des Routers aktualisiert werden.

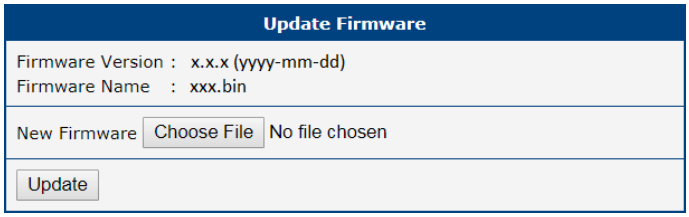


Abb. 107: Aktualisierung der Firmware

Um eine neue Firmware auf den Router zu laden, klicken Sie auf die Schaltfläche **Choose File**,
wählen Sie die Firmware-Datei aus und drücken Sie die Schaltfläche **Update**, um das Firmware-Update zu starten.

Während des Firmware-Updates zeigt der Router die folgenden Meldungen an. Wenn das Update beendet ist, startet der Router automatisch neu.
Klicken Sie nach dem Neustart auf den Link **here**, um die Weboberfläche erneut zu öffnen.

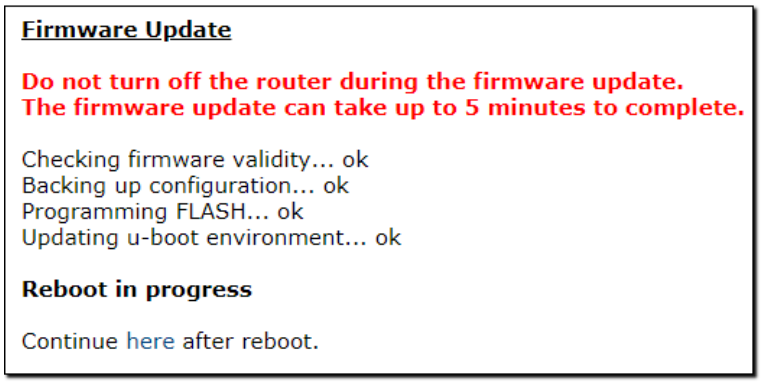


Abb. 108: Automatischer Neustart des Routers

7.13 Reboot (Neustart)

Der Neustart des Routers kann durch die Auswahl der Option **Reboot** im Menü und durch die anschließende Betätigung der Schaltfläche **Reboot** aufgerufen werden.

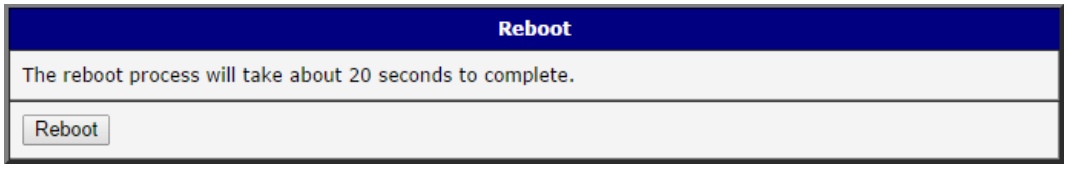


Abb. 109: Router neustarten

7.14 Abmelden

Durch das klicken der Schaltfläche **Logout** wird der Benutzer von der Web-Oberfläche abgemeldet.

8 KONFIGURATION IN TYPISCHEN SITUATIONEN

Obwohl wienet Router über verschiedenste Einsatzbereiche verfügen, werden sie typischerweise in den folgenden Situationen verwendet. Alle nachfolgenden Beispiele beschreiben IPv4-Netzwerke.

HINWEIS Diese Beispiele sind nicht für die wienet LAN-Router geeignet (kein Mobilfunkmodul).

8.1 Internetzugang über LAN

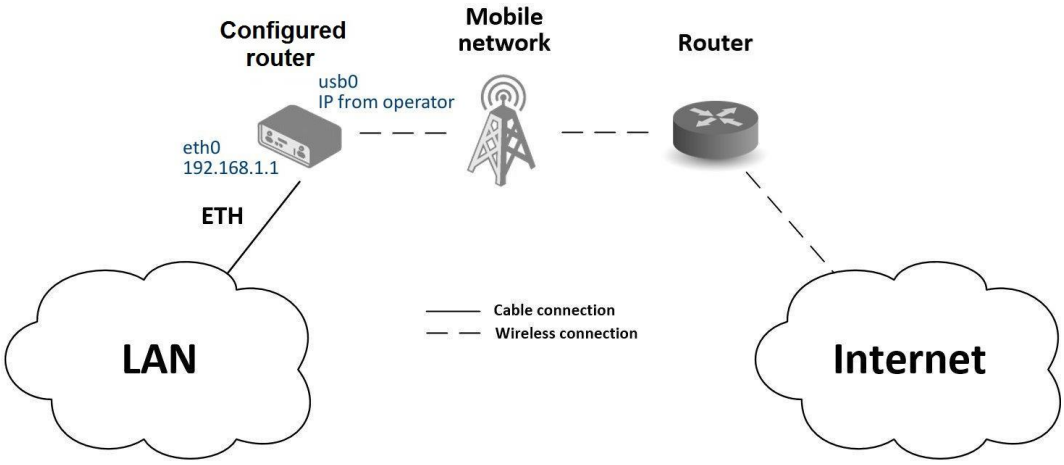


Abb. 110: Zugang zum Internet über LAN

In diesem Beispiel, einem LAN, das über ein Mobilfunknetz mit dem Internet verbunden ist, muss die SIM-Karte mit einem Datentarif vom Mobilfunknetzbetreiber bereitgestellt werden. Dies erfordert keine Erstkonfiguration. Sie müssen nur die SIM-Karte in den **SIM1**-Steckplatz (primäre SIM-Karte) einlegen, die Antenne an den **ANT**-Anschluss und den Computer (oder Switch und Computer) an die ETH0-Schnittstelle (LAN) des Routers anschließen. Warten Sie nach dem Einschalten des Routers einen Moment. Der Router verbindet sich mit dem Mobilfunknetz und dem Internet. Dies wird durch die LEDs auf der Vorderseite des Routers angezeigt (**WAN** und **DAT**).

Eine zusätzliche Konfiguration kann in den Optionen LAN und Mobile WAN im Abschnitt **Configuration** des Web-Interface erfolgen.

LAN-Konfiguration

Die Werkeinstellung für die IP-Adresse der Routerschnittstelle ETH0 ist im Format 192.168.1.1. Dies kann (nach Anmeldung im Router) in der Option Ethernet/**LAN** im Abschnitt **Configuration** geändert werden, siehe Abb. 111. In diesem Fall ist keine zusätzliche Konfiguration erforderlich, der DHCP-Server wird ebenfalls durch die Werkeinstellung aktiviert (der erste verbundene Computer erhält also die IP-Adresse 192.168.1.2 usw.). Andere Konfigurationsmöglichkeiten werden in Kapitel 5.1 "Ethernet- bzw. LAN-Konfiguration", S. 30, beschrieben.

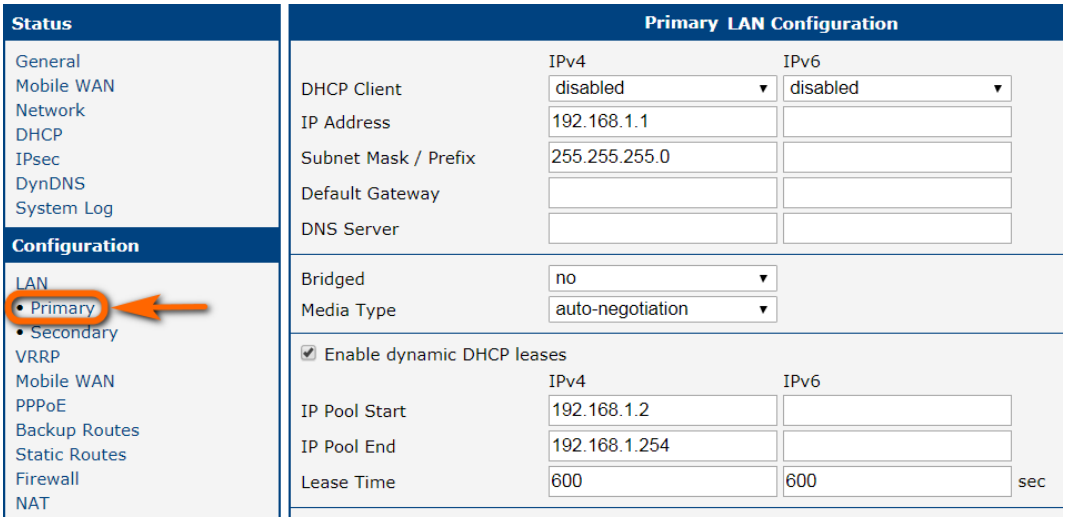


Abb. 111: Zugang vom Internet vom LAN aus – Ehternet/LAN configuration

Mobile WAN Konfiguration

Verwenden Sie das Element **Mobile WAN** im Abschnitt **Configuration**, um die Verbindung zum Mobilfunknetz zu konfigurieren, siehe Abbildung unten. In diesem Fall (je nach SIM-Karte) kann das Konfigurationsformular leer sein. Stellen Sie jedoch sicher, dass **Create connection to mobile network** aktiviert ist (dies ist die Werkseinstellung). Weitere Einzelheiten finden Sie im Kapitel 5.3.1.

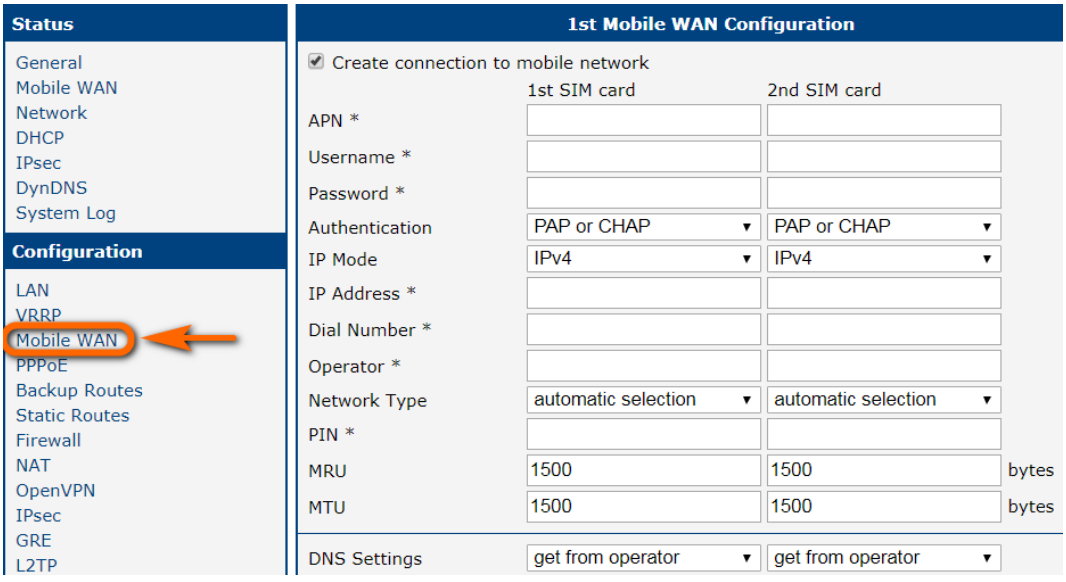


Abb. 112: Zugang zum Internet aus dem LAN – mobile WAN-Konfiguration

Um zu überprüfen, ob die Verbindung ordnungsgemäß funktioniert, klicken Sie auf die Option **Mobile WAN** im Abschnitt **Status**. Dort sind Informationen zum Netzbetreiber, zur Signalstärke usw. verfügbar. Unten wird die Nachricht **Connection successfully established** angezeigt. Das Menü-Element **Network** zeigt Informationen zu einer neu erstellten Netzwerkschnittstelle usb0 an (mobile Verbindung). Die IP-Adresse des Netzbetreibers, Routen-Tabelle usw. sind hier zu entnehmen. Das Internet ist jetzt über LAN zugänglich.

8.2 Backup-Zugang zum Internet aus dem LAN

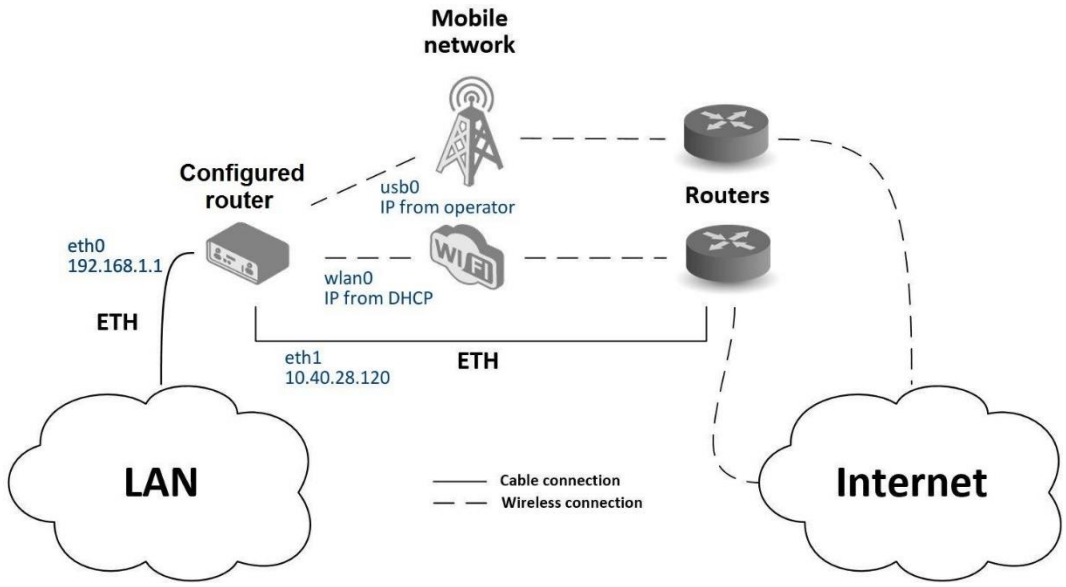


Abb. 113: Gesicherter Zugang zum Internet vom LAN

Mit dem Konfigurationsformular auf der Seite **Backup Routes** können Sie die primäre Verbindung mit alternativen Verbindungen zum Internet/Mobilnetz sichern.
Jeder Backup-Verbindung kann eine Priorität zugewiesen werden.

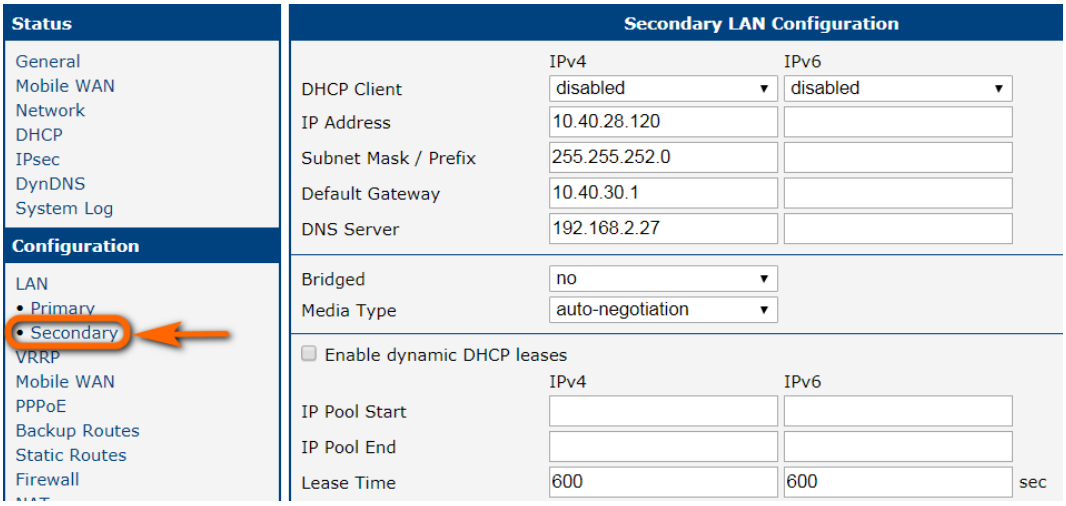


Abb. 114: Gesicherter Zugang zum Internet – Ethernet/LAN-Konfiguration

LAN-Konfiguration

In der Option Ethernet/**LAN** – ETH0/**Primary LAN** – können Sie die Konfiguration der Werkeinstellung wie in der vorherigen Situation nutzen. Die **ETH1**-Schnittstelle auf der Vorderseite des Routers wird zur Verbindung mit dem Internet verwendet. Es kann im ETH1/**Secondary LAN** konfiguriert werden. Verbinden Sie das Kabel mit dem Router und stellen Sie die geeigneten Werte wie in Abb. 114 ein. Hier werden statische IP-Adresse, Standard-Gateway und DNS-Server konfiguriert. Änderungen wirken nach Betätigung der Schaltfläche **Apply**. Die detaillierte Konfiguration des Ethernet/LAN wird in Kapitel 5.1 "Ethernet- bzw. LAN-Konfiguration", S. 30, beschrieben.

WLAN-Konfiguration

Um das WLAN zu verwenden, muss der Router über ein WLAN-Modul verfügen. Dann müssen Sie die Wi-Fi-Station im Element **WiFi > Station** konfigurieren, wie in Abb. 115 gezeigt.
Aktivieren Sie **Enable WiFi STA**, aktivieren Sie den DHCP-Client und geben Sie die Adressen des Standardgateways und des DNS-Servers ein. Geben Sie als Nächstes die Daten für die Verbindung ein (SSID, Authentifizierung, Verschlüsselung, WPA PSK-Typ und Passwort). Für weitere Informationen siehe Kapitel 5.6 "Wi-Fi-Station-Konfiguration", S. 52. Klicken Sie auf die Schaltfläche **Apply**, um die Änderungen zu bestätigen.

Zur Überprüfung der erfolgreichen Wi-Fi-Verbindung, siehe Sektion **Status**, Option **WiFi**. Bei einer erfolgreichen Verbindung finden Sie die Nachricht: `wpa_state=COMPLETED`

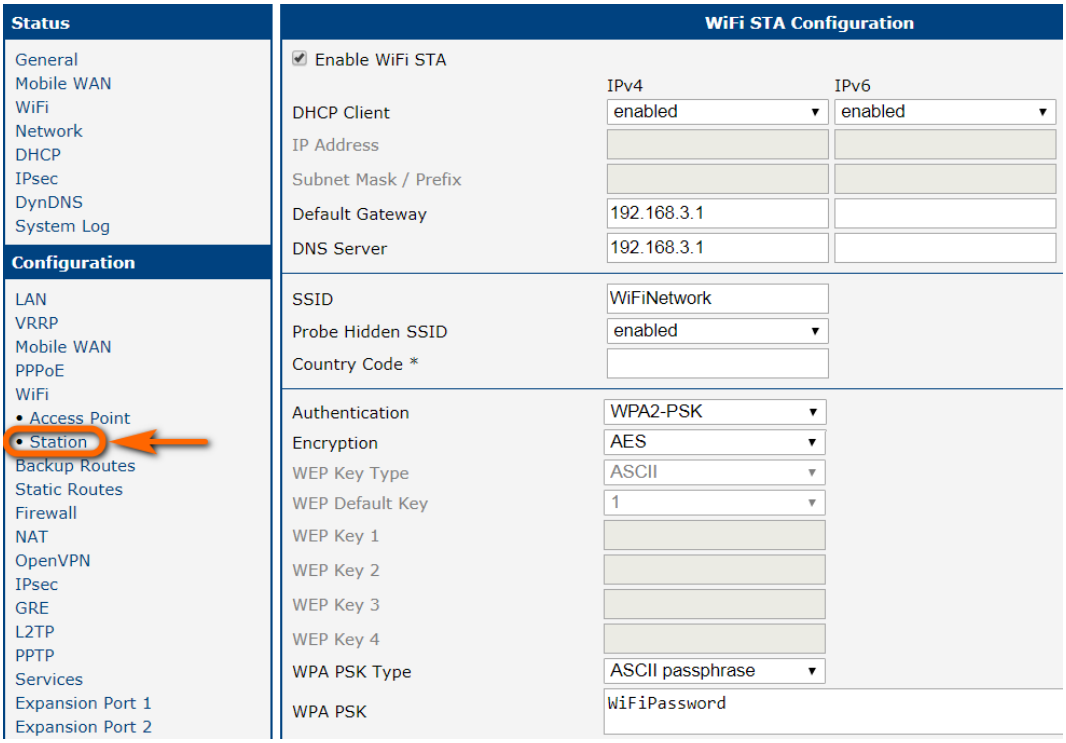


Abb. 115: Gesicherter Zugang zum Internet – WLAN-Konfiguration

Mobile WAN Konfiguration

Zur Konfiguration der mobilen Verbindung ist es ausreichend, die SIM-Karte in den **SIM1**-Slot einzuführen und die Antenne am **ANT**-Steckverbinder anzubringen wie in der vorherigen Situation (je nach verwendeter SIM-Karte).

Um Backup-Routen einzurichten, muss {**Check Connection** im Element **Mobile WAN** aktiviert sein, siehe Abb. 116.Setzen Sie die Option **Check connection option to enabled + bind** und geben Sie eine IP-Adresse von z. B. DNS-Server des Betreibers oder jeden anderen sicher verfügbaren Server und Zeitintervall der Überprüfung.
Für detaillierte Konfiguration siehe Kapitel 5.3.1 "Mobilfunkverbindung", S. 39.

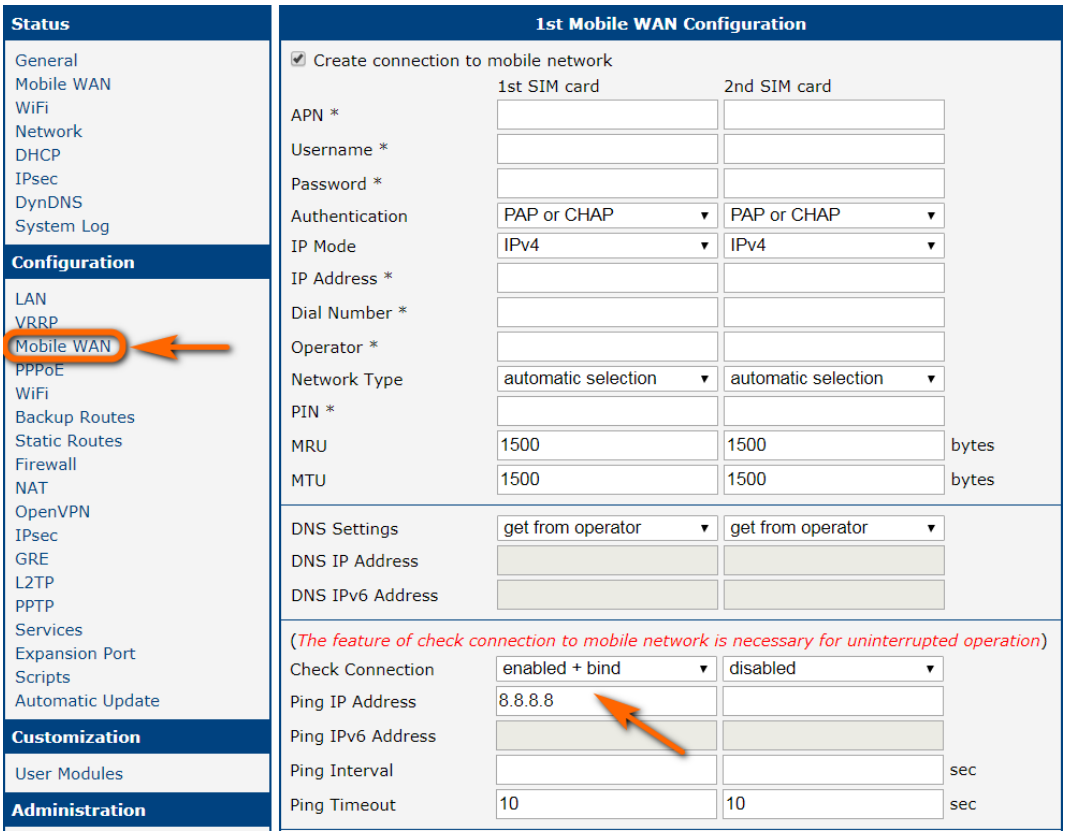


Abb. 116: Gesicherter Zugang zum Internet – mobiles WAN

Backup-Routes-Konfiguration

Nachdem Sie die Backup-Routen eingerichtet haben, müssen Sie deren Prioritäten festlegen. In Abb. 117. Hat die kabelgebundene ETH1-Verbindung die höchste Priorität. Wenn diese Verbindung fehlschlägt, ist die zweite Wahl die Wi-Fi wlan0-Netzwerkschnittstelle. Die dritte Wahl ist die mobile Verbindung – USB0-Netzwerkschnittstelle.

Das Backup-Routen-System muss aktiviert werden, indem für jede der Routen der Punkt **Enable backup routes switching** aktiviert wird. Klicken Sie auf die Schaltfläche **Apply**, um die Änderungen zu bestätigen.
Detaillierte Konfiguration siehe Kapitel 5.7 "Backup-Routen", S. 55.

Sie können die konfigurierten Netzwerkschnittstellen im Abschnitt **Status section** im Punkt **Network** überprüfen.
Sie sehen die aktiven Netzwerkschnittstellen: eth0 (Verbindung zum LAN), eth1 (kabelgebundene Verbindung zum Internet), wlan0 (WLAN-Verbindung zum Internet) und usb0 (mobile Verbindung zum Internet). IP-Adressen und andere Daten sind enthalten.

Unten auf der Seite sehen Sie die **Route Table** und die entsprechenden Änderungen, wenn eine kabelgebundene Verbindung fehlschlägt oder ein Kabel getrennt wird (die Standardroute ändert sich in wlan0).
Ebenso wird die mobile Verbindung verwendet, wenn keine Wi-Fi-Verbindung verfügbar ist.

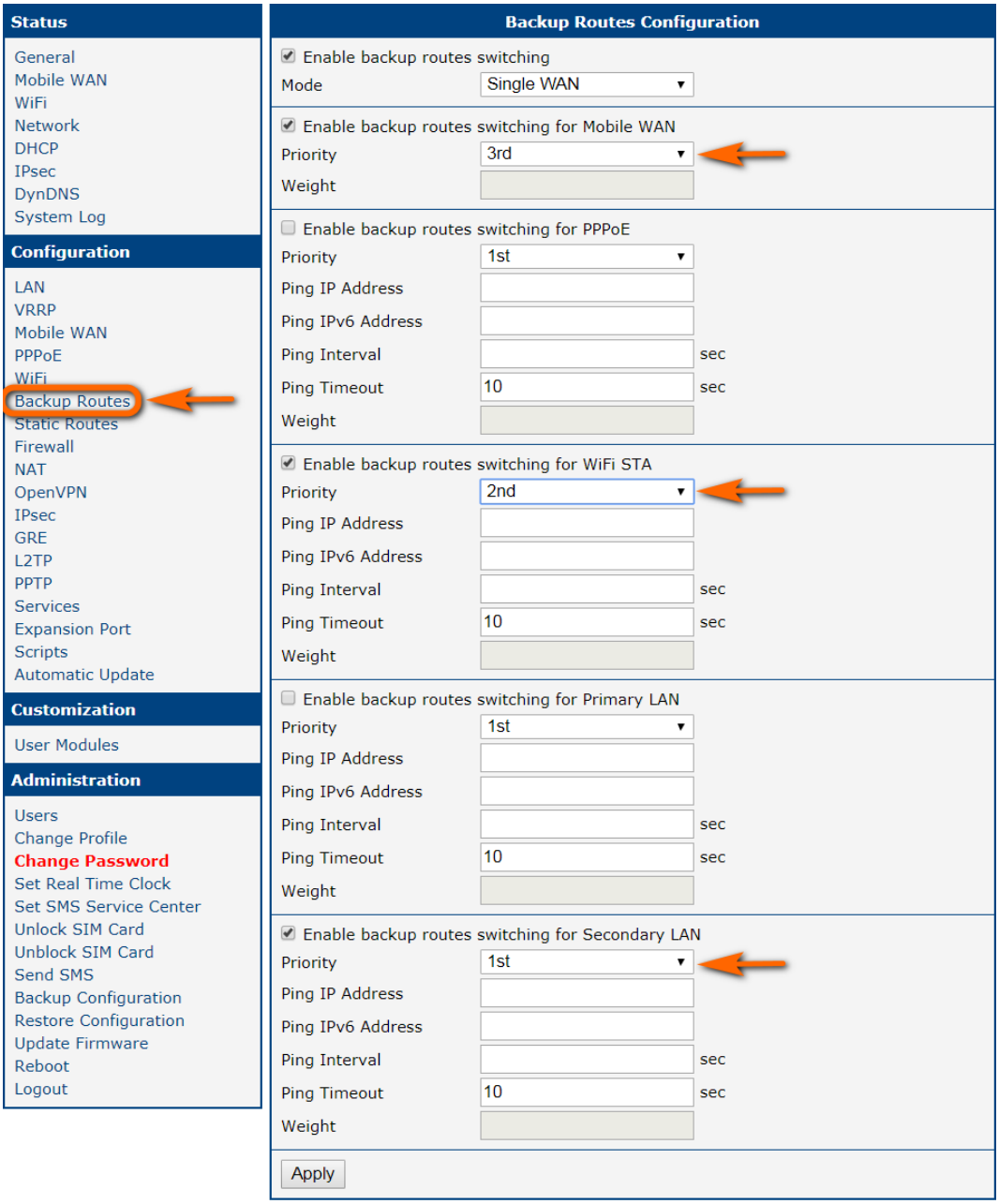


Abb. 117: Gesicherter Zugang zum Internet – Konfiguration der Backup-Routen

Derartig konfigurierte Router gewährleisten jetzt für Computer im LAN einen gesicherten Zugang zum Internet. Mit Auswahl der Option **Network** in der Sektion **Status** kann die Konfiguration der Netzwerk-Schnittstellen überprüft werden. Dort sollten Sie aktive Netzwerk-Schnittstellen eth0 (Verbindung zum LAN), eth1 (Kabelverbindung zum Internet), wlan0 (Wi-Fi-Verbindung zum Internet) und usb0 (mobile Verbindung zum Internet) sehen. IP-Adressen und andere Daten sind beinhaltet. Unten können Sie die **Route Table** und entsprechende Änderungen davon sehen, z. B. wenn die Kabelverbindung ausfällt oder das Kabel getrennt wird (die Standardroute wechselt dann zu wlan0) und gleichermaßen, wenn Wi-Fi nicht verfügbar ist, wird die mobile Verbindung verwendet.

Backup-Routen funktionieren, selbst wenn sie nicht in der Option **Backup Routes** aktiviert sind, aber der Router nutzt die Werkeinstellungen.

8.3 Sichere Netzzusammenschaltung oder mittels VPN

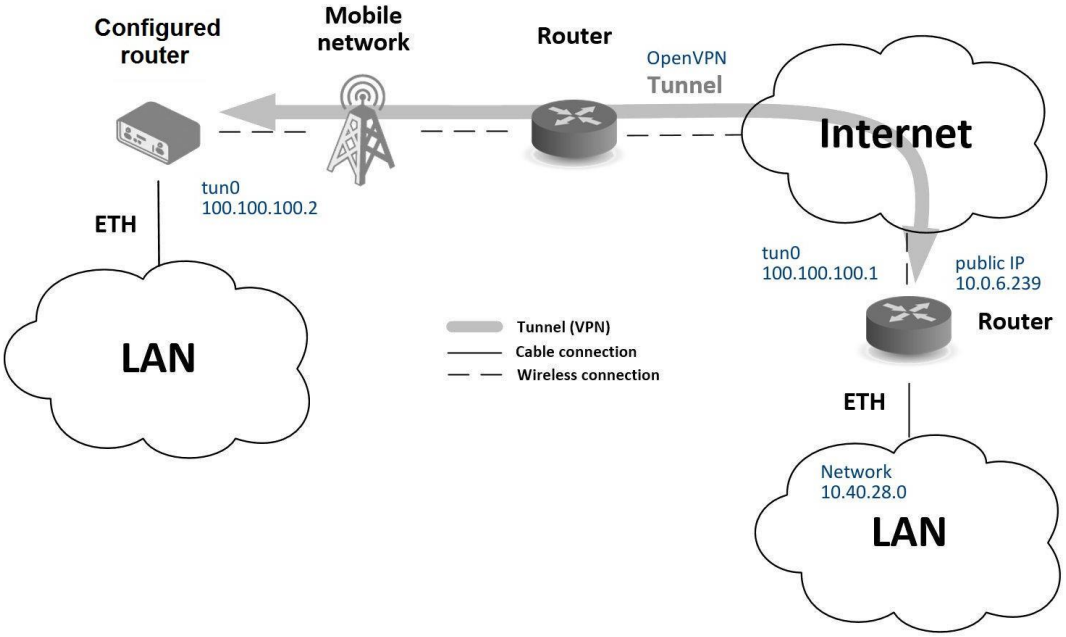


Abb. 118: Sichere Netzzusammenschaltung – Topologie des Beispiels

VPN (Virtual Private Network) ist ein Protokoll, das genutzt wird, um eine sichere Verbindung zwischen zwei LANs aufzubauen, die als ein gemeinsames LAN fungieren. Die Verbindung ist gesicherte (verschlüsselte) und authentifizierte (überprüfte). Diese Verbindung wird über ein öffentliches, nicht vertrauenswürdiges Netz (Internet) genutzt, siehe Abb. 118. Sie können mehrere verschiedene sichere Protokolle nutzen:

- **OpenVPN** (dies ist auch eine Konfigurationsoption im Webinterface des Routers), siehe Kap. 5.11 "Konfiguration des OpenVPN-Tunnels", S. 68.
- **IPsec** (dies ist auch eine Konfigurationsoption im Webinterface des Routers), siehe Kapitel 5.12 "Konfiguration des IPSec-Tunnels", S. 74.

Mit dem wienet Router ist es auch möglich, nicht verschlüsselte Tunnel zu erstellen: **GRE**, **PPTP** und **L2TP**. Sie können GRE- oder L2TP-Tunnel in Kombination mit IPsec zur Erstellung von VPN einsetzen.

Ein Beispiel für einen OpenVPN-Tunnel finden Sie in Abb. 99.
Um diesen Tunnel aufzubauen, benötigen Sie die IP-Adresse des gegenüberliegenden Routers, die Netzwerk-IP-Adresse des gegenüberliegenden Routers (nicht erforderlich) und das Pre-Shared Secret (Schlüssel). Erstellen Sie den OpenVPN-Tunnel, indem Sie die Elemente **Mobile WAN** und **OpenVPN** im Abschnitt **Configuration** konfigurieren.

Mobile WAN Konfiguration

Die mobile Verbindung kann gleichermaßen wie in den vorherigen Situationen konfiguriert werden. (Der Router verbindet sich selbst nach Einlegen der SIM-Karte in den **SIM1**-Slot und Anbringen der Antenne am **ANT**-Steckverbinder.) Die Konfiguration ist zugänglich in der Sektion **Configuration**, Unterpunkt **Mobile WAN** (siehe Kapitel 5.3.1 "Mobilfunkverbindung", S. 39), wo die mobile Verbindung aktiviert werden muss.

OpenVPN-Konfiguration

Die Konfiguration für OpenVPN ist möglich in der Sektion **Configuration**, Unterpunkt **OpenVPN**. Wählen Sie einen der beiden möglichen Tunnel und aktivieren Sie ihn durch Markieren von **Create 1st OpenVPN tunnel**. Das Protokoll und der Port müssen ausgefüllt werden (gemäß Daten über Gegenseite des Tunnels oder Open VPN-Server). Geben Sie die öffentliche IP-Adresse der Gegenseite des Tunnels einschließlich Remote Subnet und Mask ein (nicht notwendig). Wichtige Einträge sind **Local** und **Remote Interface IP Address**, bei denen die Information über die Enden des Tunnels eingegeben werden müssen. Für das hier vorliegende Beispiel war der **Pre-shared Secret** bekannt, wählen Sie deshalb diese Möglichkeit in der Option **Authentication Mode** und geben Sie den Schlüssel in das Feld ein. Bestätigen Sie die Konfiguration durch Anklicken der Schaltfläche **Apply**. Für eine detaillierte Konfiguration siehe Kapitel 5.11 5.11 "Konfiguration des OpenVPN-Tunnels", S. 68.

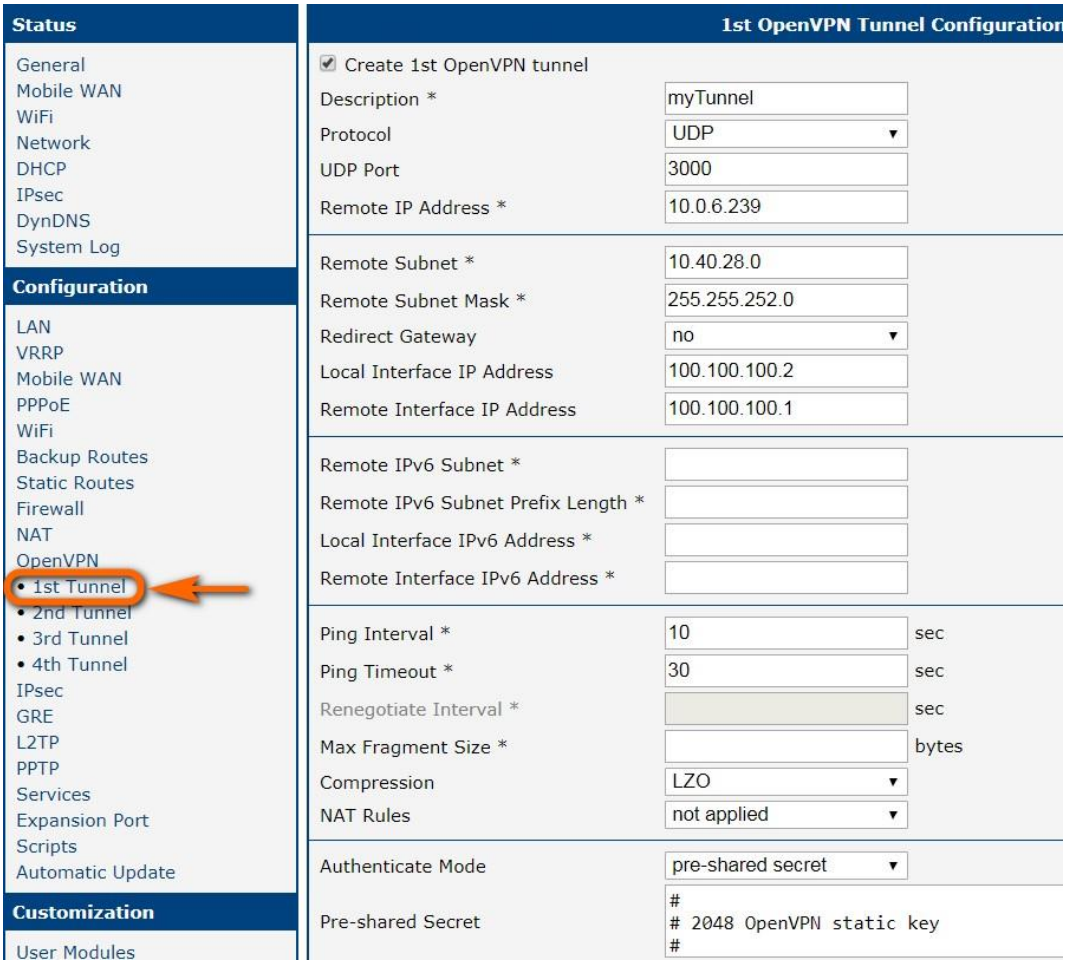


Abb. 119: Sichere Netzzusammenschaltung – OpenVPN configuration

In der Sektion **Status**, Unterpunkt **Network** können Sie die aktivierte Netzwerk-Schnittstelle tun0 für den Tunnel mit den IP-Adressen der Tunnelenden überprüfen. Die erfolgreiche Verbindung kann im **System Log** überprüft werden, wo Sie folgende Nachricht sehen: **Initialization Sequence Completed**. Die Netzwerke werden jetzt zusammengeschaltet. Dies kann auch durch das Ping-Programm überprüft werden. (Ping zwischen den IP-Adressen der Tunnelendpunkte von einem der Router. Konsole über SSH zugänglich).

8.4 Serielles Gateway

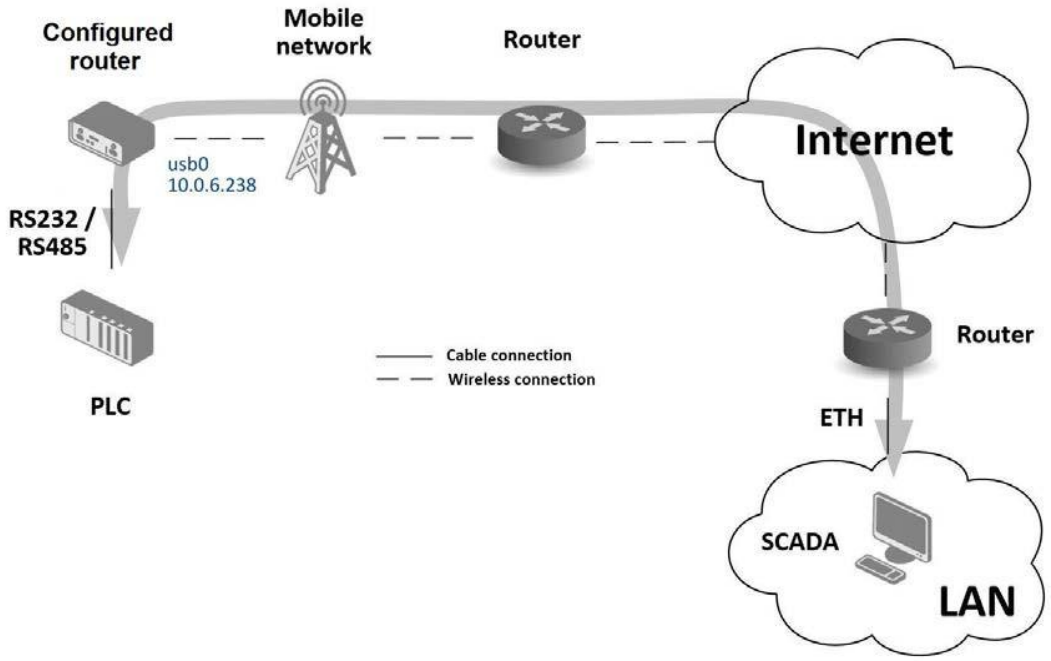


Abb. 120: Serielles Gateway – Beispieltopologie

Mit der seriellen Gateway-Funktion des Routers können Sie eine serielle Verbindung über das Internet oder mit einem anderen Netzwerk herstellen. Serielle Geräte (Zähler, SPS usw.) können dann Daten hoch- und herunterladen (siehe Abb. 94.).

Die Konfiguration erfolgt im Abschnitt **Configuration**, **Mobile WAN** mit dem Element **Expansion Port 1** für RS232 oder **Expansion Port 2** für RS485. In diesem Beispiel wird die RS232-Schnittstelle des Routers verwendet.

Mobile WAN Konfiguration

Die Konfiguration des mobilen WAN ist ähnlich wie in den vorherigen Beispielen. Setzen Sie einfach die SIM-Karte in den Steckplatz **SIM1** auf der Rückseite des Routers ein und schließen Sie die Antenne an den Anschluss **ANT** an der Vorderseite an. Es ist keine weitere Konfiguration erforderlich (je nach verwendeter SIM-Karte). Weitere Informationen finden Sie in Kapitel 5.1.3 "802.1X Authenticator beim RADIUS-Server", S. 33.

Konfiguration Expansion Port 1

Die RS232-Schnittstelle (Port) kann im Abschnitt **Configuration** über das Element **Expansion Port 1** konfiguriert werden (siehe Abb. 95.). Sie müssen den RS232-Port aktivieren, indem Sie **Enable expansion port 1 access over TCP/UDP** aktivieren. Sie können die seriellen Kommunikationsparameter bearbeiten (in diesem Beispiel nicht erforderlich). Die wichtigen Elemente sind **Protocol**, **Mode** und **Port**. Damit werden die Parameter für die Kommunikation mit dem Netzwerk und dem Internet festgelegt. In diesem Beispiel wird das TCP-Protokoll gewählt, und der Router arbeitet als Server, der auf dem TCP-Port 2345 hört. Bestätigen Sie die Konfiguration, indem Sie auf die Schaltfläche **Apply** klicken.

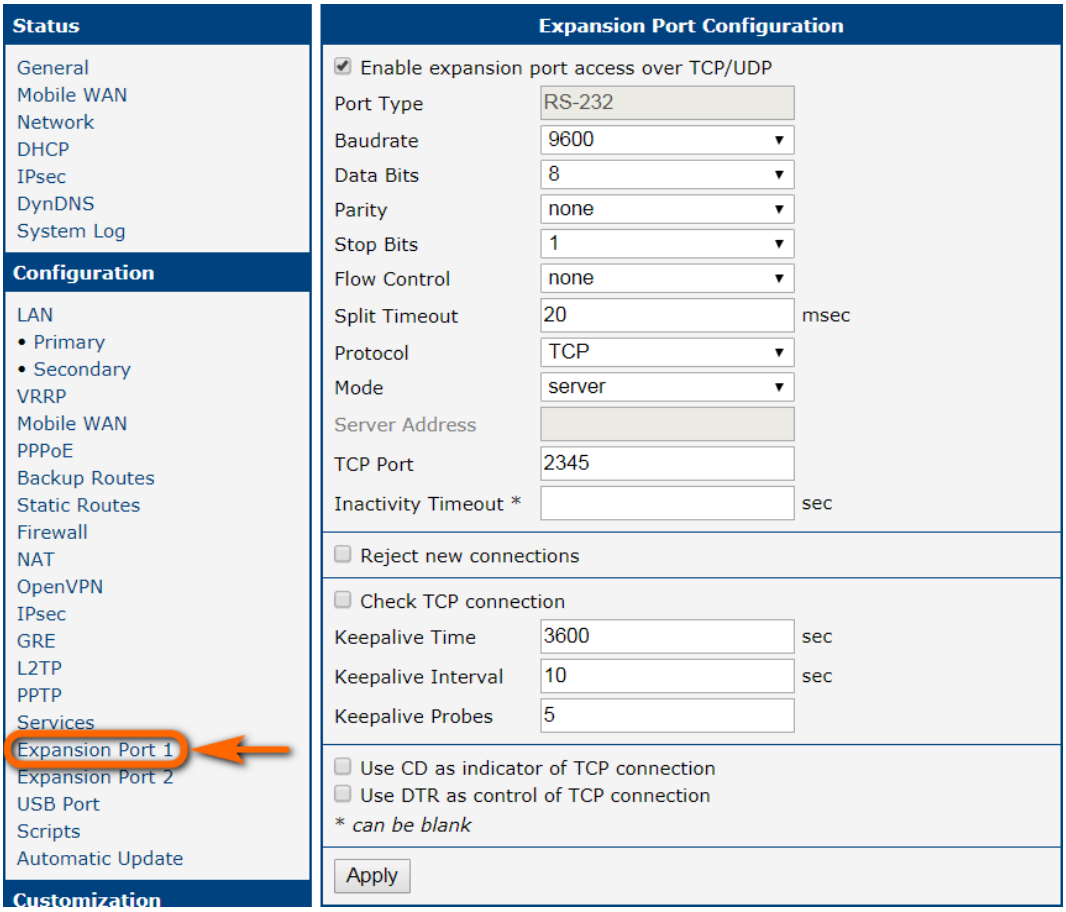


Abb. 121: Serielles Gateway – Konfiguration Expansion Port 1

Um mit dem seriellen Gerät (SPS) zu kommunizieren, verbinden Sie sich vom PC (in Abb. 94 als SCADA gekennzeichnet) als TCP-Client mit der IP-Adresse 10.0.6.238, Port 2345 (die öffentliche IP-Adresse der im Router verwendeten SIM-Karte, die der Netzwerkschnittstelle usb0 entspricht). Die Geräte können nun miteinander kommunizieren. Um die Verbindung zu überprüfen, gehen Sie ins **System Log** (**Status section**) und suchen Sie nach der Meldung **TCP connection established**.

9 ENTSORGUNG

Die WEEE-Richtlinie 2012/19/EU ("Waste Electrical and Electronic Equipment" – Elektro- und Elektronikgeräte-Abfall) wurde eingeführt um sicherzustellen, dass Elektro-/Elektronikprodukte unter Verwendung der besten verfügbaren Wiederverwendungstechnik recycelt werden, um die Auswirkungen auf die Umwelt so gering wie möglich zu halten. Dieses Produkt enthält hochwertige Materialien und Teile, die recycelt werden können. Am Ende seiner Lebensdauer darf dieses Produkt KEINESFALLS mit anderen Gewerbeabfällen vermischt und entsorgt werden. Informationen zur Entsorgung finden Sie in den Geschäftsbedingungen Ihres Lieferanten.

10 SERVICE UND SUPPORT

Service-Hotline

+49 (0) 951 9324-991

E-Mail: industry@wieland-electric.com

Wieland Electric GmbH |

Brennerstraße 10–14

D-96052 Bamberg

Tel. 49 (0) 951 / 9324-0

Fax 49 (0) 951 / 9324-128

E-Mail info@wieland-electric.com

http://eshop.wieland-electric.com

http://www.wieland-electric.com

11 ANHANG

11.1 Glossar

Backup-Routen

Ermöglicht dem Benutzer, die primäre Verbindung mit alternativen Verbindungen zum Internet/Mobilnetz zu sichern. Jeder Backup-Verbindung kann eine Priorität zugewiesen werden. Das Umschalten zwischen Verbindungen erfolgt basierend auf festgelegten Prioritäten und dem Zustand der Verbindungen.

DHCP

Das Dynamic Host Configuration Protocol (DHCP) ist ein Netzwerkprotokoll, das verwendet wird, um Geräte zu konfigurieren, die mit einem Netzwerk verbunden sind, damit sie in diesem Netzwerk über das Internet Protocol (IP) kommunizieren können. Das Protokoll ist in einem Client-Server-Modell implementiert, bei dem DHCP-Clients Konfigurationsdaten wie eine IP-Adresse, eine Standardroute und eine oder mehrere DNS-Serveradressen von einem DHCP-Server anfordern.

DHCP-Client

Fordert die Netzwerkkonfiguration an von DHCP-Server.

DHCP-Server

Beantwortet die Konfigurationsanfrage von DHCP-Client und sendet Details zur Netzwerkkonfiguration.

DNS

Das Domain Name System (DNS) ist ein hierarchisches verteiltes Namenssystem für Computer, Dienste oder jede Ressource, die mit dem Internet oder einem privaten Netzwerk verbunden ist. Es verknüpft verschiedene Informationen mit Domänennamen, die jeder der teilnehmenden Entitäten zugewiesen sind. Am bekanntesten ist, dass es leicht zu merkende Domänennamen in numerische IP-Adressen übersetzt, die zum Auffinden von Computerdiensten und -geräten weltweit benötigt werden. Durch die Bereitstellung eines weltweit verteilten, schlüsselwortbasierten Umleitungsdienstes ist das Domain Name System ein wesentlicher Bestandteil der Funktionalität des Internets.

DynDNS-Client

Mit dem DynDNS-Dienst können Sie mit einem leicht zu merkenden benutzerdefinierten Hostnamen aus der Ferne auf den Router zugreifen.
Dieser Client überwacht die IP-Adresse des Routers und aktualisiert ihn bei Änderungen.

GRE

Generic Routing Encapsulation (GRE) ist ein Tunneling-Protokoll, das eine Vielzahl von Netzwerkschichtprotokollen in virtuelle Punkt-zu-Punkt-Verbindungen über ein Internet Protocol-Netzwerk einkapseln kann. Es können vier verschiedene Tunnel erstellt werden.

HTTP

Das Hypertext Transfer Protocol (HTTP) ist ein Anwendungsprotokoll für verteilte, kollaborative, hypermediale Informationssysteme. HTTP ist die Grundlage der Datenkommunikation für das World Wide Web.

Hypertext ist strukturierter Text, der logische Verknüpfungen (Hyperlinks) zwischen Knoten verwendet, die Text enthalten. HTTP ist das Protokoll zum Austauschen oder Übertragen von Hypertext.

HTTPS

Das Hypertext Transfer Protocol Secure (HTTPS) ist ein Kommunikationsprotokoll für die sichere Kommunikation über ein Computernetzwerk mit besonders breitem Einsatz im Internet. Technisch gesehen ist es kein Protokoll an sich; Vielmehr ist es das Ergebnis der einfachen Überlagerung des Hypertext Transfer Protocol (HTTP) über das SSL/TLS-Protokoll, wodurch die Sicherheitsfunktionen von SSL/TLS zur Standard-HTTP-Kommunikation hinzugefügt werden.

IP-Adresse

Eine Internetprotokolladresse (IP-Adresse) ist ein numerisches Kennzeichen, das jedem Gerät (z. B. Computer, Drucker) zugewiesen wird, das an einem Computernetzwerk teilnimmt, das das Internetprotokoll für die Kommunikation verwendet. Eine IP-Adresse dient zwei Hauptfunktionen: Host- oder Netzwerkschnittstellenidentifikation und Standortadressierung. Seine Rolle wurde wie folgt charakterisiert: Ein Name zeigt an, was wir suchen. Eine Adresse zeigt an, wo sie sich befindet. Eine Route zeigt den Weg dorthin. Die Entwickler des Internet Protocol haben eine IP-Adresse als 32-Bit-Zahl definiert und dieses als Internet Protocol Version 4 (IPv4) bekannte System wird noch heute verwendet. Aufgrund des enormen Wachstums des Internets und der prognostizierten Erschöpfung der verfügbaren Adressen wurde jedoch 1995 eine neue IP-Version (IPv6) entwickelt, die 128 Bits für die Adresse verwendet.

IP-Maskerade/ IP Masquerading → siehe **NAT**.

IPsec

Internet Protocol Security (IPsec) ist eine Protokollsuite zum Sichern der Internet Protocol (IP)-Kommunikation durch Authentifizierung und Verschlüsselung jedes IP-Pakets einer Kommunikationssitzung. Der Router ermöglicht es dem Benutzer, den Kapselungsmodus (Tunnel oder Transport), den IKE-Modus (Main oder Aggressive), den IKE-Algorithmus, die IKE-Verschlüsselung, den ESP-Algorithmus, die ESP-Verschlüsselung und vieles mehr auszuwählen. Es können vier verschiedene Tunnel erstellt werden.

IPv4

Das Internet Protocol Version 4 (IPv4) ist die vierte Version in der Entwicklung des Internet Protocol (IP) und die erste Version des Protokolls, die weit verbreitet ist. Es ist eines der Kernprotokolle der auf Standards basierenden Internetworking-Methoden des Internets und leitet den meisten Datenverkehr im Internet weiter. Es wurde jedoch ein Nachfolgeprotokoll, IPv6, definiert und befindet sich in verschiedenen Phasen der Produktionsbereitstellung. IPv4 wird in der IETF-Publikation RFC 791 (September 1981) beschrieben und ersetzt eine frühere Definition (RFC 760, Januar 1980).

IPv6

Das Internet Protocol Version 6 (IPv6) ist die neueste Version des Internet Protocol (IP), des Kommunikationsprotokolls, das ein Identifizierungs- und Ortungssystem für Computer in Netzwerken bereitstellt und den Datenverkehr über das Internet leitet.
IPv6 wurde von der Internet Engineering Task Force (IETF) entwickelt, um das lang erwartete Problem der Erschöpfung der IPv4-Adressen zu lösen. IPv6 soll IPv4 ersetzen, das auch 2013 noch den überwiegenden Teil des Internetverkehrs trägt. Ende November 2012 soll der Anteil des IPv6-Verkehrs bei etwa 1% liegen. IPv6-Adressen werden als acht Gruppen von vier hexadezimalen Ziffern dargestellt, die durch Doppelpunkte getrennt sind (2001:0db8:85a3:0042:1000:8a2e:0370:7334), aber es gibt Methoden zur Abkürzung dieser vollständigen Notation.

L2TP

Layer 2 Tunneling Protocol (L2TP) ist ein Tunneling-Protokoll, das zur Unterstützung virtueller privater Netzwerke (

VPNs) oder als Teil der Bereitstellung von Diensten durch ISPs verwendet wird. Es bietet selbst keine Verschlüsselung oder Vertraulichkeit. Stattdessen verlässt es sich auf ein Verschlüsselungsprotokoll, das innerhalb des Tunnels weitergegeben wird, um die Privatsphäre zu gewährleisten.

LAN

Ein lokales Netzwerk (LAN) ist ein Computernetzwerk, das Computer in einem begrenzten Bereich wie einem Haus, einer Schule, einem Computerlabor oder einem Bürogebäude unter Verwendung von Netzwerkmedien miteinander verbindet. Zu den bestimmenden Merkmalen von LANs gehören im Gegensatz zu Weitverkehrsnetzen (WANs) ihre üblicherweise höheren Datenübertragungsraten, ein kleineres geografisches Gebiet und der fehlende Bedarf an gemieteten Telekommunikationsleitungen.

NAT

In Computernetzwerken ist Network Address Translation (NAT) der Prozess der Änderung von IP-Adressinformationen in IPv4-Headern während der Übertragung über ein Traffic-Routing-Gerät. Die einfachste Art von NAT bietet eine Eins-zu-Eins-Übersetzung von IP-Adressen. RFC 2663 bezeichnet diese Art von NAT als Basis-NAT, das oft auch als Eins-zu-Eins-NAT bezeichnet wird. Bei dieser Art von NAT werden nur die IP-Adressen, die IP-Header-Prüfsumme und alle übergeordneten Prüfsummen, die die IP-Adresse enthalten, geändert. Der Rest des Pakets bleibt unberührt (zumindest für die grundlegende TCP/UDP-Funktionalität; einige Protokolle höherer Ebene müssen möglicherweise weiter übersetzt werden). Basic-NATs können verwendet werden, um zwei IP-Netzwerke mit inkompatibler Adressierung miteinander zu verbinden.

NAT-T

NAT-Traversal (NAT-T) ist eine Computernetzwerkmethode mit dem Ziel, Internetprotokollverbindungen über Gateways aufzubauen und aufrechtzuerhalten, die die Netzwerkadressübersetzung (NAT) implementieren.

NTP

Network Time Protocol (NTP) ist ein Netzwerkprotokoll zur Taktsynchronisation zwischen Computersystemen über paketvermittelte Datennetze mit variabler Latenz.

OpenVPN

OpenVPN implementiert virtuelle private Netzwerktechniken (

VPN) zum Erstellen sicherer Punkt-zu-Punkt- oder Site-to-Site-Verbindungen. Es ist möglich, vier verschiedene Tunnel zu erstellen.

PAT

Port and Address Translation (PAT) oder Network Address Port Translation (NAPT), siehe NAT.

Port

In Computernetzwerken ist ein Port ein anwendungsspezifisches oder prozessspezifisches Softwarekonstrukt, das als Kommunikationsendpunkt im Host-Betriebssystem eines Computers dient. Ein Port ist mit einer IP-Adresse des Hosts sowie dem für die Kommunikation verwendeten Protokolltyp verknüpft. Der Zweck von Ports besteht darin, verschiedene Anwendungen oder Prozesse, die auf einem einzelnen Computer ausgeführt werden, eindeutig zu identifizieren und ihnen dadurch zu ermöglichen, eine einzige physische Verbindung zu einem paketvermittelten Netzwerk wie dem Internet gemeinsam zu nutzen.

PPTP

Das Point-to-Point Tunneling Protocol (PPTP) ist ein Tunneling-Protokoll, das auf der Sicherungsschicht (Schicht 2) des OSI-Referenzmodells arbeitet. PPTP ist eine proprietäre Technik, die Point-to-Point Protocol (PPP)-Frames in Internet Protocol (IP)-Pakete unter Verwendung des Generic Routing Encapsulation (GREGRE)-Protokolls kapselt. Paketfilter bieten Zugriffskontrolle, Ende-zu-Ende und Server-zu-Server.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) ist ein Netzwerkprotokoll, das eine zentrale Authentifizierungs-, Autorisierungs- und Abrechnungsverwaltung (AAA oder Triple A) für Benutzer bietet, die sich mit einem Netzwerkdienst verbinden und ihn verwenden. Aufgrund der breiten Unterstützung und des allgegenwärtigen Charakters des RADIUS-Protokolls wird es häufig von ISPs und Unternehmen verwendet, um den Zugriff auf das Internet oder interne Netzwerke, drahtlose Netzwerke und integrierte E-Mail-Dienste zu verwalten.

Root-Zertifikat

In der Kryptographie und Computersicherheit ist ein Stammzertifikat entweder ein unsigniertes öffentliches Schlüsselzertifikat oder ein selbstsigniertes Zertifikat, das die Stammzertifizierungsstelle (CA) identifiziert.
Ein Root-Zertifikat ist Teil eines Public-Key-Infrastruktur-Schemas. Die gängigste kommerzielle Variante basiert auf dem ITU-T X.509-Standard, der normalerweise eine digitale Signatur einer Zertifizierungsstelle (CA) enthält. Digitale Zertifikate werden mithilfe einer Vertrauenskette verifiziert. Der Vertrauensanker für das digitale Zertifikat ist die Root Certificate Authority (CA). Siehe X.509.

Router

Ein Router ist ein Gerät, das Datenpakete zwischen Computernetzwerken weiterleitet und ein Overlay-Netzwerk erstellt. Ein Router ist mit zwei oder mehr Datenleitungen aus unterschiedlichen Netzwerken verbunden. Wenn ein Datenpaket in einer der Leitungen ankommt, liest der Router die Adressinformationen im Paket, um sein endgültiges Ziel zu bestimmen. Dann leitet es das Paket unter Verwendung von Informationen in seiner Routing-Tabelle oder Routing-Richtlinie an das nächste Netzwerk auf seiner Reise weiter. Router führen die Verkehrsleitfunktionen im Internet aus. Ein Datenpaket wird typischerweise von einem Router zu einem anderen durch die Netzwerke weitergeleitet, die das Internetzwerk bilden, bis es seinen Zielknoten erreicht.

SFTP

Secure File Transfer Protocol (SFTP) ist eine sichere Version des File Transfer Protocol (FTP), das den Datenzugriff und die Datenübertragung über einen Secure Shell-Datenstrom (SSH) erleichtert. Es ist Teil des SSH-Protokolls. Dieser Begriff wird auch als SSH File Transfer Protocol bezeichnet.

SMTP

Das SMTP (Simple Mail Transfer Protocol) ist ein Standard-E-Mail-Protokoll im Internet und Teil der TCP/IP-Protokollsuite gemäß IETF RFC 2821. SMTP definiert das Nachrichtenformat und den Message Transfer Agent (MTA), der die Mail speichert und weiterleitet. SMTP verwendet standardmäßig TCP-Port 25. Das Protokoll für die E-Mail-Übermittlung ist dasselbe, verwendet jedoch Port 587. Durch SSL gesicherte SMTP-Verbindungen, bekannt als SMTPS, verwenden standardmäßig Port 465.

SMTPS

SMTPS (Simple Mail Transfer Protocol Secure) bezieht sich auf eine Methode zur Sicherung von SMTP mit Transport Layer Security. Weitere Informationen zu SMTP finden Sie in der Beschreibung von SMTPSMTP.

SNMP

Das Simple Network Management Protocol (SNMP) ist ein Internet-Standardprotokoll zur Verwaltung von Geräten in IP-Netzwerken. Zu den Geräten, die normalerweise SNMP unterstützen, gehören Router, Switches, Server, Workstations, Drucker, Modem-Racks und mehr. Es wird hauptsächlich in Netzwerkverwaltungssystemen verwendet, um an das Netzwerk angeschlossene Geräte auf Bedingungen zu überwachen, die eine administrative Aufmerksamkeit erfordern. SNMP ist eine Komponente der Internet Protocol Suite, wie von der Internet Engineering Task Force (IETF) definiert. Es besteht aus einer Reihe von Standards für das Netzwerkmanagement, einschließlich eines Anwendungsschichtprotokolls, eines Datenbankschemas und einer Reihe von Datenobjekten.

SSH

Secure Shell (SSH), manchmal auch als Secure Socket Shell bekannt, ist eine UNIX-basierte Befehlsschnittstelle und ein Protokoll für den sicheren Zugriff auf einen Remote-Computer. Es wird häufig von Netzwerkadministratoren verwendet, um Web- und andere Arten von Servern aus der Ferne zu steuern. SSH ist eigentlich eine Suite von drei Dienstprogrammen – slogin, ssh und scp – die sichere Versionen der früheren UNIX-Dienstprogramme rlogin, rsh und rcp sind. SSH-Befehle sind auf verschiedene Weise verschlüsselt und sicher. Beide Enden der Client/Server-Verbindung werden mit einem digitalen Zertifikat authentifiziert und Passwörter werden durch Verschlüsselung geschützt.

TCP

Das Transmission Control Protocol (TCP) ist eines der zentralen Protokolle der Internet Protocol Suite (IP) und ist so verbreitet, dass die gesamte Suite oft als TCP/IP bezeichnet wird. TCP bietet eine zuverlässige, geordnete und fehlergeprüfte Übermittlung eines Oktettstroms zwischen Programmen, die auf Computern ausgeführt werden, die mit einem lokalen Netzwerk, Intranet oder dem öffentlichen Internet verbunden sind. Es befindet sich auf der Transportschicht. Webbrowser verwenden TCP, wenn sie eine Verbindung zu Servern im World Wide Web herstellen, und es wird verwendet, um E-Mails zuzustellen und Dateien von einem Ort zum anderen zu übertragen.

UDP

Das User Datagram Protocol (UDP) ist eines der zentralen Mitglieder der Internet Protocol Suite (der Satz von Netzwerkprotokollen, die für das Internet verwendet werden). Mit UDP können Computeranwendungen Nachrichten, in diesem Fall als Datagramme bezeichnet, an andere Hosts in einem Internet Protocol (IP)-Netzwerk ohne vorherige Kommunikation senden, um spezielle Übertragungskanäle oder Datenpfade einzurichten. Das Protokoll wurde 1980 von David P. Reed entworfen und formell in RFC 768 definiert.

URL

Ein Uniform Resource Locator, abgekürzt URL, auch Webadresse genannt, ist eine bestimmte Zeichenfolge, die einen Verweis auf eine Ressource darstellt.
In den meisten Webbrowsern wird die URL einer Webseite oben in einer Adressleiste angezeigt. Ein Beispiel für eine typische URL wäre http://www.example.com/index.html, die ein Protokoll (http), einen Hostnamen (www.example.com) und einen Dateinamen (index.html) enthält. Eine URL ist technisch gesehen eine Art von Uniform Resource Identifier (URI), aber in vielen technischen Dokumenten und verbalen Diskussionen wird URL oft als Synonym für URI verwendet, und dies wird nicht als Problem angesehen.

VPN

Ein virtuelles privates Netzwerk (VPN) erweitert ein privates Netzwerk über ein öffentliches Netzwerk, beispielsweise das Internet. Es ermöglicht einem Computer, Daten über freigegebene oder öffentliche Netzwerke zu senden und zu empfangen, als wäre er direkt mit dem privaten Netzwerk verbunden, während er von den Funktionalitäts-, Sicherheits- und Verwaltungsrichtlinien des privaten Netzwerks profitiert. Dies geschieht durch den Aufbau einer virtuellen Punkt-zu-Punkt-Verbindung durch die Verwendung von dedizierten Verbindungen, Verschlüsselung oder einer Kombination aus beidem. Eine VPN-Verbindung über das Internet ähnelt einer Weitverkehrsnetzverbindung (WANWAN) zwischen den Standorten. Aus Benutzersicht wird auf die erweiterten Netzwerkressourcen auf dieselbe Weise zugegriffen wie auf Ressourcen, die aus dem privaten Netzwerk verfügbar sind.

VPN server → siehe

VPN

VPN tunnel → siehe

VPN

VRRP

Mit dem VRRP-Protokoll (Virtual Router Redundancy Protocol) können Sie das Paket-Routing vom Hauptrouter auf einen Backup-Router übertragen, falls der Hauptrouter ausfällt. (Dies kann verwendet werden, um in kritischen Anwendungen ein drahtloses Mobilfunk-Backup für einen primären kabelgebundenen Router bereitzustellen).

WAN

Ein Weitverkehrsnetz (WAN) ist ein Netz, das ein weites Gebiet (d. h. jedes Telekommunikationsnetz, das über städtische, regionale oder nationale Grenzen hinweg verbindet) unter Verwendung privater oder öffentlicher Netztransporte abdeckt. Unternehmen und Behörden verwenden WANs, um Daten zwischen Mitarbeitern, Kunden, Käufern und Lieferanten von verschiedenen geografischen Standorten aus zu übertragen. Im Wesentlichen ermöglicht diese Art der Telekommunikation einem Unternehmen, seine täglichen Aufgaben unabhängig vom Standort effektiv auszuführen. Das Internet kann auch als WAN betrachtet werden und wird von Unternehmen, Regierungen, Organisationen und Einzelpersonen für fast jeden erdenklichen Zweck verwendet.

X.509

In der Kryptographie ist X.509 ein ITU-T-Standard für eine Public-Key-Infrastruktur (PKI) und Privilege Management Infrastructure (PMI). X.509 spezifiziert unter anderem Standardformate für Public-Key-Zertifikate, Zertifikatssperrlisten, Attributzertifikate und einen Validierungsalgorithmus für den Zertifizierungspfad.

Wieland Electric GmbH |
Brennerstraße 10 – 14
DE-96052 Bamberg

Tel +49 951 9324-0
Fax +49 951 9324-198
info@wieland-electric.com
www.**wieland**-electric.com