Cellular Industrial

v2 Routers

Konfigurations-Handbuch

B+B SmartWorx

Powered by ADVANTECH

www.lucom.de

16-01-17

Verwendete Symbole

Gefahr – Informationen zur Anwendersicherheit oder zu möglichen Schäden für den Router .

Achtung – Probleme, die in bestimmten Situationen auftreten können..

Information, Hinweis – Nützliche Hinweise oder Informationen von besonderem Interesse.

Firmware-Version

Aktuelle Version der Firmware: 6.0.2 (21. Oktober 2016)

Open Source Software-Lizenzen

Die Software in diesem Gerät verwendet verschiedene Teile von Open Source Software, die unter folgenden Lizenzen stehen: GPL versions 2 und 3, LGPL version 2, BSD-style Lizenzen, MIT-style Lizenzen. Die Liste der Komponenten zusammen mit den vollständigen Lizenztexten finden Sie auf dem Gerät: Klicken Sie auf den Link *Lizenzen* am Ende der Startseite (*Allgemein*) oder tragen Sie in Ihrem Browser die Adresse DEVICE_IP/licenses.cgi ein. Falls Sie an den Sourcen interessiert sind, schreiben Sie bitte an:

cellularsales@advantech-bb.com

Advantech B+B SmartWorx s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Handbuch-Stand 1 veröffentlicht in der Tschechischen Republik, 19. Dezember 2016

Inhaltsverzeichnis

LUCOM GmbH — Flößaustr. 22a — 90763 Fürth — Tel.: +49 911/ 957 606 00 — E-Mail: info@lucom.de — www.lucom.de

Abbildungsverzeichnis

Tabellenverzeichnis

16-01-17

1. Konfiguration über den Web-Browser

Hinweis! Der Router erfordert einen richtig konfigurierten Mobilfunkzugang, der aktiviert ist und Datenübertragung bereitstellt. Füe UMTS- und LTE-Anbieter muss ein SIM-Karte im Gerät stecken. Stecken Sie die SIM-Karte nur dann in den Router, wenn dieser ausgeschaltet (stromlos) ist.

Zustandsüberwachung, Konfiguration und Verwaltung des Routers erfolgt über eine Web-Schnittstelle. Diese kann durch die Eingabe der IP-Adresse des Routers in einem Web-Browser aufgerufen werden. Die Standard-IP-Adresse des Routers lautet „http://192.168.1.1“. Die Konfiguration kann nur der Benutzer ***root*** mit dem voreingestellten Passwort ***root*** vornehmen.

Nach der erfolgreichen Eingabe der Anmeldeinformationen wird die grafische Oberfläche angezeigt.

Abbildung 1: Beispiel für die Web-Konfiguration

Im linken Teil der Seite befindet sich die Navigationsspalte mit folgenden Menüpunkten: Überwachung des Zustandes (*Status*), Konfiguration (*Configuration*), Verwaltung der Benutzermodule (*Customization*) und Verwaltung (*Administration*) des Routers.

Um die Sicherheit der Netzwerkverbindung zu erhöhen, sollten Sie das Standardpasswort ändern. Wenn das ursprüngliche Passwort nicht geändert wurde, wird der Menüpunkt ***Change password*** Rot gekennzeichnet.

Nachdem die PWR-LED auf dem Frontpanel zu blinken beginnt, ist es möglich, die Werkseinstellung des Routers durch Drücken der RST-Taste auf dem Frontpanel wiederherzustellen. Nach Drücken der RST-Taste wird das Reset des Routers vorgenommen (Erneuerung der Konfiguration und danach Reboot des Routers/die grüne LED beginnt zu leuchten).

1.1 Gesicherter Zugang zur Web-Schnittstelle

Der Zugang zur Web-Schnittstelle kann auch mittels einer über das Protokoll HTTPS gesicherten Verbindung erfolgen.

Bei einem Router mit der Standard-IP-Adresse erfolgt der Zugang zur gesicherten Router-Konfiguration, indem Sie in der Adresszeile des Web-Browsers die Adresse https://192.168.1.1 eingeben. Möglicherweise erscheint zunächst eine Meldung mit dem Hinweis auf das Sicherheitszertifkat der Web-Site. Klicken Sie in diesem Fall auf die Schaltfläche *Weiter zu dieser Web-Site*. Um bei jedem Neustart des Routers die Sicherheitsmeldung abzuschalten, gehen Sie vor wie folgt:

Jeder Router verfügt über ein selbst-signiertes HTTPS-Zertifikat. Falls Sie ihr eigenes Zertifikat verwenden wollen, z. B. in Kombination mit einem dynamischen DNS-Dienst), ersetzen Sie die Dateien /etc/certs/https_cert und /etc/certs/https_key auf dem Router.

Die Erzeugung von HTTPS-Zertifikaten wurde mit Firmware 5.3.5 sicherer. Bereits vorhandene HTTPS-Zertifkate auf ausgelieferten Routern werden nicht automatisch mit dem Firmware-Update erneuert! Initiieren Sie ein manuelles Upgrade, indem Sie die Dateien /etc/certs/https* auf dem Router löschen (z. B. über SSH). Die Zertifikate werden dann beim nächsten Start des Routers automatisch neu erzeugt.

Um bei jedem Neustart des Routers die Sicherheitsmeldungen bei der Verwendung von selbst-signierten Zertifikaten abzuschalten, gehen Sie vor wie folgt:

Hinweis Sie müssen den auf der MAC-Adresse des Router basierenden Domain-Name verwenden. Dabei kann nicht garantiert werden, dass dies mit jeder möglichen Kombination von Betriebssystem und Browser funktioniert.

LUCOM GmbH — Flößaustr. 22a — 90763 Fürth — Tel.: +49 911/ 957 606 00 — E-Mail: info@lucom.de — www.lucom.de

- Erstellen Sie einen neuen Eintrag mit der IP-Adresse des Routers und dem Domain-Name, basierend auf der MAC-Adresse der ersten Netzwerk-Schnittstelle, siehe Menüpunkt *Status -> General Status*, Abschnitt *Primary LAN*, Kapitel 2.1.2.

  Die Doppelpunkt ersetzen Sie durch –.

  Beispiel: Aus der MAC-Adresse 00:11:22:33:44:55 wird der Domain-Name 00-11-22-33-44-55.

- Greifen Sie auf den Router über die neue Domain-Name-Adresse zu (Beispiel: https://00-11-22-33-44-55).

  Wird die Sicherheitsmeldung angezeigt, fügen Sie eine Ausnahme hinzu, damit die Meldung beim nächsten Mal nicht mehr angezeigt wird. Ist es nicht möglich eine Ausnahme hinzuzufügen, exportieren Sie das Zertifikat als Datei und importieren Sie es im Browser oder Betriebssystem.

16-01-17

2. Status

2.1 General Status

Die Auswahl des Menüpunkts *General* öffnet den Bildschirm *General Status*, siehe Abbildung 1. Dieser zeigt einen generellen Überblick über den Router und seine Aktivitäten. Dieser Bildschirm ist gleichzeitig die Startseite für die Web-Schnittstelle.

Die Informationen sind in verschiedene Bereiche aufgeteilt, abhängig von der Art der Aktivität oder der Eigenschaften: *Mobile Connection*, *Primary LAN*, *Peripheral Ports* und *System Information*.

Falls der Router mit einer WLAN-Erweiterung ausgestattet ist, wird entsprechend der Bereich *WiFi* angezeigt.

2.1.1 Mobile Connection

Element	Beschreibung
SIM Card	Identifikation der SIM-Karte (*Primary* (Erste) or *Secondary* (Zweite)).
Interface	Gibt die Netzwerk-Schnittstelle an.
Flags	Statusindikator.
IP Address	IPv4-Adresse der Netzwerk-Schnittstelle.
IPv6 Address	IPv6-Adresse oder Adressen der Netzwerk-Schnittstelle. Einer Schnittstelle können mehrere IPv6-Adressen zugewiesen werden.
MTU	Maximale Paketgröße, die übermittelt werden kann.
Rx Data	Gesamtzahl der empfangenen Bytes
Rx Packets	Empfangene Pakete
Rx Errors	Fälschlich empfangene Pakete
Rx Dropped	Verworfene empfangene Pakete
Rx Overruns	Wegen Überlast verlorene empfangen Pakete.
Tx Data	Gesamtzahl der gesendeten Bytes
Tx Packets	Gesendete Pakete
Tx Errors	Fälschlich gesendete Pakete
Tx Dropped	Verworfene gesendete Pakte
Tx Overruns	Wegen Überlast verlorene gesendete Pakete.
Uptime	Laufzeit; gibt an, wie lange die Verbindung ins Mobilfunknetz schon besteht.

Tabelle 1: Mobile Connection

2.1.2 Primary LAN, Secondary LAN und WiFi

Die in diesem Abschnitt angezeigten Elemente entsprechen den Elementen im vorherigen Abschnitt. Zudem zeigt das Element *MAC Address* die korrespondierende Schnittstelle des Routers (*Primary LAN – eth0, Secondary LAN – eth1, WiFi – wlan0*). Die angezeigten Informationen hängen von der vorhandenen Ausstattung des Routers ab, siehe Kapitel 3.1 oder 3.5).

2.1.3 Peripheral Ports

Element	Beschreibung
Expansion Port 1	Erweiterungsport (Position 1) *None* zeigt an, dass kein Port installiert ist
Expansion Port 2	Erweiterungsport (Position 2) *None* zeigt an, dass kein Port installiert ist
Binary Input	Status des binären Eingangs
Binary Output	Status des binären Ausgangs

Tabelle 2: Erweiterungs-Ports

2.1.4 System Information

Element	Beschreibung
Firmware Version	Information zur Version der Firmware
Serial Number	Seriennummer des Routers (*N/A* gibt an, dass keine Seriennummer vorhanden ist)
Profile	Aktuelles Profil – Standardprofil oder alternative Profile (Profile werden beispielsweise dazu genutzt zwischen verschiedenen Betriebsmodus zu wechseln)
Supply Voltage	Versorgungsspannung des Routers
Temperature	Temperatur im Router
Time	Akutelles Datum und aktuelle Uhrzeit
Uptime	Laufzeit, gibt an, wie lange der Router seit dem letzten Boot-Vorgang in Betrieb ist.
Licenses	Link zur Liste der Open-Source-Software-Komponenten der Firmware und der vollständigen Lizenztexte (GPL Versionen 2 und 3, LGPL Version 2, BSD-style Lizenzen, MIT-style Lizenzen).

Tabelle 3: System-Information

2.2 Mobile WAN Status

Der Industrie-Router XR5i v2 hat keine Statusoption für mobiles WAN.

Über den Menüpunkt *Mobile WAN* rufen Sie Informationen zum aktuellen Status der Mobilfunkverbindungen ab.

Im Abschnitt *Mobile Network Information* werden Basisinformationen zum Mobilfunknetzwerk, mit dem der Router verbunden ist, angezeigt. Zusätzlich werden Informationen über die im Router eingebauten Module angezeigt.

Element	Beschreibung
Registration	Status der Netzwerkregistrierung
Operator	Name des Netzwerkbetreibers
Technology	Übertragungstechnologie
PLMN	PLNM-Kennung des Anbieters
Cell	Funkzelle mit welcher der Router verbunden ist
LAC	Aufenthaltsbereich – eindeutige Nummer des Aufenthaltsbereichs
Channel	Kanal auf dem der Router kommuniziert
Signal Strength	Signalstärke der ausgewählten Funkzelle
Signal Quality	Signalqualität der ausgewählten Funkzelle: • EC/IO für UMTS und CDMA (Verhältnis des auf dem Pilotkanals (EC) empfangenen Signals zum Gesamtpegel der Spektraldichte, d. h., die Summe der Signale der anderen Funkzellen (IO) • RSRQ für LTE (definiert als Verhältnis $\frac{N \times RSRP}{RSSI}$) • Der Wert ist für EDGE nicht verfügbar.
CSQ	Signalqualität der Funkzelle, relativer Wert RSSI in dBm. 2 – 9: marginal; 14 – 14: OK; 15 – 16: Gut: 20 – 30: hervorragend.
Neighbours	Signalstärke der benachbarten Zellen
Manufacturer	Hersteller des Moduls
Model	Typ des Moduls
Revision	Revision des Moduls
IMEI	IMEI-Nummer des Moduls (International Mobile Equipment Identity)
ESN	ESN (Electronic Serial Number) Nummer des Moduls (CDMA-Router)
MEID	MEID-Nummer des Moduls (Mobile Equipment Identifier)
ICCID	Eindeutige Seriennummer der SIM-Karte (Integrated Circuit Card IDentifier).

Tabelle 4: Mobile Network Information

16-01-17

Ist eine benachbarte Zelle rot markiert, besteht die Gefahr, dass der Router ständig zwischen dieser Funkzelle und der ersten Funkzelle wechselt. Dieses Verhalten kann die Leistung des Routers beeinflussen. Zur Abhilfe richten Sie die Antenne anders aus oder benutzen Sie eine Richtantenne.

Im Abschnitt *Mobile Network Statistics* werden Informationen über die Qualität der Mobilfunkverbindung während vergangenen Aufzeichnungsperioden angezeigt. Neben den Standardintervallen, z. B. die letzten 24 Stunden oder die vergangene Woche, können Sie selbst ein Intervall definieren.

Period	Beschreibung
Today	Heute von 0:00 bis 23:59
Yesterday	Gestern von 0:00 bis 23:59
This week	Diese Woche von Montag 0:00 bis Sonntag 23:59
Last week	Vergangene Woche von Montag 0:00 bis Sonntag 23:59
This period	Akuteller Aufzeichnungszeitraum
Last period	Vorheriger Aufzeichnungszeitraum

Tabelle 5: Beschreibung der Aufzeichnungszeiträume

Element	Beschreibung
Signal Min	Minimale Signalstärke
Signal Avg	Durchschnittliche Signalstärke
Signal Max	Maximale Signalstärke
Cells	Anzahl der Wechsel zwischen Funkzellen
Availability	Verfügbarkeit des Routers über das Mobilfunknetzwerk (in Prozent)

Tabelle 6: Mobilfunkstatistik

Tipps zur Tabelle *Mobilfunkstatistik*:

- *Availability* wird als Prozentsatz ausgegeben. Dieser beschreibt das Verhältnis von der Zeitspanne der Verbindungen ins Netzwerk zu der Zeitspanne, in der der Router eingeschaltet war.
- Wenn Sie den Cursor auf den Eintrag *Signal Min* oder *Signal Max* führen, wird der Zeitpunkt angezeigt, an dem der Router das letzte Mal diese Signalstärke gemessen hat.

Im Abschnitt *Traffic Statistics for Primary/Secondary SIM card* werden Informationen zu Übertragungsraten und die Anzahl der Verbindungen für beide SIM-Karten während der entsprechenden Aufzeichnungszeiträume angezeigt.

Element	Beschreibung
RX data	Gesamtvolumen der empfangenen Daten
TX data	Gesamtvolumen der gesendeten Daten
Connections	Anzahl der Verbindungen ins Mobilfunknetz

Tabelle 7: Verkehrsstatistik

Im Abschnitt *Mobile Network Connection Log* werden Informationen zum Verbindungsaufbau und damit verbundenen Problemen angezeigt.

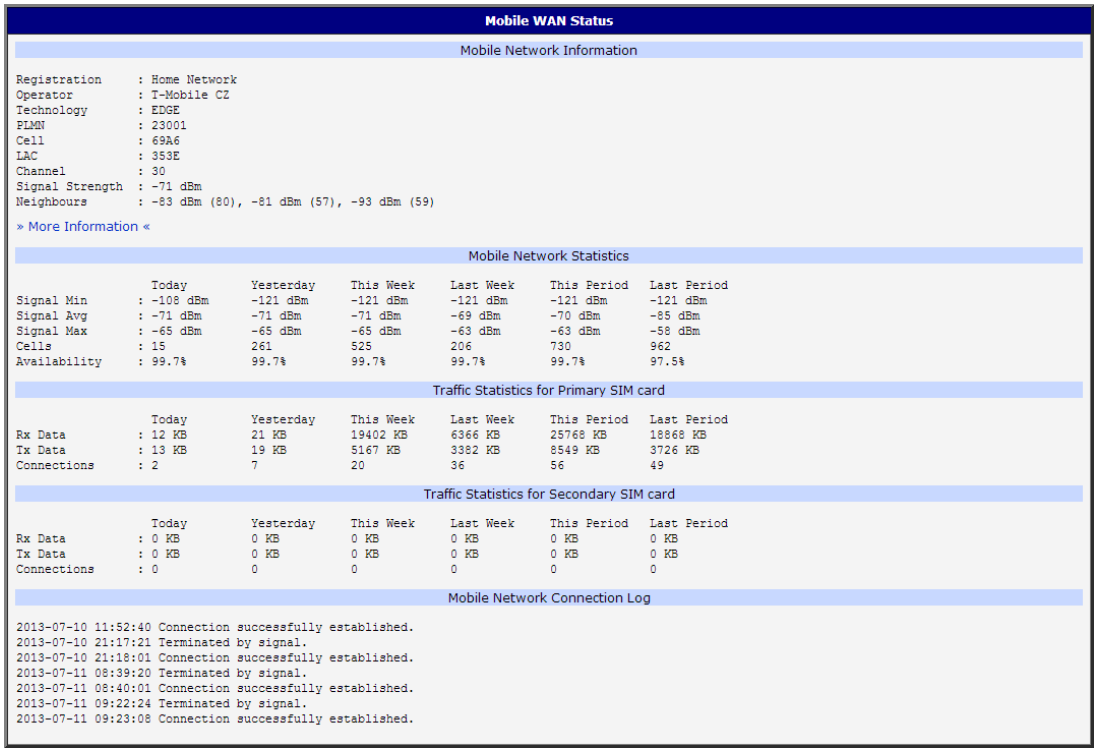


Abbildung 2: Status Mobile WAN

2.3 WiFi

Diese Konfigurationsseite wird nur angezeigt, wenn der Router mit einem WLAN-Modul ausgerüstet ist.

Wählen Sie den Menüpunkt *WiFi* in der Navigationsspalte. Der Bildschirm *WiFi Status* zeigt Informationen über den Access Point (AP) und verbundene Stationen an.

Element	Beschreibung
hostapd state dump	Zeitpunkt der Datenerhebung
num_sta	Anzahl der verbundenen Stationen
num_sta_non_erp	Anzahl der verbundenen Stationen, die 802.11b in 802.11g BSS-Verbindungen benutzen
num_sta_no_short_slot_time	Anzahl der Stationen, die Short Slot Time nicht unterstützen
num_sta_no_short_preamble	Anzahl der Stationen, die Short Preamble nicht unterstützen

Tabelle 8: Status – Access Point

Für jeden verbundenen Client werden Informationen, meist interne Daten, angezeigt.

Beispiele

Element	Beschreibung
STA	MAC-Adresse des verbundenen Geräts (Station)
AID	Kennung der verbundenen Geräte (1 – 2007). 0 zeigt an, dass die Station aktuell nicht verbunden ist.

Tabelle 9: Statusinformation über verbundene Clients

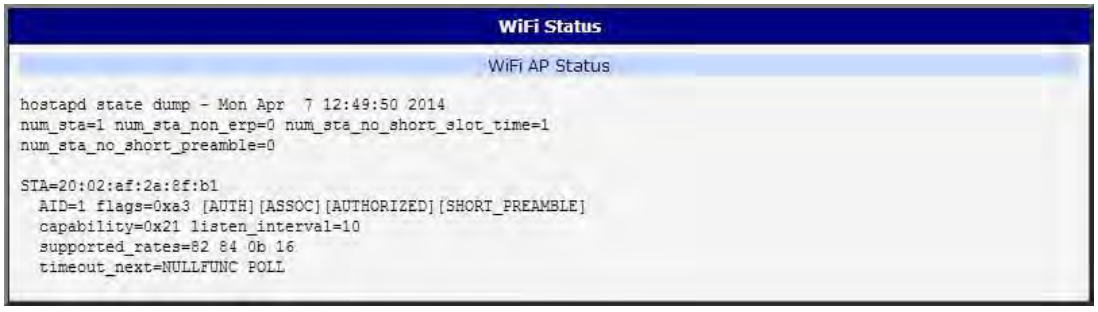


Abbildung 3: Status – WLAN

2.4 WiFi Scan

Diese Konfigurationsseite wird nur angezeigt, wenn der Router mit einem WLAn-Modul ausgerüstet ist.

Wählen Sie den Menüpunkt *WiFi Scan* in der Navigationsspalte. Der Bildschirm *WiFi Scan* zeigt die Ergebnisse des Scans nach benachbarten WLANs. **Scannen ist nur möglich, wenn der Access Point (WiFi AP) ausgeschaltet ist.**

Element	Beschreibung
BSS	MAC-Adresse des Access Points (AP)
TSF	Die Funktion Timing Synchronization Function (TSF) sorgt für die Synchronisation der Timer aller Stationen im gleichen Basic Service Set (BSS). Alle Stationen sollten einen lokalen TSF-Timer unterstützen.
freq	Frequenzband des WLANs [kHz]
beacon interval	Frist für die Zeitsynchronisation
capability	Liste der Eigenschaften des Access Points (AP)
signal	Signalpegel des Access Points (AP)
last seen	letzte Antwortzeit des Access Points (AP)
SSID	Kennung des Access Points (AP)
Supported rates	vom Access Point (AP) unterstützte Datenraten (Anzahl: 8)
DS Parameter set	Sendekannel des Access Points (AP)
ERP	Extended Rate PHY – Rückwärtskompatibilität zu 802.11
Extended supported rates	unterstützte Datenraten des Access point (AP), die über die in Zeile *Supported rates* angezeigten hinausgehen
RSN	Robust Secure Network – Diese Protokoll stellt eine sichere Kommunikation über Funknetzwerke (802.11)

Tabelle 10: Informationen über benachbarte WLANs

LUCOM GmbH — Flößaustr. 22a — 90763 Fürth — Tel.: +49 911/ 957 606 00 — E-Mail: info@lucom.de — www.lucom.de

Die Ausgabe von *WiFi Scan* kann wie folgt aussehen:

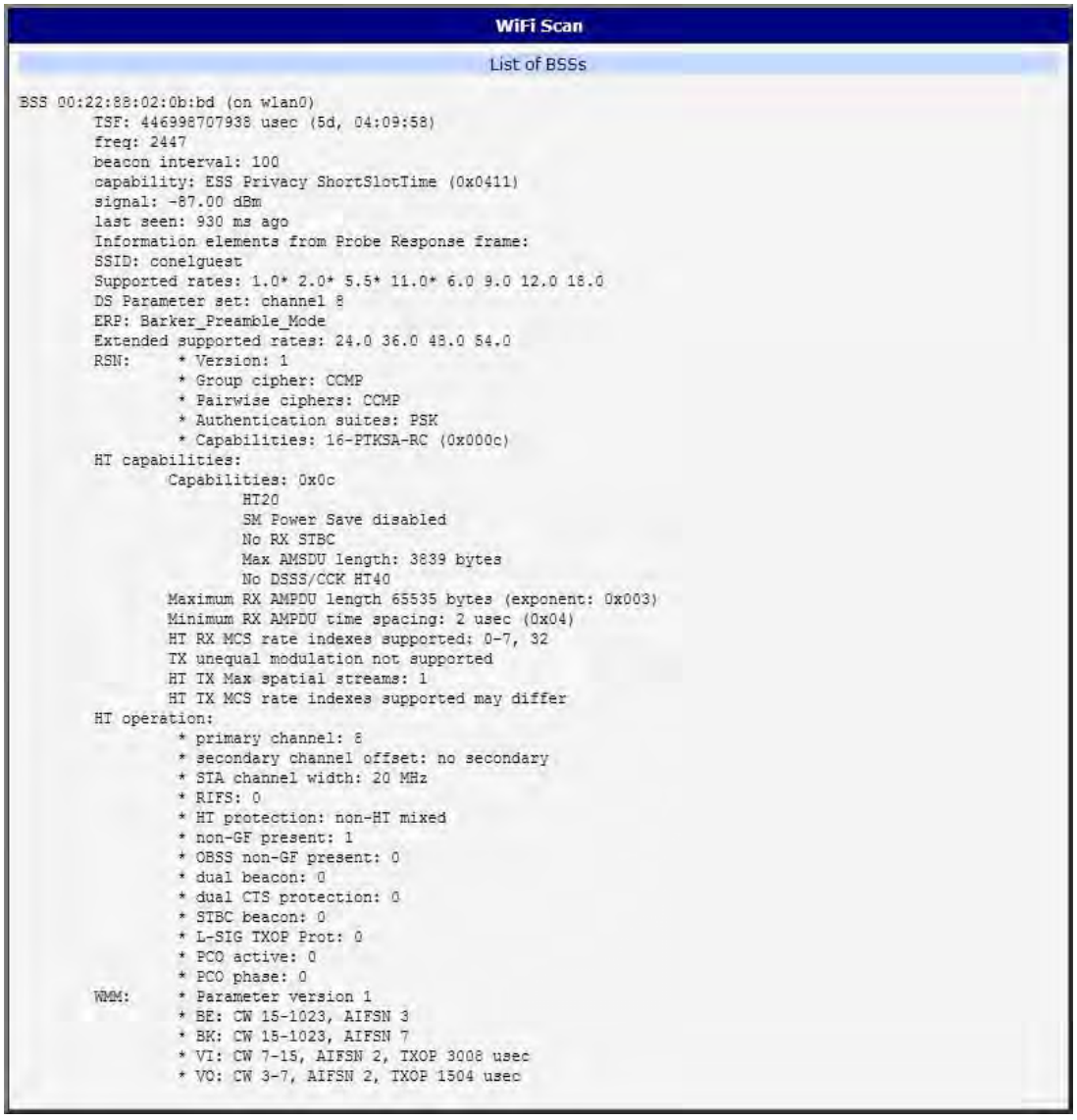


Abbildung 4: Status – WiFi Scan

2.5 Network Status

Wählen Sie den Menüpunkt *Network* in der Navigationsspalte. Der Bildschirm *Network Status* zeigt Informationen über die Schnittstellen und den Routing Table.

Der Abschnitt *Interfaces* zeigt detaillierte Informationen zu den aktiven Schnittstellen an.

Schnittstelle	Beschreibung
eth0, eth1	Netzwerk-Schnittstellen (Ethernet-Verbindung)
ppp0	Aktive PPP-Schnittstelle – Das WLAN-Module ist über die USB-Schnittstelle angeschlossen.
wlan0	WLAN-Schnittstelle
tun0	OpenVPN-Tunnel-Schnittstelle
ipsec0	IPSec-Tunnel-Schnittstelle
gre1	GRE-Tunnel-Schnittstelle
usb0	USB-Schnittstelle

Tabelle 11: Beschreibung der Schnittstellen

Die folgenden Informationen werden für jede Netzwerk-Schnittstelle angezeigt:

Element	Beschreibung
HWaddr	eindeutige MAC-Adresse der Netzwerk-Schnittstelle
inet addr	IPv4-Adresse der Schnittstelle
P-t-P	IP-Adresse der Gegenseite (im Fall einer Point-to-Point-Verbindung).
Bcast	Broadcast-Adresse
Mask	Subnetzmaske
MTU	Maximale übertragbare Paketgröße.
Metric	Anzahl der Router, über die das Paket geleitet werden muß.
RX	• **packets** – empfangene Pakete • **errors** – Anzahl der Fehler • **dropped** – verworfen Pakete • **overruns** – wegen Überlast verlorene einkommende Pakete • **frame** – falsche einkommende Paket mit unrichtiger Paketgröße

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite	
Element	**Beschreibung**
TX	• **packets** – übertragene Pakete • **errors** – Anzahl der Fehler • **dropped** – verworfen Pakete • **overruns** – wegen Überlast verlorene ausgehende Pakete • **carrier** – falsch ausgehende Pakete mit Fehlern in der physikalischen Schicht
collisions	Anzahl der Kollisiooen in der physikalischen Schicht
txqueuelen	Puffergröße (Warteschlange) der Netzwerk-Schnittstelle
RX bytes	Gesamtzahl der empfangenen Bytes
TX bytes	Gesamtzahl der übertragenen Bytes

Tabelle 12: Beschreibung der Informationen

Der Status der Verbindung ins mobilen Netzwerk wird auch auf der Seite *Network Status* angezeigt. Eine aktive Verbindung ins mobile Netzwerk erscheint als Schnittstellen *usb0*.

Der Abschnitt *Route Table* enthält die Einträge für *Route Table*.

Beim Router XR5i v2 entspricht die Schnittstelle ppp0 der PPPoE-Verbindung.

Network Status

Interfaces

```
eth0      Link encap:Ethernet  HWaddr 7C:66:9D:35:A3:F6
          inet addr:10.40.28.66  Bcast:10.40.31.255  Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:171724 errors:0 dropped:12 overruns:0 frame:0
          TX packets:1192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13537612 (12.9 MB)  TX bytes:698267 (681.9 KB)
          Interrupt:56

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:784 (784.0 B)  TX bytes:784 (784.0 B)

usb0      Link encap:Ethernet  HWaddr A6:50:8B:AD:3D:84
          inet addr:10.0.5.218  Bcast:10.255.255.255  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:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:568 (568.0 B)  TX bytes:3058 (2.9 KB)
```

Route Table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.254.254 0.0.0.0         UG    0      0        0 usb0
10.40.28.0      0.0.0.0         255.255.252.0   U     0      0        0 eth0
192.168.254.254 0.0.0.0         255.255.255.255 UH    0      0        0 usb0
```

Abbildung 5: Netzwerk-Status

LUCOM GmbH — Flößaustr. 22a — 90763 Fürth — Tel.: +49 911/ 957 606 00 — E-Mail: info@lucom.de — www.lucom.de

2.6 DHCP Status

Über den Menüpunkt *DHCP* rufen Sie Informationen zu den Aktivitäten des DHCP-Servers auf. Der DHCP-Server bietet automatischen Konfiguration von Clients, die mit dem Router verbunden sind. Der DHCP-Server vergibt für jedes Geräte eine eigene IP-Adresse und Subnetzmaske sowie die IP-Adresse des Standard-Gateways.

Element	Beschreibung
lease	zugewiesene IPv4-Adresse
starts	Zeitpunkt der Adresszuweisung
ends	Zeitpunkt, wenn die Adresszuweisung endet
hardware ethernet	eindeutige MAC-Adresse der Hardware
uid	eindeutige ID
client-hostname	Hostname des Geräts

Tabelle 13: Status – DHCP

Der DHCP-Status kann gelegentlich zwei Einträge für eine IP-Adresse anzeigen. Dies kann von einem Reset der Netzwerk-Schnittstelle des Clients verursacht werden.

Abbildung 6: Status – DHCP

Einträge auf der Seite *DHCP Status* sind in zwei Teile geteilt: *Active DHCP Leases (Primary LAN)* und *Active DHCP Leases (WLAN)*.

2.7 IPsec Status

Über den Menüpunkt *IPsec* rufen Sie Informationen über eingerichtete IPsec-Tunnel auf. Wurde der Tunnel korrekt eingerichtet, wird **IPsec SA established** angezeigt (rote Umrandung in der folgenden Abbildung).

Wird diese Meldung nicht angezeigt, wurde der Tunnel nicht eingerichtet!

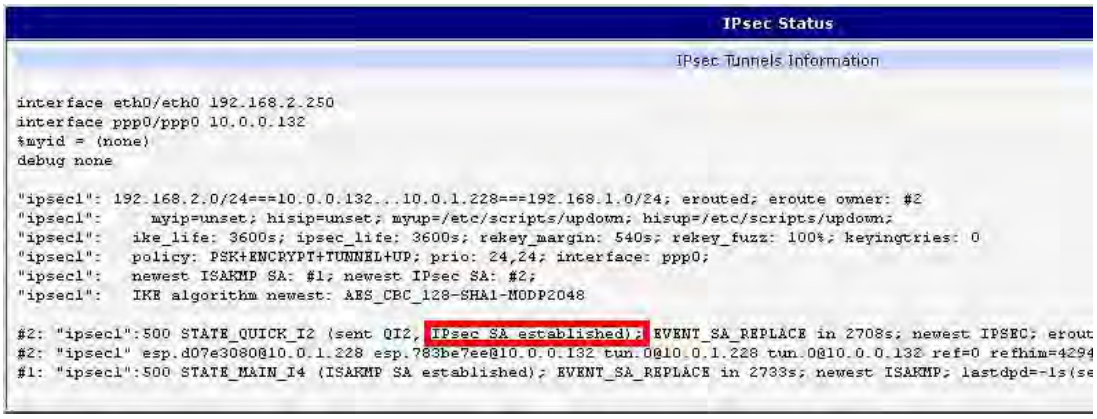


Abbildung 7: Status – IPsec

2.8 DynDNS Status

Wurde Dynamic DNS konfiguriert, wird der Status angezeigt, wenn Sie den Menüpunkt *DynDNS* wählen.

Das Gerät unterstützt DynamicDNS über einen DNS-Server bei folenden Anbieter. Weitere Informationen zur Einrichtung eine Dynamic DNS-Clients finden Sie z. B. auf www.dyndns.org.

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

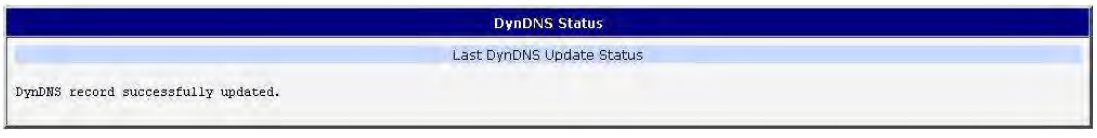


Abbildung 8: Status – DynDNS

Entdeckt das Gerät eine Aktualisierung eines DynDNS-Eintrags, wird mindestens eine der folgenden Meldungen angezeigt:

- DynDNS client is disabled. (DynDNS-Client ist deaktiviert.)
- Invalid username or password. (Benutzername oder Passwort ungültig.)
- Specified hostname doesn't exist. (Der angegebene Hostname existiert nicht.)

- Invalid hostname format. (Ungültiges Format für Hostname.)
- Hostname exists, but not under specified username. (Der Hostname existiert, aber nicht unter dem angegebenen Benutzernamen.)
- No update performed yet. (Bis jetzt kein Update durchgeführt.)
- DynDNS record is already up to date. (DynDNS-Eintrag ist bereits aktuell.)
- DynDNS record successfully update. (DynDNS-Eintrag wurde erfolgreich aktualisiert.)
- DNS error encountered. (Es ist ein DNS-Fehler aufgetreten.)
- DynDNS server failure. (DynDNS-Server-Fehler)

Der SIM-Karte des Geräts muss eine öffentliche IP-Adresse zugewiesen sein, damit DynDNS korrekt funktioniert.

2.9 System Log

Über den Menüpunkt *System Log* können Sie sich die System-Protokolldatei anzeigen lassen. Hier werden z. B. die Meldungen bei Verbindungsproblemen oder zu den auf dem Gerät laufenden Anwendungen angezeigt.

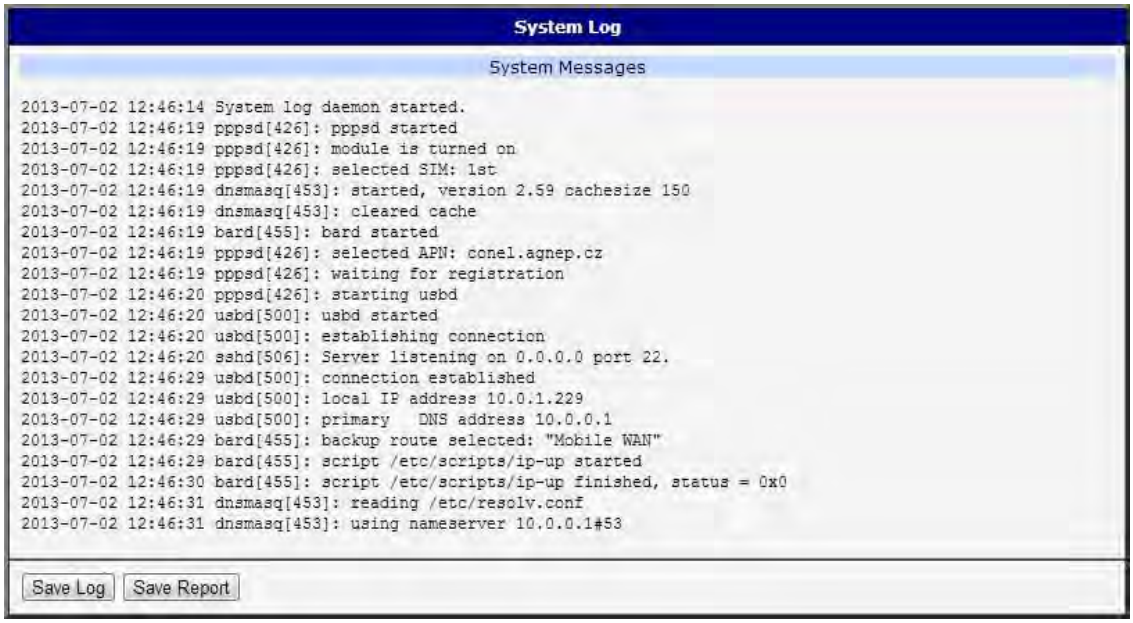


Abbildung 9: System-Log

Über die Schaltfläche *Save Log* können Sie das aktuelle System-Protokoll lokal als Textdatei (.txt) speichern.

Über die Schaltfläche *Save Report* erstellen Sie einen detaillierten Bericht im Textformat (.txt). Der Bericht enthält statistische Daten, Routing- und Prozess-Tabellen, das System-Protokoll sowie Angaben zur Konfiguration.)

Die Standardlänge des System-Protokolls sind 1.000 Zeilen, danach wird eine zweite Protokolldatei geschrieben. Sobald diese 1.000 Zeilen lang ist, wird die erste Datei überschrieben.

Das Programm *Syslogd* erzeugt das Systemprotokoll. Es kann mit zwei Parameter gestartet werden. Der Parameter „*-S*“, gefolgt von einer Dezimalzahl, legt die Anzahl der Zeilen der Protokolldatei fest. Der Parameter „*-R*“, gefolgt von Hostname oder IP-Adresse, erlaubt das Protokollieren auf einen fernen Syslog-Daemon. Um *syslogd* mit den angegebenen Parameter zu starten, bearbeiten Sie das Skript */etc/init.d/syslog* über eine SSH-Verbindung zum Gerät oder Sie ergänzen die Parameter im Skript *Startup Script* entsprechend Abbildung 10, siehe Kapitel *Configuration*.

Unter Linux wird der Syslog-Daemon typischerweise über den Befehl „*syslogd -R*“ gestartet. Unter Windows muss ein Syslog-Server installiert sein, z. B. *Syslog Watcher*.

Die folgende Abbildung zeigt die Einstellungen im *Startup Script*, damit die Protokolldaten an den fernen Server mit der IP-Adresse 192.168.2.115 gesendet werden.

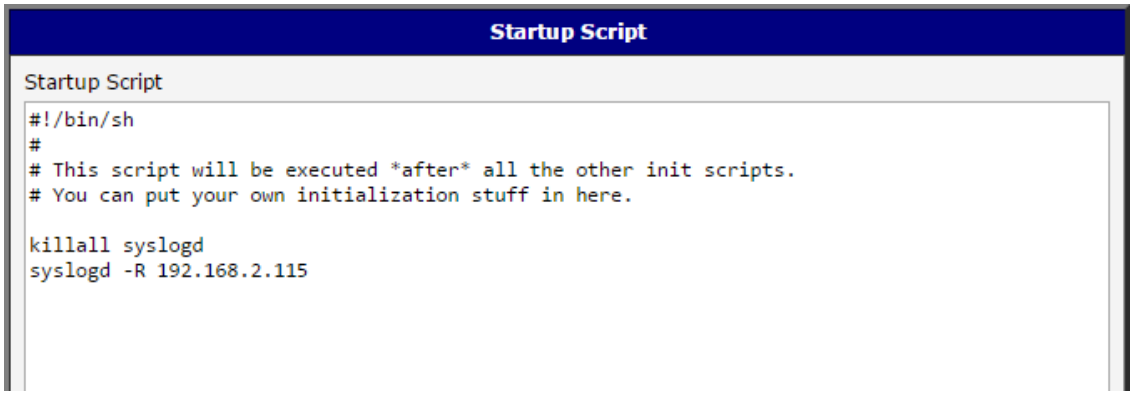


Abbildung 10: Beispiel: Syslogd mit dem Parameter -R starten

LUCOM GmbH — Flößaustr. 22a — 90763 Fürth — Tel.: +49 911/ 957 606 00 — E-Mail: info@lucom.de — www.lucom.de

3. Konfiguration

3.1 LAN Configuration

Öffnen Sie die Konfigurationsseite für das Local Area Network, indem Sie in der Navigationsspalte auf den Menüpunkt *LAN* klicken.

Element	Beschreibung
DHCP Client	Schaltet die Funktion ein oder aus. • **disabled** – Das Gerät verhindert die automatische Zuweisung einer IP-Adresse durch einen DHCP-Server im Netzwerk. • **enabled** – Das Gerät erlaubt die automatische Zuweisung einer IP-Adresse durch einen DHCP-Server im Netzwerk.
IP address	Feste IP-Adresse der Netzwerk-Schnittstelle *eth0*
Subnet Mask	Subnetzmaske zu dieser IP-Adresse
Bridged	Schaltet die Funktion ein oder aus. • **no** – Die Brigde ist inaktiv (Standard). • **yes** – Die Bridge ist aktiv.
Media type	Art des Duplex und Geschwindigkeit im Netzwerk • **Auto-negation** – Das Gerät entscheidet automatisch über die Geschwindigkeit und den Duplex-Modus entsprechend der Möglichkeiten im Netzwerk. • **100 Mbps Full Duplex** – Geschwindigkeit 100 Mbps Duplex-Modus: voll • **100 Mbps Half Duplex** – Geschwindigkeit 100 Mbps Duplex-Modus: halb • **10 Mbps Full Duplex** – Geschwindigkeit 10 Mbps Duplex-Modus: voll • **10 Mbps Half Duplex** – Geschwindigkeit 10 Mbps Duplex-Modus: halb

Fortsetzung auf der nächsten Seite

16-01-17

Fortsetzung von der vorherigen Seite

Element	Beschreibung
Default Gateway	IP-Adresse des Standard-Gateways. Wenn angegeben, werden alle Pakete, deren Ziel nicht im Routing Table gefunden werden, an diese Adresse geleitet.
DNS server	IP-Adresse des DNS-Servers. Wird eine IP-Adresse nicht im Routing Table gefunden, sendet das Gerät eine Anfrage an den angegebenen DNS-Server.

Tabelle 14: Konfiguration der Netzwerk-Schnittstelle

Der Menüpunkt *Primary LAN* öffnet die Konfigurationsseite für die Hauptschnittstelle *eth0*.

Ist das Gerät mit einer zusätzlichen Ethernet-Schnittstelle (*PORT1* oder *PORT2*) ausgestattet, wird diese über den Menüpunkt *Secondary LAN* konfiguriert. Verfügt der Router über zwei zusätzliche Ethernet-Schnittstellen (*PORT1* und *PORT2*), werden diese automatisch im Bridge-Modus verbunden.

Der Router nimmt an, dass die letzte IP-Adresse im Adressbereich die Broadcast-Adresse ist, unabhängig davon, ob diese Adresse als Broadcast-Adresse gesetzt ist oder nicht. Daher funktioniert die Kommunikation (Ping) mit dieser Adresse nicht.

Default Gateway und *DNS Server* werden nur verwendet, wenn der *DHCP Client* auf *disabled* (ausgeschaltet) gesetzt ist und wenn das Primäre oder Sekundäre LAN vom Backup-Routen-System als Standardroute ausgewählt wurde. Der entsprechende Algorithmus wird in Kapitel 3.7 beschrieben. Seit Firmware-Version 5.3.0 werden *Default Gateway* und *DNS Server* auch auf Schnittstellen, die als Bridge konfiguriert sind (z. g. eth0 + eth1), unterstützt.

Auf dem Gerät kann immer nur eine Bridge aktiv sein. Die Parameter *DHCP Client*, *IP Address* und *Subnet Mask* der ersten Schnittstelle werden für die Bridge verwendet. Weitere Schnittstellen (wlan0, wifi) können jederzeit zu einer Bridge hinzugefügt oder von ihr entfernt werden. Eine Bridge kann bei Bedarf für diese Schnittstellen erstellt werden, aber nicht, wenn ihre Parameter entsprechend konfiguriert sind.

Der DHCP-Server teilt einem anfragenden DHCP-Client eine IP-Adresse und die Subnetzmaske zu und sendet die IP-Adressen des Gateways und des DNS-Servers. Hat der Benutzer Werte vorgegeben, werden diese Werte bevorzugt.

Der DHCP-Server unterstützt die Vergabe von statischen und dynamischen IP-Adressen. *Dynamic DHCP* weist IP-Adressen entsprechend den vorgegebenem Adressbereich (IP Pool) zu. *Static DHCP* weist zuvor eingetragene, feste IP-Adresse entsprechend der MAC-Adresse des anfragenden Clients zu.

Element	Beschreibung
Enable dynamic DHCP leases	Schaltet den dynamischen DHCP-Server ein oder aus.
IP Pool Start	Erste IP-Adresse des Adressbereichs aus dem Adressen an anfragende Clients vergeben werden.
IP Pool End	Letzte IP-Adresse des Adressbereichs aus dem Adressen an anfragende Clients vergeben werden.
Lease time	„Leihzeit“: Zeit in Sekunden, die die IP-Adresse vor der Wiederverwertung nicht vergeben wird.

Tabelle 15: Konfiguration – Dynamischer DHCP-Server

Achten Sie darauf, dass sich statischen IP-Adressen (Adressbereich) nicht mit den dynamischen IP-Adressen (Adressbereich) überschneiden. IP-Adress-Konflikte und fehlerhafte Netzwerkfunktionen können die Folge sein.

Element	Beschreibung
Enable static DHCP leases	Schaltet den statischen DHCP-Server ein oder aus.
MAC Address	MAC-Adresse des DHCP-Clients
IPv4 Address	Zuzuweisende IPv4-Adresse / IPv4-Format

Tabelle 16: Konfiguration – Statischer DHCP-Server

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

- Adressbereich für dynamische IPv4-Adressen: zwischen 192.168.1.2 und 192.168.1.4
- Die Adresse wird für 600 Sekunden (10 Minuten) zugewiesen.

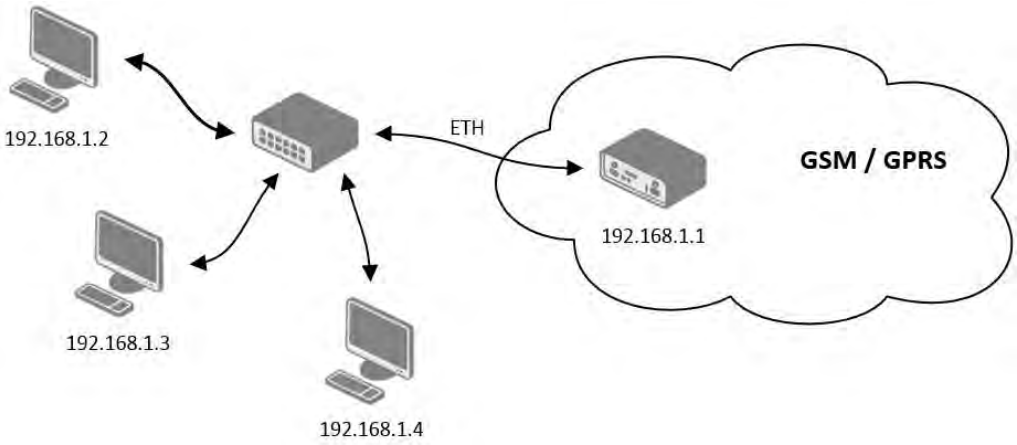


Abbildung 11: Beispiel 1: LAN-Konfiguration

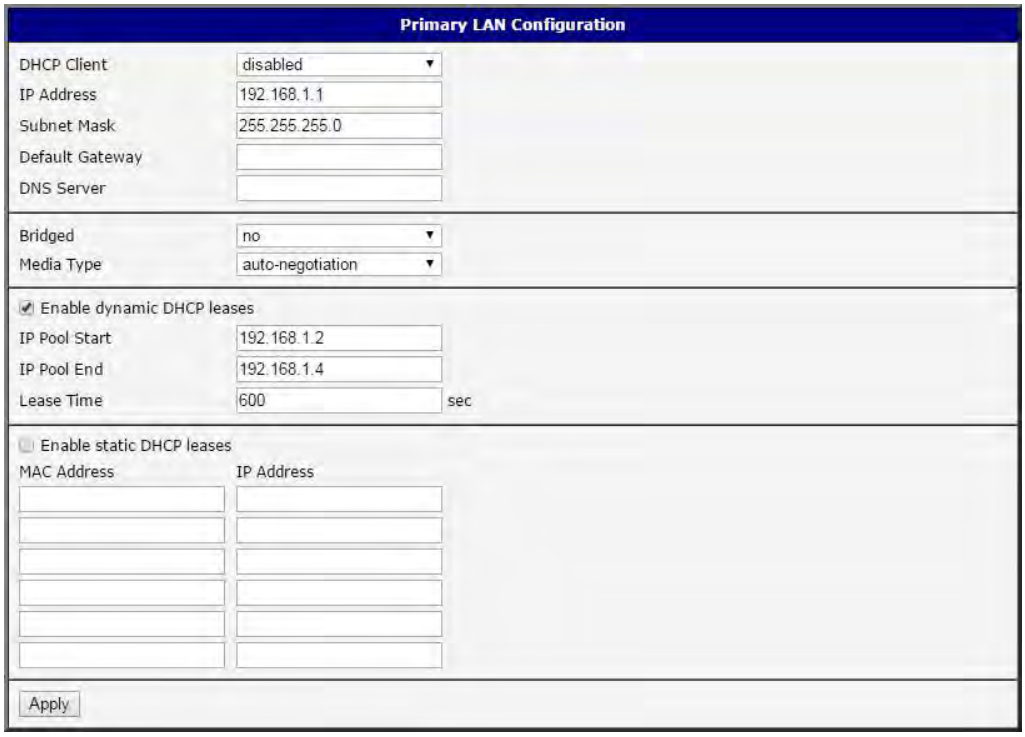


Abbildung 12: Example 1 – LAN Configuration Page

Beispiel 2: Dynamische IPv4-Adressen und statischer DHCP-Server

- Adressbereich für dynamische IPv4-Adressen: zwischen 192.168.1.2 und 192.168.1.4
- Die Adresse wird für 600 Sekunden (10 Minuten) zugewiesen.
- Dem Client mit der MAC-Adresse 01:23:45:67:89:ab wird die IP-Adresse 192.168.1.10 zugewiesen.
- Dem Client mit der MAC-Adresse 01:54:68:18:ba:7e wird die IP-Adresse 192.168.1.11 zugewiesen.

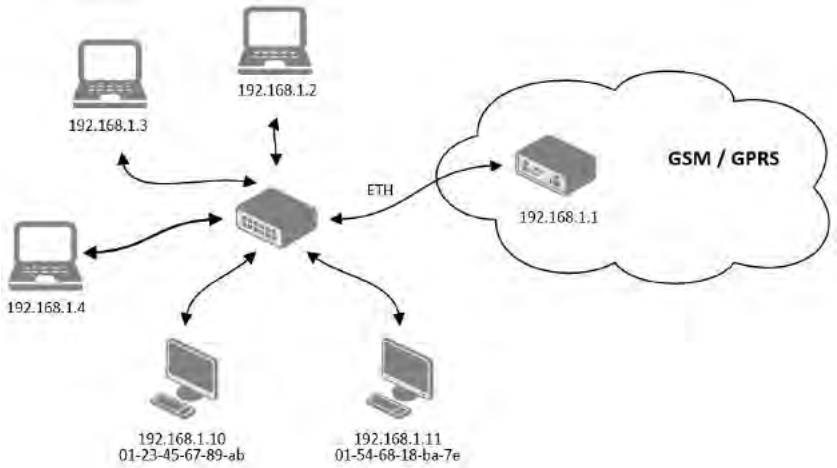


Abbildung 13: Beispiel 2: Netzwerk-Topologie

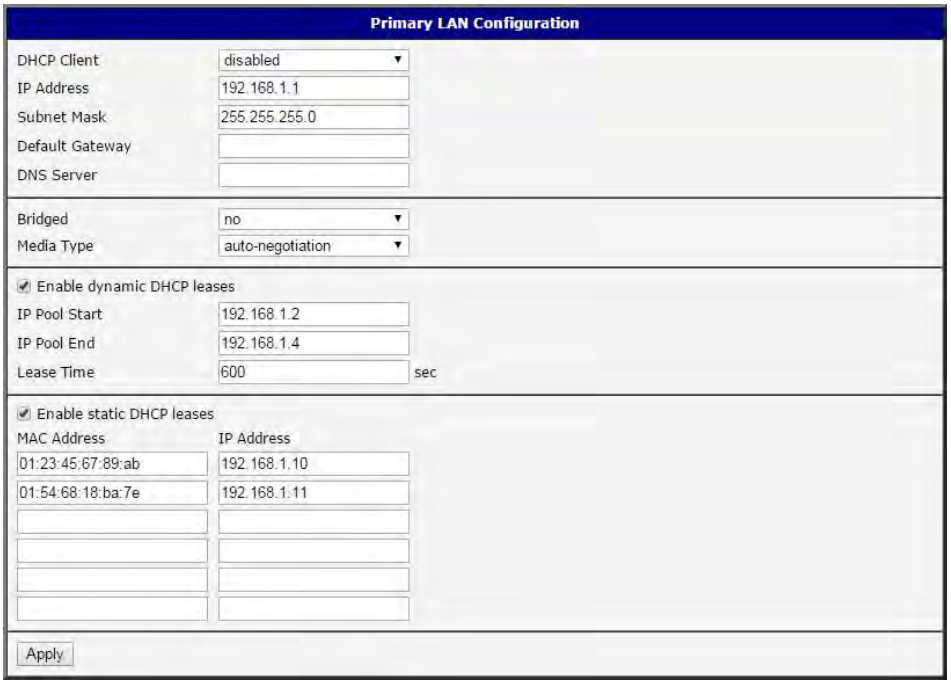


Abbildung 14: Beispiel 2: LAN-Konfiguration

Beispiel 3: Standard-Gateway und DNS-Server

- IP-Adresse des Standard-Gateways: 192.168.1.20
- IP-Adresse des DNS-Servers:192.168.1.20

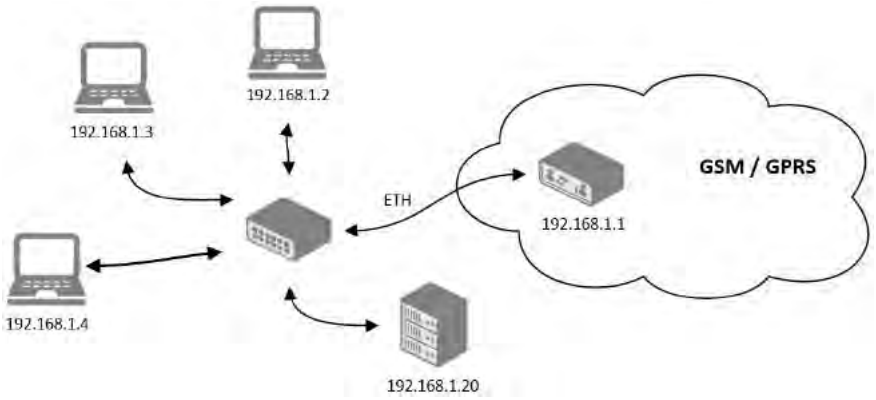


Abbildung 15: Beispiel 3: Netzwerk-Topologie

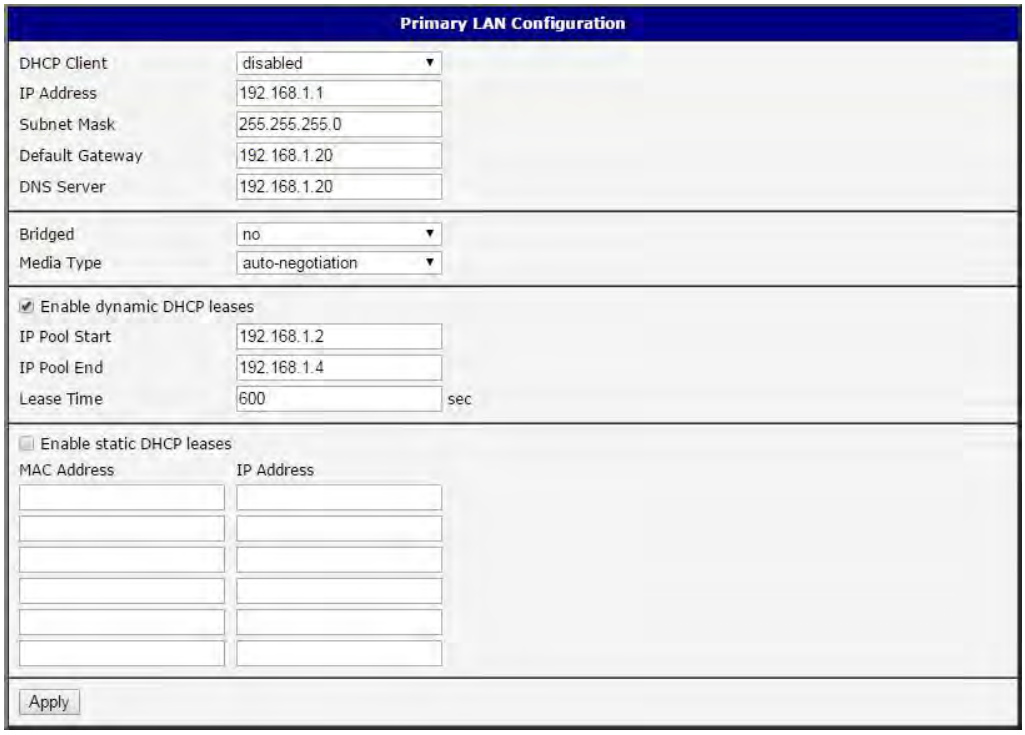


Abbildung 16: Beispiel 3: LAN-Konfiguration

3.2 VRRP Configuration

Das Protokoll VRRP (Virtual Router Redundancy Protocol) erlaubt den Wechsel der Routen vom Haupt-Router zu einem Backup-Router für den Fall, dass der Haupt-Router ausfällt. Für kritische Anwendungen kann so z. B. eine Ersatzverbindung über Mobilfunk eingerichtet werden.

Sie öffnen die Konfigurationsseiten für *VRRP*, indem Sie in der Navigationsspalte auf den Menüpunkt *VRRP* klicken.

Aktivieren Sie die Option *Enable VRRP*, um die weiteren Parameter einzurichten.

Element	Beschreibung
Virtual Server IP Address	IP-Adresse des virtuelle Servers. Diese Adresse muss für den primären und den Backup-Router übereinstimmen. Geräte im Netzwerk verwenden diese Adresse als Standard-Gateway.
Virtual Server ID	ID zur Unterscheidung der virtuellen Router. Beide müssen den gleichen Wert für diesen Parameter verwenden.
Host Priority	Der Router mit der höchsten Priorität ist der Haupt-Router. Entsprechend RFC 2338 sollte der Haupt-Router die Priorität 255 haben, der Backup-Router eine Priorität im Bereich zwischen 1 und 254 (Standardwert: 100). Der Wert 0 für die Priorität ist nicht erlaubt.

Tabelle 17: Konfiguration – VRRP

Sie können die Verbindung überprüfen. Dazu aktivieren Sie die Option *Check connection* im unteren Teil des Fensters. Jetzt werden automatische Testnachrichten in Funknetz gesendet. In einigen Fällen ist die mobile WAN-Verbindung noch aktiv, jedoch kann der Router darüber keine Daten mehr senden. Diese Option kann die Daten über eine PPP-Verbindung senden und ergänzt so die Behandlung der VRRP-Nachrichten.

Der aktive Router sendet in festgelegten Intervallen (*Ping Interval*) Testnachrichten an die angegebene Adresse (*Ping IP Address*) und wartet eine bestimmte Zeit (*Ping Timeout*) auf eine Antwort. Bleibt diese aus, wiederholt der Router es noch mehrfach (*Ping Probes*) und schaltet dann auf den Backup-Router um, solange bis die PPP-Verbindung wiederhergestellt ist.

Sie können den DNS-Server des Mobilfunkanbieters als Zieladresse für das Ping-Kommando verwenden.

Die Option *Enable traffic monitoring* kann zur Reduzierung der Anzahl der versendeten Testnachrichten für die PPP-Verbindung verwendet werden. Wenn die Option aktiviert ist, überwacht der Router die Schnittstelle auf Nicht-Ping-Pakete. Wird innerhalb der Wartezeit eine Antwort auf ein Paket empfangen, geht der Router davon aus, dass die Verbindung noch aktiv ist. Erfolgt keine Antwort innerhalb der Wartezeit, versucht der Router die mobile WAN-Verbindung über Ping-Kommando zu testen.

Element	Beschreibung
Ping IP Address	Zieladresse für das Ping-Kommando. Es muss eine IP-Adresse verwendet werden.
Ping Interval	Zeit in Sekunden zwischen Ping-Kommandos
Ping Timeout	Wartezeit in Sekunden
Ping Probes	Maximale Anzahl der unbeantwortete Ping-Anfragen

Tabelle 18: Überprüfung der Verbindung

Beispiel VRRP

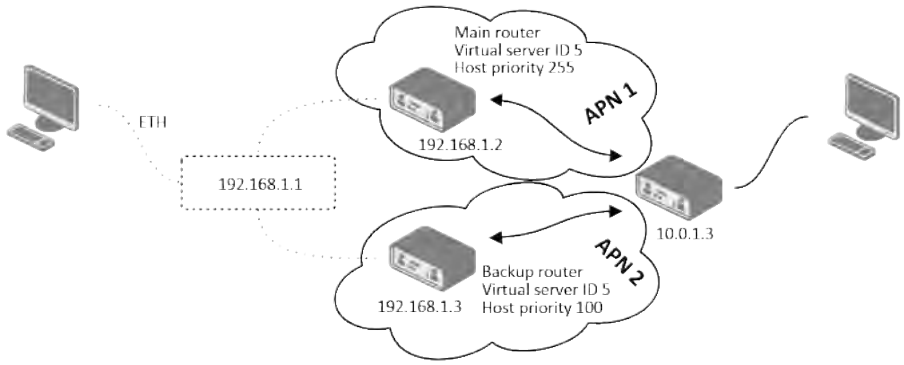


Abbildung 17: Beispieltopologie – VRRP

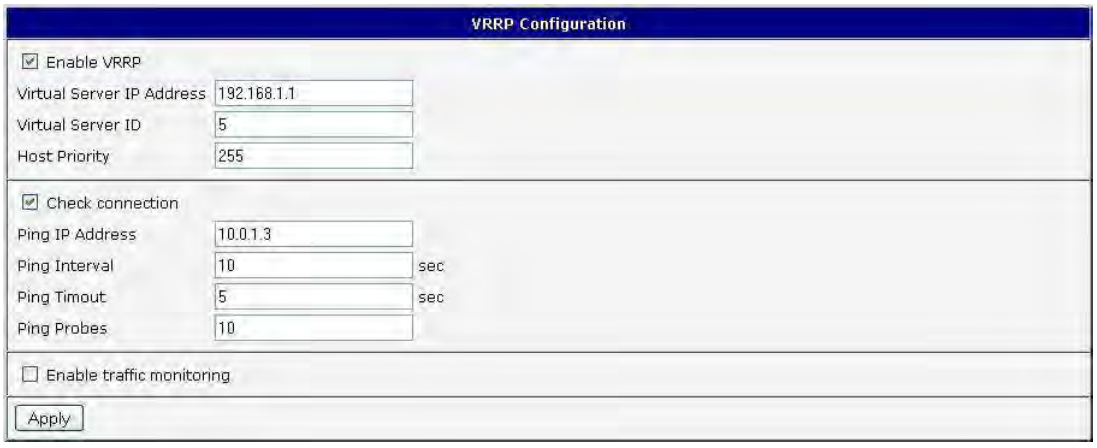


Abbildung 18: Beispielkonfiguration – VRRP – Haupt-Router

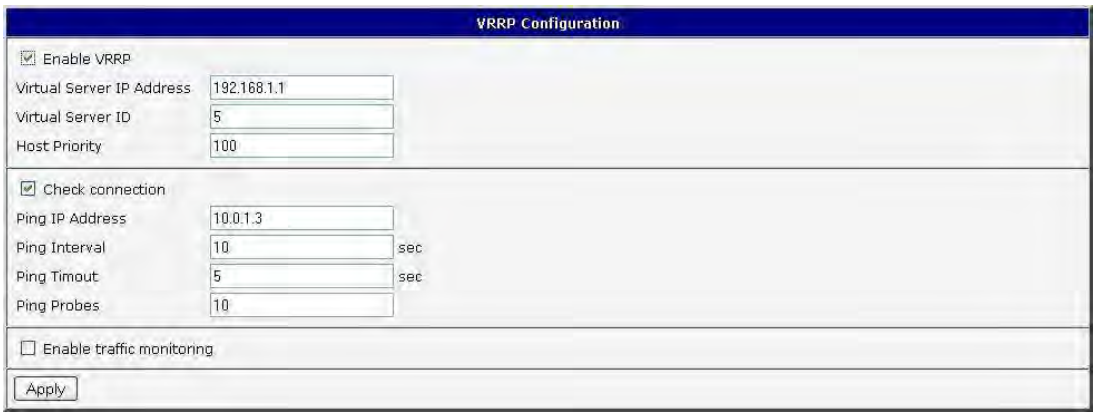


Abbildung 19: Beispielkonfiguration – VRRP – Backup-Router

3.3 Mobile WAN Configuration

Der Industrie-Router XR5i v2 hat keine Statusoption für mobiles WAN.

Sie öffnen die Konfigurationsseiten für *Mobile WAN*, indem Sie in der Navigationsspalte auf den Menüpunkt *Mobile WAN* klicken.

3.3.1 Verbindung zum Mobilfunknetz

Aktiveren Sie die Option *Create connection to mobile network*, damit das Gerät nach dem Booten automatisch eine Verbindung aufbaut. Sie können die folgenden Parameter für jede SIM-Karte separat konfigurieren, für Router in Vollausstattung mit zwei Steckplätzen für SIM-Karte. Für Router in der Basisausstattung können Sie hier zwei verschiedene APNs konfigurieren, zwischen denen gewechselt werden kann.

Element	Beschreibung
APN	Netzwerkkennung (Access Point Name).
Username	Benutzername für das Anmelden in GSM-Netzwerk.
Password	Passwort für die Anmeldung am GSM-Netzwerk.
Authentication	Authentifizierungmethode im GSM-Netzwerk: • **PAP or CHAP** – Das Gerät wählt die Methode. • **PAP** – Das Gerät verwendet die Methode PAP. • **CHAP** – Das Gerät verwendet die Methode CHAP.
IP Address	IP-Adresse der SIM-Karte. Manuelle Eingabe der IP-Adresse, wenn vom Netzwerkbetreiber zugewiesen.
Phone Number	Rufnummer mit der das Gerät über eine GPRS- oder CSD-Verbindung wählt. Das Gerät verwendet die Standardrufnummer *99***1 #.
Operator	Anbieterkennung (PLNM)
Network type	Protokoll im mobilen Netzwerk • **Automatic selection** – Das Gerät wählt eine geeignete und verfügbare Übertragungsmethode. • Manuelle Auswahl, entsprechend dem Router-Typ: GPRS, UMTS, . . .
PIN	Geheimnummer zum Entsperren der SIM-Karte. Nur verwenden, wenn erforderlich für die SIM-Karte. Die SIM-Karte wird nach einigen fehlerhaften Entsperrversuchen gesperrt.

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite

Element	Beschreibung
	Hinweis Abweichende Einstellungen bei MRU und MTU können zu fehlerhaften Datenübertragung führen.
MRU	Maximum Receive Unit – maximale Größe für das Empfangen von Datenpaketen. Standardwert: 1.500 B. Minimalwert: 128 B.
MTU	Maximum Transmission Unit – maximale Größe für das Senden von Datenpaketen. Standardwert: 1.500 B. Minimalwert: 128 B.

Tabelle 19: Konfiguration – Mobile WAN

Die nachfolgende Liste enthält einige Hinweise zur Konfiguration des mobilen Netzwerks:

- Ein falscher Wert für MTU führt zu Problemen bei der Datenübertragung. Ist der Wert zu niedrig, wird sich die Fragmentierung der Daten erhöhen. Höhere Fragmentierung bedeutet mehr Aufwand und die Möglichkeit von Beschädigungen an Paketen während der Defragmentierung. Dagegen kann ein zu höher Wert dazu führen, dass Pakete im Netzwerk verworfen werden.
- Bleibt das Feld *IP address* leer, weist der Dienstanbieter automatisch eine IP-Adresse zu. Weisen Sie selbst eine IP-Adresse zu, baut das Gerät die Verbindung schneller auf.
- Bleibt das Feld ***APN*** leer, wählt das Gerät automatisch den APN basierend auf dem IMSI-Code der SIM-Karte. Ist die Anbieterkennung (PLMN) nicht in der APN-Liste, verwendet das Gerät als Standard-APN **internet**. Wird ein AT&T-Netzwerk erkannt, wird als Standard-APN **phone** verwendet. Der Dienstanbieter definiert den APN.
- Tragen Sie im Feld *APN* das Wort `blank` ein, interpretiert das Gerät das als Leerzeichen.

- Für Router in Vollausstattung mit zwei Steckplätzen für SIM-Karten, ist ein Wechsel zwischen den Karten möglich.
- Für Router in der Basisausstattung können Sie zwei verschiedene APNs konfigurieren, zwischen denen gewechselt werden kann.
- Bei SIM-Karten mit zwei APNs wird die gleiche PIN für beide APNs verwendet.
- Geben Sie unbedingt die richtige PIN ein. Nach einigen Fehlversuchen wird die SIM-Karte gesperrt.

Mit einem Sternchen (*) markierte Parameter müssen nur bearbeitet werden, wenn der Dienstanbieter diese Informationen fordert.

Kann das Gerät keine Verbindung ins Mobilfunknetz herstellen, sollten Sie die eingegebenen Daten genau überprüfen. Oder Sie versuchen es mit eine anderen Authentifizierungsmethode bzw. Netzwerktyp.

3.3.2 DNS Address Configuration

Die Einstellungen der DNS-Parameter dienen der einfachen Konfiguration auf Seiten des Clients. Wählen Sie in der Auswahlliste den Eintrag *get from operator* ein, versucht das Gerät die IP-Adressen für den primäre und sekundären DNS-Server automatisch vom Netzbetreiber zu beziehen.

Sie können die IP-Adresse auf manuell eingeben. Dazu wählen Sie in der Auswahlliste den Eintrag *set manually* und tragen dann wenigstens eine IP-Adresse (IPv4, IPv6 oder beide) für einen DNS-Server ein, abhängig von den Einstellungen für *IP Mode*, siehe Abschnitt 3.3.1.

3.3.3 Check Connection to Mobile Network Configuration

In den Einstellungen *enabled* oder *enabled + bind* wird das Bestehen der Verbindung ins mobile Netzwerk regelmäßig überprüft. Das Gerät sendet in bestimmten Abständen (*Ping Interval*) Ping-Anfragen an eine voreingestellte Domain oder IP-Adresse (*Ping IP Address* oder *Ping IPv6 Address*). Wird die Anfrage nicht beantwortet, wird nach z. B. 10 Sekunden eine weitere Anfrage gesendet. Wird dreimal hintereinander die Anfrage an die angegebene IP-Adresse nicht beantwortet, beendet das Gerät die Verbindung und versucht eine neue aufzubauen. Diese Überprüfung kann für beide SIM-Karten getrennt eingestellt werden. Senden Sie ein ICMP-Ping an eine IP-Adresse, von der Sie wissen, dass sie noch funktioniert, z. B. den DNS-Server des Netzwerkbetreibers.

In der Option *enabled* werden die Ping-Anfragen auf Basis des Routing Tables gesendet, wobei jede der verfügbaren Schnittstellen verwendet werden kann. Sollen die Ping-Anfragen nur über die Schnittstellen mit Verbindung ins mobile Netzwerk gesendet werden, wählen Sie die Option *enabled + bind*. Die Option *disabled* unterbindet die Überprüfung ins mobile Netzwerk.

Element	Beschreibung
Ping IP Address	Zieladresse für das Ping-Kommando
Ping Interval	Zeit in Sekunden zwischen den Ping-Kommandos

Tabelle 20: Überprüfung der Verbindung ins mobile Netzwerk

Aktivieren Sie die Option *Enable Traffic Monitoring*, senden der Router keine Ping-Anfragen, sondern überwacht den Datenstrom ins mobile Netzwerk. Ist die Verbindung länger als der Wert *Ping Interval* ohne Datenfluss, sendet das Gerät wieder eine Ping-Anfrage an die Zieladresse.

Für den ununterbrochenen und kontinuierlichen Betrieb des Geräts sollte die Funktion *Check Connection* unbedingt eingeschaltet sein.

LUCOM GmbH — Flößaustr. 22a — 90763 Fürth — Tel.: +49 911/ 957 606 00 — E-Mail: info@lucom.de — www.lucom.de

3.3.4 Data Limit Configuration

Element	Beschreibung
Data Limit	Maximale erwartete Menge der übertragenen (empfangen und gesendet) Daten in einer Abrechnungsperiode (1 Monat). Maximalwert: 2 TB (2.097.152 MB)
Warning Threshold	Schwellwert als Prozentsatz im Bereich zwischen 50 % to 99 %. Wird der eingestellte Schwellwert überschritten, sendet das Gerät eine SMS mit folgendem Inhalt „Router has exceeded (value of Warning Threshold) of data limit.“ (Der Router hat den eingestellten Schwellwert (eingestellter Wert) überschritten.)
Accounting Start	Erster Tag der Abrechnungsperiode für die jeweilige SIM-Karte, falls die Abrechnungsperiode nicht am Monatsersten beginnt.

Tabelle 21: Konfiguration Datenlimit

Hat der Parameter *Data Limit State* (siehe unten) den Wert *not applicable* oder wenn *Send SMS when data limit is exceeded* (siehe Abschnitt *SMS Configuration* nicht ausgewählt ist, wird das hier eingestellt *Datenlimit* ignoriert.

3.3.5 SIM-Karten-Konfigurationen wechseln

Im unteren Bereich der Konfigurationsseite können Sie die Hauptkarte festlegen bzw. zwischen den SIM-Karten wechseln.

Der Router schaltet automatisch zwischen den SIM-Karten und ihrer Konfiguration um, abhängig von den hier gemachten Einstellungen (manual permission, roaming, data limit, binary inputs state). Beachten Sie, dass die Karte über welche die Verbindung hergestellt wird das Resultat aus der AND-Verknüpfung der hier konfigurierten Parameter ist, siehe nachstehende Tabelle.

Element	Beschreibung
SIM Card	Schaltet die SIM-Karte ein oder aus. Sind alle SIM-Karten auf *disabled* gesetzt, wird das gesamte Mobilfunkmodul abgeschaltet. • **enabled** – SIM-Karte kann verwendet werden. • **disabled** – SIM-Karte kann nicht verwendet werden.

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite

Element	Beschreibung
Roaming State	Schaltet die Verwendung der SIM-Karte über Roaming-Erkennung. Funktioniert nur bei aktiviertem Roaming für die SIM-Karte! • **not applicable** – Die SIM-Karte kann überall eingesetzt werden. • **home network only** – Die SIM-Karte wird nur benutzt, wenn kein Roaming erkannt wird.
Data Limit State	Schaltet die Verwendung der SIM-Karte über das Datenlimit, siehe oben: • **not applicable** – Die SIM-Karte wird ohne Rücksicht auf ein Datenlimit verwendet. • **not exceeded** – Die SIM-Karte wird nur solange eingesetzt ist, wie das Datenlimit noch nicht überschritten ist.
BIN0 State	Schaltet die Verwendung der SIM-Karte basierend auf dem Zustand *binary input 0 state*. • **not applicable** – Die SIM-Karte wird ohne Rücksicht auf den Status BIN0 verwendet. • **on** – Die SIM-Karte wird nur verwendet, wenn der Status BIN0 logisch 0 (Spannung vorhanden) ist. • **off** – Die SIM-Karte wird nur verwendet, wenn der Status BIN0 logisch 1 (kein Spannung vorhanden) ist.

Tabelle 22: Konfiguration des Wechsels zwischen den SIM-Karten

Legen Sie mit den folgenden Parameter die Entscheidungsfindung über den Wechsel der SIM-Karte fest.

Element	Beschreibung
Default SIM Card	egt die Standardkarte fest. Das Gerät stellt die Verbindung ins mobile Netzwerk über die Standardkarte her. • **1st** – Die erste SIM-Karte ist Standardkarte. • **2nd** – Die zweite SIM-Karte ist die Standardkarte.

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite

Element	Beschreibung
Initial State	Legt Aktion fest, die das Mobilfunkmodul nach der Auswahl der SIM-Karte ausführt. • **online** – stellt Verbindung ins mobile Netzwerk her. (Standard) • **offline** – schaltet in den Off-line-Modus. Hinweis: Sie können den Zustand von *Initial State* nur per SMS ändern – siehe Abschnitt 3.19 *SMS Configuration*. Das Mobilfunkmodul geht in den Off-line-Modus, wenn keine SIM-Karte ausgewählt wurde.
Switch to other SIM card when connection fails	Nur anwendbar, wenn eine Verbindung über die Standardkarte herstellt wurde und diese Verbindung dann ausfällt. Wird der Ausfall der Verbindung über die Funktion *Check Connection* festgestellt, wechselt das Gerät auf die andere SIM-Karte (Backup).
Switch to default SIM card after timeout	Wenn diese Option aktiviert ist, versucht das Gerät nach Ablauf der Wartezeit (*Initial Timeout*) wieder zur Standardkarte zu wechseln. Dies funktioniert nur, wenn eine Standardkarte festgelegt wurde und die andere SIM-Karte (Backup) wegen Ausfall der Standardkarte gewählt wurde oder wenn einer der obigen Parameter (*Roaming*) der Wechselgrund war. Diese Funktion ist nur verfügbar, wenn die Funktion *Switch to other SIM card when connection fails* eingeschaltet ist.
Initial Timeout	Zeitspanne, die das Gerät wartet, bevor es versucht wieder zur Standardkarte zu wechseln. Bereich: 1 bis 10.000 Minuten.
Subsequent Timeout	Zeitspanne, die das Gerät wartet, wenn der Versuch zur Standardkarte zu wechseln nicht erfolgreich war. Bereich: 1 bis 10.000 Minuten.
Additive Constant	Zeitspanne, die das Gerät wartet, bevor weitere Versuche unternommen werden zur Standardkarte zu wechseln. Die Zeitspanne setzt zusammen aus der Zeitspanne *Subsequent Timeout* und der hier angegebenen Zeitspanne. Bereich: 1 bis 10.000 Minuten.

Tabelle 23: Parameter für den Wechsel der SIM-Karte

Beispiel: Wechsel nach Zeitüberschreitung (Timeout)

Aktivieren Sie die Option *Switch to default SIM card after timeout* und ergänzen Sie die folgenden Werte:

- *Initial Timeout* – 60 Minuten
- *Subsequent Timeout* – 30 Minuten
- *Additional Timeout* – 20 Minuten

Der erste Versuch zur Standardkarte bzw. APN zu wechseln wird nach 60 Minuten unternommen. Schlägt dieser Versuch fehl, wird der nächste Versuch nach weiteren 30 Minuten unternommen; der dritte Versuch wird dann nach 50 Minuten (30 + 20), der vierte nach 70 Minuten (30 + 20 + 20).

3.3.6 Konfiguration einer Einwahlverbindung

Die Konfiguration einer Einwahlverbindung (Dial-In) wird nur von folgenden Routern unterstützt: ER75i, UR5, ER75i v2 and UR5 v2.

Aktivieren Sie die Option *Enable Dial-In Access* für den Zugang über eine CSD-Verbindung.
Der Zugang kann über die Verwendung von *Username* und *Password* abgesichert werden,
Hat der Router keine Verbindung in ein mobiles Netzwerk, können Sie über diese Funktion für einen Zugang zum Router über eine Einwahlverbindung (Modem). Der Router wartet zwei Minuten, um die Verbindung zu bestätigen. Erfolgt in dieser Zeit kein Anmeldeversuch, unternimmt der Router einen weiteren Versuch eine GPRS-Verbindung herzustellen.

Element	Beschreibung
Username	Benutzername für einen gesicherten Zugang.
Password	Passwort für einen gesicherten Zugang.

Tabelle 24: Konfiguration – Einwahlverbindung

3.3.7 PPPoE Bridge Mode Configuration

Wenn Sie die Option *Enable PPPoE bridge mode* aktivieren, verwendete der Router das Bridge-Protokoll PPPoE (Point-to-Point over Ethernet). Dieses Protokoll verkapselt PPP-Frames innerhalb von Ethernet-Frames. Der Bridge-Modus erlaubt das Herstellen einer PPPoE-Verbindung von einem Gerät hinter dem Router, z. B. ein Computer verbindet sich mit dem *eth*-Port des Routers. Sie können dem Computer die IP-Adresse der SIM-Karte zuweisen.

Die Änderungen gelten erst nach einem Klick auf die Schaltfläche *Apply*.

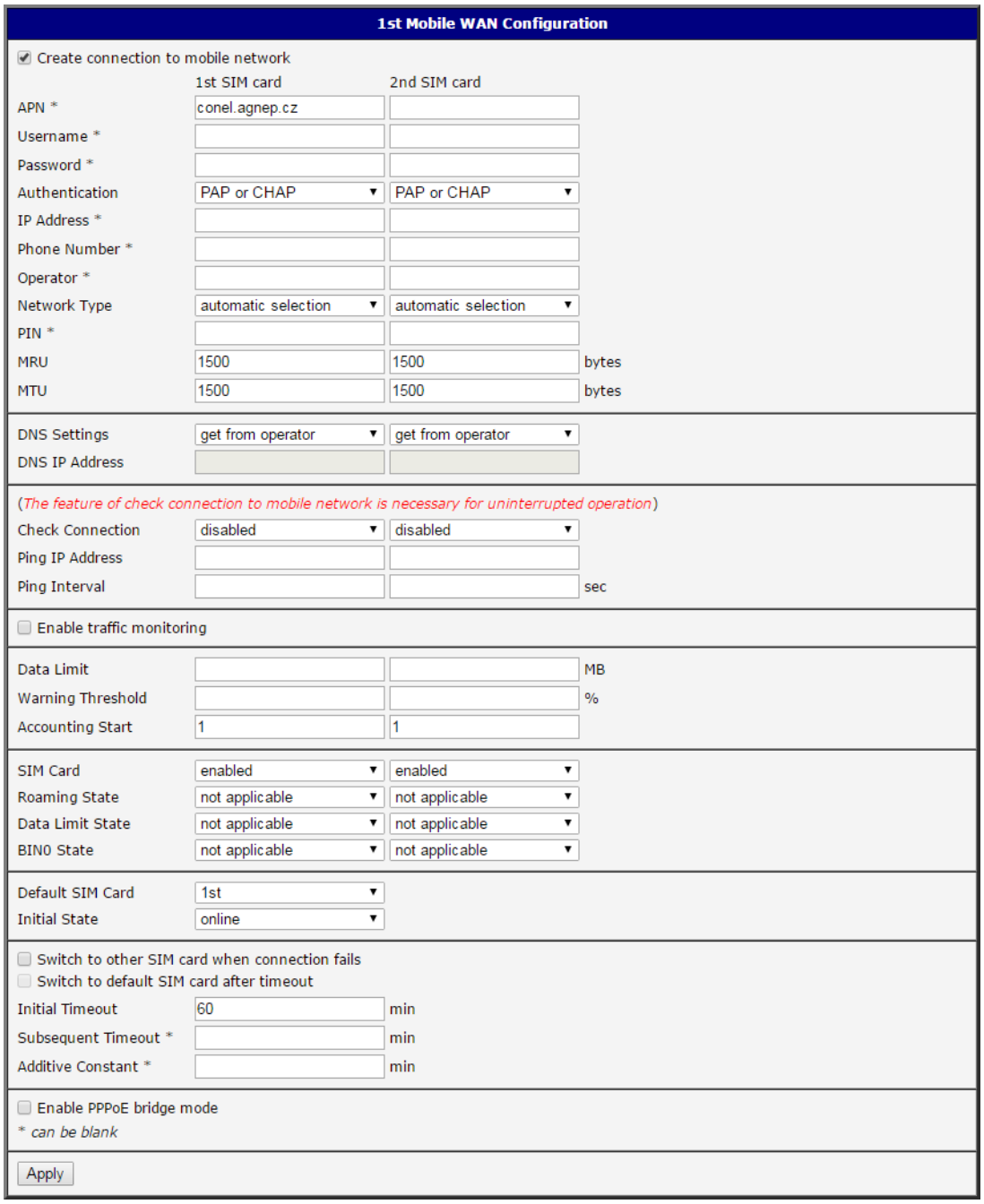


Abbildung 20: Konfiguration – Mobile WAN

Beispiel 1: Verbindung überprüfen

Die folgende Abbildung zeigt folgendes Szenario: Die Verbindung ins mobile Netzwerk wird über die IP-Adresse 8.8.8.8 bzw. den Domain Namen www.google.com überprüft.

Stellen Sie die Option *Check Connection* beide Male auf enabled. Tragen Sie im ersten Feld Ping IP Address 8.8.8.8 als IP-Adresse ein und im zweiten Feld den Domain-Namen www.google.com. Als Zeitintervall tragen Sie im ersten Feld 60 und im zweite Feld 80 Sekunden ein. Aktivieren Sie die Option *Enable traffic monitoring*.

Im Falle des Betriebs über einen Router werden keine Kontroll-Pings gesandt, sondern es wird der Betrieb überwacht.

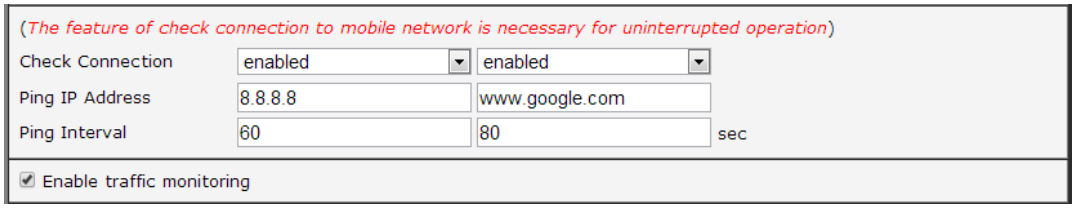


Abbildung 21: Beispiel 1: Verbindung überprüfen

Beispiel 2: Wechsel bei Datenlimit

Die folgende Abbildung zeigt ein Szenario, in dem der Router zur zweiten SIM-Karte wechselt, nachdem das Datenlimit (800 MB) der ersten SIM-Karte erreicht wurde. Wird der Schwellwert von 400 MB überschritten, sendet das Gerät eine SMS als Warnung. Dieses Verhalten stellen Sie auf der Seite *SMS Configuration* ein, siehe Abschnitt 3.19. Die Abrechnungsperiode beginnt am 18ten Tag des Monats.

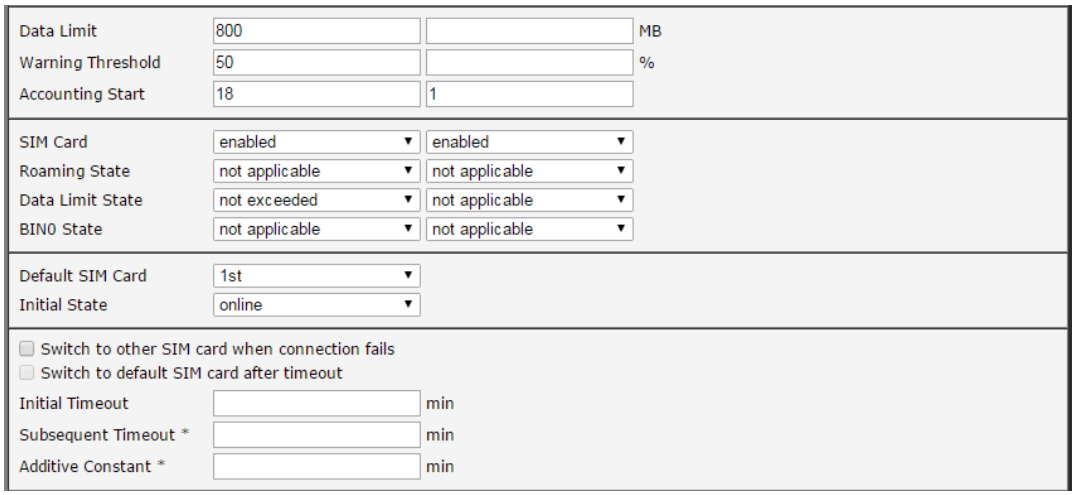


Abbildung 22: Beispiel 2: Wechsel bei Datenlimit

3.4 PPPoE Configuration

Das Netzwerkprotokoll PPPoE (Point-to-Point over Ethernet) verkapselt PPP-Frames innerhalb von Ethernet-Frames. Der Router verwendet einen PPPoE-Client zur Verbindung mit Geräten, die PPPoE-Bridge oder -Server unterstützen. Als Bridge oder Server dient typischerweise ein ADSL-Router.

Sie öffnen die Konfigurationsseiten für *PPPoE*, indem Sie in der Navigationsspalte auf den Menüpunkt *PPPoE* klicken. Aktivieren Sie die Option *Create PPPoE connection*, damit der Router nach dem Boot-Vorgang eine PPPoE-Verbindung aufbaut. Ist die Verbindung hergestellt, bezieht der Router seine IP-Adresse von dem verbundenen Gerät. Die Kommunikation von einem Gerät hinter dem PPPoE-Server wird zum Router weitergeleitet.

Element	Beschreibung
Username	Benutzername für den sicheren Zugang über PPPoE
Password	für den sicheren Zugang über PPPoE
Authentication	Authentifizierungsmethode • **PAP oder CHAP** – Das Gerät wählt die Methode. • **PAP** – Das Gerät verwendet die Methode PAP. • **CHAP** – Das Gerät verwendet die Methode CHAP.
MRU	Abweichende Werte können zu fehlerhafter Datenübertragung führen. Größe der Maximum Receiving Unit. MRU gibt die maximale Paketgröße an, die der Router über PPPoE empfangen kann. Standard: 1492 B Minimalwert: 128 B
MTU	Größe der Transmission Unit . MTU gibt die maximale Paketgröße an, die der Router in der vorhandenen Netzwerkumgebung übertragen kann. Standard: 1492 B Minimalwert: 128 B

Tabelle 25: PPPoE-Konfiguration

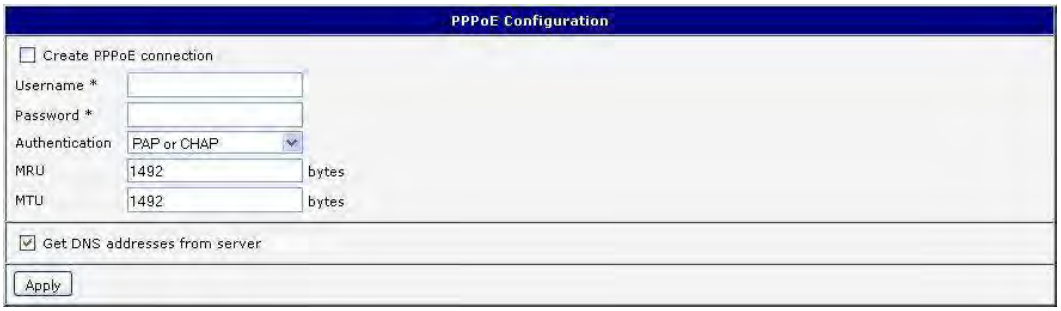


Abbildung 23: PPPoE-Konfiguration

Vom Standard abweichende Werte für MRU und MTU können zu fehlerhafter Datenübertragung führen.

3.5 WiFi Configuration

Diese Seite ist nur verfügbar, wenn der Router mit einem WLAN-Modul ausgestattet ist.

Sie öffnen die Konfigurationsseiten für *WLAN*, indem Sie in der Navigationsspalte auf den Menüpunkt *WiFI* klicken. Aktiveren Sie die Option *Enable WiFi*, um das WLAN einzuschalten. Nehmen Sie die folgenden Einstellungen vor.

Das Netzwerkprotokoll RADIUS (Remote Authentication Dial-In User Service) bietet zentrale Authentifizierung und Autorisierung sowie eine Kontoverwaltung. Der Router arbeitet nur als RADIUS-Client – typischerweise als WLAN Access Point (AP), der mit dem RADIUS-Server verhandelt. Wird der Router als Client (WiFi STA (Station)) betrieben, wird nur die Authentifizierungsmethode EAP-PEAP/MSCHAPv2 (sowohl PEAPv0 als auch PEAPv1) unterstützt.

Element	Beschreibung
Operating mode	WiFi operating mode: • **Access Point (AP)** – Der Router arbeitet als Zugangspunkt für Geräte im Client Mode. • **Station (STA)** – Der Router arbeitet als Client an verfügbaren Access Points. Empfangene Daten über die Kabelverbindung werden über das WLAN weitergeleitet.
SSID	Netzwerkkennung
Broadcast SSID	Sendemethode für das Senden der Netzwerkkennung. Diese wird periodisch ausgestrahlt. • **Enabled** – Die SSID wird als Beacon frame ausgestrahlt. • **Zero length** – Die SSID ist nicht im Beacon frame enthalten. Anforderungen, die SSID zu senden, werden ignoriert. • **Clear** – Alle Zeichen der SSID im Beacon frame werden durch 0 ersetzt. Die Originallänge der SSID bleibt erhalten. Anforderungen, die SSID zu senden, werden ignoriert.
Probe Hidden SSID	nach verborgenen SSID suchen (nur im Client Modus)
Client Isolation	nur im Access Point-Modus. ist diese Option aktiviert, werden verbundene Clients gegeneinander abgeschirmt, so dass sie sich nicht sehen können (unterschiedliche Netzwerke). Ist die Option nicht aktiviert, arbeitet der Router wie ein Switch – Die über WLAN verbundenen Clients sind im gleichen LAN und können einander sehen.

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite

Element	Beschreibung
Country Code	Landeskennung. Die Kennung muss im Format ISO 3166-1 alpha-2 eingegeben werden. Wird eine Länderkennung eingegeben, die der Router nicht erkennt, wird die Länderkennung „US“ als Standard verwendet. Wird keine Länderkennung angegeben oder eine falsche Kennung, verstößt der Router beim Betrieb des WLANs möglicherweise gegen landesspezifische Vorschriften für den Betrieb eines WLANs.
HW Mode	unterstützte WLAN-Standards • IEE 802.11b (2.4 GHz) • IEE 802.11b+g (2.4 GHz) • IEE 802.11b+g+n (2.4 GHz)
Channel	verwendeter Kanal Unterstützte Kanäle für 2,4 GHz: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13.
BW 40 MHz	Option für den Standard 802.11n: gleichzeitige Übertragung über 2 20 MHz-Kanäle. Diese Option ist nur im Client Modus verfügbar und sowohl für den Client als auch für den Server eingeschaltet sein.
WMM	(Basis)-Quality of Service. Ein bestimmter Datendurchsatz wird von dieser Version nicht garantiert. WMM eignet sich daher für einfache Anwendungen, die QoS erfordern.

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite

Element	Beschreibung
Authentication	Zugangskontrolle und Autorisierung der Benutzer des WLANs • **Open** – keine Zugangskontrolle (freier Access Point) • **Shared** – Basis-Authentifizierung über WEP-Schlüssel • **WPA-PSK** – Authentifizierung über PSK-PSK (verbesserte Verschlüsselung) • **WPA2-PSK** – Authentifizierung über WPA-PSK (verwendet die neuere AES-Verschlüsselung) • **WPA-Enterprise** – RADIUS-Authentifizierung über einen externen Server mit Benutzernamen und Passwort • **WPA2-Enterprise** – RADIUS-Authentifizierung mit besserer Verschlüsselung • **802.1X** – RADIUS-Authentifizierung mit port-basierte Netzwerkszugangskontrolle (port-based Network Access Control (PNAC)) über das Protokoll Extensible Authentication Protocol (EAP) over LAN – EAPOL.
Encryption	Art der Datenverschlüsselung im WLAN: • **None** – keine Verschlüsselung • **WEP** – Verschlüsselung mit statischem WEP-Schlüssel. Diese Verschlüsselung kann bei der Authentifizierungsmethode *Shared* verwendet werden. • **TKIP** – Das Sicherheitsprotokoll Temporal Key Integrity Protocol kann für die Authentifizierungsmethoden *WPA-PSK* und *WPA2-PSK* verwendet werden. • **AES** – Verbesserte Verschlüsselung für die Authentifizierungsmethode *WPA2-PSK*
WEP Key Type	Art des WEP-Schlüssels: • **ASCII** – ASCII-Format • **HEX** – Hexadezimalformat
WEP Default Key	Standard-WEP-Schlüssel

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite

Element	Beschreibung
WEP Key 1–4	Es können bis zu vier WEP-Schlüssel eingetragen werden. • WEP-Schlüssel im ASCII-Format müssen in Hochkommata eingegeben werden. Mögliche Schlüssellängen: – 5 ASCII-Zeischen (40b WEP-Schlüssel) – 13 ASCII-Zeichen (104b WEP-Schlüssel) – 16 ASCII-Zeichen (128b WEP-Schlüssel) • WEP-Schlüssel im Hexadezimalformat müssen als Hexadezimalzeichen eingegeben werden. Mögliche Schlüssellängen: – 10 Hexadezimalziffern (40b WEP-Schlüssel) – 26 Hexadezimalziffern (104b WEP-Schlüssel) – 32 Hexadezimalziffern (128b WEP-Schlüssel)
WPA PSK Type	Optionen für die Authentifizierungsmethode WPA-PSK • 256-Bit Geheimnis (secret) • ASCII-Passphrase • PSK-Datei
WPA PSK	Schlüssel für die Methode WPA-PSK. Der Schlüssel muss entsprechend der Auswahl des WPA PSK Types erfolgen: • **256-bit secret** – 64 Hexadezimalziffern • **ASCII passphrase** – 8 bis 63 Zeichen • **PSK File** – Absoluter Pfad zur Datei, welche die Schlüsselpaare PSK-Schlüssel und MAC-Adresse enthält
Hinweis RADIUS Auth Server IP	Die folgenden Optionen gelten nur im Access Point-Modus und wenn eine der RADIUS Authentifizierungsmethoden ausgewählt wurde. IPv4- oder IPv6-Addresse des RADIUS-Servers.
RADIUS Auth Password	Authentifizierungspasswort für den Zugang auf den RADIUS-Server.
RADIUS Auth Port	Port des RADIUS-Servers. Standard: 1812.

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite

Element	Beschreibung
RADIUS Acct Server IP	IPv4- oder IPv6-Adresse des RADIUS Accounting-Server. Adresse nur eintragen, wenn es verschiedene Server für Authentifizierung und Autorisierung gibt.
RADIUS Acct Password	Autorisierungspasswort für den Zugang auf den RADIUS Accounting-Server. Passwort nur eintragen, wenn es verschiedene Server für Authentifizierung und Autorisierung gibt.
RADIUS Acct Port	Port des RADIUS Accounting-Servers. Standard: 1813. Port nur eintragen, wenn Authentifizierungs- und Autorisierungs-Server unterschiedliche Ports verwenden.
Hinweis RADIUS Identity	Die folgenden Optionen gelten nur im Client-Modus und wenn eine der RADIUS Authentifizierungsmethoden ausgewählt wurde. RADIUS-Benutzername – Identität
RADIUS Password	RADIUS-Zugangspasswort
Access List	Zugangsliste (Zugang erlaubt/verboten) • **Disabled** – Die Zugangsliste wird nicht verwendet. • **Accept** – Client auf der Zugangsliste haben Zugriff auf das Netzwerk. • **Deny** – Client auf der Zugangsliste haben keinen Zugriff auf das Netzwerk.
Accept/Deny List	Liste der MAC-Adressen der Clients, die (keinen) Zugriff auf das Netzwerk haben. Eine MAC-Adresse pro Zeile.
Syslog Level	Stufe der Erfassung, falls das System eine Log-Datei schreibt • **Verbose debugging** – höchste Stufe • **Debugging** • **Informational** – Standard • **Notification** • **Warning** – niedrigste Stufe
Extra options	Der Benutzer kann zusätzliche Parameter definieren und einfügen.

Tabelle 26: WLAN-Konfiguration

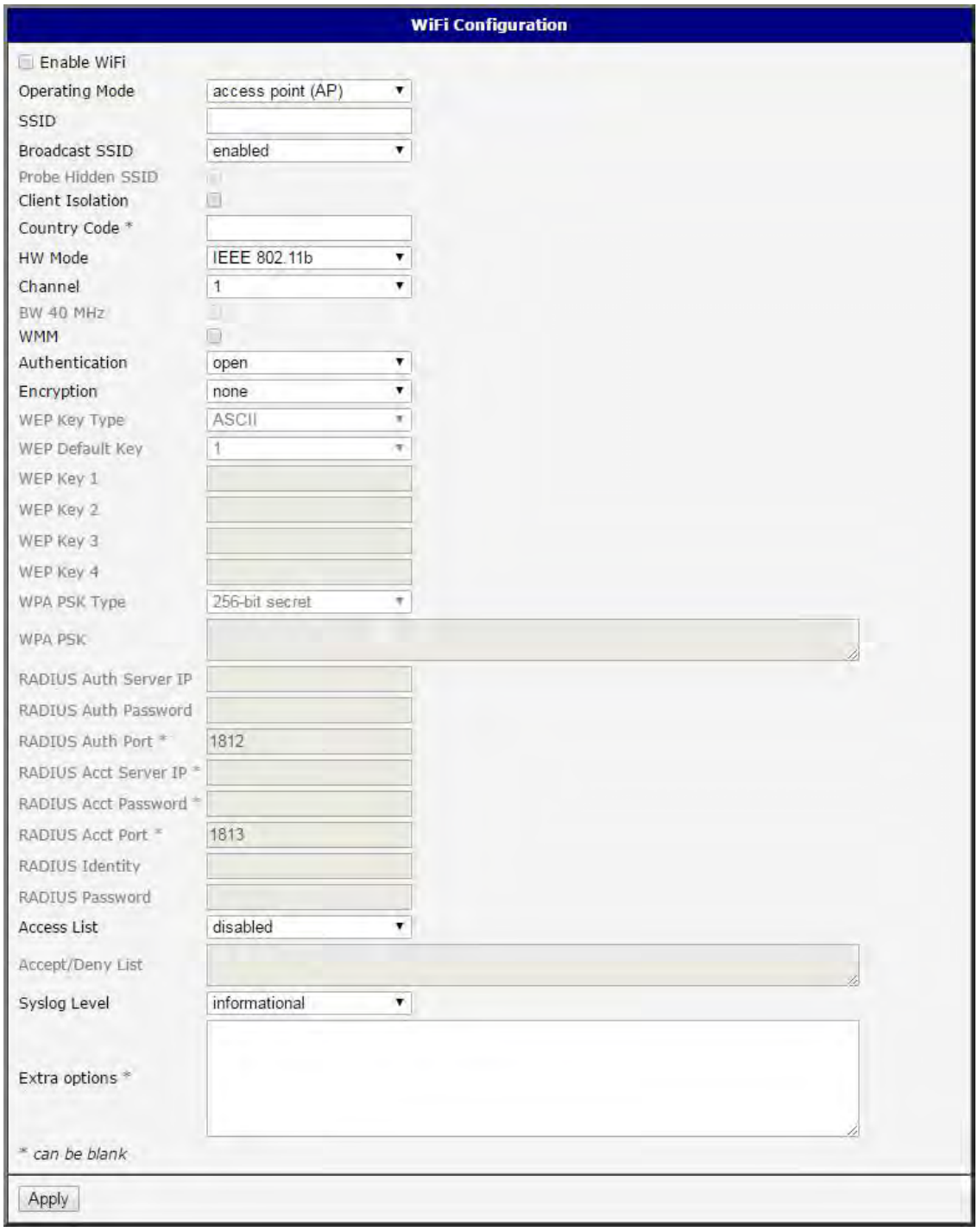


Abbildung 24: WiFi Configuration

3.6 WLAN Configuration

Diese Seite ist nur verfügbar, wenn der Router mit einem WLAN-Modul ausgestattet ist.

Wählen Sie den Menüpunkt *WiFi*, um die Konfigurationsseite für WLAN- und DHCP-Server-Einstellungen zu öffnen. Aktiveren Sie die Option *Enable WLAN interface*, um das WLAN einzuschalten. Nehmen Sie die folgenden Einstellungen vor.

Element	Beschreibung
Operating Mode	WLAN-Betriebsmodus: • **Access Point (AP)** – Der Router arbeitet als Zugangspunkt für Geräte im Client Mode. • **Station (STA)** – Der Router arbeitet als Client an verfügbaren Access Points. Empfangene Daten über die Kabelverbindung werden über das WLAN weitergeleitet.
DHCP Client	DHCP-Client ein- oder ausschalten.
IP Address	Feste IP-Adresse der WLAN-Schnittstelle
Subnet Mask	Subnetzmaske zu dieser Adresse
Bridged	Bridge-Modus ein-/ausschalten • **no** – Der Bridge-Modus ist nicht erlaubt (Standard). Das WLAN wird nicht mit dem LAN des Routers verbunden. • **yes** – Der Bridge-Mouds ist erlaubt. Das WLAN ist mit mindestens einem LAN des Routers verbunden. In diesem Fall werden die meisten Einstellungen dieser Tabelle ignoriert. Stattdessen verwendet der Router die Einstellungen der ausgewählten Netzwerkschnittstelle (LAN).
Default Gateway	IP address of the default gateway. When entering the IP address of the default gateway, all packets for which the record was not found in the routing table will be sent to this address.
DNS Server	Address to which all DNS queries are forwarded.

Tabelle 27: WLAN-Konfiguration

Aktivieren Sie die Option *Enable dynamic DHCP leases* im unteren Teil der Seite, für die dynamische Vergabe von IP-Adresse durch den DHCP-Server.

Element	Beschreibung
IP Pool Start	rste IP-Adresse des Adressbereichs aus dem Adressen an anfragende Clients vergeben werden.
IP Pool End	Letzte IP-Adresse des Adressbereichs aus dem Adressen an anfragende Clients vergeben werden.
Lease Time	„Leihzeit“: Zeit in Sekunden, die die IP-Adresse vor der Wiederverwertung nicht vergeben wird.

Tabelle 28: Konfiguration des DHCP-Servers

Die Änderungen gelten erst nach einem Klick auf die Schaltfläche *Apply*.

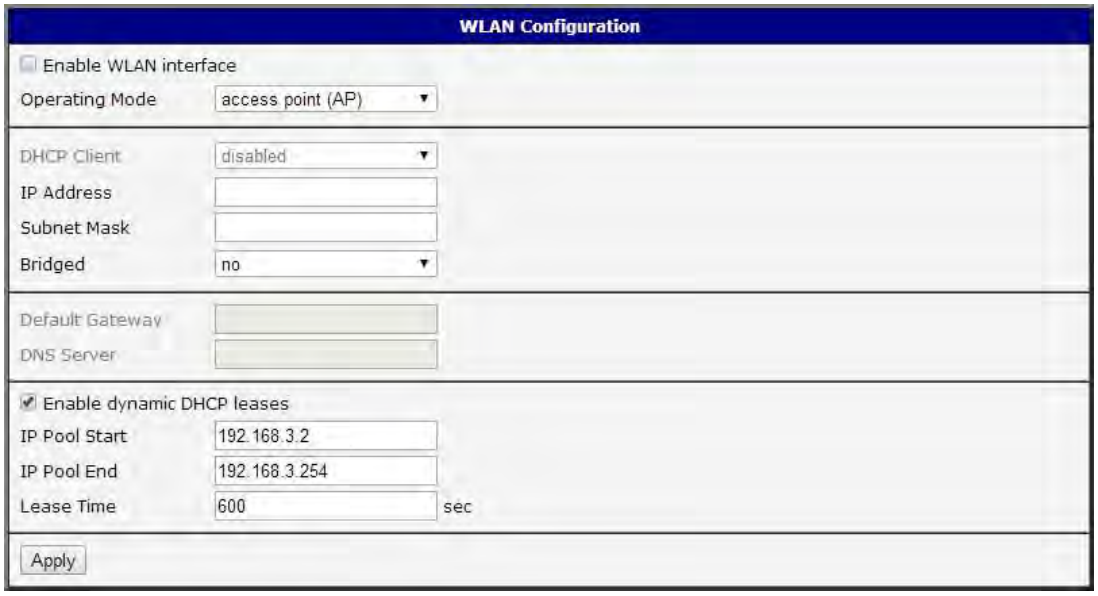


Abbildung 25: WLAN-Konfiguration

3.7 Backup Routes

Sie öffnen die Konfigurationsseiten für *Backup Routes*, indem Sie in der Navigationsspalte auf den Menüpunkt *backup Routes* klicken. Sie können die primäre Verbindung durch alternative Verbindungen ins Internet (Mobilfunk oder multiple WANs) für den Ausfall sichern. Der Wechsel zwischen den Verbindungen wird über die Prioritäten und den Status der Verbindungen gesteuert.

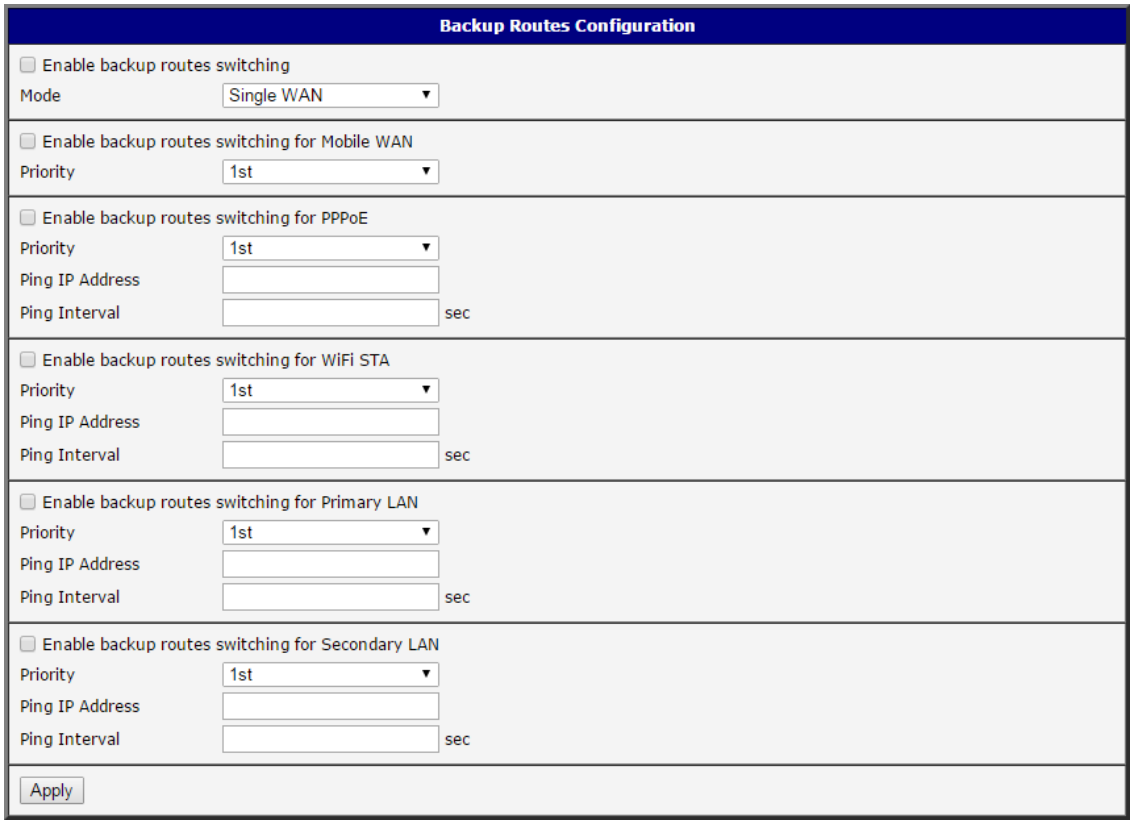


Abbildung 26: Konfiguration Backup-Routen

Element	Beschreibung
Enable backup routes switching	Die Standardroute wird gemäß den Einstellungen ausgewählt. Ist die Option nicht aktiviert, arbeitet das Backup-Routen-System im Rückwärtskompatibilitätmodus, basierend auf den nachfolgenden Einstellungen für die Netzwerkschnittstelle.
Mode	• **Single WAN** – Standardeinstellung. Es wird immer nur eine Schnittstelle für die WAN-Kommunikation verwendet. Entsprechend der gesetzten Prioritäten werden die übrigen Schnittstellen verwendet, wenn die bevorzugte Schnittstelle ausfällt. • **Multiple WANs** – Mehrere Schnittstellen werden für die WAN-Kommunikation verwendet. Eingehende Kommunikation über eine Schnittstelle wird auch über diese beantwortet. Die gespeicherten Prioritäten werden beachtet, wenn Daten vom Router oder aus dem Netzwerk hinter dem Router gesendet werden. Die Schnittstelle mit der höchsten Priorität wird verwendet.

Tabelle 29: Konfiguration Backup-Routen

Sie können verschiedene Schnittstellen für das Backup-Routen-System verwenden. Aktivieren Sie dazu die gewünschte(n) Option(en).

- *Enable backup routes switching for Mobile WAN*: über Mobilfunk
- *Enable backup routes switching for PPPoE*: über PPPoE
- *Enable backup routes switching for WiFi STA*: über WLAN im Client Modus
- *Enable backup routes switching for Primary LAN*: über die erste LAN-Schnittstelle
- *Enable backup routes switching for Secondary LAN*: über die zweite LAN-Schnittstelle

Aktivierte Schnittstellen werden für den WAN-Zugang entweder im Modus *Single WAN* mode (immer nur eine Schnittstelle) oder im Modus *Multiple WANs* (mehrere Schnittstellen gleichzeitig) verwendet, basierend auf den gespeicherten Prioritäten.

Element	Beschreibung
Priority	Priorität der Schnittstelle.
Ping IP Address	Zieladresse oder Domain Name für das Ping-Kommando bei der Verbindungsüberprüfung
Ping Interval	Zeit in Sekunden zwischen den Ping-Kommandos

Tabelle 30: Backup-Routen

Hinweis! Wollen Sie eine Verbindung ins Mobilfunknetz als Backup Route verwenden, müssen Sie auf der Seite *Mobile WAN* die Option *enable + bind* aktivieren und eine Zieladresse für das Ping-Kommando eingeben, siehe Abschnitt 3.3.3 im Kapitel 3.3.1.

Bei Schnittstellen, die zu einer Backup Route gehören, werden die „flags“ überprüft, die den Zustand der Schnittstelle anzeigen, z. B.: RUNNING auf der Seite *Network Status* (siehe Kapitel 2.5). So kann beispielsweise das Entfernen eines Ethernetkabel verhindert werden. Die Änderungen gelten erst nach einem Klick auf die Schaltfläche *Apply*.

Standardprioritäten für Backup-Routen Ist die Option *Enable backup routes switching* nicht aktiviert, arbeitet das Backup-Routen-System im Rückwärtskompatibilitätmodus, basierend auf den nachfolgenden Einstellungen für die Netzwerkschnittstelle. Der Router wählt die Route dann basierend auf den Standardprioritäten der einzelnen Schnittstellen, einschließlich der entsprechenden Dienste für die Schnittstelle. Die folgende Liste enthält die Namen der Backup-Routen und der dazugehörigen Netzwerk-Schnittstellen in der Reihenfolge der Standardprioritäten:

- Mobile WAN (pppX, usbX): siehe Kapitel 3.3.1
- PPPoE (ppp0): siehe Kapitel 3.4
- WiFi STA (wlan0): siehe Kapitel 3.6
- Secondary LAN (eth1)
- Primary LAN (eth0): siehe Kapitel 3.1

Beispiel für Standardprioritäten: Die Option *Backup Routes* ist deaktiviert, ebenso die folgenden Optionen:

- *Create connection to mobile network* auf der Seite *Mobile WAN* (siehe Kapitel 3.3.1),
- *Create PPPoE connection* auf der Seite *PPPoE* (siehe Kapitel 3.4)
- *Enable WiFi* auf der Seite *WiFi* (siehe Kapitel 3.6) oder Sie verwenden das WLAN im AP-Modus.

Der Router wählt nun das *Secondary LAN* als Standard-Route.
Um das *Primary LAN* auszuwählen, löschen Sie auf der Seite *Secondary LAN* die IP-Adresse und schalten dort auch den *DHCP Client* aus.

Hinweis: Beachten Sie, dass es ein Konzept von variablen WAN- und LAN-Schnittstellen gibt, auch wenn die Option *Backup Routes* nicht aktiviert ist. So mag eine Situation entstehen, in der die für das LAN bestimmte Schnittstelle die WAN-Schnittstelle wird wegen der festgelegten Prioritäten oder der Standardprioritäten. Die Kommunikation von der WAN zur LAN-Schnittstelle kann, abhängig von der *NAT* und *Firewall* Konfiguration, blockiert werden.

3.8 Firewall Configuration

Der erste Schritt bei eingehenden Datenpakete ist eine Überprüfung der IP-Adresse der Quelle und des Ports des Ziels.

Sie öffnen die Konfigurationsseiten für die Firewall, indem Sie in der Navigationsspalte auf den Menüpunkt *Firewall* klicken.

Aktivieren Sie die Option *Enable filtering of incoming packets*. Die Erreichbarkeit wird gegen den IP Address Table geprüft, d. h., dass nur auf im Address Table enthaltene Adresse zugegriffen werden kann. Sie können bis zu acht Adresse erlauben/verbieten. Folgende Parameter können bearbeitet werden.

Element	Beschreibung
Source	IP-Adresse, für die die Regel gilt.
Protocol	Protokoll für das die Regel gilt: • **all** – alle Protokolle • **TCP** – nur TCP • **UDP** – nur UDP • **ICMP** – nur ICMP
Target Port	Port für den die Regel angewendet wird
Action	Regel – Art der Aktion des Routers: • **allow** – Der Router lässt Pakete ins Netzwerk. • **deny** – Der Router lässt keine Pakete ins Netzwerk.

Tabelle 31: Filtern von eingehenden Paketen

Im nächsten Abschnitt konfigurieren Sie die Regeln für die Weiterleitung. Ist die Option *Enabled filtering of forwarded packets* nicht aktiviert, werden automatisch alle Pakete akzeptiert. Ist die Option aktiviert, wird ein Paket, welches an eine andere Netzwerkschnittstelle adressiert ist, vom Router an die FORWARD-Kette weitergeleitet. Wird das Paket dort akzeptiert und eine Weiterleitungsregel existiert, sendet der Router das Paket. Gibt es keine Weiterleitungsregel, verwirft der Router das Paket.

Sie können mehrere Filterregeln aufstellen, indem Sie z. B. Daten nur für einen bestimmten Protokolltyp zulassen oder auch detaillierter Werte für die IP-Adresse der Quelle und/oder des Ziels sowie die Ports festlegen.

Schalten Sie die Option *Enable filtering of locally destined packets* ein, verwirft der Router alle Pakete die einen nicht-unterstützten Dienst anfordern ohne weitere Information.

Zum Schutz vor Denial-of-Service-Attacken (DoS) aktivieren Sie die Option *Enable protection against DoS attacks*. Dadurch wird die Anzahl der erlaubten Verbindungen auf 5 pro Sekunde limitiert. Bei einer DoS-Attacke wird das angegriffene System mit bedeutungslosen Anfragen geflutet.

Element	Beschreibung
Source	Quell-IP-Adresse, für die die Regel gilt.
Ziel	Ziel-IP-Adresse, für die die Regel gilt.
Protocol	Protokoll, für das die Regel gilt: • **all** – alle Protokolle • **TCP** – nur TCP • **UDP** – nur UDP • **ICMP** – nur ICMP
Target Port	Port für den die Regel angewendet wird
Action	Regel – Art der Aktion des Routers: • **allow** – Der Router lässt Pakete ins Netzwerk. • **deny** – Der Router lässt keine Pakete ins Netzwerk.

Tabelle 32: Filtern von weitergeleiteten Paketen

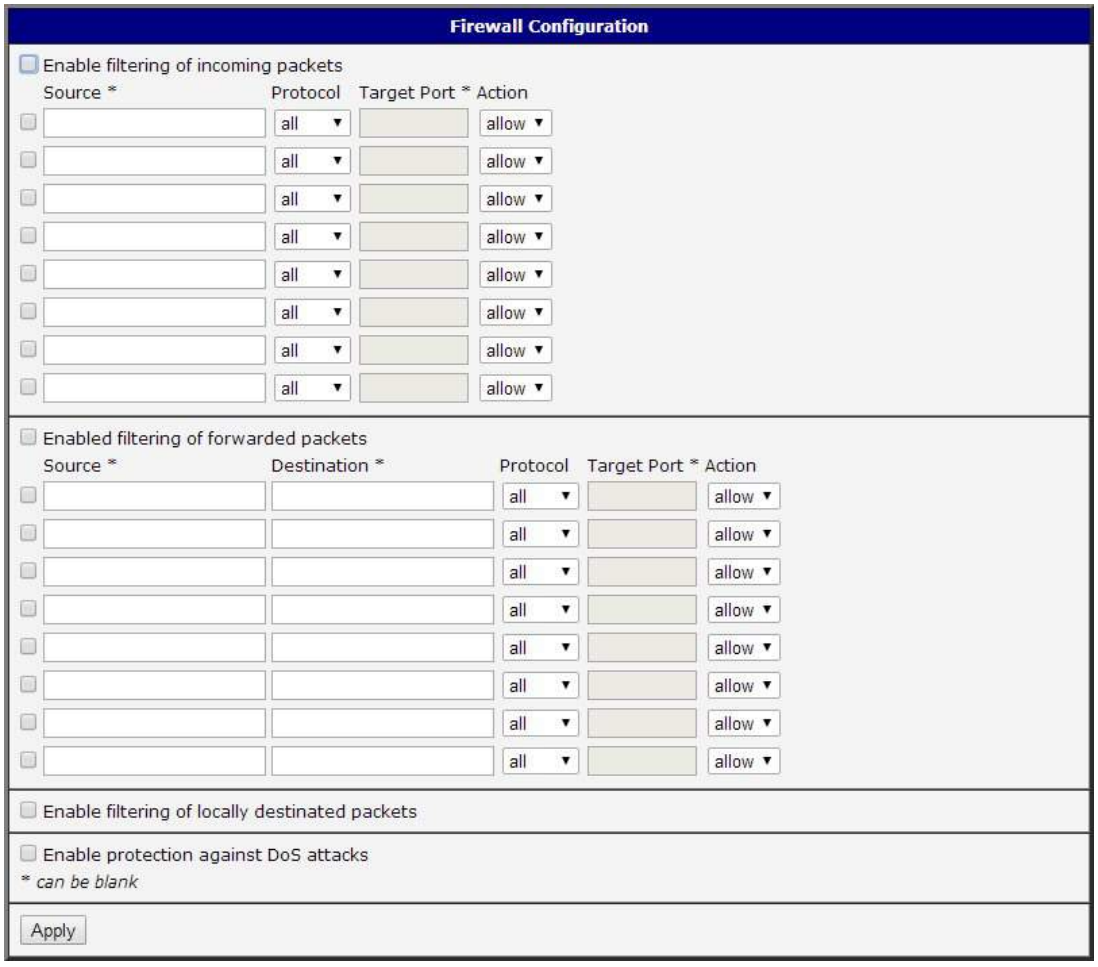


Abbildung 27: Konfiguration Firewall

Beispielkonfiguration IPv4-Firewall

Der Router erlaubt die folgenden Zugriffe:

- von der IP-Adresse 171.92.5.45, jedes Protokoll
- von der IP-Adresse 10.0.2.123, Protokoll: TCP, Port: 1000
- von der IP-Adresse 142.2.26.54, Protokol: ICMP.

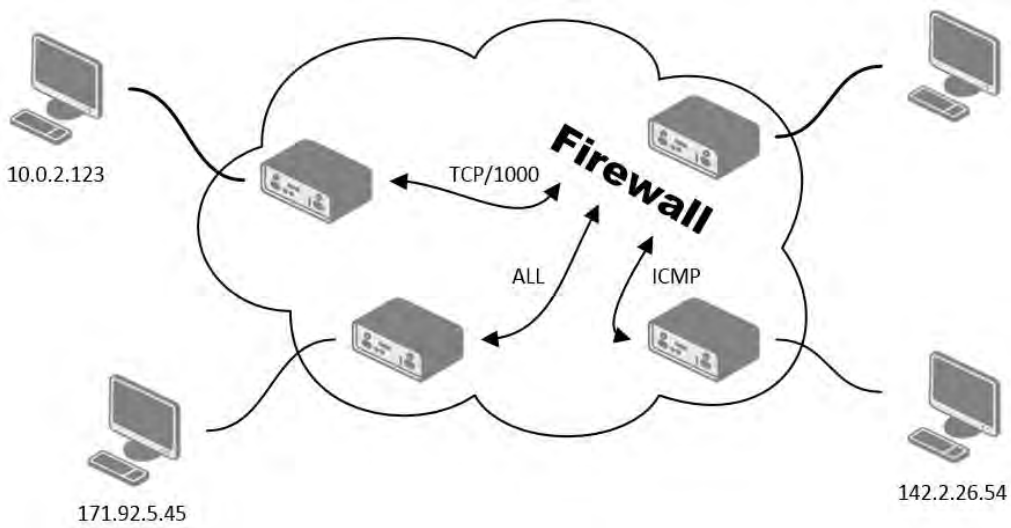


Abbildung 28: Beispieltopologie für Firewall

Abbildung 29: Beispielskonfiguration Firewall

3.9 NAT Configuration

Über den Menüpunkt *NAT* öffnen Sie die Konfigurationsseite für die Funktion *Address Translation*.

Der Router verwendet Port Address Translation (PAT), eine Methode, beider ein TCP/UDP-Port auf einen anderen gemappt wird. Dabei modifiziert der Router die Informationen im *Paketkopf*, wenn die Paket den Router durchlaufen. Sie können bis zu 16 PAT-Regeln aufstellen.

Element	Beschreibung
Public Port	Öffentlicher Port für die Übersetzungsregel
Private Port	Privater Port für die Übersetzungsregel
Type	Protokolltyp – TCP oder UDP.
Server IP address	IP-Adresse an welche die eingehenden Daten weitergeleitet werden.

Tabelle 33: Konfiguration NAT

Falls mehr als 16 Regeln benötigen, können Sie die weiteren Regeln im Startup Script integrieren. Die Seite *Startup Script* rufen Sie über den Menüpunkt *Scripts* auf, siehe Kapitel 3.22.

Verwenden Sie das Kommando `iptables`:

```
iptables -t nat -A napt -p tcp --dport [PORT\_PUBLIC] -j DNAT --to-destination
[IPADDR]:[PORT1\_PRIVATE]
```

Tragen Sie die IP-Adresse [IPADDR], die Nummern des Public Ports [PORT_PUBLIC] und des Private Ports [PORT_PRIVATE] in eckigen Klammern ein.

Verwenden Sie die folgenden Parameter für die Weiterleitung von über PPP eingehenden Daten an einen verbundenen Computer.

Element	Beschreibung
Send all remaining incoming packets to default server	(De)Aktiviert die Weiterleitung von nicht passenden eingehenden Paketen an den Standard-Server. Dazu müssen Sie wenigstens die IP-Adresse eines Standard-Server in einem der beiden Eingabefelder eingeben. Der Router leitet dann die eingehenden Daten von GPRS zu dem Computer mit der angegebenen IP-Adresse.
Default Server IP Address	IP-Adresse des Standard-Servers.

Tabelle 34: Konfiguration – Sende alle eingehenden Paket zum Server

Wenn Sie die foglenden Optionen aktivieren und die Nummer des Ports eintragen, können Sie aus der Ferne über die PPP-Schnittstelle auf den Router zugreifen.

Element	Beschreibung
Enable remote HTTP access on port	Falls aktiviert und ein Wert im Feld *Port* eingetragen ist, kann der Router über die Web-Schnittstelle konfiguriert werden. (Standard: nicht aktiviert)
Enable remote HTTPS access on port	Falls aktiviert und ein Wert im Feld *Port* eingetragen ist, kann der Router über die Web-Schnittstelle konfiguriert werden. (Standard: nicht aktiviert)
Enable remote FTP access on port	Falls aktiviert und ein Wert im Feld *Port* eingetragen ist, kann per FTP auf den Router zugegriffen werden.
Enable remote SSH access on port	Falls aktiviert und ein Wert im Feld *Port* eingetragen ist, kann per SSH auf den Router zugegriffen werden. (Standard: nicht aktiviert)
Enable remote Telnet access on port	Falls aktiviert und ein Wert im Feld *Port* eingetragen ist, kann per Telnet auf den Router zugegriffen werden.
Enable remote SNMP access on port	Falls aktiviert und ein Wert im Feld *Port* eingetragen ist, kann per SNMP auf den Router zugegriffen werden. (Standard: nicht aktiviert)
Masquerade outgoing packets	Funktion Network Address Translation ein-/ausschalten.

Tabelle 35: Konfiguration – Fernzugang

Beispiel 1: Konfiguration IPv4 NAT mit einem verbundenen Gerät

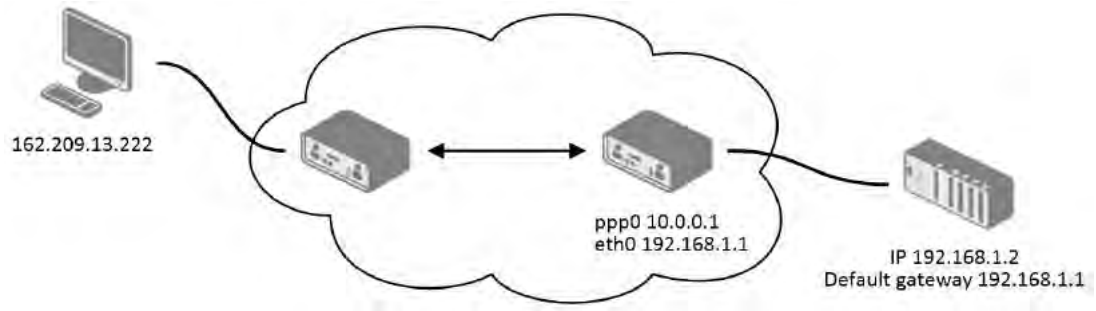


Abbildung 30: Beispieltopologie – NAT 1

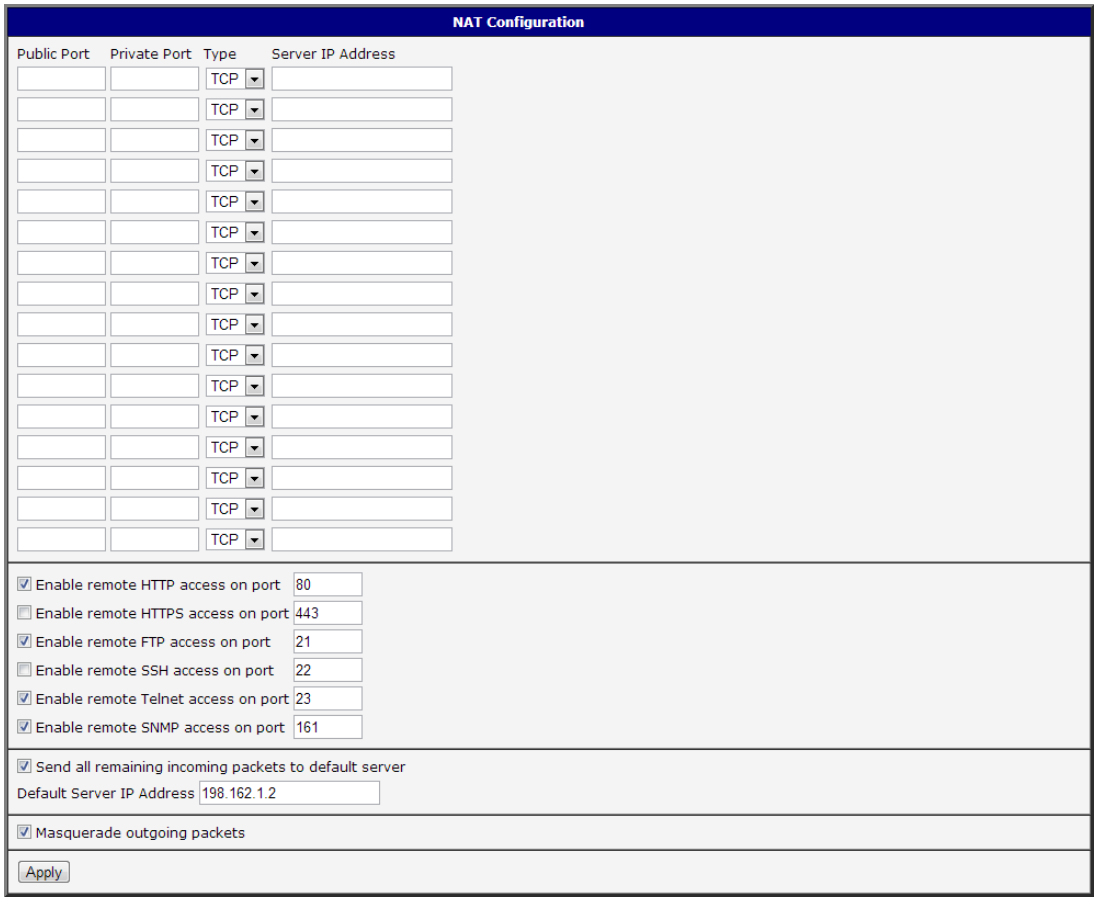


Abbildung 31: Beispielkonfiguration – NAT 1

Wichtig ist für diese Konfiguration ist, dass Sie die Option*Send all remaining incoming packets to default server* aktivieren. Die IP-Adresse gehört zu einem Gerät hinter dem Router. Das Standard-Gateway des Gerätes im gleichen Subnetz wie der Router hat die IP-Adresse wird im Feld *Default Server IPv4 Address* eingetragen. Das angeschlossene Gerät antwortet, wenn ein Ping an die IP-Adresse der SIM-Karte gesendet wird.

Beispiel 2: Konfiguration IPv4 NAT mit mehreren verbundenen Geräten

In diesem Beispiel sind mehrere Geräte über den Switch hinter dem Router verbunden. Jedes Gerät hat seine eigene IP-Adresse.

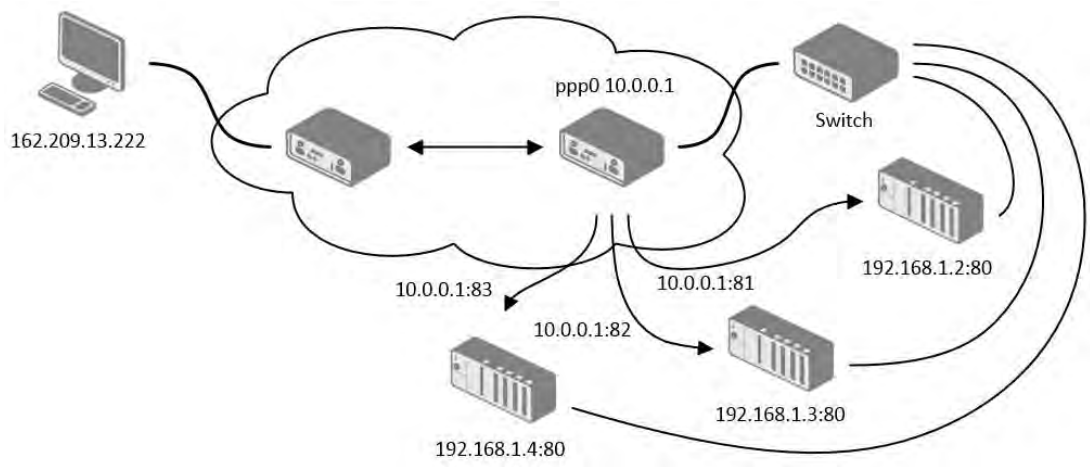


Abbildung 32: Beispieltopologie – NAT – 2

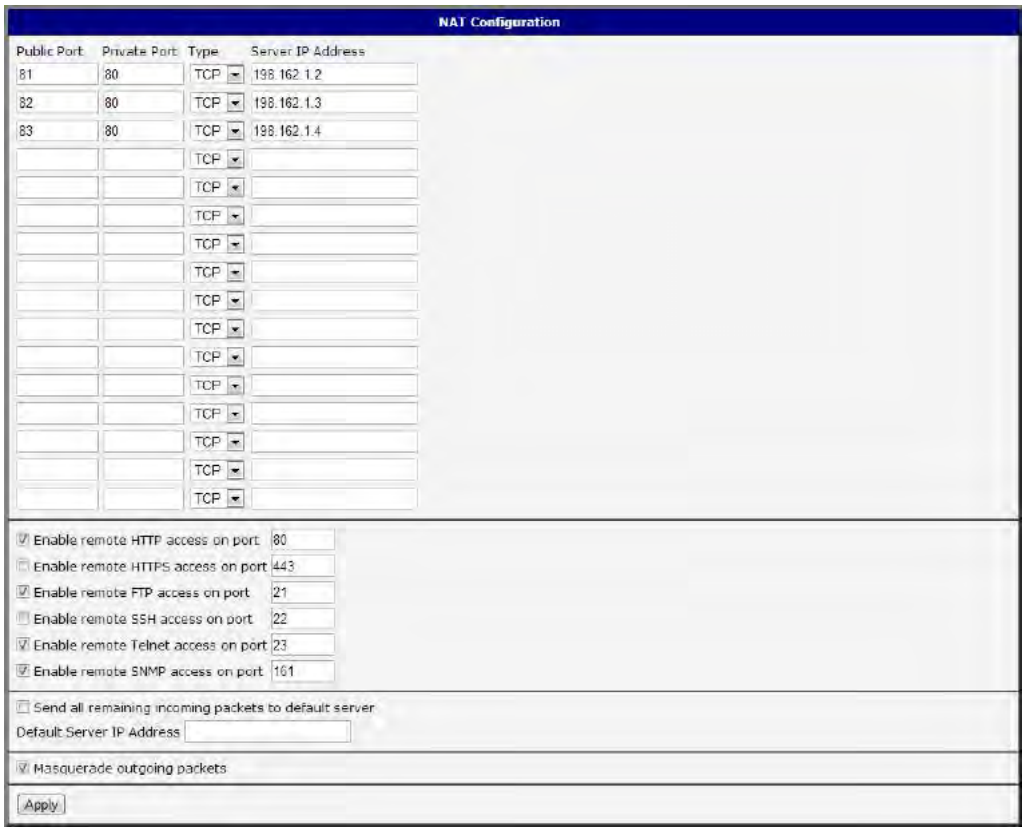


Abbildung 33: Beispielkonfiguration – NAT – 2

Tragen Sie die IP-Adresse auf der Seite *NAT Configuration* im Feld *Server IPv4 Address* ein. Die Geräte kommunizieren über Port 80. Sie können aber auch eine Port-Weiterleitung über die Felder *Public Port* und *Private Port* einstellen.

Der Router greift nun auf den Socket 192.168.1.2:80 hinter dem Router zu, wenn über das Internet auf die IP-Adresse 10.0.0.1:81 zugegriffen wird. Senden Sie ein Ping-Kommando an die öffentliche IP-Adresse des Router (10.0.0.1), antwortet der Router wie gewohnt, ohne Weiterleitung.

Geben Sie die IP-Adresse 10.0.0.1 im Browser ein,passiert nichts, da der Zugriff auf Port 80 erfolgt. Dieser ist in der Liste *Public Port* aber nicht aufgeführt und die Option *Enable remote HTTP access on port 80* ist nicht aktiviert. Da die Option *Send all remaining incoming packets to default server* nicht aktiviert ist, verweigert der Router den Verbindungsaufbau.

3.10 OpenVPN Tunnel Configuration

Die Funktion OpenVPN-Tunnel erlaubt die Einrichtung einer sicheren Verbindung zwischen zwei getrennten LANs. Sie können bis zu vier OpenVPN-Tunnel einrichten.

Sie öffnen die Konfigurationsseiten für *OpenVPN tunnel*, indem Sie in der Navigationsspalte auf den Menüpunkt *OpenVPN* klicken. Danach rufen Sie eine der vier Konfigurationsseiten auf: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* und *4th Tunnel*. Die Konfigurationsseiten entsprechen sich.

Element	Beschreibung
Description	Name oder Beschreibung des Tunnels
Protocol	verwendetes Kommunikationsprotokoll • **UDP** – OpenVPN über UDP • **TCP server** – OpenVPN über TCP im Server-Modus • **TCP client** – OpenVPN über TCP im Client-Modus.
UDP/TCP port	Port des gewählten Protokolls (UDP oder TCP).
Remote IP Address	IP-Adresse oder Domain Name der Gegenseite
Remote Subnet	IP-Adresse des Netzwerks hinter der Gegenseite
Remote Subnet Mask	Subnetzmaske des Netzwerks der Gegenseite
Redirect Gateway	Ergänzt oder überschreibt das Standard-Gateway. Alle Paket werden über den Tunnel an dieses Gateway gesendet, es sei denn, sie enthalten ein anderes Standard-Gateway.
Local Interface IP Address	IP-Adresse einer lokalen Schnittstelle.
Remote Interface IP Address	IP-Adresse oder Domain Name der Schnittstelle der Gegenseite.
Ping Interval	Zeitspanne nach der der Router eine Nachricht an die Gegenseite sendet, um das Bestehen des Tunnels zu überprüfen.
Ping Timeout	Wartezeit die der Router auf eine Antwort der Gegenseite wartet. Für eine korrekte Überprüfung sollte der Wert für *Ping Timeout* größer sein als der Wert für *Ping Interval*.
Renegotiate Interval	Zeitspanne nach der die Authorisierung des OpenVPN-Tunnels neu verhandelt wird. Dieser Parameter ist nur dann konfigurierbar, wenn der Authentifizierungs-Modus *username/password* oder *X.509 certificate* ausgewählt wurde. Nach Ablauf der Zeitspanne wechselt der Router die Verschlüsselung, um die laufende Sicherheit des Tunnels zu gewährleisten.
Max Fragment Size	Maximale Größe eines gesendeten Pakets

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite

Element	Beschreibung
Compression	Die Daten können für das Senden komprimiert werden: • **none** – keine Kompression • **LZO** – verlustfreie Kompression; muss auf beiden Seiten des Tunnels eingestellt sein
NAT Rules	NAT-Regel für den OpenVPN-Tunnel: • **not applied** – NAT-Regel werden nicht angewendet. • **applied** – NAT-Regeln werden angewendet.
Authenticate Mode	Authentifizierungs-Modus: • **none** – Keine Authentifizierung • **Pre-shared secret** – Authentifizierung mit *Shared key* auf beiden Seiten des Tunnels • **Username/password** – Authentifizierung mit CA-Zertifikat, Benutzernamen und Passwort • **X.509 Certificate (multiclient)** – X.509-Authentifizierung im Multi-Client-Modus • **X.509 Certificate (client)** – X.509-Authentifizierung im Client-Modus • **X.509 Certificate (server)** – X.509-Authentifizierung im Server-Modus
Pre-shared Secret	Authentifizierung mit *Pre-shared secret*; für jeden Authentifizierungs-Modus möglich
CA Certificate	CA-Zertifikat zusammen mit Benutzernamen/Passwort im X.509-Zertifikats-Authentifizierungs-Modus
DH Parameters	Protokoll für den DH-Parameter-Schlüsselaustausch für die X.509-Zertifikats-Authentifizierung im Server-Modus
Local Certificate	Zertifikat auf dem lokalen Gerät; für den X.509-Zertifikats-Authentifizierungs-Modus
Local Private Key	Schlüssel auf dem lokalen Gerät; für den X.509-Zertifikats-Authentifizierungs-Modus
Username	Benutzernamen für die Authentifizierung im Benutzernamen/Passwort-Modus

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite

Element	Beschreibung
Password	Passwort für die Authentifizierung im Benutzernamen/Passwort-Modus
Extra Options	Zusätzliche Parameter für den OpenVPN-Tunnel, z. B. DHCP-Optionen. Stellen Sie den Parametern 2 - voran. Weitere Informationen finden Sie auf dem Router über eine SSH-Verbindung. Rufen Sie den Befehl `openvpnd --help` auf.

Tabelle 36: Konfiguration OpenVPN

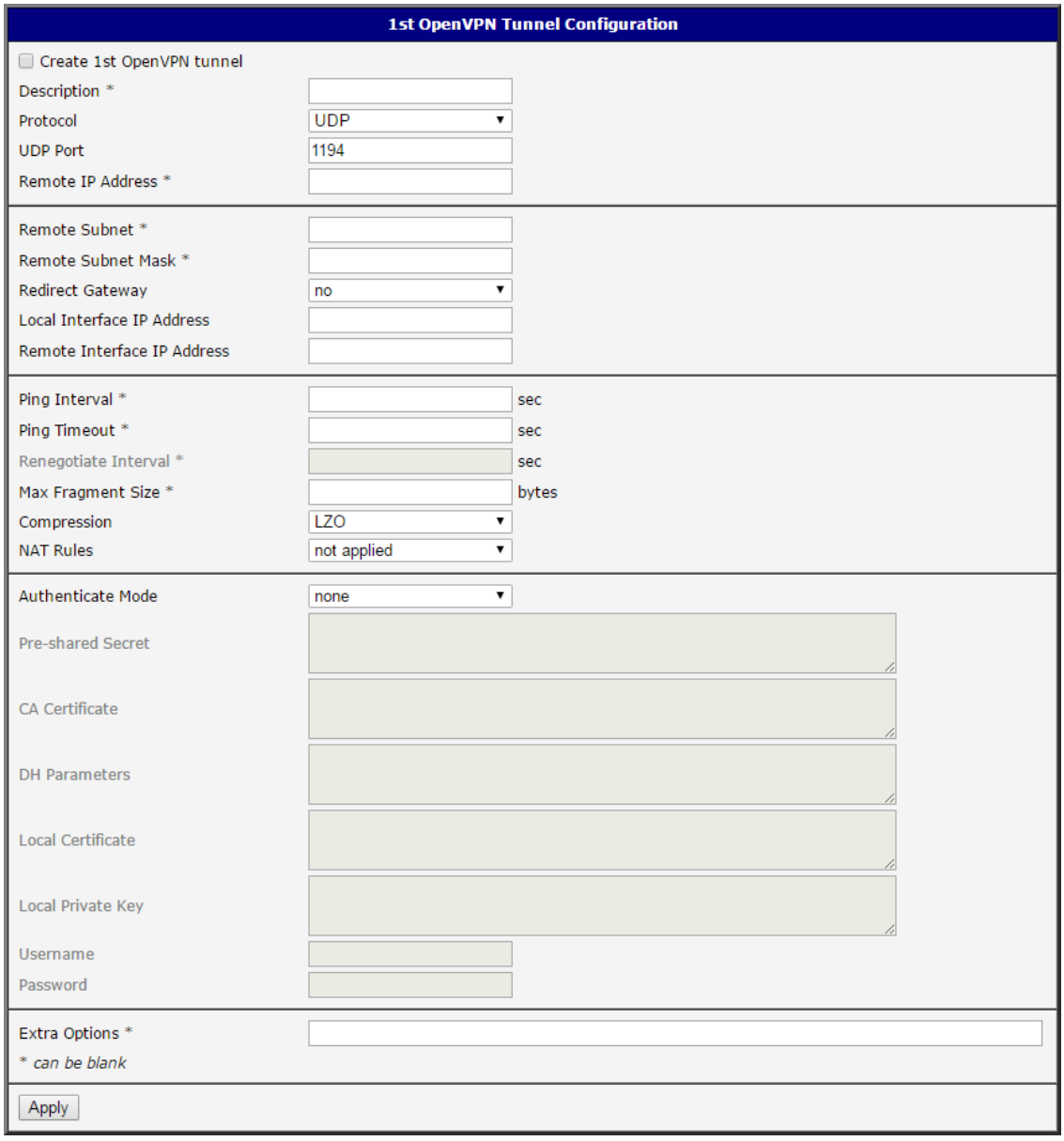


Abbildung 34: Konfiguration OpenVPN-Tunnel

Folgende Bedingung muss für die Errichtung des Tunnels erfüllt sein: Die WAN-Route muss aktiv sein, z. B. eine aufgebaute Mobilfunkverbindung, selbst wenn der Tunnel nicht über das WAN geht.

Die Änderungen gelten erst nach einem Klick auf die Schaltfläche *Apply*.

Beispielkonfiguration OpenVPN-Tunnel im IPv4-Netzwerk

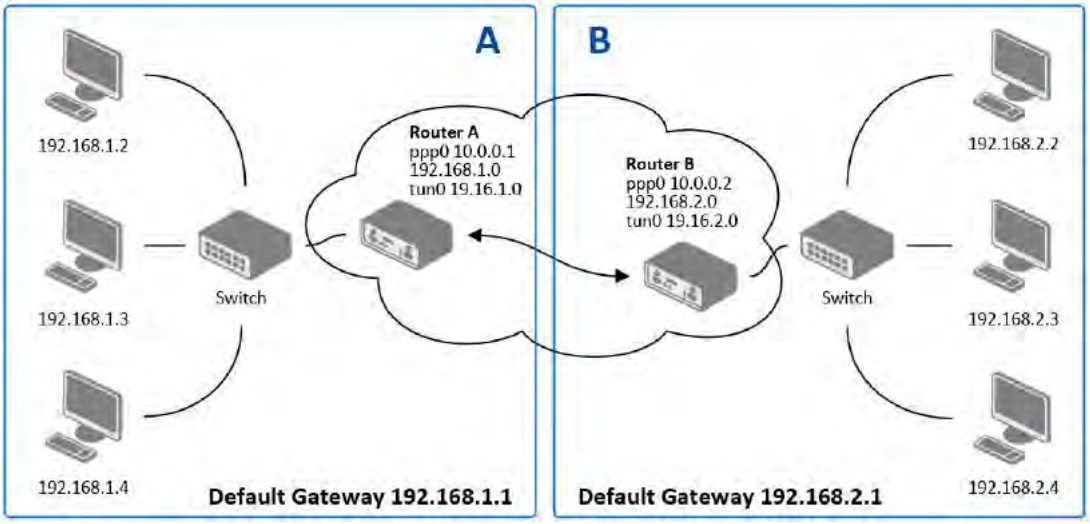


Abbildung 35: Beispieltopologie für OpenVPN

Konfiguration des OpenVPN-Tunnels:

Konfiguration	A	B
Protocol	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	none	none

Tabelle 37: Konfigurationsbeispiel OpenVPN

Beispiele für die verschiedenen Optionen für Konfiguration und Authentifizierung eines OpenVPN-Tunnels finden Sie im Dokument *OpenVPN Tunnel* [5].

3.11 IPsec Tunnel Configuration

Die Funktion IPsec-Tunnel erlaubt die Einrichtung einer sicheren Verbindung zwischen zwei getrennten LANs. Sie können bis zu vier IPsec-Tunnel einrichten. Dual Stack (IPv4 und IPv6) wird unterstützt.

Sie öffnen die Konfigurationsseiten für *IPsec Tunnel*, indem Sie in der Navigationsspalte auf den Menüpunkt *IPsec* klicken. Danach rufen Sie eine der vier Konfigurationsseiten auf: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* und *4th Tunnel*. Die Konfigurationsseiten entsprechen sich.

Damit der Datenstrom zwischen den Subnetzen verschlüsselt übertragen wird, müssen Sie die entsprechenden Werte in die Felder *Remote Subnet* und *Local Subnet* eintragen. Soll der Datenstrom nur zwischen den Router verschlüsselt werden, lassen Sie die beiden Felder für das Subnetz frei.

Wenn Sie Protokoll und Port in den entsprechenden Felder eintragen, kapselt der Router nur solche Pakete, auf die die Einstellungen passen.

Element	Beschreibung
Description	Name oder Beschreibung des Tunnels
Remote IP Address	IP-Adresse oder Domain Name der Gegenstelle
Remote ID	Kennzeichner (ID) der Gegenseite, bestehen aus *Hostname* und *Domain Name*.
Remote Subnet	IP-Adresse des Netzwerks hinter der Gegenstelle
Remote Subnet Mask	Subnetzmaske des Netzwerks hinter der Gegenstelle
Remote Protocol/Port	Protokoll und Port der Gegenseite. Standardformat: *Protokoll*/*Port*, z. B. 17/1701 für UDP (Protokoll 17 und Port 1701). Sie können zwar nur die Nummer des Protokoll eintragen, jedoch wird das Standardformat bevorzugt.
Local ID	Kennzeichner (ID) der lokalen Seite, bestehen aus *Hostname* und *Domain Name*
Local Subnet	IP-Adresse des lokalen Netzwerks
Local Subnet Mask	Subnetzmaske des lokalen Netzwerks
Local Protocol/Port	Protokoll und Port des lokalen Netzwerk. Standardformat: *Protokoll*/*Port*, z. B. 17/1701 für UDP (Protokoll 17 und Port 1701). Sie können zwar nur die Nummer des Protokoll eintragen, jedoch wird das Standardformat bevorzugt.
Encapsulation Mode	IPsec-Modus, entsprechend der Kapselungsmethode. Wählen Sie *tunnel*, um das gesamte IP-Datagram zu kapseln oder *transport*, wenn nur der IP-Header gekapselt werden soll

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite

Element	Beschreibung
NAT traversal	Network Address Translation einschalten, wenn Sie NAT zwischen den Endpunkte des Tunnels benutzen wollen.
IKE Mode	Modus für den Verbindungsaufbau: (*main* oder *aggressive*). Bei *aggressive* baut der Router die Verbindung schneller auf, dabei wird die Verschlüsselung aber fest auf 3DES-MD5 eingestellt. **Empfehlung: Wegen der geringeren Sicherheit sollten Sie diesen Modus nicht verwenden!**
IKE Algorithm	Auswahlkriterien für die Wahl des Algorithmus durch den Router: • **auto** – Verschlüsselung und Hash-Algorithmus werden automatisch gewählt. • **manual** – Verschlüsselung und Hash-Algorithmus werden vom Benutzer gewählt.
IKE Encryption	Verschlüsselungsalgorithmus – 3DES, AES128, AES192, AES256.
IKE Hash	Hash-Algorithmen – MD5, SHA1, SHA256, SHA384 or SHA512.
IKE DH Group	Diffie-Hellman-Gruppen, welche die Schlüsselstärke im Austauschprozess festlegen. Gruppen mit höheren Nummern sind sicherer, benötigen aber mehr Zeit für die Schlüsselberechnung.
ESP Algorithm	Auswahlkriterien für die Wahl des Algorithmus durch den Router: • **auto** – Verschlüsselung und Hash-Algorithmus werden automatisch gewählt. • **manual** – Verschlüsselung und Hash-Algorithmus werden vom Benutzer gewählt.
ESP Encryption	Verschlüsselungsalgorithmus – DES, 3DES, AES128, AES192, AES256.
ESP Hash	Hash-Algorithmus – MD5, SHA1, SHA256, SHA384 or SHA512.
PFS	Funktion Perfect Forward Secrecy ein-/ausschalten. Diese Funktion stellt sicher, dass die abgeleiteten Sitzungsschlüssel nicht kompromittiert werden, sollte in der Zukunft ein privater Schlüssel kompromittiert werden.
PFS DH Group	Nummer der Diffie-Hellman-Gruppe (siehe *IKE DH Group*).
Key Lifetime	Gültigkeitsdauer des Schlüssels für den Datenbereich des Tunnels, in Sekunden – Minimalwert: 60 s, Maximalwert: 86.400 s.

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite

Element	Beschreibung
IKE Lifetime	Gültigkeitsdauer des Schlüssels für den Steuerbereich des Tunnels, in Sekunden – Minimalwert: 60 s, Maximalwert: 86.400 s.
Rekey Margin	Dieser Wert gibt an, wie früh vor Ablauf der Verbindung der Router mit der Neuverhandlung der Sitzungsschlüssel beginnen soll. Geben Sie einen Wert ein, der weniger als die Hälfte der Werte für *IKE* und *Key Lifetime*.
Rekey Fuzz	Prozentwert der Abweichung vom eingestellten Wert *Rekey Margin*. Damit werden die Rekey-Intervalle zufälliger ausgewählt.
DPD Delay	Verzögerung in Sekunden nach der die Funktionalität des IPsec-Tunnels getestet wird.
DPD Timeout	Wartezeit in Sekunden
Authenticate Mode	Authentifizierungs-Modus • **Pre-shared key** – Pre-Shared-Key auf beiden Seiten • **X.509 Certificate** – X.509-Authentifizierung im Multiclient-Modus
Pre-shared Key	Geteilter Schlüssel auf beiden Seiten des Tunnelstunnel. Authentifizierungs-Modus *Pre-shared key* erforderlich
CA Certificate	CA-Zertifikat; Authentifizierungs-Modus: *X.509 Certificate*
Remote Certificate	Zertifikat auf der Gegenstelle; Authentifizierungs-Modus: *X.509 Certificate*
Local Certificate	Zertifikat auf dem lokalen Gerät; Authentifizierungs-Modus: *X.509 Certificate*
Local Private Key	Schlüssel auf dem lokalen Gerät; Authentifizierungs-Modus: *X.509 Certificate*
Local Passphrase	während der Erstellung des privaten Schlüssels verwendete Passphrase
Debug	Informationstiefe des System-Logs. *Silent* (Standard), *audit*, *control*, *control-more*, *raw*, *private* (Enthält neben den privaten Schlüssel die meisten Informationen).

Tabelle 38: Konfiguration IPsec-Tunnel

- Sind die beiden Subnetze nicht konfiguriert, werden die Pakete zwischen lokaler und ferner IP-Adresse nur gekapselt; lediglich die Kommunikation zwischen den Routern wird verschlüsselt.
- Sind *protocol* und *fields* konfiguriert, werden passende Pakete gekapselt.

Die folgende Prozedur beschreibt die Erstellung von Zertifikaten und Schlüsseln ohne Passwort-Phrase:

```
******************** 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
```

Zertifikate mit der Passphrase *router* (Die Certification Authority 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
```

Die Funktion IPsec unterstützt die folgenden Kennungstypen (ID) für beide Seiten des Tunnels: Parameter für *Remote ID* und *Local ID*

- IP-Adresse (z. B.: 192.168.1.1)
- DN (z. B.: C=CZ,O=CompanyName,OU=TP,CN=A)
- FQDN (z. B.: @director.companyname.cz) – **Das Symbol @ symbol geht der FQDN voran.**
- User FQDN (z. B.: director@companyname.cz)

Zertifikate und private Schlüssel müssen im Format PEM sein. Verwenden Sie nur Zertifikate mit Start- und Stop-Tags.

Definition der zufälligen Zeitspanne, nach der der Router die Schlüssel austauscht:

*Lifetime - (Rekey margin + random value in range (from 0 to Rekey margin * Rekey Fuzz/100))*

Der Standardaustausch der Schlüssel erfolgt innerhalb der folgende Zeitspanne:

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

Wir empfehlen die Standardeinstellungen beizubehalten. Wenn Sie den Zeitraum für den Schlüsselaustausch erhöhen, erzeugt der Tunnel zwar geringere Betriebskosten, jedoch bieten diese Einstellungen weniger Sicherheit. Umgekehrt, wenn Sie den Zeitraum verringert, steigen die Betriebskosten, zugleich wird aber auch die Sicherheit höher.

Die Änderungen gelten erst nach einem Klick auf die Schaltfläche *Apply*.

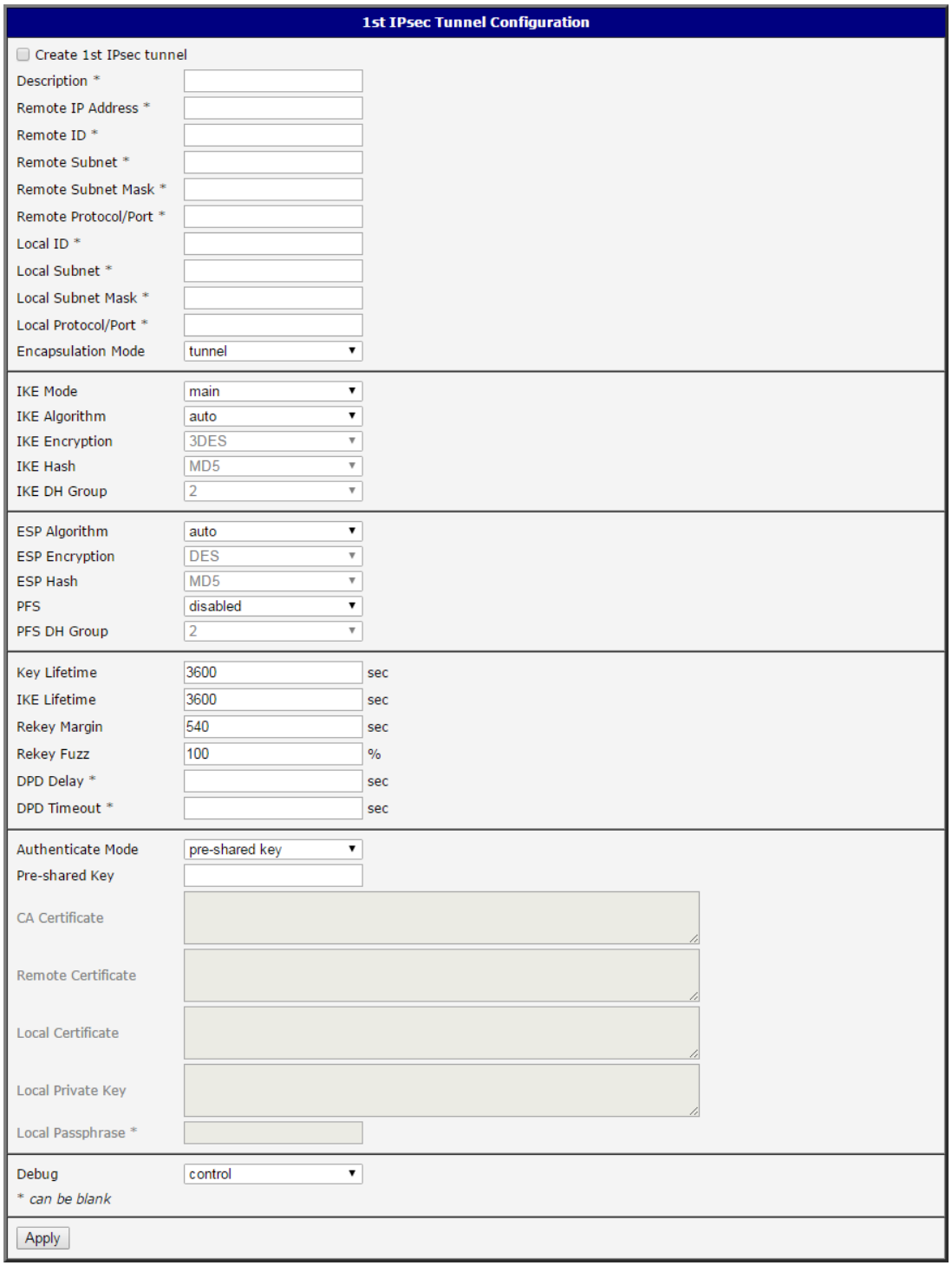


Abbildung 36: Konfiguration IPsec-Tunnel

Beispielkonfiguration IPSec-Tunnel im IPv4-Netzwerk

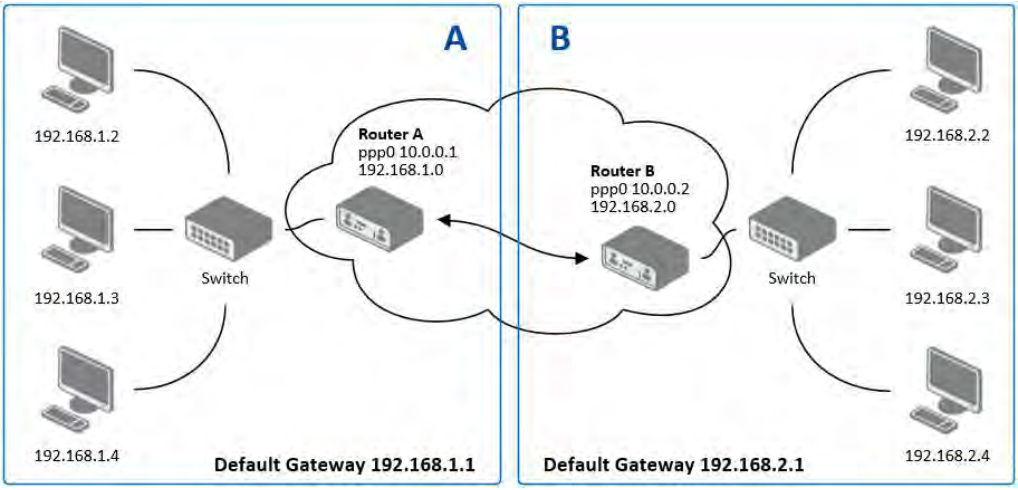


Abbildung 37: Beispieltopologie für IPsec

Konfiguration IPsec-Tunnel:

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
Local Subnet	192.168.1.0	192.168.2.0
Local Subnet Mas:	255.255.255.0	255.255.255.0
Authenticate mode	pre-shared key	pre-shared key
Pre-shared key	test	test

Tabelle 39: Konfigurationsbeispiel IPsec

Beispiele für die verschiedenen Optionen für Konfiguration und Authentifizierung eines IPsec-Tunnels finden Sie im Dokument *IPsec Tunnel* [6].

3.12 GRE Tunnels Configuration

GRE ist ein unverschlüsseltes Protokoll.

Die Funktion GRE-Tunnel erlaubt die Einrichtung einer unverschlüsselten Verbindung zwischen zwei getrennten LANs. Sie können bis zu vier GRE-Tunnel einrichten.

Sie öffnen die Konfigurationsseiten für *GRE Tunnel*, indem Sie in der Navigationsspalte auf den Menüpunkt *GRE* klicken. Danach rufen Sie eine der vier Konfigurationsseiten auf: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* und *4th Tunnel*.

Die Konfigurationsseiten entsprechen sich.

Element	Beschreibung
Description	Name oder Beschreibung des GRE-Tunnels
Remote IP Address	IP-Adresse der Gegenseite
Remote Subnet	IP-Adresse des Netzwerks hinter der Gegenseite
Remote Subnet Mask	Subnetzmaske des Netzwerks hinter der Gegenseite
Local Interface IP Address	lokale IP-Adresse
Remote Interface IP Address	interne IP-Adresse der Gegenseite
Multicasts	Schaltet Multicast für den Tunnel: • **disabled** – Multicast in den Tunnel ist inaktiv. • **enabled** – Multicast in den Tunnel ist inaktiv.
Pre-shared Key	optionaler Wert für den Shared Key (32 bit) im numerischen Format. Wird vom Router für das Senden der gefilterten Daten durch den Tunnel verwendet. Geben Sie diesen Schlüssel auf beiden Router ein, da sonst die empfangene Pakete verwerfen werden.

Tabelle 40: Konfiguration – GRE-Tunnel

Hinweis! GRE-Tunnel können NAT nicht durchlaufen.

Die Änderungen gelten erst nach einem Klick auf die Schaltfläche *Apply*.

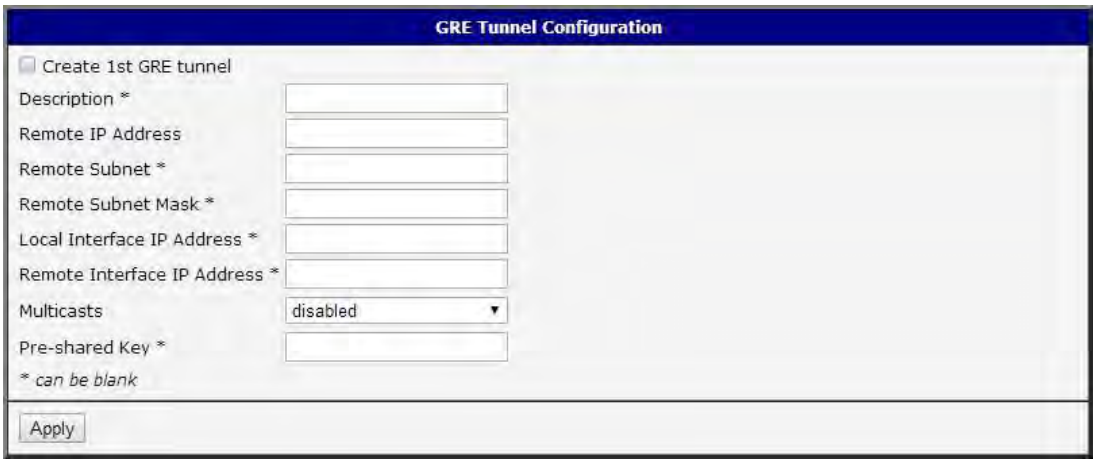


Abbildung 38: Konfiguration – GRE-Tunnel

3.12.1 Konfigurationsbeispiel GRE-Tunnel

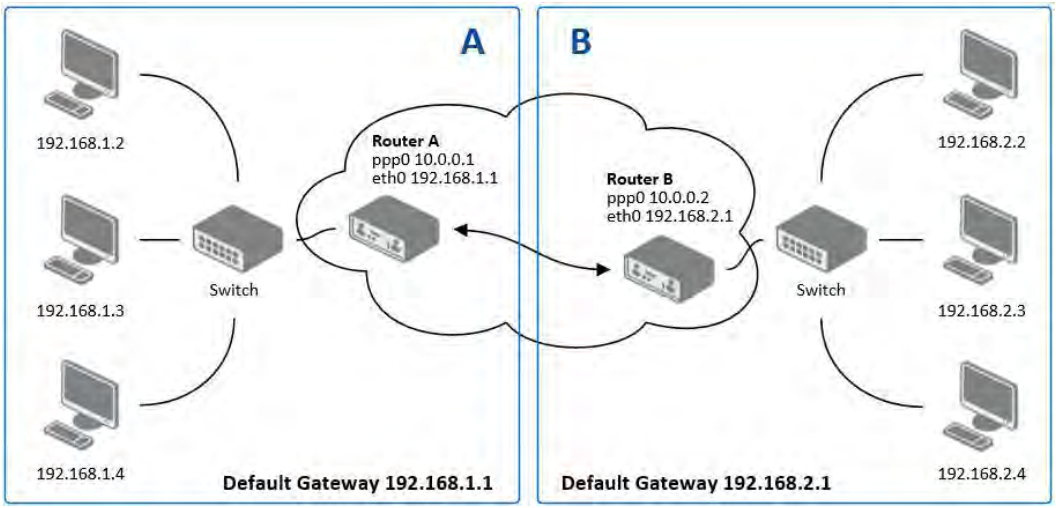


Abbildung 39: Beispieltopologie – GRE-Tunnel

Konfiguration GRE-Tunnel:

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

Tabelle 41: Beispielskonfiguration – GRE-Tunnel

Beispiele für die verschiedenen Optionen für Konfiguration eines GRE-Tunnels finden Sie im Dokument *GRE Tunnel* [7].

3.13 L2TP Tunnel Configuration

L2TP ist ein unverschlüsseltes Protokoll.

Die Funktion L2TP-Tunnel erlaubt die Einrichtung einer mit Passwort geschützten Verbindung zwischen zwei LANs.

Sie öffnen die Konfigurationsseiten für *L2TP Tunnel*, indem Sie in der Navigationsspalte auf den Menüpunkt *L2TP* klicken.

Element	Beschreibung
Mode	Modus des L2TP-Tunnel auf der Seite des Routers: • **L2TP server** – Router arbeitet als Server / *Client Start IP Address* und *Client End IP Address* erforderlich • **L2TP client** – Router arbeitet als Client / *Server IP Address* erforderlich.
Server IP Address	IP-Adresse des Server
Client Start IP Address	erste IP-Adresse des Adressbereichs (IP-Adressen für Clients)
Client End IP Address	letzte IP-Adresse des Adressbereichs
Local IP Address	lokale IP-Adresse
Remote IP Address	IP-Adresse der Gegenseite
Remote Subnet	IP-Adresse des Netzwerks hinter der Gegenseite
Remote Subnet Mask	Subnetzmaske des Netzwerks hinter der Gegenseite
Username	Benutzername für das Login des L2TP-Tunnels
Password	Passwort für das Login des L2TP-Tunnels

Tabelle 42: Konfiguration – L2TP-Tunnel

Die Änderungen gelten erst nach einem Klick auf die Schaltfläche *Apply*.

Abbildung 40: Konfiguration – L2TP-Tunnel

Die Tunnel sind aktiviert, wenn Sie die Option *Create L2TP tunnel* aktivieren.

3.13.1 Konfigurationsbeispiel L2TP-Tunnel

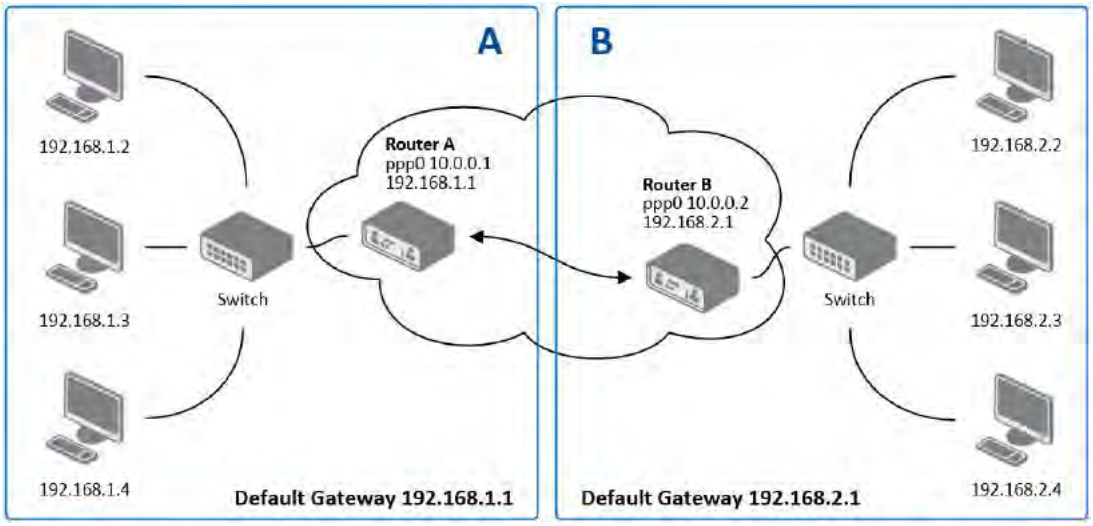


Abbildung 41: Beispieltopologie – L2TP-Tunnel

Konfiguration	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	—	10.0.0.1
Client Start IP Address	192.168.2.5	—
Client End IP Address	192.168.2.254	—
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	username	username
Password	password	password

Tabelle 43: Beispielkonfiguration – L2TP-Tunnel

3.14 PPTP Tunnel Configuration

PPTP ist ein unverschlüsseltes Protokoll.

Die Funktion PPTP-Tunnel erlaubt die Einrichtung einer mit Passwort geschützten Verbindung zwischen zwei LANs. PPTP ist ähnlich wie L2TP.

Sie öffnen die Konfigurationsseiten für *PPTP Tunnel*, indem Sie in der Navigationsspalte auf den Menüpunkt *PPTP* klicken.

Item	Description
Mode	Modus des PPTP-Tunnel auf der Seite des Routers: • **PPTP server** – Router arbeitet als Server / *Server IP Address* und *Local IP Address* erforderlich • **PPTP client** – Router arbeitet als Client / *Server IP Address* erforderlich.
Server IP Address	IP-Adresse des Server
Local IP Address	lokale IP-Adresse
Remote IP Address	IP-Adresse der Gegenseite
Remote Subnet	IP-Adresse des Netzwerks hinter der Gegenseite
Remote Subnet Mask	Subnetzmaske des Netzwerks hinter der Gegenseite
Username	Benutzername für das Login des PPTP-Tunnels
Password	Passwort für das Login des PPTP-Tunnels

Tabelle 44: Konfiguration – PPTP-Tunnel

Die Änderungen gelten erst nach einem Klick auf die Schaltfläche *Apply*.

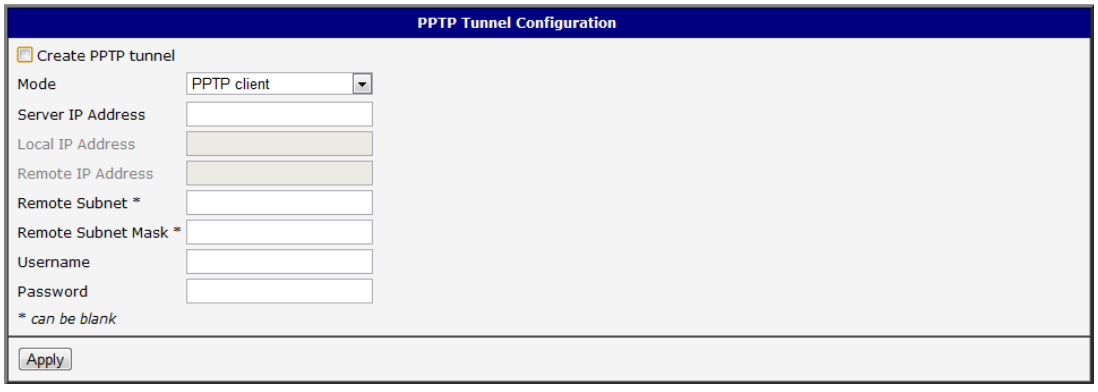


Abbildung 42: Konfiguration – PPTP-Tunnel

Die Tunnel sind aktiviert, wenn Sie die Option *Create PPTP tunnel* aktivieren.

Die Firmware unterstützt auch PPTP Passthrough. Sie können einen Tunnel durch den Router einrichten.

3.14.1 Beispielkonfiguration PPTP-Tunnel

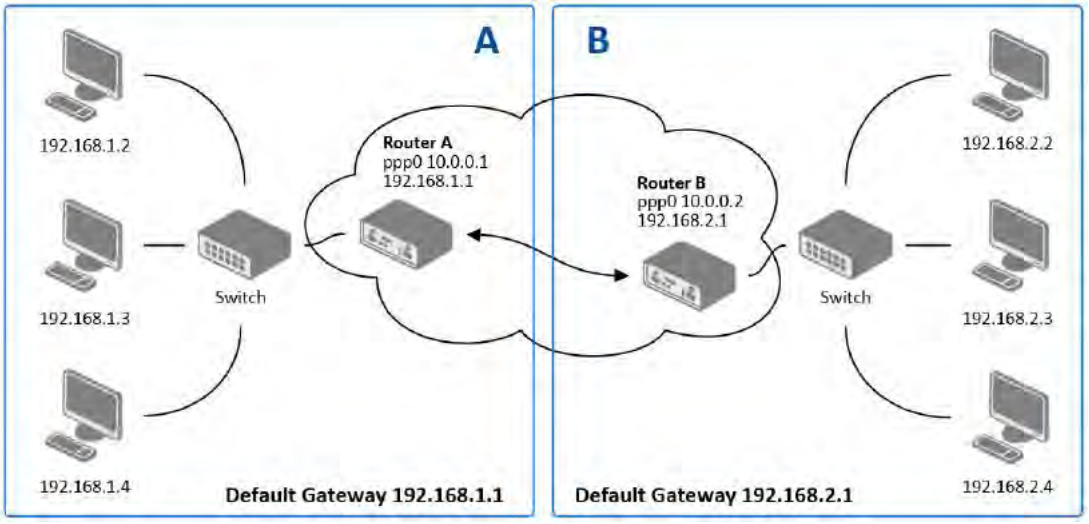


Abbildung 43: Beispieltopologie – PPTP-Tunnel

Konfiguration	A	B
Mode	PPTP Server	PPTP Client
Server IP Address	—	10.0.0.1
Local IP Address	192.168.1.1	—
Remote IP Address	192.168.2.1	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Tabelle 45: Beispielkonfiguration – PPTP-Tunnel

3.15 DynDNS Configuration

Die Funktion DynDNS erlaubt den Zugriff auf den Router über das Internet unter Verwendung eines einfach zu merkenden eigenen Hostnamens. Der DynDNS-Client überwacht die IP-Adresse des Routers und übernimmt deren Änderungen.

Für die Nutzung dieser Funktion benötigen Sie eine öffentliche IP-Adresse (statisch oder dynamisch) und ein Konto bei www.dyndns.org oder einem der in der Tabelle aufgeführten Dienstanbieter (siehe Element *Server*).

Registrieren Sie Ihre Domain (third-level) mit den notwendigen Kontoinformationen auf der Seite *DynDNS Configuration*.

Sie öffnen die Konfigurationsseiten für *OpenVPN tunnel*, indem Sie in der Navigationsspalte auf den Menüpunkt *DynDNS* klicken.

Element	Beschreibung
Hostname	Der Name der Third Level Doamin, registriert bei einem der genannten Dienstanbieter.
Username	Benutzername für das Einloggen auf dem Server.
Password	Passwort für das Einloggen auf dem Server.
Server	Server des DynDNS-Service-Anbieters; neben www.dyndns.org sind folgende Anbieter möglich: www.spdns.de, www.dnsdynamic.org, www.noip.com Tragen Sie die notwendigen Informationen ein. Lassen Sie dieses Feld leer, wird als Standard-Server *members.dyndns.org* verwendet.

Tabelle 46: Konfiguration – DynDNS

Konfigurationsbeispiel DynDNS-Client über company.dyndns.org

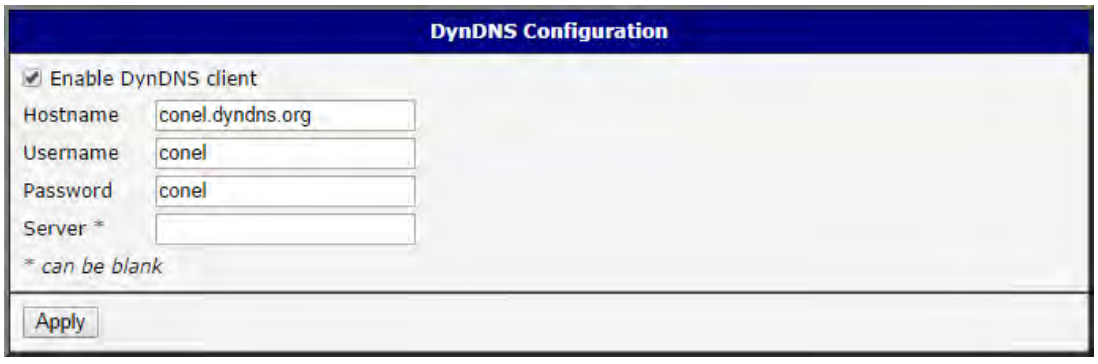


Abbildung 44: Beispielkonfiguration – DynDNS

Um auf die Konfiguration dieses Router zugreifen zu können, müssen Sie die Option *Enable remote HTTPS access on port* (im unteren Teil der Seite) aktiviert haben, siehe Kapitel 3.9.

3.16 NTP Configuration

Das Protokoll NTP (Network Time Protocol) dient der Synchronisation der internen Uhr des Routers mit eine Zeitquelle im Netzwerk oder Internet.

Sie öffnen die Konfigurationsseiten für *NTP*, indem Sie in der Navigationsspalte auf den Menüpunkt *NTP* klicken.

- Aktivieren Sie die Option *Enable local NTP service*, damit der Router selbst als NTP-Server im Netzwerk auftritt.
- Aktivieren Sie die Option *Synchronize clock with NTP server*, verhält sich der Router wie ein NTP-Client und synchronisiert seine interne Uhr alle 24 Stunden automatisch.

Element	Beschreibung
Primary NTP Server Address	IP-Adresse (IPv4 oder IPv6) oder Domain Namen des primären NTP-Servers
Secondary NTP Server Address	IP-Adresse (IPv4 oder IPv6) oder Domain Namen des sekundären NTP-Servers
Timezone	Zeitzone des Routers
Daylight Saving Time	Sommerzeitumstellung • **No** – Zeit wird nicht umgestellt. • **Yes** – Zeit wird umgestellt.

Tabelle 47: Konfiguration – NTP

Das folgende Beispiel zeigt eine NTP-Konfiguration mit *ntp.cesnet.cz* als primären und *tik.cesnet.cz* als sekundären Zeitserver sowie der automatischen Umstellung auf die Sommerzeit.

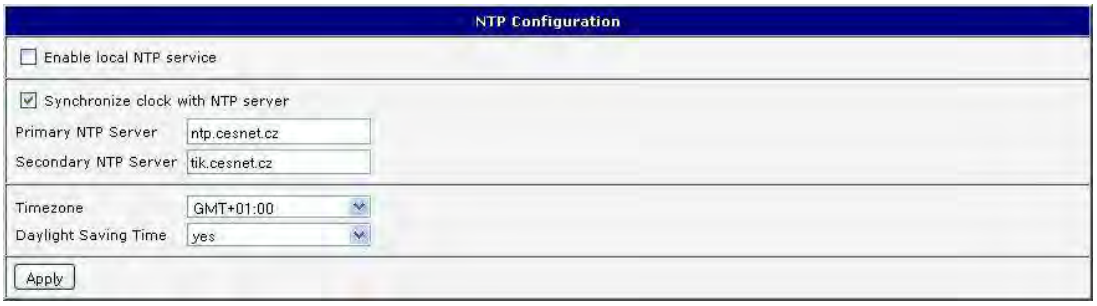


Abbildung 45: Beispielskonfiguration – NTP

3.17 SNMP Configuration

Ein SNMP (Simple Network Management Protocol) v1/v2 oder v3-Agent sendet Statusinformationen des Routers und seiner Erweiterungen an eine Management-Station. In der Version v3 ist die Kommunikation verschlüsselt. Das Senden von SNMP-Traps an IPv6-Adressen wird unterstützt.

Öffnen Sie die Konfigurationsseite für das Simple Network Management Protokoll, indem Sie in der Navigationsspalte auf den Menüpunkt *SNMP* klicken.

Um den SNMP-Dienst einzuschalten, aktivieren Sie die Option *Enable the SNMP agent*.

Element	Beschreibung
Name	Name des Routers
Location	Standort des Routers
Contact	Kontaktonformationen über die Person, die den Router verwaltet

Tabelle 48: Konfiguration – SNMP-Agent

Um die SNMP-Funktionen einzuschalten, aktivieren Sie die Option *Enable SNMPv1/v2 access*. Legen Sie ein Passwort für den Zugriff auf den SNMP-Agenten *Community* fest. Das Standardpasswort ist: *public*.

Für die SNMP-Agenten *Read* (Nur lesen) und *Write* (Lesen und Schreiben) können Sie verschiedene Passworte vergeben.

Sie können auch 2 SNMP-Agenten für SNMPv3 anlegen: *Read* und *Write* und bearbeiten die folgenden Parameter bearbeiten.

Der Router verwendet diese Parameter nur für den SNMP-Zugang.

Um die SNMP-Funktionen v3 einzuschalten, aktivieren Sie die Option *Enable SNMPv3 access*.

Element	Beschreibung
Username	Benutzername
Authentication	Verschlüsselungsalgorithmus für den Authentifizierung des Benutzers
Authentication Password	dazugehöriges Passwort
Privacy	Verschlüsselungsalgorithmus für die Datensicherheit
Privacy Password	dazugehöriges Passwort

Tabelle 49: Konfiguration – SNMPv3

Zusätzlich können Sie noch folgende Einstellungen vornehmen:

- Um die binären Eingänge des Routers zu überwachen, aktivieren Sie die Option *Enable I/O extension*.
- Um den Erweiterungs-Port *CNT* (Ein- und Ausgänge) zu überwachen, aktivieren Sie die Option *Enable XC-CNT extension*.
- Um den Erweiterungs-Port *MBUS* zu überwachen, aktivieren Sie die Option *Enable M-BUS extension*. Tragen Sie Werte für *Baudrate*, *Parity* und *Stop Bits* ein.

Element	Beschreibung
Baudrate	Kommunikationsgeschwindigkeit
Parity	Kontrollprüfbit: • **none** – Daten werden ohne Parität versandt. • **even** – Daten werden mit gerader Parität versandt. • **odd** – Daten werden mit ungerader Parität versandt.
Stop Bits	Anzahl der Stop Bits

Tabelle 50: Konfiguration – SNMP – MBUS

Die Optionen *Enable XC-CNT extension* und *Enable M-BUS extension* können nicht gleichzeitig aktiviert sein.

Um statistische Daten an das Monitoring-System R-SeeNet zu senden, aktivieren Sie die Option *Enable reporting to supervisory system*. Ergänzen Sie die *IP-Adresse* des Systems und den *Zeitraum* der Überwachung (in Minuten).

Element	Beschreibung
IP Address	IP-Adresse
Period	Zeitraum für das Senden der statistischen Daten (in Minuten)

Tabelle 51: Konfiguration – SNMP – R-SeeNet

Jeder Monitor hat eine eindeutige numerische Kennnung *OID – Object Identifier*.

Die OIDs bestehen aus einer durch einen Punkt getrennte Folgen von Zahlen. Jeder OID stellt einen Knoten in einem hierarchisch zugewiesenen Namensraum dar, siehe Abbildung. Der Wert eines OIDs wird durch die Kennung des Elternelement bestimmt, ergänzt um einen Punkt und die laufende Nummer.

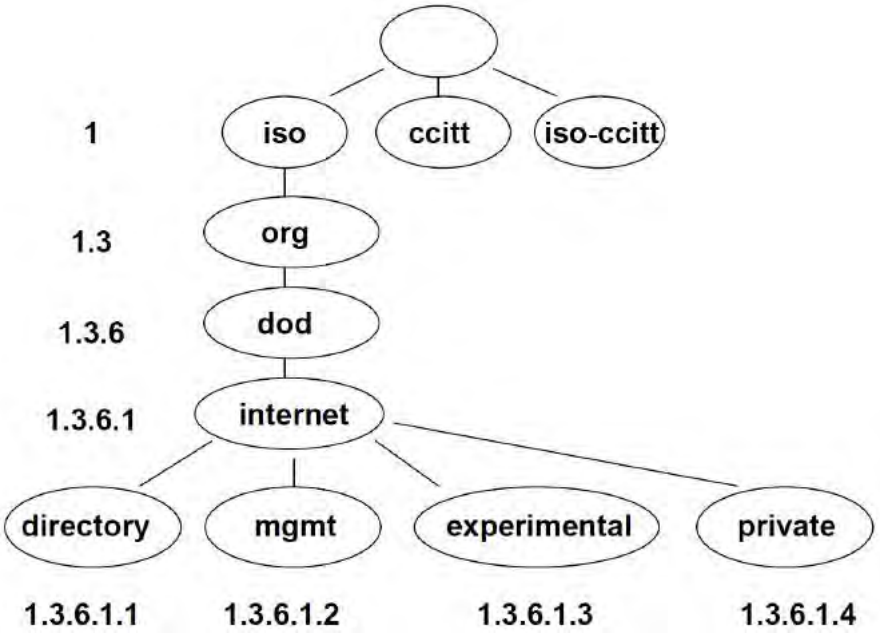


Abbildung 46: Basisstruktur OID

Die SNMP-Werte der Router starten mit OID = .1.3.6.1.4.1.30140. Gemäß OID-IRI-Notation wird daraus:

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

Der Router stellt Informationen über die interne Temperatur (OID 1.3.6.1.4.1.248.40.1.3.3) oder über die Versorgungsspannung (OID 1.3.6.1.4.1.248.40.1.3.4) bereit. Für die binären Ein- und Ausgänge wird folgender OID-Bereich verwendet:

OID	Beschreibung
.1.3.6.1.4.1.30140.2.3.1.0	Binärer Eingang BIN0 (values 0,1)
.1.3.6.1.4.1.30140.2.3.2.0	Binärer Ausgang OUT0 (values 0,1)

Tabelle 52: Objektkennung – Binäre Ein- und Ausgänge

Für den Erweiterungs-Port *CNT* wird folgender OID-Bereich verwendet:

OID	Beschreibung
.1.3.6.1.4.1.30140.2.1.1.0	Analoger Eingang AN1 (Bereich 0-4095)
.1.3.6.1.4.1.30140.2.1.2.0	Analoger Eingang AN2 (Bereich 0-4095)
.1.3.6.1.4.1.30140.2.1.3.0	Zählereingang CNT1 (Bereich 0-4294967295)
.1.3.6.1.4.1.30140.2.1.4.0	Zählereingang CNT2 (Bereich 0-4294967295)
.1.3.6.1.4.1.30140.2.1.5.0	Binärer Eingang BIN1 (Werte 0,1)
.1.3.6.1.4.1.30140.2.1.6.0	Binärer Eingang BIN2 (Werte 0,1)
.1.3.6.1.4.1.30140.2.1.7.0	Binärer Eingang BIN3 (Werte 0,1)
.1.3.6.1.4.1.30140.2.1.8.0	Binärer Eingang BIN4 (Werte 0,1)
.1.3.6.1.4.1.30140.2.1.9.0	Binärer Ausgang OUT1 (Werte 0,1)

Tabelle 53: Objektkennung – Erweiterungs-Port *CNT*

Für den Erweiterungs-Port *M-BUS* wird folgender OID-Bereich verwendet:

OID	Beschreibung
.1.3.6.1.4.1.30140.2.2.<Adresse>.1.0	IdNumber – Nummer des Messgeräts
.1.3.6.1.4.1.30140.2.2.<Adresse>.2.0	Manufacturer – Hersteller
.1.3.6.1.4.1.30140.2.2.<Adresse>.3.0	Version – Version des Messgeräts
.1.3.6.1.4.1.30140.2.2.<Adresse>.4.0	Medium – Typ des gemessenen Mediums
.1.3.6.1.4.1.30140.2.2.<Adresse>.5.0	Status – Meldungen der Fehlerzustände
.1.3.6.1.4.1.30140.2.2.<Adresse>.6.0	0. VIF – Informationsfeld mit Wert
.1.3.6.1.4.1.30140.2.2.<Adresse>.7.0	0. gemessener Wert
.1.3.6.1.4.1.30140.2.2.<Adresse>.8.0	1. VIF – Informationsfeld mit Wert
.1.3.6.1.4.1.30140.2.2.<Adresse>.9.0	1. gemessener Wert
.1.3.6.1.4.1.30140.2.2.<Adresse>.10.0	2. VIF – Informationsfeld mit Wert
.1.3.6.1.4.1.30140.2.2.<Adresse>.11.0	2. gemessener Wert
⋮	⋮
.1.3.6.1.4.1.30140.2.2.<address>.100.0	47. VIF – Informationsfeld mit Wert
.1.3.6.1.4.1.30140.2.2.<address>.101.0	47. gemessener Wert

Tabelle 54: Objektkennung – Erweiterungs-Port *M-BUS*

Die Adresse des Messgerätes kann aus dem Bereich 0..254 sein, wobei 254 Broadcast ist.

Seit Firmware 3.0.4 zeigen alle v2 Router (mit RB-v2-6 und neuer) Informationen über die Netzspannung (OID 1.3.6.1.4.1.30140.3.4) und die interne Temperatur des Gerätes (OID 1.3.6.1.4.1.30140.3.3).

Beispiele für verfügbare und unterstützte OIDs und andere Details finden Sie im Dokument *SNMP Object Identifier* [8].

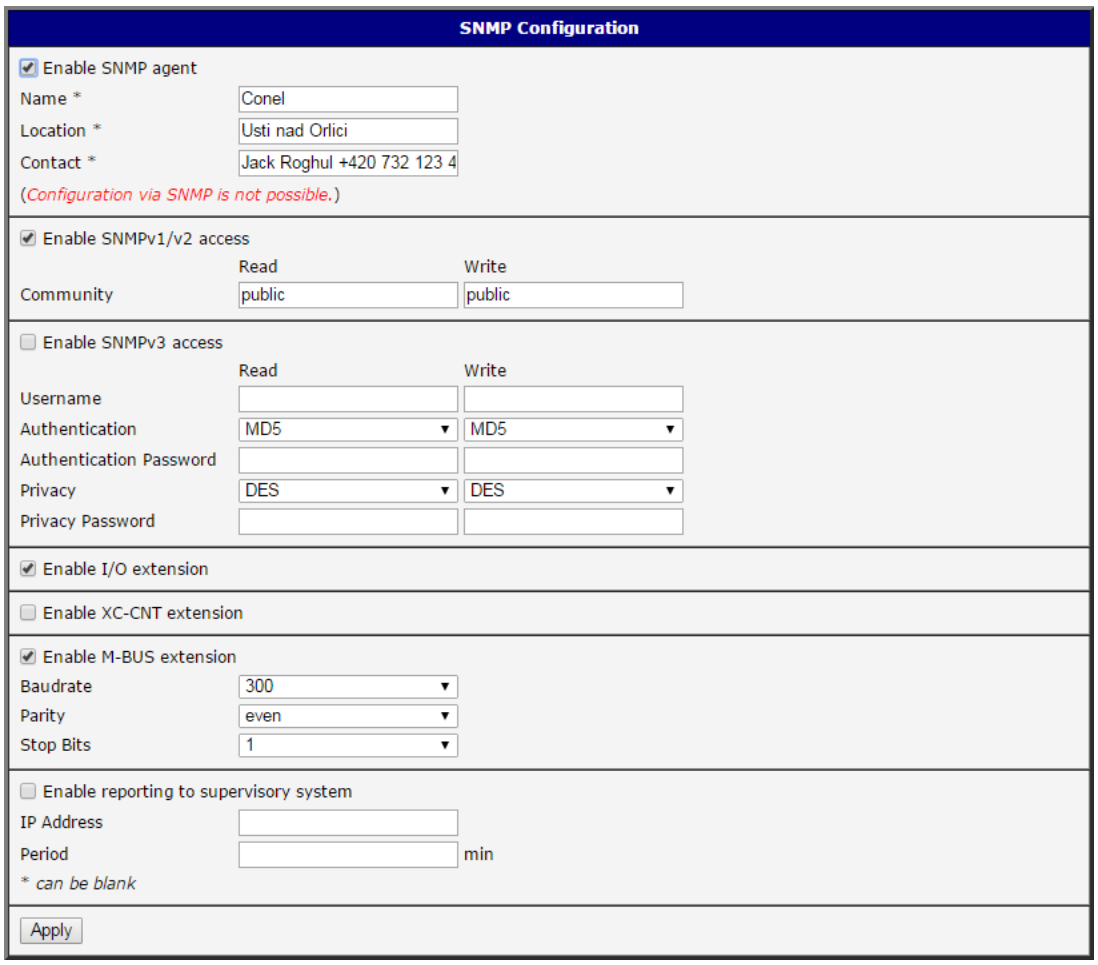


Abbildung 47: Beispielskonfiguration – SNMP

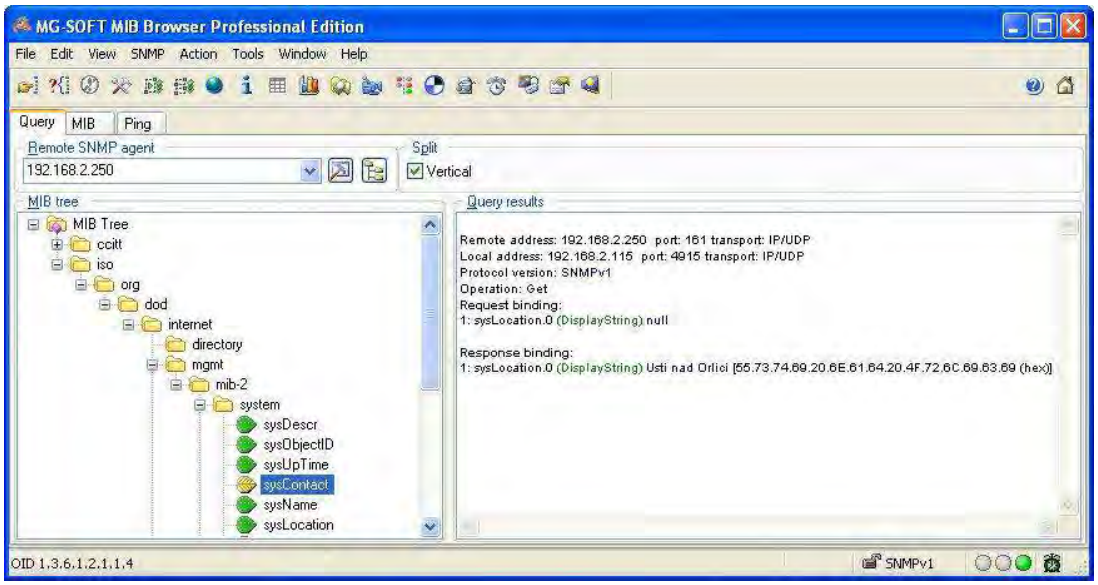


Abbildung 48: Beispiel – MIB-Browser

Es ist wichtig, die IP-Adresse des SNMP-Agenten (Router) im Feld *Remote SNMP agent* einzustellen. Nach der Eingabe der IP-Adresse ist es im Teil MIB tree möglich, die internen Variablen anzuzeigen. Weiter kann der Status der internen Variablen durch Eingabe deren OIDs festgestellt werden.

Der Pfad zu den Variablen ist:

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

Der Pfad zu den Grundangaben des Routers ist:

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

3.18 SMTP Configuration

Öffnen Sie die Konfigurationsseite für den Simple Mail Transfer Protocol-Client (SMTP), indem Sie in der Navigationsspalte auf den Menüpunkt *SMTP* klicken.

Element	Beschreibung
SMTP Server Address	IP-Adresse oder Domain Name des Mail-Servers
SMTP Port	Port des SMTP-Servers
Secure Method	*none*, *SSL/TLS*, oder *STARTTLS*. Die sichere Methode muss vom SMTP-Server unterstützt werden.
Username	Name des E-Mail-Kontos
Password	dazugehöriges Passwort. Das Passwort kann folgende Spezialzeichen beinhalten: * + , - . / : = ? ! # % [ ] _ { } ~ Die folgenden Spezialzeichen sind nicht erlaubt: ” $ & ’ ( ) ; < >
Own E-mail Address	Absendeadresse

Tabelle 55: Konfiguration SMTP-Client

Der Mobilfunk-Service-Provider kann andere SMTP-Server blockieren, in diesem Fall können Sie nur den SMTP-Server des Providers verwenden.

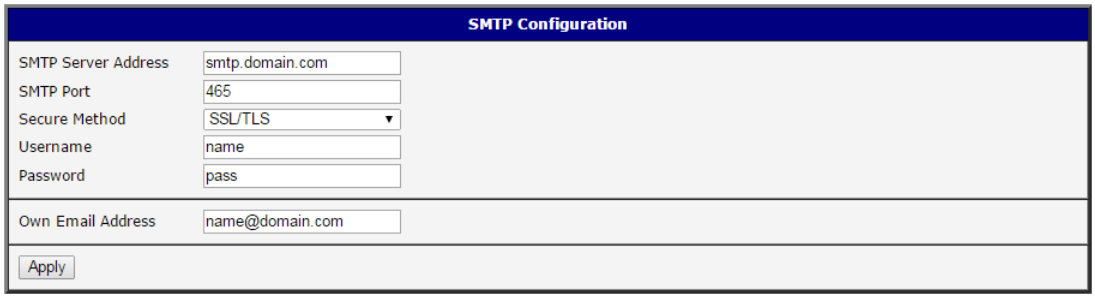


Abbildung 49: Konfigurationsbeispiel SMTP-Client

Sie können E-Mails auch über das Startup-Skript versenden. Öffnen Sie dazu den Konfigurationsseite *Startup Script*, indem Sie in der Navigationsspalte auf den Menüpunkt *Scripts* klicken. Sie können E-Mails auch über eine SSH-Verbindung versenden. Das E-Mail-Kommando kennt folgende Parameter:

-t	E-Mail-Adresse des Empfängers	-s	Betreffzeile: Text in Anführungszeichen
-a	angehängte Datei(en)	-m	Textkörper der Nachricht:
-r	Anzahl der Sendeversuche (Standard: 2)		Text in Anführungszeichen

Kommandos und Parameter können **nur** als Kleinbuchstaben eingegeben werden.

Beispiel

email -t name@domain.com -s ”subject” -m ”message” -a c:\directory\abc.doc -r 5

Das obige Kommando versendet an die Adresse *name@domain.com* eine E-Mail mit dem Betreff *”subject”*, dem Textkörper *”message”* und der angehängten Datei *abc.doc* aus dem Verzeichnis *c:\directory*.

3.19 SMS Configuration

Für der Industrie-Router XR5i v2 wird die Konfigurationsseite *SMS Configuration* nicht agezeigt.

Öffnen Sie die Konfigurationsseite für *SMS*, indem Sie in der Navigationsspalte auf den Menüpunkt *SMS* klicken.

Legen Sie nun die Ereignisse fest, wegen denen eine SMS-Nachricht gesendet werden soll.

Element	Beschreibung
Send SMS on power up	Automatischer SMS-Versand nach dem Einschalten der Stromversorgung.
Send SMS on connect to mobile network	Automatischer SMS-Versand beim Start der Verbindung zum Mobilfunknetz.
Send SMS on disconnect to mobile network	Automatischer SMS-Versand beim Beenden der Verbindung zum Mobilfunknetz.
Send SMS when datalimit exceeded	Automatischer SMS-Versand beim Überschreiten des Datenlimits.
Send SMS when binary input on I/O port (BIN0) is active	Automatischer SMS-Versand, wenn binärer Eingang BIN0 aktiv ist. Der Text wird durch den Parameter *BIN0 –SMS* (siehe unten) festgelegt.
Send SMS when binary input on expansion port (BIN1 – BIN4) is active	Automatischer SMS-Versand, wenn binäre Eingänge BIN1 bis BIN4 (Erweiterungs-Port) aktiv ist. Der Text wird durch die Parameter *BINX – SMS* (siehe unten) festgelegt.
Add timestamp to SMS	Fügt einen Zeitstempel in die gesendeten SMS ein. Der Zeitstempel hat das 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	Name des Routers, der in der SMS verschickt wird.
BIN0 – SMS	Text der SMS-Nachricht bei Aktivierung des binären Eingangs BIN0 zum Router.

Fortsetzung auf der nächsten Seite

Fortsetzung von der vorherigen Seite

Element	Beschreibung
BIN1 – SMS	Text der SMS-Nachricht bei Aktivierung des binären Eingangs BIN1 auf dem Erweiterungs-Port.
BIN2 – SMS	Text der SMS-Nachricht bei Aktivierung des binären Eingangs BIN2 auf dem Erweiterungs-Port.
BIN3 – SMS	Text der SMS-Nachricht bei Aktivierung des binären Eingangs BIN3 auf dem Erweiterungs-Port.
BIN4 – SMS	Text der SMS-Nachricht bei Aktivierung des binären Eingangs BIN4 auf dem Erweiterungs-Port.

Tabelle 56: Konfiguration SMS

Nachdem Sie im Feld *Phone Number 1* eine Telefonnummer eingetragen haben, können Sie die weitere Konfiguration vornehmen. Sie können bis zu 3 Telefonnummern eintragen, von denen der Router SMS-Nachrichten entgegen nimmt. Dazu aktivieren Sie die Option *Enable remote control via SMS*. Damit sind die Standardeinstellung der Kontrolle des Routers per SMS aktiviert. **Hinweis:** Jede empfangene Kontroll-SMS wird verarbeitet und dann gelöscht.

Element	Beschreibung
Phone Number 1 Phone Number 2 Phone Number 3	Es können bis zu drei Telefonnummern eingestellt werden, von denen der Router SMS-Nachrichten entgegen nimmt.

Tabelle 57: Kontrolle per SMS

- Tragen Sie im Feld *Phone Number* nichts, können Sie den Router über eine Reboot-Nachricht per SMS von einer beliebigen Nummer neu starten.
- Tragen Sie mindestens eine Telefonnummer ein, können Sie den Router nur von den eingetragenen Nummern per SMS kontrollieren.
- Tragen Sie im Feld *Phone Number* den Platzhalter $*$ ein, können Sie den Router per SMS von einer beliebigen Nummer kontrollieren.

Kontroll-SMS ändern nichts an der Konfiguration des Routers. Wurde der Router z. B. per SMS *Off line* geschaltet, bleibt er in diesem Modus. Damit der Router wird *On line* geht, müssen Sie ihn rebooten oder die Stromversorgung des Gerätes wiederherstellen. Dieses Verhalten ist bei allen Kontroll-SMS gleich.

Für die Kontrolle des Routers per SMS senden Sie als Nachrichtentext nur das Kontrollkommando.

SMS	Beschreibung
go online sim 1	Umschaltung auf erste SIM-Karte
go online sim 2	Umschaltung auf zweite SIM-Karte
go online	Der Router wird in den Online-Modus umgeschaltet.
go offline	Der Router wird in den Offline-Modus umgeschaltet.
set out0=0	Stellt den binären Ausgang des I/O-Konnektors auf 0
set out0=1	Stellt den binären Ausgang des I/O-Konnektors auf 1
set out1=0	Stellt den binären Ausgang von XC-CNT auf 0
set out1=1	Stellt den binären Ausgang von XC-CNT auf 1
set profile std	Umstellen des Profils auf das Standardprofil
set profile alt1	Umstellen des Profils auf das alternative Profil 1
set profile alt2	Umstellen des Profils auf das alternative Profil 2
set profile alt3	Umstellen des Profils auf das alternative Profil 3
reboot	Router rebooten
get ip	Sendet als Antwort IP-Adresse der SIM-Karte

Tabelle 58: SMS-Kontrollnachricht

Aktivieren Sie die Option *Enable AT-SMS protocol on expansion port 1* und tragen Sie einen Wert für *Baudrate* ein, damit der Router auch über die serielle Schnittstelle Port 1 Nachrichten senden oder empfangen kann.

Element	Beschreibung
Baudrate	Kommunikationsgeschwindigkeit für Erweiterungs-Port 1

Tabelle 59: SMS über serielle Schnittstelle Port 1

Aktivieren Sie die Option *Enable AT-SMS protocol on expansion port 2* und tragen Sie einen Wert für *Baudrate* ein, damit der Router auch über die serielle Schnittstelle Port 2 Nachrichten senden oder empfangen kann.

Element	Beschreibung
Baudrate	Kommunikationsgeschwindigkeit für Erweiterungs-Port 2

Tabelle 60: SMS über serielle Schnittstelle Port 2

Aktivieren Sie die Option *Enable AT-SMS protocol over TCP* und tragen Sie einen Wert für *TCP Port* ein, damit der Router auch über die Netzwerk-Schnittstelle Nachrichten senden oder empfangen kann. Der Router sendet die SMS-Nachrichten im Standard-AT-Forma

Element	Beschreibung
TCP Port	TCP-Port über den SMS-Nachrichten gesendet oder empfangen werden

Tabelle 61: SMS über Ethernet PORT1 senden

3.19.1 SMS senden

Wenn eine Verbindung zum Router über eine serielle Schnittstelle oder das Ethernet besteht, können Sie AT-Kommandos zur Verwaltung der SMS-Nachrichten verwenden.

3.19.2 AT-Kommandos

Die folgende Liste zeigt alle vom Router unterstützten AT-Kommandos. Andere AT-Kommandos beantwortet der Router mit *OK*; komplexe AT-Kommandos mit *ERROR*.

AT-Kommando	Beschreibung
AT+CGMI	Fragt den Herstellers ab
AT+CGMM	Fragt das Modells ab
AT+CGMR	Fragt Revisionsinformationen des Modells ab
AT+CGPADDR	Fragt die IP-Adresse der usb0-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 Speicher 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-Speichertyp, der für den SMS-Betrieb verwendet wird
AT+CREG	Zeigt den Status der Netzwerkregistrierung an
AT+CSCA	Stellt die Telefonnummer des SMS-Service-Centers ein
AT+CSCS	Wählt den Zeichensatz
AT+CSQ	Gibt die Signalstärke des registrierten Netzwerks aus
AT+GMI	Fragt den Herstellers ab
AT+GMM	Fragt das Modell ab
AT+GMR	Fragt Revisionsinformationen des Modells ab
AT+GSN	Fragt die Seriennummer des Produktes ab
ATE	Empfangene Zeichen wiederholen oder nicht (Echo)
ATI	Überträgt die herstellerspezifischen Informationen über das Gerät

Tabelle 62: Liste der AT-Kommandos

Eine detaillierte Beschreibung und Beispiele für diese AT-Befehle finden Sie im Dokument *AT commands* [9].

Beispiel 1: Konfiguration für SMS senden

Nachdem der Router hochgefahren ist, wird an die angegebene Telefonnummer eine Nachricht im folgenden Format gesendet:

Router (Unit ID) has been powered up. Signal strength xx dBm.

Nachdem die Verbindung in das Mobilfunknetzwerk hergestellt wurde, wird folgende Nachricht gesendet:

Router (Unit ID) has established connection to mobile network. IP address xxx.xxx.xxx.xxx

Wird die Verbindung ins Mobilfunknetzwerk beendet, wird folgende Nachricht gesendet:

Router (Unit ID) has lost connection to mobile network. IP address xxx.xxx.xxx.xxx

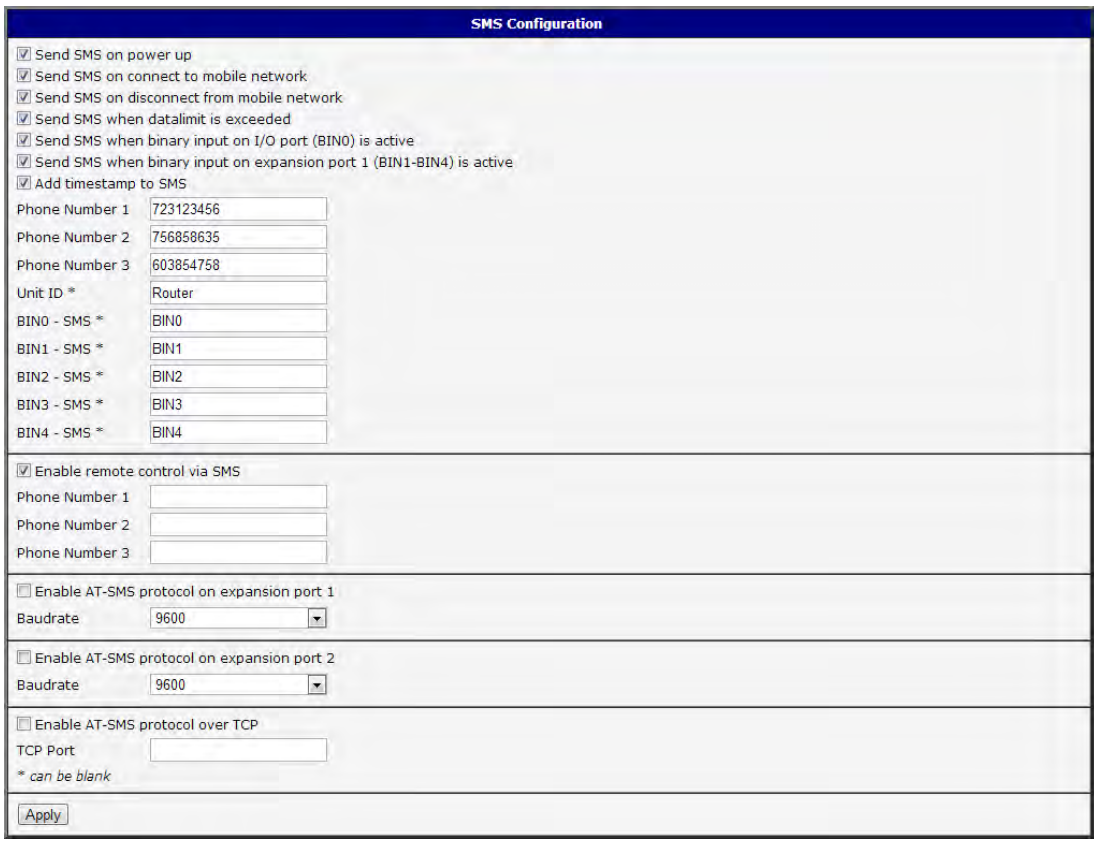


Abbildung 50: Beispielkonfiguration 1 – SMS

Beispiel 2: SMS über die serielle Schnittstelle auf Port 1 senden

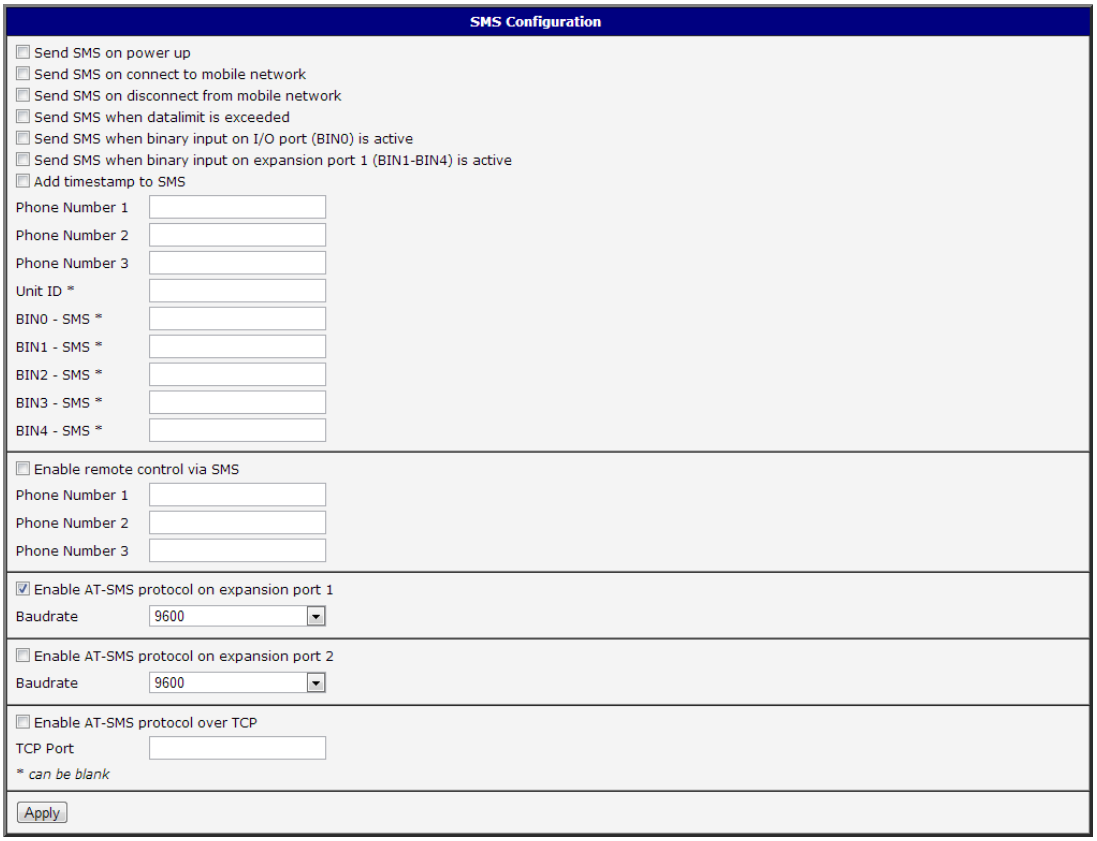


Abbildung 51: Beispielkonfiguration 2 – SMS

Beispiel 3: Kontrolle des Routers über SMS von einer beliebigen Telefonnummer aus

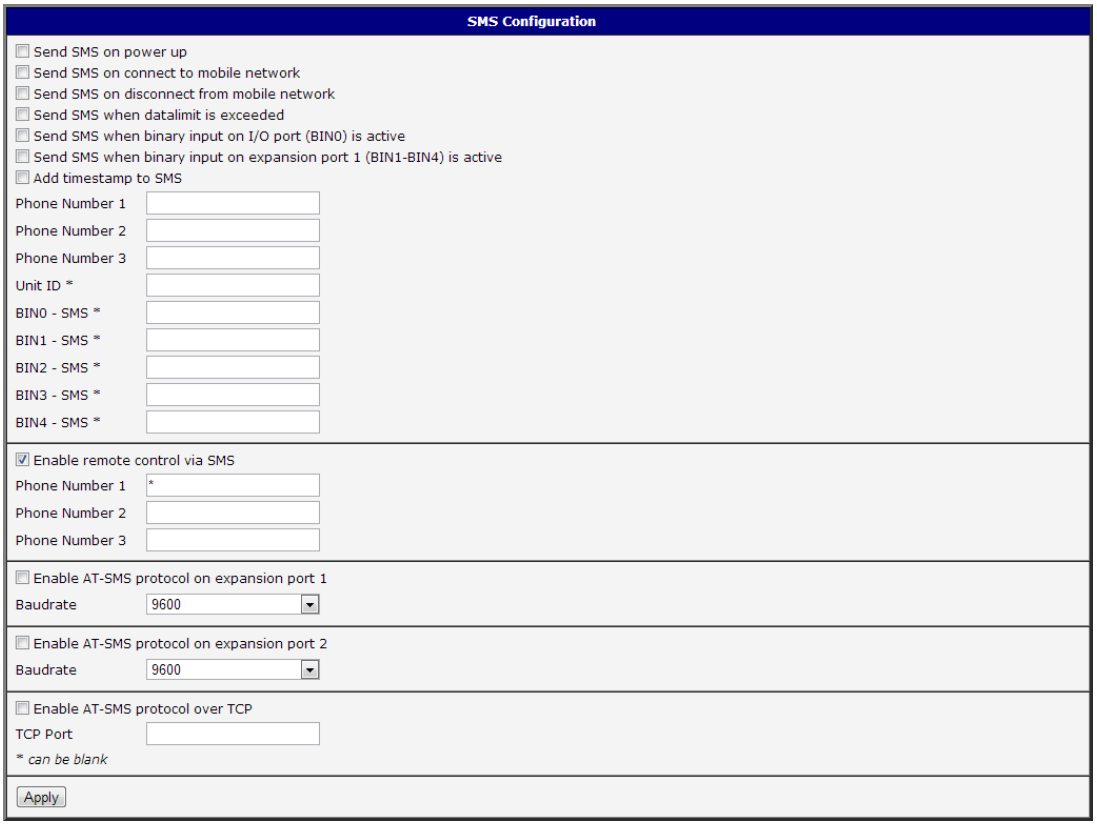


Abbildung 52: Beispielkonfiguration 3 – SMS

Beispiel 4: Kontrolle des Routers über SMS von 2 Telefonnumnern aus

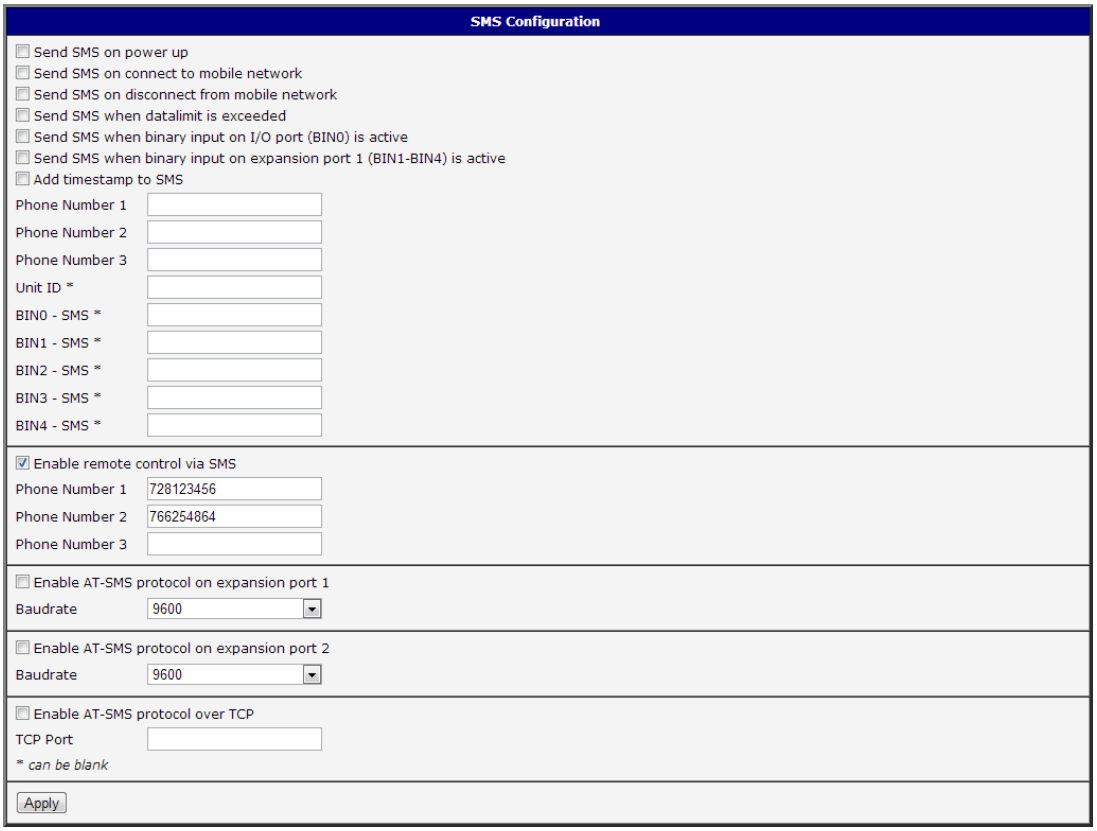


Abbildung 53: Beispielkonfiguration 4 – SMS

3.20 Expansion Port Configuration

Öffnen Sie die Konfigurationsseite für *Expansion Ports*, indem Sie in der Navigationsspalte auf den Menüpunkt *Expansion Port 1* bzw. *Expansion Port 2* klicken.

Aktivieren Sie die Option *Enable expansion port 1/2 access over TCP/UDP* und wählen Sie den *Port Type* entsprechend dem installierten Erweiterungs-Ports.

Element	Beschreibung
Baudrate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Kontroll-Paritätsbit: • none – Daten werden ohne Parität versandt. • even – Daten werden mit gerade Parität versandt. • odd – Daten werden mit ungerade Parität versandt.
Stop Bits	Anzahl der Stoppbits
Split Timeout	Split Timeout stellt die Zeit für die Zerteilung der Nachricht ein. Wird beim Empfang eine Lücke zwischen zwei Zeichen erkannt, die länger als der Wert des Parameters in Millisekunden ist, wird der Empfang als fehlerhaft angezeigt und es folgt der Anfang der nächsten Nachricht gesucht.
Protocol	Protokoll: • TCP – Kommunikation TCP (verbindungsorientiert) • UDP – Kommunikation UDP (verbindungslos)
Mode	Kommunikationsmodus: • TCP server – Der Router empfängt ankommende Befehle am eingegebenen Port. • TCP client – Der Router verbindet sich mit der eingegebenen Server-Adresse am eingegebenen Port.
Server Address	Im Modus *TCP client* ist es notwendig, die Server-Adresse einzugeben.
TCP Port	TCP-/UDP-Port für die Kommunikation
Inactivity Timeout	Zeitspanne nach der die TCP-/UDP-Verbindung im Fall von Inaktivität unterbrochen wird.

Tabelle 63: Konfiguration – Serielle Schnittstellen – 1

Aktivieren Sie die Option *Reject new connections*, dann lehnt der Router jeden weiteren (zusätzlichen) Verbindungsaufbau ab. Der Router unterstützt dann keine Mehrfachverbindungen mehr.

Aktivieren Sie die Option *Check TCP connection*, wird der Aufbau der TCP-Verbindung überprüft.

Element	Beschreibung
Keepalive Time	Zeitdauer, während der das Bestehen der Verbindung überwacht wird
Keepalive Interval	Zeitdauer, während der auf eine Antwort gewartet wird
Keepalive Probes	Anzahl der Versuche

Tabelle 64: Konfiguration – Erweiterungs-Port – 2

Aktivieren Sie die Option *Use CD as indicator of the TCP connection*, verwendet der Router das CD-Signal (DTR auf Seiten des Routers), um den Status der TCP-Verbindung zu überprüfen. Das CD-Signal prüft nach, ob auf der Gegenseite das Kabel eingesteckt ist.

CD	Beschreibung
Active	TCP-Verbindung wurde aufgebaut
Nonactive	TCP-Verbindung wurde nicht aufgebaut

Tabelle 65: Verbindungsüberprüfung mit CD-Signal

Aktivieren Sie die Option *Use DTR as control of TCP connection*, verwendet der Router das DTR-Signal (Data Terminal Ready) um den Status der TCP-Verbindung zu überprüfen. Die Gegenstelle sendet ein DTR-Signal, welches dem Router anzeigt, dass die Gegenstelle für die Kommunikation bereit ist.

DTR	Verhalten des Servers	Verhalten des Clients
Active	Der Router erlaubt den Aufbau der TCP-Verbindung.	Der Router baut die TCP-Verbindung auf.
Nonactive	Der Router erlaubt den Aufbau der TCP-Verbindung nicht.	Der Router trennt die TCP-Verbindung.

Tabelle 66: Verbindungsüberprüfung mit DTR-Signal

Die Änderungen gelten erst nach einem Klick auf die Schaltfläche *Apply*.

Seit Firmware 3.0.9 verfügen alle v2 Router über das Programm getty. Über dieses Programm können Sie eine Verbindung zum Router über eine serielles Kabel herstellen, vorausgesetzt, der Router ist mit dem Erweiterung-Port RS232 ausgerüstet.

Das Programm Getty zeigt eine Anmeldezeilen an. Geben Sie den Benutzernamen ein und anschließend, nach Aufforderung, das Passwort. Getty verifiziert die eingegebenen Daten, meldet Sie an und zeigt dann eine Kommandozeile. Sie können nun, entsprechend einer Verbindung über Telnet, das System verwalten.

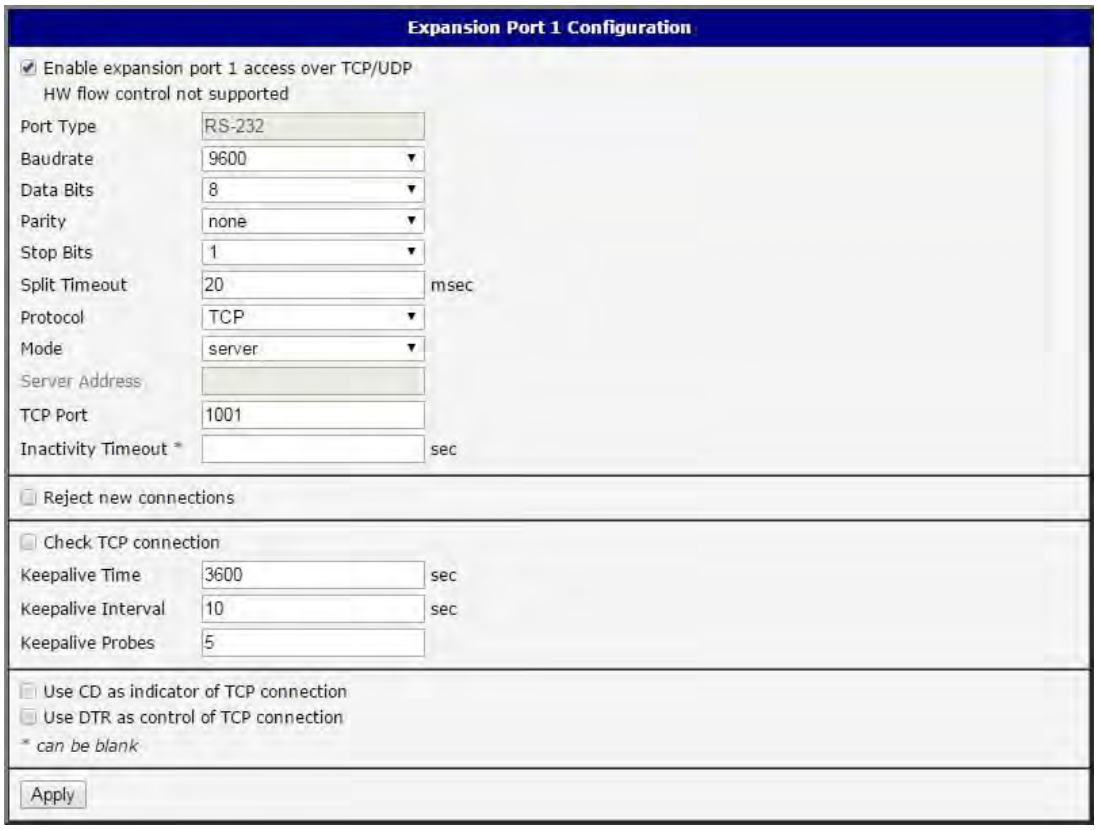


Abbildung 54: Konfiguration – Erweiterungs-Port

Konfigurationsbeispiele für Erweiterungs-Port

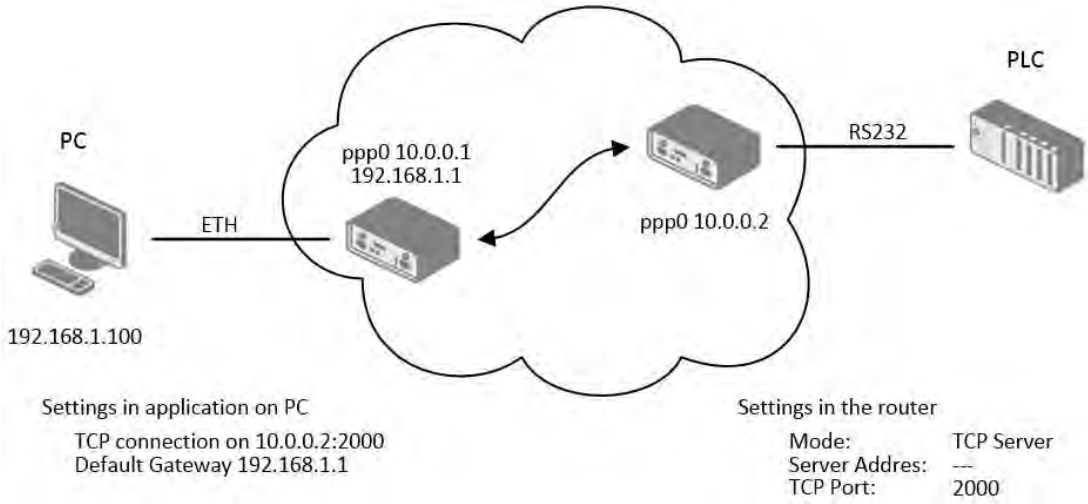


Abbildung 55: Beispiel: Kommunikation Ethernet zu Seriell

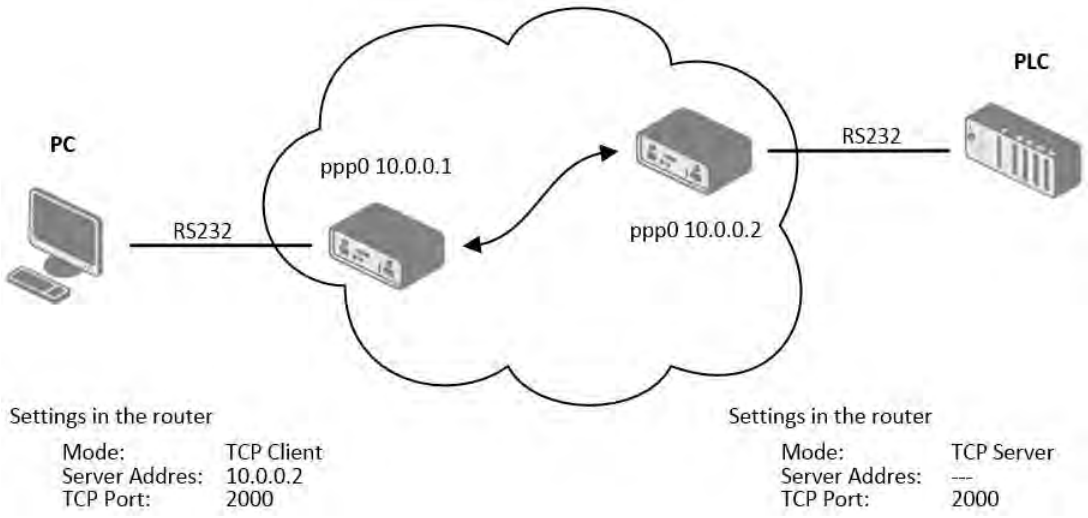


Abbildung 56: Beispiel für seriellen Erweiterungs-Port

3.21 USB Port Configuration

Sie können einen USB-zu-RS232-Konverter zum Versenden von Daten aus der seriellen Schnittstelle ins Ethernet verwenden, analog zum Verhalten des Erweiterungs-Port RS232.

Öffnen Sie die Konfigurationsseite *USB Port*, indem Sie in der Navigationsspalte auf den Menüpunkt *USB Port* klicken.

Element	Beschreibung
Baudrate	Geschwindigkeit der Kommunikation
Data Bits	Anzahl der Datenbits
Parity	Kontroll-Paritätsbit: • none – Daten werden ohne Parität versandt. • even – Daten werden mit gerader Parität versandt. • odd – Daten werden mit ungerader Parität versandt.
Stop Bits	Anzahl der Stoppbits
Split Timeout	Split Timeout stellt die Zeit für die Zerteilung der Nachricht ein. Wird beim Empfang eine Lücke zwischen zwei Zeichen erkannt, die länger als der Wert des Parameters in Millisekunden ist, wird der Empfang als fehlerhaft angezeigt und es folgt das Aufsuchen eines neuen Anfangs der Nachricht.
Protocol	Protokoll: • TCP – Kommunikation über das Protokoll TCP (verbindungsorientiert) • UDP – Kommunikation über das Protokoll UDP (verbindungslos)
Mode	Kommunikationsmodus: • TCP server – der Router empfängt ankommende Befehle am eingegebenen Port • TCP client – der Router verbindet sich zur eingegebenen Server-Adresse am eingegebenen Port
Server Address	Im Modus TCP Client ist es notwendig, die Server-Adresse einzugeben.
TCP Port	Der TCP/UDP Port, wo die Kommunikation stattfindet.
Inactivity Timeout	Zeitspanne nach der die TCP/UDP-Verbindung im Fall von Inaktivität unterbrochen wird.

Tabelle 67: Konfiguration – USB Port – 1

Aktivieren Sie die Option *Reject new connections*, dann lehnt der Router jeden weiteren (zusätzlichen) Verbindungsaufbau ab. Der Router unterstützt dann keine Mehrfachverbindungen mehr.

Aktivieren Sie die Option *Check TCP connection*, wird der Aufbau der TCP-Verbindung überprüft.

Element	Beschreibung
Keepalive Time	Zeitdauer, während der das Bestehen der Verbindung überwacht wird
Keepalive Interval	Zeitdauer, während der auf eine Antwort gewartet wird
Keepalive Probes	Anzahl der Versuche

Tabelle 68: Konfiguration – USB Port – 2

Aktivieren Sie die Option *Use CD as indicator of the TCP connection*, verwendet der Router das CD-Signal (DTR auf Seiten des Routers), um den Status der TCP-Verbindung zu überprüfen. Das CD-Signal prüft nach, ob auf der Gegenseite das Kabel eingesteckt ist.

CD	Beschreibung
Active	TCP-Verbindung wurde aufgebaut
Nonactive	TCP-Verbindung wurde nicht aufgebaut

Tabelle 69: Verbindungsüberprüfung mit CD-Signal

Aktivieren Sie die Option *Use DTR as control of TCP connection*, verwendet der Router das DTR-Signal (Data Terminal Ready) um den Status der TCP-Verbindung zu überprüfen. Die Gegenstelle sendet ein DTR-Signal, welches dem Router anzeigt, dass die Gegenstelle für die Kommunikation bereit ist.

DTR	Verhalten des Servers	Verhalten des Clients
Active	Der Router erlaubt den Aufbau der TCP-Verbindung.	Der Router baut die TCP-Verbindung auf.
Nonactive	Der Router erlaubt den Aufbau der TCP-Verbindung nicht.	Der Router trennt die TCP-Verbindung.

Tabelle 70: Verbindungsüberprüfung mit DTR-Signal

Unterstützte USB/RS232-Konverter

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210×

Die Änderungen gelten erst nach einem Klick auf die Schaltfläche *Apply*.

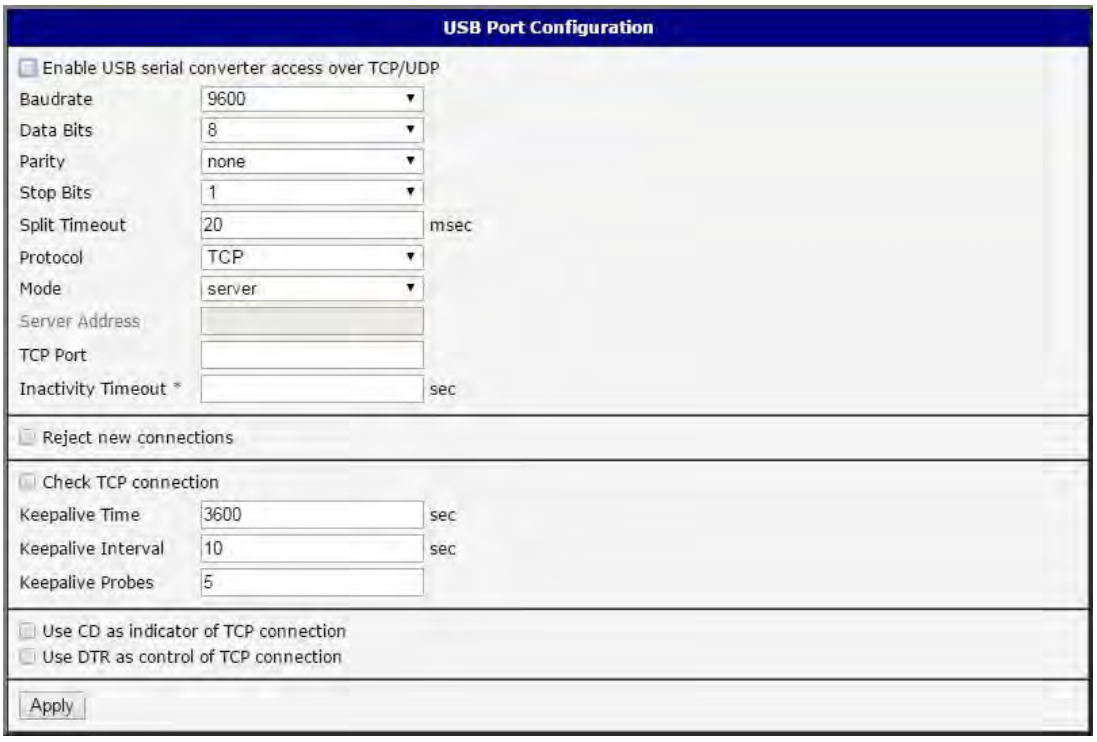


Abbildung 57: Konfiguration – USB

Konfigurationsbeispiele für USB

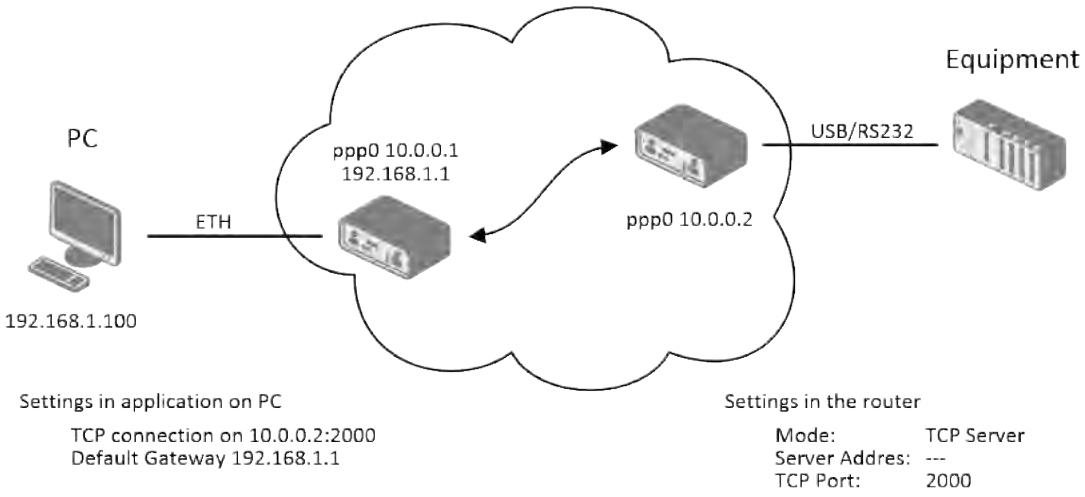


Abbildung 58: Konfigurationsbeispiel – USB-Port – 1

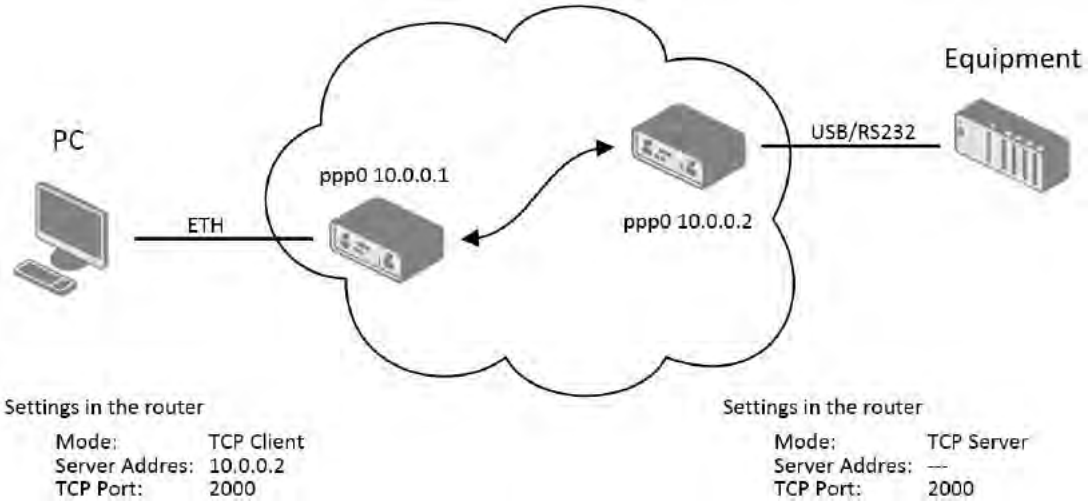


Abbildung 59: Konfigurationsbeispiel – USB-Port – 2

3.22 Skripte

Sie könne eigene Shell-Skripte erstellen, die in bestimmten Situationen ausgeführt werden.

Klicken Sie in der Navigationsspalte auf den Menüpunkt *Scripts* und wählen die gewünschte Unterseite *Startup Script*, *Up/Down IPv4* oder *Up/Down IPv6*.

Weitere Beispiele für Skripte und mögliche Kommandos finden Sie im Dokument *Commands and Scripts* [1].

3.22.1 Startup Script

Auf der Konfigurationsseite *Startup Script* können Sie die Kommandos eingeben, die direkt nach dem Einschalten oder Neustart des Routers ausgeführt werden
Die Änderungen gelten erst nach einem Klick auf die Schaltfläche *Apply*.

Änderungen am *Startup Script* wirken erst nach eine (Neu-)Start des Routers. Sie können einen Neustart über die Schaltfläche *Reboot* in der Navigationsspalte oder per SMS-Nachricht auslösen.

Beispiel für Startup-Skript

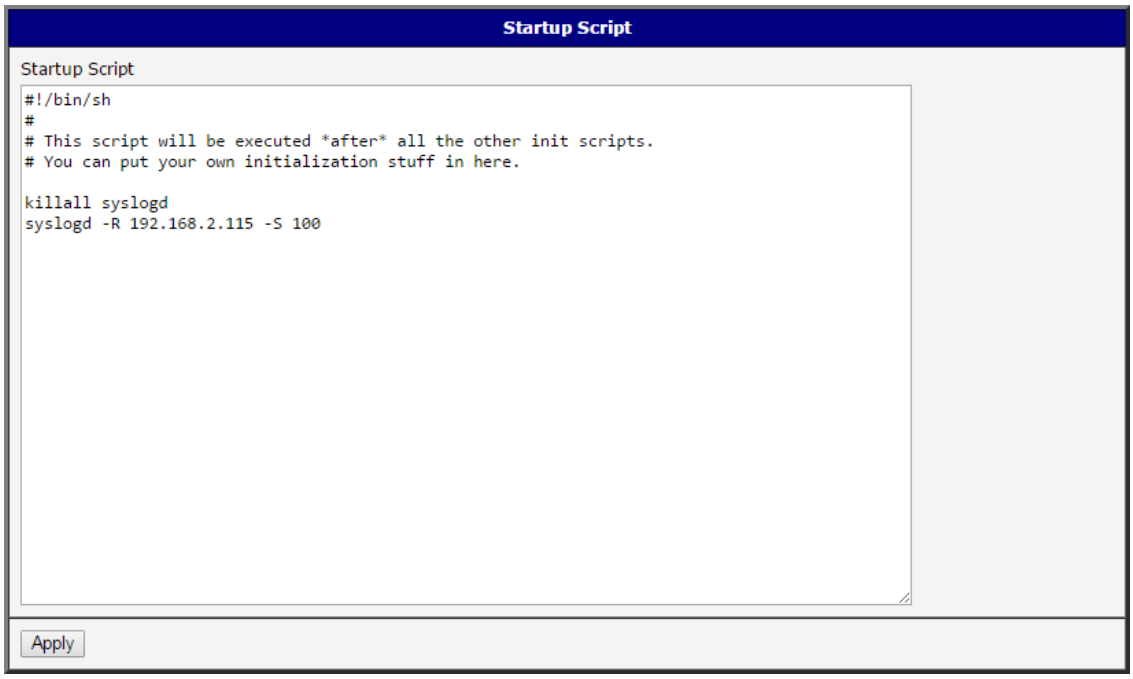


Abbildung 60: Beispiel – Startup-Skript

Nach dem Start des Routers wird das Programm syslog beendet und mit den angegebenen Parameter neugestartet. Die Log-Datei (limitiert auf 100 Einträge) wird auf dem Server mit der Adresse 192.168.2.115 abgelegt.

3.22.2 Up/Down Script

Auf der Konfigurationsseite *Up/Down IPv4* bzw. *Up/Down IPv6* können Sie die Kommandos eingeben, die ausgeführt werden sollen, wenn die Verbindung ins mobile WAN aufgebaut (*up*) bzw. beendet (*down*) wurde; jeweils für IPv4 und IPv6.

Das *Up Script* wird ausgeführt, wenn ein WAN-Verbindung aufgebaut wurde, entsprechend wird das *Down Script* ausgeführt, wenn die WAN-Verbindung beendet wurde.

Die Änderungen gelten erst nach einem Klick auf die Schaltfläche *Apply*. Danach müssen Sie den Router neustarten.

Beispiel für Up/Down-Skript

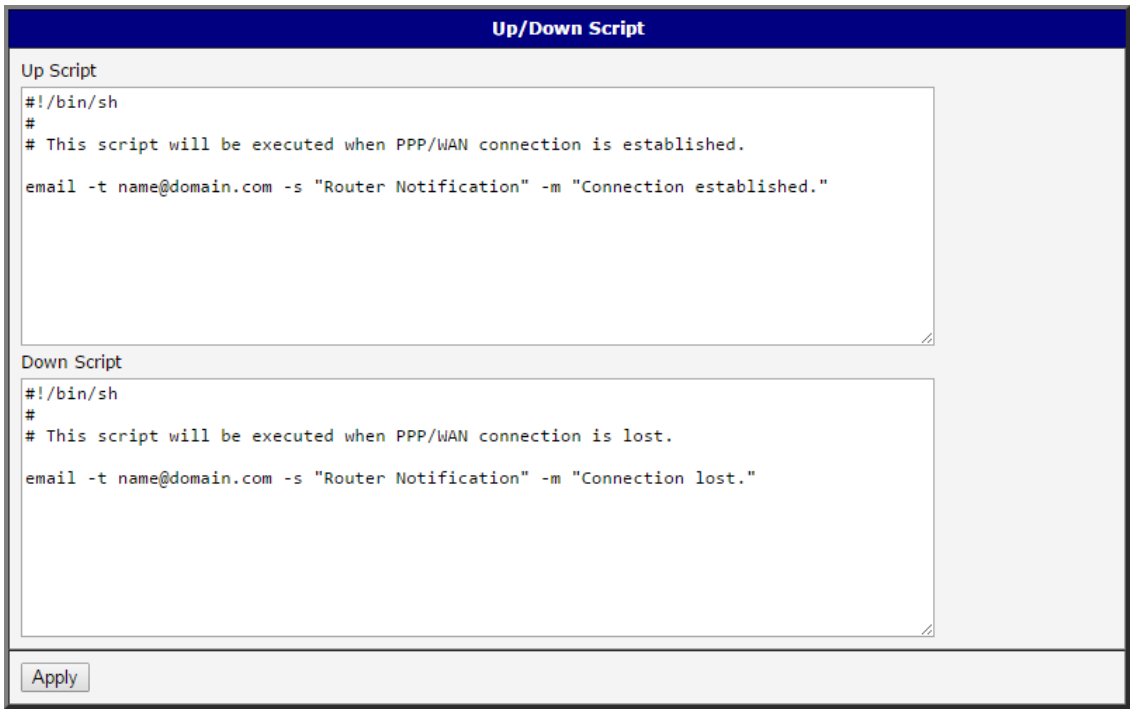


Abbildung 61: Beispiel – Up/Down-Skript

Damit nach Aufbau/Beendigung einer WAN-Verbindung eine E-Mail mit dem Status der Verbindung versendet wird, müssen Sie vorher *SMTP* konfigurieren, siehe Kapitel 3.18.

3.23 Automatic Update Configuration

Der Router kann so konfiguriert werden, dass regelmäßig auf einem FTP- oder Web-Server überprüft wird, ob eine neue Version der Firmware oder der Konfiguration vorhanden ist und diese ggf. heruntergeladen und installiert wird.

Öffnen Sie die Konfigurationsseite, indem Sie in der Navigationsspalte auf den Menüpunkt *Automatic Update* klicken.

Sie können Konfiguration und Firmware auf über den USB-Anschluss (USB Host) des Routers aufspielen.

Zum Schutz vor manipulierten Dateien überprüft der Router die heruntergeladene Datei auf das Format tar.gz. Danach wird der Architekturtyp und jede Datei im Archiv überprüft.

Aktivieren Sie die Option *Enable automatic update of configuration*, damit der Router auf dem Server überprüft, ob eine neue Konfigurationsdatei vorhanden ist. Ist diese unterschiedlich zur aktuellen Konfiguration, wird aktualisiert und anschließend der Router neu gestartet.

Aktivieren Sie die Option *Enable automatic update of firmware*, damit der Router auf dem Server überprüft, ob eine neue Firmware-Datei vorhanden ist und ggf. die Aktualisierung startet.

Element	Beschreibung
Source	Gibt an, wo der Router die aktuelle Firmware herunterlädt • HTTP/FTP server – Die Aktualisierungen werden von der Adresse heruntergeladen, die in der Option *Base URL* eingegeben ist. • 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	Gibt den Grundteil des Domain-Namens oder der IP-Adresse des Servers an, von dem die Firmware- oder Konfiguration-Datei heruntergeladen werden soll.
Unit ID	Bezeichnung der heruntergeladenen Konfiguration. Falls keine Unit ID angegeben ist, wird als Dateiname die MAC-Adresse des Routers verwendet. (Benutzen Sie als Trennzeichen statt des Doppelpunkts einen Punkt).
Update Hour	Die automatische Aktualisierung der Konfiguration erfolgt 5 Minuten nach dem Einschalten des Routers und dann alle 24 Stunden. Es ist auch möglich, mit dem Parameter *Update Hour* die Stunde (im Bereich von 1-24) einzustellen, wann die Aktualisierung durchgeführt werden soll. Besteht an der eingegebenen URL eine abweichende Konfiguration als im Router, nimmt der Router diese Konfiguration auf und führt danach einen Neustart durch.

Tabelle 71: Konfiguration Automatic Update

Der Name der heruntergeladenen Konfigurationsdatei besteht aus *Base URL*, MAC-Adresse der Schnittstellen eth0 und der Endung *.cfg*. Die MAC-Adresse und die Endung werden automatisch eingefügt. Der Wert des Parameters *Unit ID* definiert einen bestimmten Konfigurationsnamen, der heruntergeladen wird; die MAC-Adresse wird in diesem Fall nicht verwendet.

Der Name der heruntergeladenen Firmware-Datei besteht aus *Base URL*, Typ des Routers und der Endung *.bin*. Weitere Informationen über den richtigen Dateinamen finden Sie auf der Seite *Update Firmware* (Navigationsspalte, Menüpunkt *Administration*); siehe auch Kapitel 5.10.

Es ist notwendig, dass zwei Dateien (*.bin* und *.ver*) auf dem Server vorhanden sind. Ist nur die *.bin*-Datei auf dem Server, kann es vorkommen, dass der HTTP-Server die falsche Antwort *200 OK* statt der erwarteten *404 Not Found* sendet. Dies führt dazu, dass der Router unablässig versucht, die nicht vorhandene *.ver*-Datei herunterzuladen.

Die Aktualisierung der Firmware kann zu Inkompatibilitäten mit den Modulen (eigene Programme) führen. Wir empfehlen, die Module immer auf dem neuesten Stand zu halten, siehe Kapitel 4.1. Informationen über die Module und die Firmware-Kompatibilität finden Sie in der Dokumentation zu den Modulen.

Beispiel für Automatische Aktualisierung

Im folgenden Beispiel überprüft der Router jeden Tag um 1 Uhr nachts, ob eine neue Firmware- oder Konfigurationsdatei für einen SmartFlex-Router vorhanden ist.

- Firmware-Datei: http://example.com/LR77-v2.bin
- Konfigurationsdatei: http://example.com/test.cfg

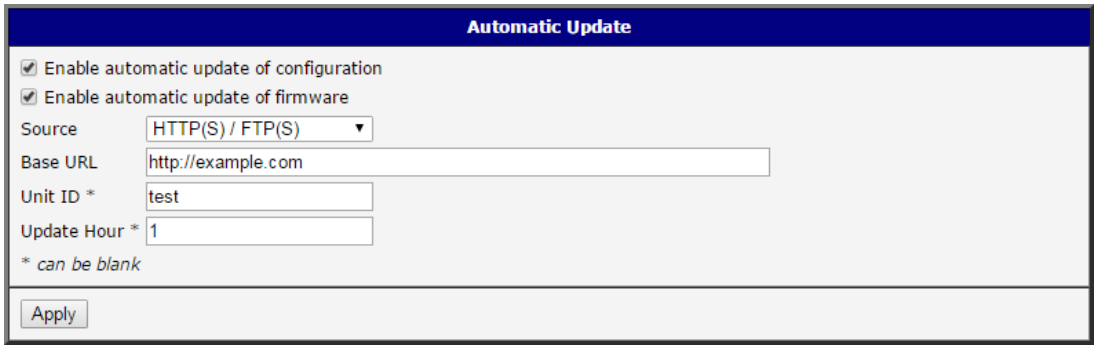


Abbildung 62: Beispiel für Automatische Aktualisierung – 1

Beispiel für Automatische Aktualisierung, basierend auf der MAC-Adresse

Im folgenden Beispiel überprüft der Router jeden Tag um 1 Uhr nachts, ob eine neue Firmware- oder Konfigurationsdatei für den Router LR77 v2 mit der MAC-Adresse 00:11:22:33:44:55 vorhanden ist.

- Firmware-Datei: http://example.com/LR77-v2.bin
- Konfigurationsdatei: http://example.com/00.11.22.33.44.55.cfg

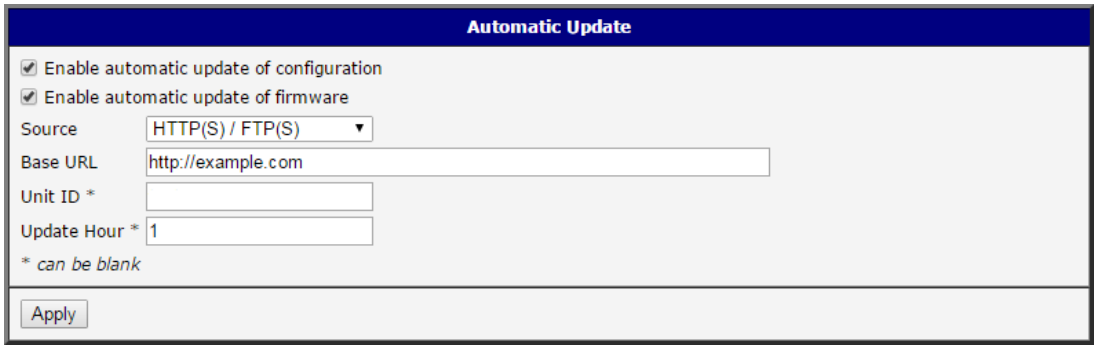


Abbildung 63: Beispiel für Automatische Aktualisierung – 2

4. Anpassungen

4.1 User Modules

Sie können Module (Programme) auf dem Router speichern und starten, um seine Fähigkeiten zu erweitern.

Öffnen Sie die Konfigurationsseite, indem Sie in der Navigationsspalte auf den Menüpunkt *User Modules* klicken. Sie können Module hinzufügen, entfernen oder konfigurieren.

Klicken Sie auf die Schaltfläche *Suchen*, um im Browser-Dialog die Modul-Datei mit der Endung *.tgz* zu suchen und zu markieren. Klicken Sie auf die Schaltfläche *Add*, um das Modul hinzuzufügen.

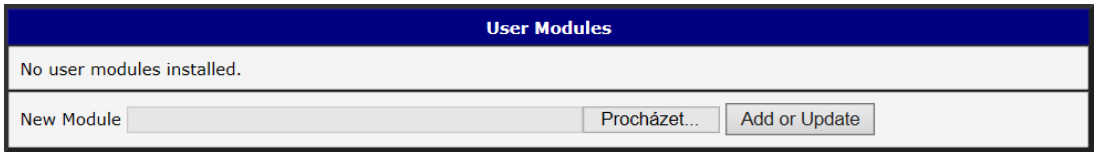


Abbildung 64: Module

Das neue Modul erscheint nun in der Liste der vorhandenen Module Enthält das Modul eine Datei namens *index.html* oder *index.cgi*, dient der Name des Moduls als Link auf diese Seite.

Um ein Modul zu löschen, klicken Sie auf die Schaltfläche *Delete*.

Module werden analog zu Installation aktualisiert. Wählen Sie die Datei mit der neueren Version und klicken Sie dann auf die Schaltfläche *Add* Die Konfiguration des Moduls wird nicht veändert.

Eine Beschreibung zu programmieren und kompilieren von Modulen finden Sie im Dokument *Programming of User Modules* [10].

Abbildung 65: Module hinzufügen

Module können kundenspezifisch programmiert werden. Sie können einige Module hier herunterladen: www.bb-smartcellular.eu.

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	erlaubt das Durchführen von TCP- und UDP-Scans
Daily Reboot	führt eine täglichen Neustart des Routers zu einem konfigurierbaren Zeitpunkt durch
HTTP Authentication	bietet Authentifizierung für Server, die diesen Service nicht anbieten
BGP, RIP, OSPF	bietet Unterstützung für dynamische Protokolle
PIM SM	bietet Unterstützung für das Multicast-Routing-Protokoll PIM-SM
WMBUS Concentrator	unterstützt den Empfang von Nachrichten von WMBUS-Zählern und speichert die Nachrichteninhalte in XML-Dateien
pduSMS	sendet Kurznachrichten (short messages/SMS) an bestimmte Rufnummern
GPS	erlaubt dem Router das Feststellen von Positions- und Zeitinformationen in jedem Wetter, überall auf oder in der Nähe der Erde, solange eine uneingeschränkte direkte Sichtlinie zu wenigstens vier GPS-Satelliten besteht
Pinger	erlaubt das automatische oder manuell Überprüfen einer Verbindung zwischen zwei Netzwerkschnittstellen (Ping)
IS-IS	bietet Unterstützung für das Protokoll IS-IS

Tabelle 72: Module

Hinweis!
Möglicherweise kann eine Aktualisierung der Firmware zu Inkompatibilitäten mit den installierten Modulen führen, da einige von ihnen von der Version des Linux-Kernels abhängen (z. B.: *SmsBE* und *PoS Configuration*).
Wir empfehlen, die Module immer auf dem neuesten Stand zu halten.

Informationen über die Module und die Firmware-Kompatibilität finden Sie in der Dokumentation zu den Modulen.

5. Administration

5.1 Users

Diese Konfiguration ist nur für Benutzer mit der zugewiesenen Rolle *Admin* verfügbar!

Öffnen Sie den Dialog *User Administration* durch Anklicken des Menüpunkts *Users* in der Navigationsspalte.

Sie können Benutzern Rollen zuweisen und die Benutzerkonten verwalten.

Angezeigt wird eine Übersicht über die angelegten Benutzer.

Schaltfläche	Beschreibung
Lock	Benutzerkonto sperren. Der Benutzer kann sich weder über die Web-Schnittstelle noch über SSH auf dem Router anmelden.
Unlock	Gesperrtes Benutzerkonto entsperren
Change Password	Passwort des ausgewählten Benutzers ändern
Delete	Ausgewähltes Benutzerkonto löschen

Tabelle 73: Benutzerübersicht

Warnung! Wenn Sie jedes Konto mit der Rolle *Admin* sperren, können Sie keines dieser Konten mehr entsperren. Dies bedeutet weiter, dass kein Benutzer mehr diese Konfigurationsseite aufrufen kann, da alle *Admin*-Konten gesperrt sind und Benutzer ohne Admin-Rolle nicht über ausreichende Berechtigungen verfügen, diese Seite auf zu rufen.

Der untere Bereich der Seite enthält die Felder für das Anlegen eines neuen Benutzer.

Element	Beschreibung
Role	Typ der Benutzerkontos: • **User** – Benutzer mit eingeschränkten Berechtigungen • **Admin** – Benutzer mit vollen Berechtigungen
Username	Benutzername
Password	zugehöriges Passwort
Confirm Password	Passwortwiederholung

Tabelle 74: Benutzer hinzufügen

Klicken Sie auf die Schaltfläche *Add User*, um das neue Benutzerkonto anzulegen.

Normale Benutzer können weder über Telnet, noch SSH oder SFTP auf den Router zugreifen. Lesender FTP-Zugang ist für diese Benutzer erlaubt.

Abbildung 66: Benutzer

5.2 Change Profile

Zusätzlich zum Standardprofil können Sie 3 weitere Router-Konfigurationen als Profile auf dem Router speichern.

Öffnen Sie den Dialog *Change Profile* durch Anklicken des Menüpunkts *Change Profile* in der Navigationsspalte.

Wählen Sie ein alternative Profil aus und aktivieren Sie die Option *Copy settings from current profile to selected profile*. Die aktuellen Einstellungen werden im alternative Profile gespeichert, wenn Sie auf die Schaltfläche *Apply* klicken.

Änderungen erfordern einen Neustart des Routers, entweder über den Menüpunkt *Reboot* in der Navigationsspalte oder über eine entsprechende SMS-Nachricht.

Beispiel für Profilwechsel

Mit Profilen können Sie zwischen verschiedenen Operations-Modus des Router, z. B.: PPP-Verbindung, VPN-Tunnel, usw., wechseln. Sie können den Wechsel über den binären Eingang, einer SMS-Nachricht oder über die Web-Schnittstelle des Router initiieren.

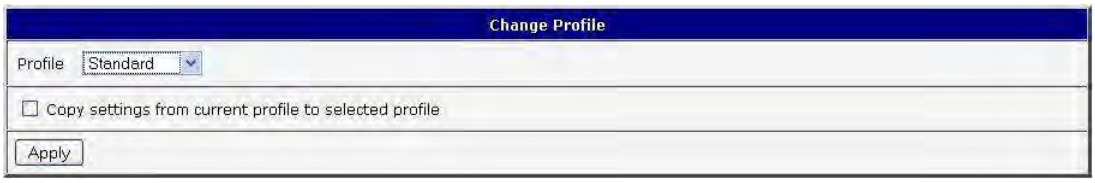


Abbildung 67: Profil ändern

5.3 Change Password

Öffnen Sie den Dialog *Change Password* durch Anklicken des Menüpunkts *Change Password* in der Navigationsspalte.

Tragen Sie im Feld *New Password* das neue Passwort für das Anmelden auf dem Router ein und wiederholen Sie die Eingabe im Feld *Confirm Password*. Klicken Sie anschließend auf die Schaltfläche *Apply*.

Aus Sicherheitsgründen sollten Sie das Standardpasswort (*root*) für den Benutzer *root* umgehend ändern. Solange das Passwort noch nicht geändert ist, haben Sie keinen Fernzugriff auf den Router.

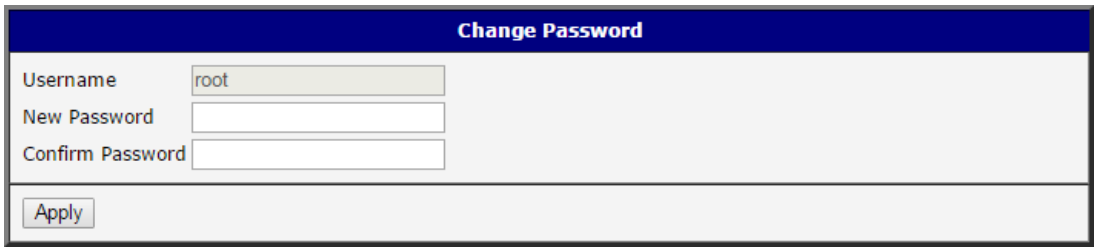


Abbildung 68: Passwort ändern

5.4 Set Real Time Clock

Öffnen Sie den Dialog *Set Real Time Clock* durch Anklicken des Menüpunkts *Set Real Time Clock* in der Navigationsspalte.

Sie können die Werte für Datum *Date* und Uhrzeit *Time* von Hand eingeben. Tragen Sie das Datum im Format JJJJ-MM-TT (yyyy-mm-dd) ein. Sie können die Uhr aber auch mit einem NTP-Server synchronisieren.

Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche *Apply*.

Abbildung 69: Echtzeituhr einstellen

5.5 Set SMS Service Center Address

> Für den Industrie-Router XR5i v2 wird die Konfigurationsseite *Set SMS Service Center Address* nicht angezeigt.

Diese Funktion erfordert die Angabe der Telefonnummer des SMS-Zentrums, damit SMS-Nachrichten gesendet werden.

Öffnen Sie den Dialog *Set SMS Service Center* durch Anklicken des Menüpunkts *Set SMS Service Center* in der Navigationsspalte.

Wenn auf der SIM-Karte bereits die Telefonnummer des SMS-Zentrums gespeichert ist, lassen Sie das Feld *Service Center Address* einfach leer.

Ansonsten tragen Sie die Telefonnummer entweder mit internationaler Vorwahl (+49-xxxxxxx) oder ohne internationale Vorwahl (0xxxxxx) ein.

Sollten Sie keine SMS-Nachrichten empfangen oder senden können, wenden Sie sich bitte an Ihren Mobilfunk-Service-Provider.

Abbildung 70: Telefonnumer für SMS-Zentrale

5.6 Unlock SIM Card

Für den Industrie-Router XR5i v2 wird die Konfigurationsseite *Unlock SIM Card* nicht angezeigt.

Öffnen Sie den Dialog *Unlock SIM Card* durch Anklicken des Menüpunkts *Unlock SIM Card* in der Navigationsspalte.

Tragen Sie die PIN (Personal Identification Number) zum Entsperren der SIM-Karte im Feld *SIM PIN* ein. Klicken Sie anschließend auf die Schaltfläche *Apply*.

Sie müssen die PIN jedes Mal eingeben, wenn Sie die SIM-Karte einschalten.

Nach drei fehlerhaften Versuchen wird die SIM-Karte gesperrt. In diesem Fall wenden Sie sich bitte an Ihren Mobilfunk-Service-Provider.

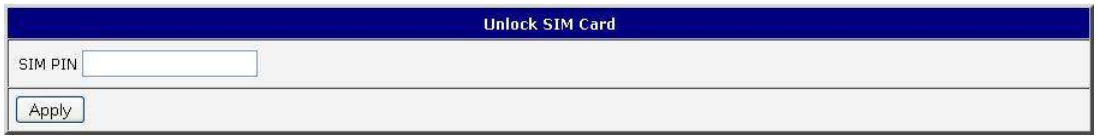


Abbildung 71: SIM-Karte entsperren

5.7 Send SMS

Für den Industrie-Router XR5i v2 wird die Konfigurationsseite *Send SMS* nicht agezeigt.

Zum Testen des mobilen Netzwerks können Sie eine SMS-Nachricht senden.

Öffnen Sie den Dialog *Send SMS* durch Anklicken des Menüpunkts *Send SMS* in der Navigationsspalte.

Abbildung 72: SMS senden

Tragen Sie im Feld *Phone number* die Telefonnumer für den Empfänger der SMS ein und im Feld *Message* den Text der Nachricht. Zum Versenden der SMS klicken Sie auf die Schaltfläche *Send*.

Die Länge der Nachricht ist auf maximal 160 Zeichen beschränkt. Wollen Sie länger Nachrichten versenden, installieren Sie das Modul *pduSMS*.

Sie können SMS-Nachrichten auch über ein CGI-Skript versenden. Einzelheiten zu dieser Methode finden Sie im Dokument *Commands and Scripts* [1].

5.8 Backup Configuration

Sie können die aktuelle Konfiguration des Routers sichern, indem Sie in der Navigationsspalte auf den Menüpunkt *Backup Configuration* klicken.

Tragen Sie im Browser-Dialog die Verzeichnis ein, in dem die Sicherungsdatei gespeichert werden soll.

5.9 Restore Configuration

Öffnen Sie den Dialog *Restore Configuration* durch Anklicken des Menüpunkts *Restore Configuration* in der Navigationsspalte.

Klicken Sie auf die Schaltfläche *Suchen* und navigieren Sie dann zum Speicherort der Sicherungsdatei (.cfg), die Sie laden möchten.

Um die Konfiguration wiederherzustellen, klicken Sie auf die Schaltfläche *Apply*.

Abbildung 73: Konfiguration wiederherstellen

5.10 Update Firmware

Öffnen Sie den Dialog *Update Firmware* durch Anklicken des Menüpunkts *Update Firmware* in der Navigationsspalte.

Angezeigt werden die aktuelle Version der Firmware und ihr Name.

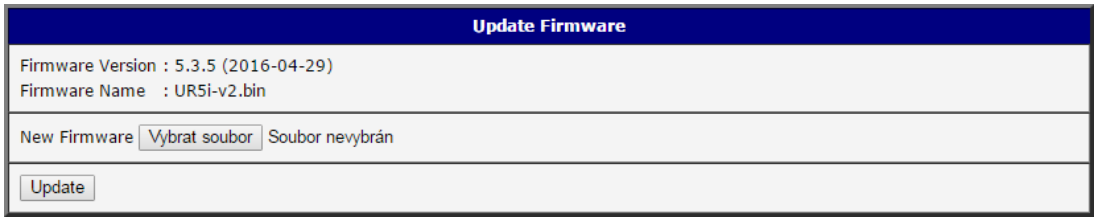


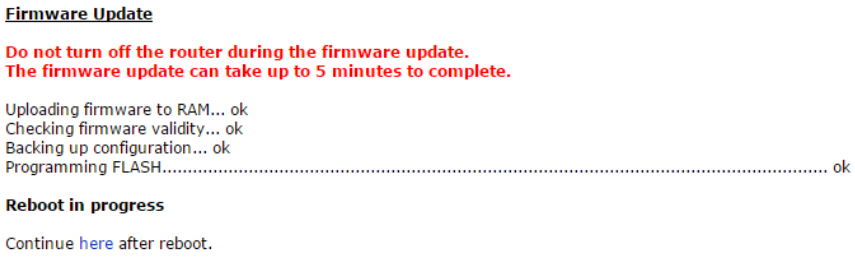
Abbildung 74: Firmware aktualisieren

Klicken Sie auf die Schaltfläche *Suchen* und navigieren Sie zum Speicherort der neuen Firmware-Datei. Die Namen der Firmware-Dateien müssen übereinstimmen.

Um die Firmware zu aktualisieren, klicken Sie auf die Schaltfläche *Update*.

Schalten Sie während der Aktualisierung den Router auf keinen Fall aus. Die Aktualisierung kann bis zu 5 Minuten dauern. Verwenden Sie nur Firmware-Dateien, deren Namen dem angezeigten Namen entspricht.

Während der Aktualisierung zeigt der Router verschiedene Meldungen an. Der Fortschritt der Aktualisierung wird mit . . angegeben.



Nach dem Abschluss der Aktualisierung bootet der Router automatisch neu.

Die Verwendung einer falschen Firmware kann den Router beschädigen.

Seit der Version 5.1.0 enthält die Firmware einen Mechanismus, der den mehrfachen Start der Firmware-Aktualisierung verhindert.

Hinweis!
Möglicherweise kann eine Aktualisierung der Firmware zu Inkompatibilitäten mit den installierten Modulen führen.
Wir empfehlen, die Module immer auf dem neuesten Stand zu halten.

Informationen über die Module und die Firmware-Kompatibilität finden Sie in der Dokumentation zu den Modulen.

5.11 Reboot

Öffnen Sie den Dialog *Reboot* durch Anklicken des Menüpunkts *Reboot* in der Navigationsspalte.

Für einen Neustart des Routers klicken Sie auf die Schaltfläche *Reboot*.

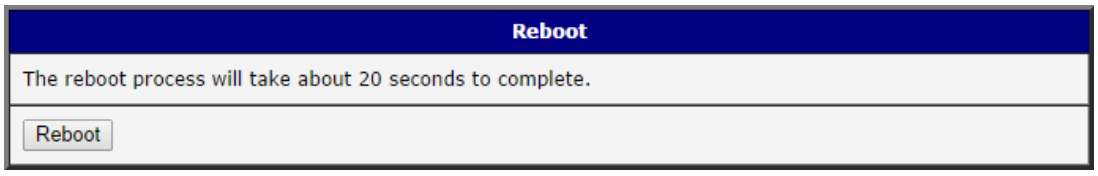


Abbildung 75: Neustart

6. Konfiguration über Telnet

Hinweis! Der Router arbeitet nicht ohne eingesetzte SIM-Karte!

Zur Zustandsüberwachung, Konfiguration und Verwaltung des Routers steht die Telnet-Schnittstelle zur Verfügung. Nach der Eingabe der IP-Adresse des Routers können Sie die Konfiguration mittels Kommados durchführen.

Die Standard-IP-Adresse des Routers lautet 192.168.1.1.

Die Konfiguration kann nur der Benutzer „root“ mit dem Standardpasswort „root“ vornehmen.

Kommando	Beschreibung
cat	Dateiinhalt ausgeben
cp	Datei kopieren
date	Systemzeit anzeigen/ändern
df	Informationen über das Dateisystem anzeigen
dmesg	Kernel-Meldungen anzeigen
echo	Zeichenkette ausgeben
email	E-Mail versenden
free	Informationen über den Speicher anzeigen
gsmat	AT-Befehlen ausgeben
gsminfo	Informationen über die Signalqualität anzeigen
gsmsms	SMS versenden
hwclock	Zeit der RTC anzeigen/ändern
ifconfig	Schnittstellenkonfiguration anzeigen/ändern
io	Outputs bestätigen/lesen
ip	Routing-Tabelle anzeigen/ändern
iptables	Regeln für den Netzfilter anzeigen/ändern
kill	Prozess beenden
killall	alle Prozesse beenden
ln	Link anlegen
ls	Inhalt des Verzeichnisse auflisten
mkdir	Verzeichnis erstellen

Fortsetzung auf der nächsten Seite

LUCOM GmbH — Flößaustr. 22a — 90763 Fürth — Tel.: +49 911/ 957 606 00 — E-Mail: info@lucom.de — www.lucom.de

Fortsetzung von der vorherigen Seite

Kommando	Beschreibung
mv	Datei/Verzeichnis verschieben
ntpdate	Synchronisierung der Systemzeit mit NTP-Server
passwd	Passwort ändern
ping	ICMP ping ausführen
ps	Informationen über Prozesse anzeigen
pwd	Name des aktuellen Verzeichnisses anzeigen
reboot	Router neu starten
rm	Datei löschen
rmdir	Verzeichnis löschen
route	Anzeige/Änderung der Routingtabelle
service	Dienst starten/beenden
sleep	Pause für die vorgegebene Sekundenanzahl
slog	System-Log anzeigen
tail	Dateiende anzeigen
tcpdump	Netzbetrieb überwachen
touch	Datei erstellen/Zeitstempel aktualisieren
vi	Texteditor

Tabelle 75: Telnet-Kommandos

7. Glossar und Abkürzungen

Backup-Routen Erlaubt das Backup einer primären Verbindung mit alternativen Verbindungen zum Internet/in ein mobiles Netzwerk. Jeder Backup-Verbindung kann ein Priorität zugewiesen werden. Der Wechsel zwischen den Verbindungen erfolgt aufgrund der Prioritäten und dem Zustand der Verbindungen.

DHCP Das Dynamic Host Configuration Protocol (DHCP) ermöglicht die Zuweisung der Netzwerkkonfiguration an DHCP-Clients durch einen DHCP-Server. Das Protokoll wurde als Client-Server-Modell implementiert, bei dem der DHCP-Client Konfigurationsdaten, wie IP-Adresse, Standardroute, ein oder mehrere DNS-Server-Adressen von einem DHCP-Server abfrag.

DHCP-Client Fragt Netzwerkkonfiguration von einem DHCP-Server ab.

DHCP-Server Weist auf Anfrage dem DHCP-Client eine Netzwerkkonfiguration zu.

DNS Das Domain Name System (DNS) ist einer der wichtigsten Dienste in vielen IP-basierten Netzwerken. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung.
Das DNS funktioniert ähnlich wie eine Telefonauskunft. Der Benutzer kennt die Domain (den für Menschen merkbaren Namen eines Rechners im Internet) – zum Beispiel www.example.org. Diese sendet er als Anfrage in das Internet. Die URL wird dann dort vom DNS in die zugehörige IP-Adresse (die Anschlussnummer im Internet) umgewandelt – zum Beispiel eine IPv4-Adresse der Form 192.0.2.42 oder eine IPv6-Adresse wie 2001:db8:85a3:8d3:1319:8a2e:370:7347, und führt so zum richtigen Rechner.

DynDNS-Client Der Dienst DynDNS erlaubt den Zugriff auf den Router über einen Hostnamen ohne Kenntnis der IP-Adresee. Der DynDNS-Client überwacht die IP-Adresse des Routers und ändert die Verknüpfung mit dem Hostnamen entsprechend.

GRE Das Generic Routing Encapsulation (GRE) ist ein Netzprotokoll, welches dazu dient, andere Protokolle einzukapseln und so in Form eines Tunnels über das Internet Protocol (IP) zu transportieren. Es ist möglich, bis zu vier verschiedene Tunnel einzurichten.

HTTP Das Hypertext Transfer Protocol (HTTP, deutsch: Hypertext-Übertragungsprotokoll) ist ein Protokoll zur Übertragung von Daten über ein Netzwerk. Es wird hauptsächlich eingesetzt, um Webseiten aus dem World Wide Web (WWW) in einen Web-Browser zu laden.

HTTPS HyperText Transfer Protocol Secure (HTTPS, deutsch: sicheres Hypertext-Übertragungsprotokoll) ist ein Kommunikationsprotokoll im World Wide Web, um Daten abhörsicher zu übertragen. Technisch gesehen, ist HTTPS kein selbständiges Protokoll; es ist eher das Ergebnis einer HTTP-Schicht über dem SSL/TLS-Protokoll. So werden die Sicherheitsmerkmale von SSL/TLS zu HTTP hinzugefügt.

IP masquerade Art des NAT.

IP masquerading siehe NAT.

IP-Adresse Eine IP-Adresse ist eine Adresse in Computernetzen, die ? wie das Internet ? auf dem Internetprotokoll (IP) basiert. Sie wird Geräten zugewiesen, die an das Netz angebunden sind, und macht die Geräte so adressierbar und

LUCOM GmbH — Flößaustr. 22a — 90763 Fürth — Tel.: +49 911/ 957 606 00 — E-Mail: info@lucom.de — www.lucom.de

damit erreichbar. Die IP-Adresse kann einen einzelnen Empfänger oder eine Gruppe von Empfängern bezeichnen (Multicast, Broadcast). Umgekehrt können einem Computer mehrere IP-Adressen zugeordnet sein.
Die IP-Adresse dient zwei prinzipielle Funktionen: Identifikation der Schnittstellen von Host oder Netzwerk und Adressierung des Standortes.
Die Rolle des Protokoll kann wie folgt charakterisiert werden: *Ein Name zeigt an, was wir suchen. Eine Adresse zeigt an, wo es sich befindet. Eine Route zeigt, wie man dort hin gelangt.*
Die bekannteste Notation der heute geläufigen IPv4-Adressen besteht aus vier Zahlen, die Werte von 0 bis 255 annehmen können und mit einem Punkt getrennt werden, beispielsweise 192.0.2.42. Technisch gesehen ist die IP-Adresse eine 32-stellige (IPv4) oder 128-stellige (IPv6) Binärzahl.

IPsec Internet Protocol Security (IPsec) ist eine Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze wie das Internet ermöglichen soll. Der Router erlaubt dem Anwender die Auswahl zwischen Encapsulation Modus (Tunnel oder Transport), IKE-Modus (Haupt- oder Aggressive Modus), IKE-Algorithmus, IKE-Verschlüsselung, ESP-Algorithmus, ESP-Verschlüsselung und weiteren Möglichkeiten.

IPv4 IPv4 (Internet Protocol Version 4), vor der Entwicklung von IPv6 einfach IP, ist die vierte Version des Internet Protocols (IP). Es war die erste Version des Internet Protocols, welche weltweit verbreitet und eingesetzt wurde, und bildet eine wichtige technische Grundlage des Internets. Es wurde in RFC 791 im Jahr 1981 definiert. Mittlerweile wurde mit dem Protokoll IPv6 ein Nachfolger definiert.

IPv6 Das Internet Protocol Version 6 (IPv6), früher auch Internet Protocol next Generation (IPnG) genannt, ist ein von der Internet Engineering Task Force (IETF) seit 1998 standardisiertes Verfahren zur Übertragung von Daten in paketvermittelnden Rechnernetzen, insbesondere dem Internet.
IPv6 soll das Protokoll IPv4, über das noch immer die Hauptlast des Internet-Datenverkehrs abgewickelt wird, ablösen.
IPv6-Adressen bestehen aus 8 Gruppen zu vier durch Doppelpunkte getrennte Hexadezimalwerte: 2001:0db8:85a3:0042:1000:8a2e:0370:7334. Methode für Abkürzungen der Vollschreibweise existieren.

L2TP Layer 2 Tunneling Protocol (L2TP) ist ein Netzwerkprotokoll, das Frames von Protokollen der Sicherungsschicht (Schicht 2) des OSI-Modells zwischen zwei Netzwerken über das Internet tunnelt, um ein virtuelles privates Netzwerk (VPN) herzustellen.
L2TP ist eine Tunnel-Lösung, die die Vorteile von PPTP (Point-to-Point Tunneling Protocol) und L2F (Layer 2 Forwarding) vereint. Mit Hilfe einer Tunnel-ID im L2TP-Header sind mehrere Tunnel nebeneinander ebenso möglich wie die Nutzung von NAT (Network Address Translation).

LAN Local Area Network (deutsch: lokales Netzwerk) ist ein Rechnernetz, das die Ausdehnung von Personal Area Networks übertrifft, die Ausdehnung von Metropolitan Area Networks, Wide Area Networks (WANs) und Global Area Networks (GAN) aber nicht erreicht. Ein LAN ist dabei in seiner Ausdehnung ohne Zusatzmaßnahmen auf 500 Meter beschränkt und wird in der Regel z. B. in Heimnetzen oder kleinen Unternehmen eingesetzt.

NAT Network Address Translation ist in Rechnernetzen der Sammelbegriff für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden. Daher kommen sie typischerweise auf Routern zum Einsatz.
Die einfache Art von NAT bietet eine 1-zu-1-Übersetzung einer IP-Adresse. RFC 2663 bezeichnet diesen NAT-Typ als Basis-NAT, oft auch 1-zu-1-NAT. Hier werden nur die IP-Adresse,

die IP-Header-Prüfsumme und alle weiteren höherschichtigen Prüfsummen, die die IP-Adresse beinhalten, geändert. Der Rest des Pakets bleibt unberührt (zumindest für die Basis-TCP/UDP-Funktionalität; einige höhere Protokolle erfordert evtl. weitere Übersetzungen). Basis-NAT wird für die Verbindung zwischen 2 IP-Netzwerken verwendet, die inkompatible Adressen verwenden.

NAT-T NAT-Traversal (z. T. als NAT-Durchdringung übersetzt) bezeichnet Techniken zum Aufbau und Halten von Verbindungen über NAT-Übergabestellen hinweg. Network Address Translation (NAT) bricht die Ende-zu-Ende-Konnektivität. Daher benötigen typischerweise Anwendungen, die von Client zu Client verbinden (zum Beispiel bei Peer-to-Peer- und IP-Telefonie-Anwendungen oder Netzwerkspiele) NAT-Durchdringungstechniken.

Netzwerkprotokoll Ein Netzwerkprotokoll (auch Netzprotokoll) ist ein Kommunikationsprotokoll für den Austausch von Daten zwischen Computern bzw. Prozessen, die in einem Rechnernetz miteinander verbunden sind (verteiltes System). Die Vereinbarung besteht aus einem Satz von Regeln und Formaten (Syntax), die das Kommunikationsverhalten der kommunizierenden Instanzen in den Computern bestimmen (Semantik).

NTP Das Network Time Protocol (NTP) ist ein Standard zur Synchronisierung von Uhren in Computersystemen über paketbasierte Kommunikationsnetze. NTP verwendet das verbindungslose Transportprotokoll UDP. Es wurde speziell entwickelt, um eine zuverlässige Zeitangabe über Netzwerke mit variabler Paketlaufzeit zu ermöglichen.

OpenVPN OpenVPN ist ein Programm zum Aufbau eines Virtuellen Privaten Netzwerkes (VPN) über eine verschlüsselte TLS-Verbindung. Zur Verschlüsselung werden die Bibliotheken des Programmes OpenSSL benutzt. OpenVPN verwendet wahlweise UDP oder TCP zum Transport.

PAT Port and Address Translation (PAT) oder Network Address Port Translation (NAPT) ist eine Technik, die in Computernetzwerken verwendet wird. Sie ist eine spezielle Form von NAT (1 zu n NAT). Dabei werden im Gegensatz zu NAT nicht nur die IP addresses, sondern auch Port-Nummern umgeschrieben. PAT wird eingesetzt, wenn mehrere private IP-Adressen aus einem LAN zu einer öffentlichen IP-Adresse übersetzt werden sollen.

Port Ein Port ist der Teil einer Netzwerk-Adresse, der die Zuordnung von TCP- und UDP-Verbindungen und -Datenpaketen zu Server- und Client-Programmen durch Betriebssysteme bewirkt. Zu jeder Verbindung dieser beiden Protokolle gehören zwei Ports, je einer auf Seiten des Clients und des Servers.

PPTP Das Point-to-Point Tunneling Protocol (PPTP) ist ein Netzwerkprotokoll, das auf das Internet Protocol aufsetzt und dem Aufbau eines Virtual Private Network (VPN) in einem Rechnernetz dient.
Mittels PPTP wird ein VPN geschaffen, indem ein Tunnel für das Point-to-Point Protocol gebildet wird. Es lässt Raum für jede denkbare Form der Authentifizierung und Verschlüsselung.[1] Die Initialisierung erfolgt über TCP-Port 1723 und die Datenflusssteuerung anschließend nach dem Generic Routing Encapsulation (GRE).
Paketfilter sorgen für Zugangskontrolle, Ende-zu-Ende und Server-zu-Server.

RADIUS Remote Authentication Dial-In User Service (RADIUS, deutsch Authentifizierungsdienst für sich einwählende Benutzer) ist ein Client-Server-Protokoll, das zur Authentifizierung, Autorisierung und zum Accounting (Triple-A-System) von Benutzern bei Einwahlverbindungen in ein Computernetzwerk dient. RADIUS ist der De-facto-Standard bei der zentralen Authentifizierung von Einwahlverbindungen über Modem, ISDN, VPN, WLAN (IEEE 802.1X) und

DSL.
Eine Weiterentwicklung ist das bisher weniger verbreitete Protokoll Diameter, welches weitere Funktionen umfasst, aber nicht vollständig abwärtskompatibel ist.

Root-Zertifikat Das Root-Zertifikat ist das oberste Zertifikat im Verzeichnisbaum einer Zertifikatshierarchie und ist selbst-signiert. Die Veröffentlichung erlaubt eine Gültigkeitsüberprüfung der in dieser Hierarchie ausgestellten Zertifikate. Durch die Installation der Wurzelzertifikate in die Anwendungen (z. B. Browser) können alle ausgegebenen Zertifikate auf Gültigkeit überprüft werden. Die Wurzelinstanz zertifiziert ausschließlich Zertifikate (CA-Zertifikate) von unmittelbar nachgeordneten Zertifizierungsstellen.
Die am häufigsten kommerzielle Variante basiert auf dem Standard ITU-T X.509, der normalerwe sie eine digitale Signatur einer Zertifizierungsstelle (Root Certificate Authority/CA) einschließt. Siehe auch X.509.

Router Router sind Netzwerkgeräte, die Netzwerkpakete zwischen mehreren Rechnernetzen weiterleiten können. Sie werden am häufigsten zur Internetanbindung, zur sicheren Kopplung mehrerer Standorte (VPN) oder zur direkten Kopplung mehrerer lokaler Netzwerksegmente, gegebenenfalls mit Anpassung an unterschiedlichen Netzwerkprotokollen eingesetzt (Ethernet, DSL, PPPoE, ISDN, ATM usw.).
Router treffen ihre Weiterleitungsentscheidung anhand von Informationen aus der Netzwerk-Schicht 3 (in der Regel ist das die IP-Adresse) oder höher. Viele Router übersetzen dabei auch zwischen privaten und öffentlichen IP-Adressen (Network Address Translation (NAT, Port Address Translation (PAT) oder bilden Firewall-Funktionen durch ein Regelwerk ab.

SFTP Das SSH File Transfer Protocol oder Secure File Transfer Protocol (SFTP) ist eine für die Secure Shell (SSH) entworfene Alternative zum File Transfer Protocol (FTP), die Verschlüsselung ermöglicht.
Im Unterschied zum FTP über TLS (FTPS) begnügt sich SFTP mit einer einzigen Verbindung zwischen Client und Server. Diese Auslegung ermöglicht, dass SFTP freistellt, statt SSH jedes andere Verfahren zur Authentifizierung und Verschlüsselung einzusetzen.

SMTP Das Simple Mail Transfer Protocol (SMTP/deutsch etwa Einfaches E-Mail-Transportprotokoll) ist ein Protokoll der Internet-Protokollfamilie, das zum Austausch von E-Mails in Computernetzen dient. Es wird dabei vorrangig zum Einspeisen und zum Weiterleiten von E-Mails verwendet. Zum Abholen von Nachrichten kommen andere, spezialisierte Protokolle wie POP3 oder IMAP zum Einsatz. SMTP-Server nehmen traditionell Verbindungen auf Port 25 entgegen. Ist die SMTP-Verbindung mit SSL gesichert, spricht man von SMTPS. Hier läuft die Verbindung über Port 465.

SMTPS SMTPS (Simple Mail Transfer Protocol Secure) bezeichnet ein Verfahren zur Absicherung der Kommunikation beim E-Mail-Transport via SMTP über SSL/TLS und ermöglicht dadurch Authentifizierung der Kommunikationspartner auf Transportebene sowie Integrität und Vertraulichkeit der übertragenen Nachrichten. Eine Ende-zu-Ende-Sicherheit wird dadurch allerdings nicht erreicht, da alle Mailserver und Mailrelays die E-Mail im Klartext verarbeiten (müssen). Eine Sicherheit der E-Mail auf Anwendungsebene ist durch SMTPS nicht erreichbar.
SMTPS ist kein eigenes Protokoll und auch keine Erweiterung von SMTP, da es vollkommen transparent und unabhängig von diesem auf der Transportschicht arbeitet.
Weitere Informationen siehe SMTP.

SNMP Das Simple Network Management Protocol (deutsch: einfaches Netzwerkverwaltungsprotokoll (SNMP)), ist ein Netzwerkprotokoll, das von der IETF entwickelt wurde, um Netzwerkelemente (z.B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Stati-

on aus überwachen und steuern zu können. Das Protokoll regelt dabei die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. SNMP beschreibt den Aufbau der Datenpakete, die gesendet werden können, und den Kommunikationsablauf. Es wurde dabei so ausgelegt, dass jedes netzwerkfähige Gerät mit in die Überwachung aufgenommen werden kann. Zu den Aufgaben des Netzwerkmanagements, die mit SNMP möglich sind, zählen: Überwachung von Netzwerkkomponenten – Fernsteuerung und Fernkonfiguration von Netzwerkkomponenten – Fehlererkennung und Fehlerbenachrichtigung.

SSH Secure Shell oder SSH bezeichnet sowohl ein Netzwerkprotokoll als auch entsprechende Programme, mit deren Hilfe man auf eine sichere Art und Weise eine verschlüsselte Netzwerkverbindung mit einem entfernten Gerät herstellen kann. Häufig wird diese Methode verwendet, um lokal eine entfernte Kommandozeile verfügbar zu machen, das heißt, auf einer lokalen Konsole werden die Ausgaben der entfernten Konsole ausgegeben und die lokalen Tastatureingaben werden an den entfernten Rechner gesendet. Genutzt werden kann dies beispielsweise zur Fernwartung eines in einem entfernten Rechenzentrum stehenden Servers. Die neuere Protokoll-Version SSH-2 bietet weitere Funktionen wie Datenübertragung per SFTP.

TCP Das Transmission Control Protocol (TCP) (zu deutsch Übertragungssteuerungsprotokoll) ist eine Vereinbarung (Protokoll) darüber, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen. Nahezu sämtliche aktuellen Betriebssysteme moderner Computer beherrschen TCP und nutzen es für den Datenaustausch mit anderen Rechnern. Das Protokoll ist ein zuverlässiges, verbindungsorientiertes, paketvermitteltes Transportprotokoll in Computernetzwerken. Es ist Teil der Internetprotokollfamilie, der Grundlage des Internets.

UDP Das User Datagram Protocol, (UDP), ist ein minimales, verbindungsloses Netzwerk-Protokoll, das zur Transportschicht der Internetprotokollfamilie gehört. Aufgabe von UDP ist es, Daten, die über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen.

URL Ein Uniform Resource Locator (deutsch einheitlicher Quellenanzeiger) identifiziert und lokalisiert eine Ressource, z. B. eine Website über die zu verwendende Zugriffsmethode (z. B. das verwendete Netzwerkprotokoll wie HTTP oder FTP) und den Ort (engl. location) der Ressource in Computernetzwerken. Der aktuelle Stand ist als RFC 1738 publiziert. Die RFC-Spezifikationen sind industrielle Standards der Internet Foundation IETF.
Beispiel für eine URL:
http://www.example.com/index.html. Sie enthält ein Protokoll (http), einen Hostname (www.example.com) und einen Dateinamen (index.html). Eine URL ist technisch gesehen eine besondere Art eines Uniform Resource Identifiers (URI/deutsch einheitlicher Quellenidentifizierer); in technischen Diskussionen wird URL oft als Synoym für URI verwendet.

VPN Virtual Private Network (deutsch: virtuelles privates Netz): ein geschlossenes Rechnernetz, das auf einer öffentlichen Netzwerk-Infrastruktur aufgebaut ist..

VPN-Server siehe VPN.

VPN-Tunnel siehe VPN.

VRRP Das Virtual Router Redundancy Protocol (VRRP) ist ein Verfahren zur Steigerung der Verfügbarkeit wichtiger Gateways in lokalen Netzen durch redundante Router. Es kann beispielsweise genutzt werden, um eine Backup-Verbindung über Mobilfunk für einen leitungsgebundenen Router einzurichten.

WAN Ein Wide Area Network, (deutsch: Weitverkehrsnetz) ist ein Rechnernetz, das sich im

LUCOM GmbH — Flößaustr. 22a — 90763 Fürth — Tel.: +49 911/ 957 606 00 — E-Mail: info@lucom.de — www.lucom.de

Unterschied zu einem LAN oder MAN über einen sehr großen geografischen Bereich erstreckt plural.

X.509 X.509 ist ein ITU-T-Standard für eine Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate. Aktuell ist Version 3 (X.509v3).

8. Index

16-01-17

9. Empfohlene Literatur

[1]	Advantech B+B SmartWorx:	**Commands and Scripts for v2 and v3 Routers**, Application Note
[2]	Advantech B+B SmartWorx:	**SmartCluster**, Application Note
[3]	Advantech B+B SmartWorx:	**R-SeeNet**, Application Note
[4]	Advantech B+B SmartWorx:	**R-SeeNet Admin**, Application Note
[5]	Advantech B+B SmartWorx:	**OpenVPN Tunnel**, Application Note
[6]	Advantech B+B SmartWorx:	**IPsec Tunnel**, Application Note
[7]	Advantech B+B SmartWorx:	**GRE Tunnel**, Application Note
[8]	Advantech B+B SmartWorx:	**SNMP Object Identifier**, Application Note
[9]	Advantech B+B SmartWorx:	**AT Commands**, Application Note