



NetModule Router NB2810

Software-Benutzerhandbuch - Version 4.6.0.107



Handbuchversion 2.1571

NetModule AG, Switzerland

20. November 2023



NetModule Router NB2810

Dieses Handbuch behandelt den *NB2810* mit sämtlichen Varianten.

Die Spezifikationen und Produktinformationen in diesem Handbuch können sich jederzeit ohne vorherige Ankündigung ändern. Wir weisen darauf hin, dass NetModule keine Zusicherungen oder Gewährleistungen in Bezug auf den Inhalt dieses Dokuments macht und nicht für Verluste oder Schäden haftet, die dem Benutzer durch die direkte oder indirekte Verwendung dieser Informationen entstehen. Dieses Dokument kann Informationen über Produkte oder Prozesse Dritter enthalten.

Solche Informationen Dritter sind in der Regel außerhalb des Einflussbereichs von NetModule, und daher kann NetModule auch keine Verantwortung für die Richtigkeit oder Rechtmäßigkeit dieser Informationen übernehmen. Der Anwender trägt die volle Verantwortung für die Anwendung der Produkte.

Copyright ©2023 NetModule AG, Switzerland Alle Rechte vorbehalten.

Dieses Dokument enthält urheberrechtlich geschützte Informationen von NetModule. Kein Teil des hier beschriebenen Werkes darf vervielfältigt werden. Reverse Engineering der Hard- oder Software ist verboten und patentrechtlich geschützt. Dieses Material oder Teile davon dürfen ohne vorherige schriftliche Genehmigung von NetModule in keiner Form oder mit keinen Mitteln kopiert, in Abfragesystemen gespeichert, übernommen oder in irgendeiner Form oder mit irgendwelchen Mitteln (elektronisch, mechanisch, fotografisch, grafisch, optisch oder anderweitig) übertragen oder in irgendeine Sprache oder Computersprache übersetzt werden.

Ein großer Teil des Quellcodes zu diesem Produkt ist unter freien und quelloffenen Lizenzen verfügbar. Das größte Teil davon unterliegt der GNU General Public License. Diese finden Sie unter www.gnu.org. Der Anteil der Open-Source-Software, der nicht der GPL unterliegt, ist normalerweise unter einer von vielen freizügigeren Lizenzen verfügbar. Detaillierte Lizenzinformationen für ein bestimmtes Softwarepaket sind auf Anfrage erhältlich.

Alle anderen erwähnten Produkte oder Firmennamen werden nur zu Identifikationszwecken verwendet und können Marken oder eingetragene Marken der jeweiligen Eigentümer sein. Die folgende Beschreibung der Software, Hardware oder Verfahren von NetModule oder eines Drittanbieters kann dem Produkt beiliegen und unterliegt den jeweiligen Software-, Hardware- oder sonstigen Lizenzvereinbarungen.

Kontakt

www.netmodule.com/support

| | |
|--------------------|---|
| NetModule AG | Tel +41 31 985 25 10 |
| Maulbeerstrasse 10 | Fax +41 31 985 25 11 |
| 3011 Bern | info@netmodule.com |
| Schweiz | https://www.netmodule.com |



Inhaltsverzeichnis

| | |
|---|----|
| 1. Willkommen bei NetModule | 10 |
| 2. Konformität | 11 |
| 2.1. Sicherheitsanweisungen | 11 |
| 2.2. Konformitätserklärung | 13 |
| 2.3. Entsorgung | 13 |
| 2.4. Nationale Einschränkungen | 13 |
| 2.5. Open-Source-Software | 14 |
| 3. Technische Daten | 15 |
| 3.1. Erscheinungsbild | 15 |
| 3.2. Funktionen | 16 |
| 3.3. Umgebungsbedingungen | 16 |
| 3.4. Schnittstellen | 17 |
| 3.4.1. Übersicht | 17 |
| 3.4.2. LED-Anzeigen | 18 |
| 3.4.3. Reset | 19 |
| 3.4.4. Mobile Kommunikation | 20 |
| 3.4.5. WLAN | 21 |
| 3.4.6. GNSS | 22 |
| 3.4.7. USB 3.0-Host-Anschluss | 23 |
| 3.4.8. M12-Ethernet-Steckverbinder | 23 |
| 3.4.9. Netzteil | 24 |
| 3.4.10. RS-232 | 25 |
| 3.4.11. 6-poliger Terminierungsblock | 25 |
| 3.4.12. Erweiterungsanschluss | 26 |
| 3.5. Datenspeicherung (Option Dx) | 37 |
| 4. Installation | 38 |
| 4.1. Installation von Micro-SIM-Karten(3FF) | 38 |
| 4.2. Installation der GSM-/UMTS-/LTE-Antennen | 39 |
| 4.3. Installation der WLAN-Antennen | 39 |
| 4.4. Installation der GNSS-Antenne | 41 |
| 4.5. Installation des lokalen Netzwerks (LAN) | 41 |
| 4.6. Installation des Netzteils und verzögertes Ausschalten | 41 |
| 4.7. Installation der Audio-Schnittstelle | 42 |
| 5. Konfiguration | 43 |
| 5.1. Erste Schritte | 43 |
| 5.1.1. Erster Zugang | 43 |
| 5.1.2. Automatische Konfiguration einer Mobilfunkverbindung | 45 |
| 5.1.3. Zurücksetzen | 45 |
| 5.2. STARTSEITE | 46 |
| 5.3. SCHNITTSTELLEN | 49 |
| 5.3.1. WAN | 49 |
| 5.3.2. Ethernet | 55 |
| 5.3.3. Mobile Kommunikation | 64 |
| 5.3.4. WLAN | 71 |
| 5.3.5. Software-Bridges | 80 |
| 5.3.6. USB | 81 |
| 5.3.7. Serial | 83 |
| 5.3.8. Audio | 88 |



| | | |
|---------|------------------------------------|-----|
| 5.3.9. | GNSS | 89 |
| 5.4. | ROUTING | 93 |
| 5.4.1. | Statisches Routing | 93 |
| 5.4.2. | Erweitertes Routing | 95 |
| 5.4.3. | Multipath-Routing | 97 |
| 5.4.4. | Multicast-Routing | 98 |
| 5.4.5. | BGP | 100 |
| 5.4.6. | OSPF | 102 |
| 5.4.7. | Mobile IP | 104 |
| 5.4.8. | Quality of Service | 107 |
| 5.5. | FIREWALL | 109 |
| 5.5.1. | Verwaltung | 109 |
| 5.5.2. | Adress-/Portgruppen | 109 |
| 5.5.3. | Regeln | 110 |
| 5.5.4. | NAPT | 112 |
| 5.6. | VPN | 116 |
| 5.6.1. | OpenVPN | 116 |
| 5.6.2. | IPsec | 122 |
| 5.6.3. | PPTP | 128 |
| 5.6.4. | GRE | 131 |
| 5.6.5. | L2TP (Layer-2-Tunneling-Protokoll) | 132 |
| 5.6.6. | Einwahl (Dial-In) | 133 |
| 5.7. | DIENSTE | 135 |
| 5.7.1. | SDK | 135 |
| 5.7.2. | DHCP-Server | 144 |
| 5.7.3. | DNS-Server | 146 |
| 5.7.4. | NTP-Server | 149 |
| 5.7.5. | Dynamic DNS | 150 |
| 5.7.6. | E-Mail | 152 |
| 5.7.7. | Ereignismanager | 154 |
| 5.7.8. | SMS | 155 |
| 5.7.9. | SSH-/Telnet-Server | 158 |
| 5.7.10. | SNMP-Agent | 161 |
| 5.7.11. | Let's Encrypt | 167 |
| 5.7.12. | Webserver | 168 |
| 5.7.13. | MQTT Broker | 169 |
| 5.7.14. | Softflow | 170 |
| 5.7.15. | Discovery (Erkennungsprotokolle) | 171 |
| 5.7.16. | Redundanz (VRRP) | 172 |
| 5.7.17. | ITxPT | 174 |
| 5.7.18. | Voice-Gateway | 182 |
| 5.8. | SYSTEM | 188 |
| 5.8.1. | System | 188 |
| 5.8.2. | Authentifizierung | 194 |
| 5.8.3. | Software-Updates | 197 |
| 5.8.4. | Updates für Modul-Firmware | 198 |
| 5.8.5. | Software-Profile | 199 |
| 5.8.6. | Konfiguration | 200 |
| 5.8.7. | Fehlersuche und Fehlerbehebung | 203 |



| | | |
|---------|---|-----|
| 5.8.8. | Schlüssel und Zertifikate | 206 |
| 5.8.9. | Lizenzierung | 211 |
| 5.8.10. | Rechtlicher Hinweis | 212 |
| 5.9. | ABMELDEN | 213 |
| 6. | Kommandozeile (CLI) | 214 |
| 6.1. | Arbeiten mit der Befehlszeile | 214 |
| 6.2. | Hilfe ausgeben | 215 |
| 6.3. | Konfigurationsparameter abrufen | 216 |
| 6.4. | Konfigurationsparameter setzen | 216 |
| 6.5. | Abschluss der Konfigurationsarbeiten prüfen | 216 |
| 6.6. | Statusinformationen abrufen | 216 |
| 6.7. | Netzwerke scannen | 217 |
| 6.8. | E-Mail oder SMS senden | 217 |
| 6.9. | Systemressourcen aktualisieren | 218 |
| 6.10. | Schlüssel und Zertifikate verwalten | 218 |
| 6.11. | Dienste neu starten | 218 |
| 6.12. | System debuggen | 219 |
| 6.13. | System auf Werkseinstellungen zurücksetzen | 220 |
| 6.14. | System neu starten | 220 |
| 6.15. | Shell-Befehl ausführen | 220 |
| 6.16. | Arbeiten mit der Verlaufsliste | 220 |
| 6.17. | CLI-PHP | 220 |
| A. | Anhang | 226 |
| A.1. | Abkürzungen | 226 |
| A.2. | System-Ereignisse | 228 |
| A.3. | Werkseinstellungen | 230 |
| A.4. | SNMP VENDOR MIB | 231 |
| A.5. | SDK-Beispiele | 232 |



Abbildungsverzeichnis

| | | |
|-------|---|-----|
| 5.1. | Erste Anmeldung | 44 |
| 5.2. | Startbildschirm | 46 |
| 5.3. | WAN-Verbindungen | 49 |
| 5.4. | Verbindungsüberwachung | 52 |
| 5.5. | WAN-Einstellungen | 54 |
| 5.6. | Ethernet-Anschlüsse | 55 |
| 5.7. | Einstellungen für die Ethernet-Verbindung | 56 |
| 5.8. | VLAN-Verwaltung | 58 |
| 5.9. | IP Einstellungen - Übersicht | 59 |
| 5.10. | IP Einstellungen - LAN Schnittstelle | 60 |
| 5.11. | IP Einstellungen - WAN Schnittstelle | 61 |
| 5.12. | SIM-Karten | 64 |
| 5.13. | eSIM-Profile | 66 |
| 5.14. | eUICC-Profil hinzufügen | 67 |
| 5.15. | WWAN-Schnittstellen | 68 |
| 5.16. | WLAN-Verwaltung | 71 |
| 5.17. | WLAN-Konfiguration | 75 |
| 5.18. | WLAN-IP-Konfiguration | 78 |
| 5.19. | USB-Verwaltung | 81 |
| 5.20. | USB-Geräteverwaltung | 82 |
| 5.21. | Verwaltung der seriellen Schnittstelle | 84 |
| 5.22. | Einstellungen der seriellen Schnittstelle | 85 |
| 5.23. | Statisches Routing | 93 |
| 5.24. | Erweitertes Routing | 95 |
| 5.25. | Multipath-Routing | 97 |
| 5.26. | Mobile IP | 106 |
| 5.27. | Firewall-Gruppen | 109 |
| 5.28. | Firewall-Regeln | 110 |
| 5.29. | Maskierung (Masquerading) | 112 |
| 5.30. | NAPT-Regeln für eingehende Pakete | 113 |
| 5.31. | Verwaltung von OpenVPN | 116 |
| 5.32. | Konfiguration von OpenVPN | 117 |
| 5.33. | OpenVPN-Client-Verwaltung | 121 |
| 5.34. | IPSec-Verwaltung | 123 |
| 5.35. | IPSec-Konfiguration | 124 |
| 5.36. | PPTP-Verwaltung | 128 |
| 5.37. | Konfiguration eines PPTP-Tunnels | 129 |
| 5.38. | PPTP-Client-Verwaltung | 130 |
| 5.39. | Einwahlserver-Einstellungen | 133 |
| 5.40. | SDK-Verwaltung | 139 |
| 5.41. | SDK-Jobs | 140 |
| 5.42. | DHCP-Server | 144 |
| 5.43. | DNS-Server | 146 |
| 5.44. | NTP-Server | 149 |
| 5.45. | Einstellungen für Dynamic DNS | 150 |
| 5.46. | E-Mail-Einstellungen | 152 |
| 5.47. | SMS-Konfiguration | 156 |



| | |
|--|-----|
| 5.48. SSH- und Telnet-Server | 158 |
| 5.49. SNMP-Agent | 162 |
| 5.50. Webserver | 168 |
| 5.51. VRRP-Konfiguration | 172 |
| 5.52. ITxPT-Konfiguration | 174 |
| 5.53. ITxPT FMS-to-IP | 175 |
| 5.54. ITxPT GNSS | 179 |
| 5.55. ITxPT Time | 180 |
| 5.56. ITxPT VEHICLEtoIP | 181 |
| 5.57. Verwaltung des Voice-Gateways | 182 |
| 5.58. System | 188 |
| 5.59. Regionseinstellungen | 191 |
| 5.60. Benutzerkonten | 194 |
| 5.61. Remote-Authentifizierung | 196 |
| 5.62. Manuelle Konfiguration per Datei | 200 |
| 5.63. Automatische Konfiguration per Datei | 201 |
| 5.64. Werkseinstellungen | 202 |
| 5.65. Log-Viewer | 204 |
| 5.66. Datei für den technischen Support | 205 |
| 5.67. Schlüssel und Zertifikate | 206 |
| 5.68. Konfiguration von Zertifikaten | 208 |
| 5.69. Lizenzierung | 211 |

Tabellenverzeichnis

| | | |
|--------|--|-----|
| 3.1. | Umgebungsbedingungen | 16 |
| 3.2. | NB2810-Schnittstellen | 18 |
| 3.3. | NB2810-Statusanzeigen | 19 |
| 3.4. | Ethernet-Statusanzeigen | 19 |
| 3.5. | Mobile Schnittstelle | 20 |
| 3.6. | Spezifikation des mobilen Antennenanschlusses | 20 |
| 3.7. | IEEE 802.11-Norm | 21 |
| 3.8. | Spezifikation des WLAN-Antennenanschlusses | 21 |
| 3.9. | GNSS-Spezifikationen, Option G | 22 |
| 3.10. | GNSS-Spezifikationen (Option Gd) | 22 |
| 3.11. | Spezifikation des GNSS-/GPS-Antennenanschlusses | 23 |
| 3.12. | Spezifikation des USB-3.0-Host-Anschlusses | 23 |
| 3.13. | Spezifikation des Ethernet-Anschlusses | 23 |
| 3.14. | Pinbelegung der 8-poligen Ethernet-Stecker | 24 |
| 3.15. | Spannungsversorgung | 24 |
| 3.16. | Spezifikation des RS-232-Anschlusses | 25 |
| 3.17. | Klemmenblockstecker | 25 |
| 3.18. | Pinbelegung des Terminierungsblocks | 25 |
| 3.19. | Pinbelegung des Erweiterungsanschlusses | 26 |
| 3.20. | Spezifikation des Audio-Anschlusses | 27 |
| 3.21. | Pinbelegung der Audioausgänge (EP1/EP2) | 27 |
| 3.22. | Spezifikation des CAN-Anschlusses | 28 |
| 3.23. | Pinbelegung der CAN-Anschlüsse (EP1/EP2) | 28 |
| 3.24. | Spezifikation des 4xCAN-Anschlusses | 29 |
| 3.25. | Pinbelegung der 4xCAN-Anschlüsse | 29 |
| 3.26. | Spezifikation des IBIS-Anschlusses | 30 |
| 3.27. | Pinbelegung der IBIS-Anschlüsse (EP1/EP2) | 30 |
| 3.28. | Spezifikation des isolierten RS-232-Anschlusses | 31 |
| 3.29. | Pinbelegung der RS-232-Portsignale (EP1/EP2) | 31 |
| 3.30. | Spezifikation des RS-485-Anschlusses | 32 |
| 3.31. | Pinbelegung der RS-485-Portsignale (EP1/EP2) | 32 |
| 3.32. | Gemeinsame PTT-Spezifikation | 33 |
| 3.33. | Spezifikation des Audio-Anschlusses | 33 |
| 3.34. | Spezifikation des digitalen Eingangs | 33 |
| 3.35. | Spezifikation des digitalen Ausgangs | 34 |
| 3.36. | Pinbelegung des Audio-PTT-Steckers | 34 |
| 3.37. | Gemeinsame Spezifikation für die digitalen Ein- und Ausgänge | 35 |
| 3.38. | Spezifikation des nicht isolierten Digitalanschlusses | 35 |
| 3.39. | Spezifikation des isolierten digitalen Ausgangs | 35 |
| 3.40. | Pinbelegung der Variante mit zwei digitalen Ein-/Ausgängen | 36 |
| 3.41. | Speicherspezifikationen | 37 |
| 4.1. | Typen von LTE-/UMTS-Antennenanschlüssen | 39 |
| 4.2. | Typen von WLAN-Antennenanschlüssen | 40 |
| 5.24. | IEEE 802.11-WLAN-Normen | 73 |
| 5.52. | Statische Routen-Flags | 94 |
| 5.100. | SMS-Steuerbefehle | 143 |



| | | |
|--------|---------------------------------------|-----|
| 5.112. | Darstellungsweisen von SMS-Rufnummern | 157 |
| 5.165. | Zertifikatsabschnitte | 207 |
| 5.166. | Zertifikatsaktionen | 207 |
| A.1. | Abkürzungen | 228 |
| A.2. | Systemereignisse | 229 |
| A.3. | SDK-Beispiele | 234 |



1. Willkommen bei NetModule

Vielen Dank, dass Sie sich für ein NetModule-Produkt entschieden haben. Dieses Dokument soll Ihnen eine Einführung in das Gerät und seine Funktionen geben. In den folgenden Kapiteln werden alle Aspekte der Inbetriebnahme des Geräts, Installationsverfahren und hilfreiche Informationen zur Konfiguration und Wartung beschrieben.

Weitere Informationen wie Beispiel-SDK-Skripte oder Konfigurationsbeispiele finden Sie in unserem Wiki auf <https://wiki.netmodule.com>.

2. Konformität

Dieses Kapitel enthält allgemeine Informationen zur Inbetriebnahme des Routers.

2.1. Sicherheitsanweisungen

Bitte beachten Sie sorgfältig alle Sicherheitshinweise im Handbuch mit dem Symbol .



Einhaltung von Vorschriften: Bei der Verwendung der NetModule-Router sind sämtliche einschlägigen nationalen und internationalen Gesetze sowie besonderen Einschränkungen, die den Einsatz des Kommunikationsmoduls in vorgeschriebenen Anwendungen und Umgebungen regeln, zu beachten.



Informationen zum Zubehör/Änderungen am Gerät:

- Um Verletzungen und Gesundheitsrisiken zu vermeiden, verwenden Sie bitte nur Originalzubehör.
- Änderungen am Gerät oder die Verwendung von nicht freigegebenem Zubehör führen zum Erlöschen der Garantie und ggf. zum Erlöschen der Betriebserlaubnis.
- NetModule-Router dürfen nicht geöffnet werden (SIM-Karten dürfen jedoch entsprechend der Anleitung eingesetzt werden).



Informationen zu den Geräteschnittstellen:

- Alle Systeme, die an die NetModule-Router-Schnittstellen angeschlossen werden, müssen die Anforderungen an SELV-Systeme (Safety Extra Low Voltage) erfüllen.
- Die Verbindungen dürfen weder das Gebäude verlassen noch durch die Karosserie eines Fahrzeugs hindurchgeführt werden.
- Antennenanschlüsse dürfen nur dann aus dem Gebäude oder dem Fahrzeugkörper herausgeführt werden, wenn transiente Überspannungen (gemäß IEC 62368-1) durch externe Schutzschaltungen auf $1\,500\text{ V}_{\text{peak}}$ begrenzt sind. Alle anderen Verbindungen müssen innerhalb des Gebäudes oder des Fahrzeugkörpers verbleiben.
- Einen Mindestabstand von 40 cm zwischen Personen und der Antenne ist einzuhalten
- Alle Antennen müssen grundsätzlich einen Abstand von mindestens 20cm zueinander haben, bei Kombiantennen (Mobilfunk / WLAN / GNSS) muss eine ausreichende Isolation zwischen den Funktechnologien vorhanden sein.
- Geräte mit WLAN-Schnittstelle dürfen nur mit konfigurierter zutreffender Regulatory Domain betrieben werden. Besondere Aufmerksamkeit benötigen die Angaben zum Land, zur Anzahl der Antennen und zum Antennengewinn gewidmet werden (siehe auch Kapitel 5.3.4). WLAN-Antennen mit höherer Verstärkung dürfen mit der NetModule-Router-Softwarelizenz Enhanced RF Configuration und der von zertifiziertem Fachpersonal korrekt konfigurierten Antennenverstärkung und Kabeldämpfung verwendet werden. Eine Fehlkonfiguration führt zum Verlust der Zulassung.
- An den Router angeschlossene Mobilfunkantennen dürfen nur einen Antennengewinn von höchstens 2,5 dBi aufweisen. Für die Einhaltung der gesetzlichen Vorschriften ist der Anwender verantwortlich.
- Zu beachten ist, dass GNSS-Signale durch böswillige Drittanbietergeräte verschleiert oder blockiert werden können.
- Es dürfen für die NetModule-Router nur CE-konforme Netzteile mit strombegrenztem SELV-Ausgangskreis verwendet werden.
- Ein Netzteil der Leistungsklasse 3 (PS3) (mit 100 W oder mehr) darf nur unter der Bedingung verwendet werden, dass eine Kabelzugentlastung am Stromkabel zum Router angebracht ist. Eine solche Kabelzugentlastung stellt sicher, dass die Leiter am Schraubanschluss des Routers nicht unterbrochen werden (z. B. wenn sich der Router im Störfall im Kabel verwickeln würde). Die Kabelzugentlastung muss einer Zugkraft von 30 N (bei einem Routergewicht von bis zu 1 kg) standhalten, die auf das Kabel des Routers ausgeübt wird.

**Allgemeine Sicherheitsvorschriften:**

- Beachten Sie die Nutzungsbeschränkungen für Funkgeräte an Tankstellen, in chemischen Fabriken, in Anlagen, die Explosivstoffe enthalten, oder in sonstigen explosionsgefährdeten Bereichen.
- Die Geräte dürfen nicht in Flugzeugen verwendet werden.
- Besondere Vorsicht ist geboten in der Nähe von persönlichen medizinischen Hilfsmitteln wie z. B. Herzschrittmachern und Hörgeräten.
- Die NetModule-Router können in der Nähe von TV-Geräten, Radioempfängern und Computern Störungen verursachen.
- Führen Sie während eines Gewitters niemals Arbeiten am Antennensystem durch.
- Die Geräte sind im Allgemeinen für den normalen Gebrauch in Innenräumen ausgelegt. Setzen Sie die Geräte keinen außergewöhnlichen Umgebungsbedingungen jenseits von Schutzklasse IP40 aus.
- Schützen Sie die Geräte auch vor aggressiven Dämpfen und Feuchtigkeit oder vor Temperaturen außerhalb der Spezifikationen.
- Wir empfehlen dringend, von einer funktionierenden Systemkonfiguration eine Kopie zu erstellen und sicher zu verwahren. Diese kann anschließend einfach auch auf eine neuere Softwareversion übertragen werden.

2.2. Konformitätserklärung



NetModule erklärt hiermit in eigener Verantwortung, dass die Router den einschlägigen Normen nach den Bestimmungen der *Richtlinie 2014/53/EU des Rates*. Die signierte Version der *Konformitätserklärung* ist hier erhältlich: <https://www.netmodule.com/downloads>

2.3. Entsorgung



Laut Anforderungen der *Richtlinie 2012/19/EU des Rates* zu Elektro- und Elektronik-Altgeräten (WEEE) müssen Sie sicherstellen, dass dieses Produkt am Ende seiner Lebensdauer getrennt von anderen Reststoffen dem WEEE-Sammelsystem in Ihrem Land zum ordnungsgemäßen Recycling zugeführt wird.

2.4. Nationale Einschränkungen

Dieses Produkt darf generell in allen EU-Ländern (und anderen Ländern, in der die *RED-Richtlinie 2014/53/EU* gilt) ohne jede Einschränkung verwendet werden. Weitere nationale Vorschriften und An-

forderungen für Funkschnittstellen für einzelne Länder finden Sie in unserer WLAN-Datenbank.

2.5. Open-Source-Software

Hiermit informieren wir Sie, dass NetModule-Produkte Open-Source-Software enthalten können. Wir stellen Ihnen diese Open-Source-Software zur Verfügung unter den Bedingungen der GNU General Public License (GPL)¹, GNU Lesser General Public License (LGPL)² oder anderen Open-Source-Lizenzen³. Diese Lizenzen erlauben das Ausführen, Kopieren, Verteilen, Untersuchen, Ändern und Verbessern von Software, die unter die GPL, Lesser GPL oder andere Open-Source-Lizenzen fällt, ohne dass wir oder unser Endbenutzer-Lizenzvertrag Einschränkungen in Bezug auf die Nutzung dieser Software vorsehen. Sofern nicht durch geltendes Recht vorgeschrieben oder schriftlich vereinbart, wird Software, die unter Open-Source-Lizenzen vertrieben wird, wie besehen, ohne ausdrückliche oder stillschweigende Gewährleistung und ohne Bedingungen gleich welcher Art, bereitgestellt.

Um den entsprechenden Open-Source-Code zu erhalten, der unter diese Lizenzen fällt, wenden Sie sich bitte an unseren technischen Support unter router@support.netmodule.com.

Danksagungen

Dieses Produkt enthält:

- PHP, frei verfügbar unter <http://www.php.net>
- Software des OpenSSL-Projekts zur Verwendung im OpenSSL-Toolkit (<http://www.openssl.org>)
- Kryptografiesoftware von Eric Young (eay@cryptsoft.com)
- Software von Tim Hudson (tjh@cryptsoft.com)
- Software von Jean-loup Gailly und Mark Adler
- MD5 Message-Digest-Algorithmus von RSA Data Security, Inc.
- Eine Implementierung des AES-Verschlüsselungsalgorithmus, basierend auf dem von Dr. Brian Gladman veröffentlichten Code
- Arithmetischer Code für Operationen mit mehrfacher Genauigkeit, ursprünglich von David Ireland geschrieben
- Software aus dem FreeBSD-Projekt (<http://www.freebsd.org>)

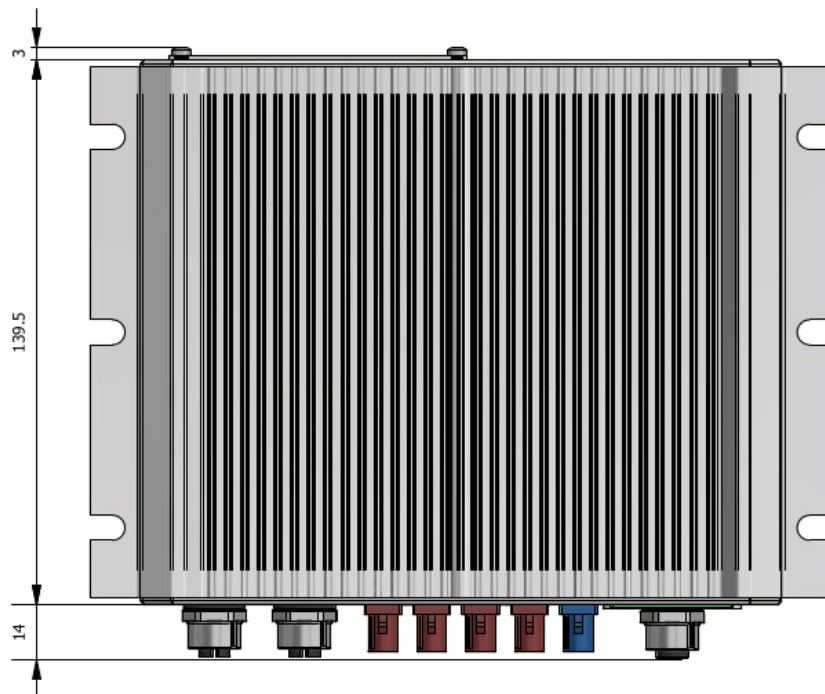
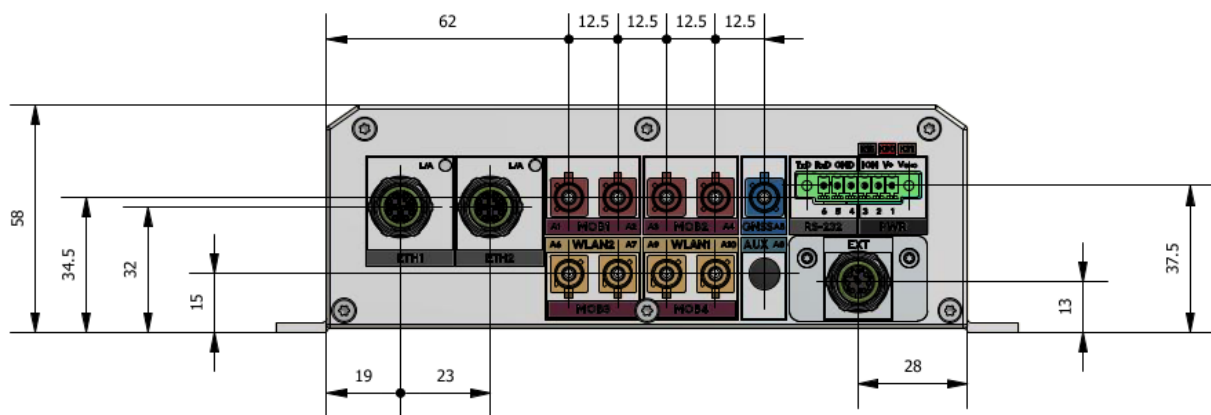
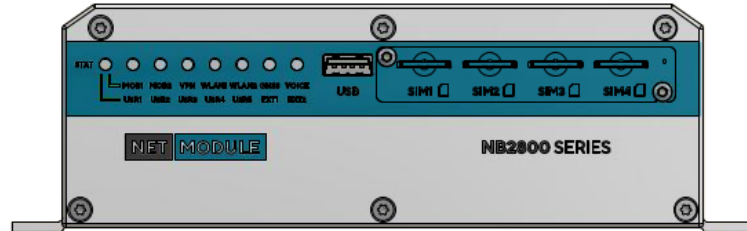
¹Den Wortlaut der GPL finden Sie unter <http://www.gnu.org/licenses/gpl-2.0.txt>

²Den Wortlaut der LGPL finden Sie unter <http://www.gnu.org/licenses/lgpl.txt>

³Den Wortlaut der OSI-Lizenzen (ISC, MIT, PHP v3.0, zlib) finden Sie unter <http://opensource.org/licenses>

3. Technische Daten

3.1. Erscheinungsbild



3.2. Funktionen

Alle NB2810-Modelle haben die folgenden Standardfunktionen:

- Spannungsversorgung mit Ignition Sense
- 2x Ethernet-Anschluss (10/100/1000 Mbit/s)
- 1x serielle Schnittstelle (RS-232)
- 1x USB 3.0-Host-Anschluss
- 4x Micro-SIM-Kartensteckplätze (3FF)
- 1 Erweiterungsanschluss

Der NB2810 kann mit den folgenden Optionen ausgestattet werden:

- LTE, UMTS, GSM
- WLAN IEEE 802.11
- GPS/GNSS
- RS-232
- RS-485
- IBIS
- CAN
- Audio
- Audio-PTT
- Digital I/O
- 1 TB interner Speicher
- Softwaretasten

Dank seines modularen Konzepts können der NB2810-Router und seine Hardwarekomponenten je beabsichtigtem Einsatzzweck konfiguriert werden. Bitte kontaktieren Sie uns, wenn Ihr Projekt spezielle Anforderungen mit sich bringt.

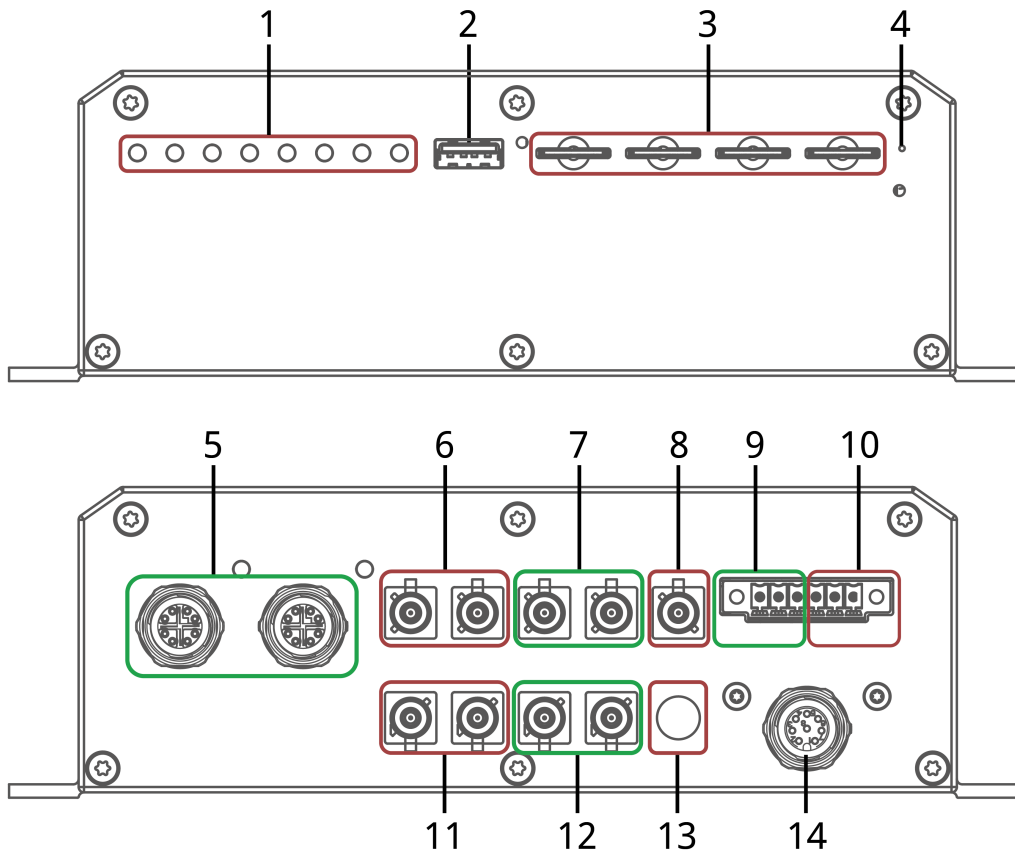
3.3. Umgebungsbedingungen

| Parameter | Rating |
|------------------------|---|
| Eingangsspannung | 12 V _{DC} bis 48 V _{DC} (±25 %) |
| Betriebstemperatur | –25 °C bis +70 °C |
| Lagertemperatur | –40 °C bis +85 °C |
| Rel. Luftfeuchtigkeit | 0 bis 95 % (nicht kondensierend) |
| Höhe ü. d. M. | bis zu 4000 m |
| Überspannungskategorie | I |
| Verschmutzungsgrad | 2 |
| Schutzklasse | IP40 (mit SIM- und USB-Abdeckungen) |

Tabelle 3.1.: Umgebungsbedingungen

3.4. Schnittstellen

3.4.1. Übersicht




















| Nr. | Beschreibung | Bedienfl. | Funktion |
|-----|----------------|-----------|--|
| 1 | LED-Anzeigen | Vorn | LED-Anzeigen für die verschiedenen Schnittstellen |
| 2 | USB | Vorn | USB-2.0-Host-Anschluss, z. B. für Software-/Konfigurations-Updates. |
| 3 | SIM 1-4 | Vorn | SIM 1-4(3FF), können per Konfiguration dynamisch einem beliebigen Modem zugeordnet werden. |
| 4 | Reset | Vorn | Schaltfläche für Neustart und Reset auf Werkseinstellungen |
| 5 | ETH 1-2 | Hinten | Gigabit-Ethernet-Anschlüsse, verwendbar als LAN- oder WAN-Schnittstelle. |
| 6 | MOB 1 | Hinten | 2x FAKRA-D-Codierbuchsen für MIMO-LTE-Antenne |
| 7 | MOB 2 | Hinten | 2x FAKRA-D-Codierbuchsen für MIMO-LTE-Antenne |
| 8 | GNSS | Hinten | FAKRA-C-Codierbuchse für GNSS-Antenne |
| 9 | RS-232 | Hinten | Nicht isolierte serielle RS-232-Schnittstelle (Pin 4 bis 6), die für die Konsolenverwaltung, serielle Geräteserver oder andere seriell basierte Kommunikationsanwendungen verwendet werden kann. |

| Nr. | Beschreibung | Bedienfe | Funktion |
|-----|---------------------|----------|--|
| 10 | PWR | Hinten | Netzteil 12-48 V _{DC} (Pin 1 und 2) und Zündung (Pin 3) |
| 11 | MOB 3/WLAN 2 | Hinten | 2x FAKRA-I/D-Codierbuchsen für MIMO-WLAN 2 oder MIMO-LTE-Antenne |
| 12 | MOB 4/WLAN 1 | Hinten | 2x FAKRA-I/D-Codierbuchsen für MIMO-WLAN- oder MIMO-LTE-Antenne |
| 13 | A8 | Hinten | Hilfsanschluss |
| 14 | EXT | Hinten | Erweiterung für Audio/CAN/IBIS/RS-232/RS-485/Audio-PTT. |

Tabelle 3.2.: NB2810-Schnittstellen

3.4.2. LED-Anzeigen

Die folgende Tabelle beschreibt die Statusanzeigen des NB2810.

| Bez. | Farbe | Status | Funktion |
|-------|--|--------|--|
| STAT |  | Blinkt | Das Gerät befindet sich in der Startsequenz oder im Software- oder Konfigurationsupdate. |
| |  | ein | Das Gerät ist bereit. Es gelten die Beschriftungen der oberen Bank. |
| |  | ein | Das Gerät ist bereit. Es gelten die Beschriftungen der unteren Bank. |
| MOB1 |  ^[1] | ein | Mobile Verbindung 1 ist aufgebaut. |
| |  | Blinkt | Mobile Verbindung 1 wird hergestellt. |
| |  | aus | Mobile Verbindung 1 ist unterbrochen. |
| MOB2 |  ^[1] | ein | Mobile Verbindung 2 ist aufgebaut. |
| |  | Blinkt | Mobile Verbindung 2 wird hergestellt. |
| |  | aus | Mobile Verbindung 2 ist unterbrochen. |
| VPN |  | ein | VPN-Verbindung ist aufgebaut. |
| |  | aus | VPN-Verbindung ist unterbrochen. |
| WLAN1 |  ^[1] | ein | WLAN-Verbindung 1 ist aufgebaut. |
| |  | Blinkt | WLAN-Verbindung 1 wird hergestellt. |
| |  | aus | WLAN-Verbindung 1 ist unterbrochen. |
| WLAN2 |  ^[1] | ein | WLAN-Verbindung 2 ist aufgebaut. |
| |  | Blinkt | WLAN-Verbindung 2 wird hergestellt. |
| |  | aus | WLAN-Verbindung 2 ist unterbrochen. |

| Bez. | Farbe | Status | Funktion |
|--------|-------|--------|--|
| GNSS | ● | ein | GNSS ist eingeschaltet und ein gültiger NMEA-Stream ist verfügbar. |
| | ● | Blinkt | GNSS sucht nach Satelliten. |
| | ○ | aus | GNSS ist ausgeschaltet oder kein gültiger NMEA-Stream ist verfügbar. |
| VOICE | ● | ein | Ein Sprachanruf ist aktiv. |
| | ○ | aus | Kein Sprachanruf ist aktiv. |
| USR1-5 | ● | ein | Benutzerdefiniert. |
| | ○ | aus | Benutzerdefiniert. |
| EXT1 | ● | ein | Erweiterungsanschluss 1 ist eingeschaltet. |
| | ○ | aus | Erweiterungsanschluss 1 ist ausgeschaltet. |
| EXT2 | ● | ein | Erweiterungsanschluss 2 ist eingeschaltet. |
| | ○ | aus | Erweiterungsanschluss 2 ist ausgeschaltet. |

^[1] Die Farbe der LED zeigt die Signalqualität für drahtlose Verbindungen an.

- Rot bedeutet niedrig
- Gelb bedeutet mäßig
- Grün bedeutet gut oder ausgezeichnet

Tabelle 3.3.: NB2810-Statusanzeigen

Ethernet-LEDs

Die folgende Tabelle beschreibt die Ethernet-Statusanzeigen.

| Bez. | Farbe | Status | Funktion |
|-------------------------|-------|--------|---|
| L/A (Link/Aktivität) | ● | ein | Verbindung ein (10 Mbit/s, 100 Mbit/s oder 1000 Mbit/s) |
| | ● | Blinkt | Aktivität |
| | ○ | aus | Keine Verbindung |

Tabelle 3.4.: Ethernet-Statusanzeigen

3.4.3. Reset

Die Reset-Taste hat zwei Funktionen:

1. System-Neustart:
Drücken Sie mindestens 3 Sekunden, um einen Systemneustart auszulösen.
Der Neustart wird durch die rot blinkende STAT-LED angezeigt.
2. Zurücksetzen auf Werkseinstellungen:

Drücken Sie mindestens 10 Sekunden, um das Gerät auf Werkseinstellungen zurückzusetzen. Die Aktion wird bestätigt, indem alle LEDs eine Sekunde lang aufleuchten.

3.4.4. Mobile Kommunikation

Die verschiedenen Varianten des NB2810 unterstützen bis zu 4 WWAN-Module für die mobile Kommunikation. Die LTE-Module unterstützen 2x2 MIMO.

| Standard | Frequenzbänder |
|--|--|
| EDGE/GPRS/GSM | B5 (850), B8 (900), B3 (1800), B2 (1900) |
| DC-HSPA+/UMTS | B5 (850), B8 (900), B2 (1900), B1 (2100) |
| LTE-, UMTS-, GSM-Modem für EMEA (Cat. 4) | B1 (2100), B3 (1800), B5 (850), B7 (2600), B8 (900), B20 (800) |
| LTE Advanced, UMTS für EMEA (Cat. 6) | B30 (2300 WCS), B41 (TDD 2500), B29 (US 700de Lower), B26 (US 850 Ext), B25 (1900), B5 (850), B20 (800DD), B13 (700c), B12 (700ac), B7 (2600), B4 (AWS), B3 (1800), B2 (1900), B1 (2100) |

Tabelle 3.5.: Mobile Schnittstelle

Hinweis: Diese Aufzählung erhebt keinen Anspruch auf Vollständigkeit.

Die Mobilfunk-Antennenanschlüsse sind wie folgt spezifiziert:

| Funktion | Spezifikation |
|---|---|
| Max. zulässige Kabellänge | 30 m |
| Max. zulässiger Antennengewinn einschließlich Kabeldämpfung | 2,5 dBi |
| Min. Abstand zwischen kollokierten Antennen | 20 cm |
| Min. Abstand zwischen Personen und Antenne | 40 cm |
| Verbindertyp | Option Jf: FAKRA (Standard) Option Js: SMA |

Tabelle 3.6.: Spezifikation des mobilen Antennenanschlusses

3.4.5. WLAN

Die Varianten des NB2810 unterstützen bis zu 2 WLAN-Module nach 802.11 a/b/g/n/ac.

| Standard | Frequenzen | Bandbreite | Datenrate |
|----------|---------------|--------------|--------------|
| 802.11a | 5 GHz | 20 MHz | 54 Mbit/s |
| 802.11b | 2,4 GHz GHz | 20 MHz | 11 Mbit/s |
| 802.11g | 2,4 GHz GHz | 20 MHz | 54 Mbit/s |
| 802.11n | 2,4/5 GHz GHz | 20/40 MHz | 300 Mbit/s |
| 802.11ac | 5 GHz | 20/40/80 MHz | 866,7 Mbit/s |

Tabelle 3.7.: IEEE 802.11-Norm

Hinweis: 802.11n und 802.11ac unterstützen 2x2 MIMO.

Die WLAN-Antennenanschlüsse sind wie folgt spezifiziert:

| Funktion | Spezifikation |
|---|---|
| Max. zulässige Kabellänge | 30 m |
| Max. zulässiger Antennengewinn einschließlich Kabeldämpfung | 3,0 dBi ¹ |
| Min. Abstand zwischen kollokierten Antennen (Beispiel: WLAN1 zu MOB1) | 20 cm |
| Min. Abstand zwischen Personen und Antenne | 40 cm |
| Verbindertyp | Option Jf: FAKRA (Standard) Option Js: SMA |

Tabelle 3.8.: Spezifikation des WLAN-Antennenanschlusses

¹**Hinweis:** WLAN-Antennen mit höherer Verstärkung dürfen mit der NetModule-Router-Softwarelizenz „Enhanced RF Configuration“ und der von zertifiziertem Fachpersonal korrekt konfigurierten Antennenverstärkung und Kabeldämpfung verwendet werden.

3.4.6. GNSS

GNSS (Option G)

Das GNSS wird von einem WWAN-Modul aus verwendet.

| Funktion | Spezifikation |
|--------------------------|--|
| Systeme | GPS/GLONASS (GALILEO/BEIDOU je nach Modul) |
| Datenstrom | JSON oder NMEA |
| Tracking-Empfindlichkeit | Bis zu -165 dBm |
| Unterstützte Antennen | Aktiv und passiv |

Tabelle 3.9.: GNSS-Spezifikationen, Option G

GNSS (Option Gd)

Das GNSS-Modul unterstützt Dead Reckoning mit eingebautem 3-D-Beschleunigungsmesser und 3-D-Gyroskop.

| Funktion | Spezifikation |
|--------------------------|--|
| Systeme | Vorbereitet für GPS/GLONASS/BEIDOU/GALILEO |
| Datenstrom | NMEA oder UBX |
| Kanäle | 72 |
| Tracking-Empfindlichkeit | Bis zu -160 dBm |
| Accuracy | Bis 2,5 m Streukreisradius |
| Dead-Reckoning-Modi | UDR: Untethered Dead Reckoning ADR: Automotive Dead Reckoning |
| Unterstützte Antennen | Aktiv und passiv |

Tabelle 3.10.: GNSS-Spezifikationen (Option Gd)

Der GNSS-Antennenanschluss ist wie folgt spezifiziert:

| Funktion | Spezifikation |
|---|---|
| Max. zulässige Kabellänge | 30 m |
| Max. zulässiger Antennengewinn | 3,0 dBi |
| Min. Abstand zwischen kollokierten Antennen (Beispiel: WLAN1 zu MOB1) | 20 cm |
| Verbindertyp | Option Jf: FAKRA (Standard) Option Js: SMA |

| Funktion | Spezifikation |
|----------|---------------|
|----------|---------------|

Tabelle 3.11.: Spezifikation des GNSS-/GPS-Antennenanschlusses

3.4.7. USB 3.0-Host-Anschluss

Der USB-3.0-Host-Anschluss ist wie folgt spezifiziert:

| Funktion | Spezifikation |
|------------------|-------------------------------|
| Geschwindigkeit | Low-, Full-, Hi-, Super-Speed |
| Stromstärke | max. 950 mA |
| Max. Kabellänge | 3 m |
| Kabelabschirmung | Obligatorisch |
| Verbindertyp | Typ A |

Tabelle 3.12.: Spezifikation des USB-3.0-Host-Anschlusses

3.4.8. M12-Ethernet-Steckverbinder

Spezifikation

Die Ethernet-Anschlüsse sind wie folgt spezifiziert:

| Funktion | Spezifikation |
|----------------------------------|-----------------------|
| Galvanische Trennung vom Gehäuse | 1500 V _{DC} |
| Geschwindigkeit | 10/100/1000 Mbit/s |
| Mode | Halb- und Vollduplex |
| Crossover | Automatisch MDI/MDI-X |
| Max. Kabellänge | 100 m |
| Kabeltyp | CAT 5e oder höher |
| Kabelabschirmung | Obligatorisch |
| Verbindertyp | M12, x-codiert |

Tabelle 3.13.: Spezifikation des Ethernet-Anschlusses

Pinbelegung

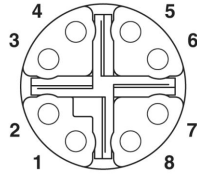
| Pin | Signal | Pins |
|-----|---------|---|
| 1 | M1+/DA+ |  |
| 2 | M1-/DA- | |
| 3 | M0+/DB+ | |
| 4 | M0-/DB- | |
| 5 | M2+/DD+ | |
| 6 | M2-/DD- | |
| 7 | M3-/DC- | |
| 8 | M3+/DC+ | |

Tabelle 3.14.: Pinbelegung der 8-poligen Ethernet-Stecker

3.4.9. Netzteil

NB2810 Router besitzen einen nicht isolierten Netzteileingang. Der Anschluss für die Spannungsversorgung ist wie folgt spezifiziert:

| Funktion | Spezifikation |
|---------------------------------------|---|
| Netzteil, Nennspannungen: | 12 V _{DC} , 24 V _{DC} , 36 V _{DC} und 48 V _{DC} |
| Spannungsbereich | 12 V _{DC} bis 48 V _{DC} ($\pm 25\%$) |
| Max. Leistungsaufnahme | 20 W |
| Leistungsaufnahme im Aus-Zustand (V+) | 12 V: max. 0,23 mA / 2,8 mW |
| | 24 V: max. 0,34 mA / 8,1 mW |
| | 36 V: max. 0,44 mA / 15,6 mW |
| | 48 V: max. 0,56 mA / 27,1 mW |
| Max. Kabellänge | 30 m |
| Kabelabschirmung | nicht erforderlich |

Tabelle 3.15.: Spannungsversorgung

Steckertyp und Anschlussbelegung siehe Kapitel [3.4.11](#).

3.4.10. RS-232

Der RS-232-Anschluss ist wie folgt spezifiziert (Fettdruck zeigt Standardkonfiguration an):

| Funktion | Spezifikation |
|----------------------------------|--|
| Protokoll | 3-Draht-RS-232: GND, TXD, RXD |
| Baudrate | 300, 1 200, 2 400, 4 800, 9 600, 19 200, 38 400, 57 600, 115 200 , 230 400, 460 800 |
| Datenbits | 7 bit, 8 bit |
| Parität | keine , ungerade, gerade |
| Stopbits | 1 , 2 |
| Software-Datenflusssteuerung | keine , XON/XOFF |
| Hardware-Datenflusssteuerung | keine |
| Galvanische Trennung vom Gehäuse | keine |
| Max. Kabellänge | 10 m |
| Kabelabschirmung | nicht erforderlich |

Tabelle 3.16.: Spezifikation des RS-232-Anschlusses

Steckertyp und Anschlussbelegung siehe Kapitel [3.4.11](#).

3.4.11. 6-poliger Terminierungsblock

Das Netzteil und die serielle Schnittstelle teilen sich den 6-poligen Terminierungsblock.

| Funktion | Spezifikation |
|--------------|---|
| Verbindertyp | 6-poliger Terminierungsblock 3,5 mm (Schraubverriegelung) |

Tabelle 3.17.: Klemmenblockstecker

Pinbelegung

| | Pin | Name | Beschreibung |
|-------|-----|------------------|---|
| PWR | 1 | V _{GND} | Spannungsversorgung Masse |
| | 2 | V ₊ | Spannungsversorgung (12 V _{DC} bis 48 V _{DC}) |
| | 3 | IGN | Spannung Zündeingang (12 V _{DC} bis 48 V _{DC}) |
| RS232 | 4 | GND | RS-232 Masse (nicht isoliert) |
| | 5 | RxD | RS-232 RxD (nicht isoliert) |
| | 6 | TxD | RS-232 TxD (nicht isoliert) |

Tabelle 3.18.: Pinbelegung des Terminierungsblocks

3.4.12. Erweiterungsanschluss

Verfügbare Optionen

Der NB2810 besitzt eine M12-A-kodierte Erweiterungsbuchse mit 8 Pins. Die 8 Pins teilen sich auf zwei logische Anschlüsse auf: Pin 1 bis 4 für Erweiterungsanschluss 1 (EP1), Pin 5 bis 8 für Erweiterungsanschluss 2 (EP2). Am EP1 und am EP2 können die folgenden Schnittstellen vorhanden sein:

- Audio (Option A)
- CAN (Option C)
- IBIS (Option I)
- Isolierter RS-485 (Option Sa)
- Isolierter RS-232 (Option Sb)
- Audio PTT (Option Ap)
- Isolierter digitaler Ein-/Ausgang (Option D)



Vorsicht: Wenn für EP1 und EP2 zwei verschiedene Schnittstellen verwendet werden, ist die geringere Isolierung der beiden obligatorisch. Der Stecker selbst besitzt eine Pin-zu-Pin-Isolierung von 800 VDC.

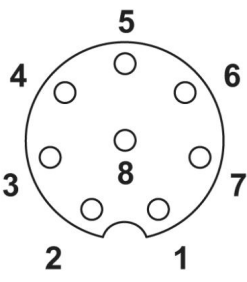
| Pin | Signal | Pins |
|-----|-------------|---|
| 1 | EP1 - Pin 1 |  |
| 2 | EP1 - Pin 2 | |
| 3 | EP1 - Pin 3 | |
| 4 | EP1 - Pin 4 | |
| 5 | EP2 - Pin 1 | |
| 6 | EP2 - Pin 2 | |
| 7 | EP2 - Pin 3 | |
| 8 | EP2 - Pin 4 | |

Tabelle 3.19.: Pinbelegung des Erweiterungsanschlusses

Spezifikation des Audio-Anschlusses (Option A)

Der Audio-Anschluss ist wie folgt spezifiziert:

| Funktion | Spezifikation |
|---|---|
| Protokoll | Audio Line In/Line Out |
| Eingangsreferenzpegel 0 dBFS | Signalpegel 1,9 V _{pp} |
| Eingangsimpedanz | 21 kΩ |
| Eingangsbandbreite | 100 Hz- 15 kHz |
| Galvanische Trennung Eingang zu Gehäuse | funktionell (max. 100 V _{DC}) |
| Ausgangsspannung @ 0 dBFS | 600 Ω, Signalpegel 3.7 V _{pp} |
| Ausgangsbandbreite | 300 Hz- 4 kHz |
| Galvanische Trennung Ausgang zu Gehäuse | funktionell (max. 100 V _{DC}) |
| Max. Kabellänge | 30 m |
| Kabelabschirmung | Obligatorisch |

Tabelle 3.20.: Spezifikation des Audio-Anschlusses

| EP-Pins | Signal |
|---------|-----------------|
| 1/5 | Eingangskanal + |
| 2/6 | Eingangskanal – |
| 3/7 | Ausgangskanal – |
| 4/8 | Eingangskanal + |

Tabelle 3.21.: Pinbelegung der Audioausgänge (EP1/EP2)

Hinweis: Bei Stereobetrieb liegt der linke Kanal auf EP1.

Spezifikation des CAN-Anschlusses (Option C)

Der CAN-Anschluss ist wie folgt spezifiziert:

| Funktion | Spezifikation |
|----------------------------------|--|
| Protokoll | CAN V2.0B |
| Geschwindigkeit | Bis zu 1 Mbit/s Standard: 125 kbit/s |
| Galvanische Trennung vom Gehäuse | 1500 V _{DC} |
| Interne Bus-Terminierung | keine |
| Externe Bus-Terminierung | 120 Ω |
| Max. Kabellänge | 100 m |
| Kabelabschirmung | Obligatorisch |
| Kabeltyp | Twisted Pair |
| Max. Anzahl Knoten | 110 |
| Reaktionslos | Option Cm: CAN-Passiv (nur Monitoring) Option Cn: CAN-Aktiv (RX und TX aktiviert) |

Tabelle 3.22.: Spezifikation des CAN-Anschlusses

| EP-Pins | Signal |
|---------|---------|
| 1/5 | CAN GND |
| 2/6 | L |
| 3/7 | H |
| 4/8 | – |

Tabelle 3.23.: Pinbelegung der CAN-Anschlüsse (EP1/EP2)

¹**Hinweis:** An jedem Ende des CAN-Busses ist eine 120-Ω-Terminierung obligatorisch

Spezifikation des 4xCAN-Anschlusses (Option 4C)

Bei Verwendung von vier CAN-Schnittstellen gilt eine andere Spezifikation.

| Funktion | Spezifikation |
|----------------------------------|--|
| Protokoll | CAN V2.0B |
| Geschwindigkeit | Bis zu 1 Mbit/s Standard: 125 kbit/s |
| Galvanische Trennung vom Gehäuse | Nein |
| Interne Bus-Terminierung | keine |
| Externe Bus-Terminierung | 120 Ω |
| Max. Kabellänge | 100 m |
| Kabelabschirmung | Obligatorisch |
| Kabeltyp | Twisted Pair |
| Max. Anzahl Knoten | 110 |
| Reaktionslos | Option Cm: CAN-Passiv (nur Monitoring) Option Cn: CAN-Aktiv (RX und TX aktiviert) |

Tabelle 3.24.: Spezifikation des 4xCAN-Anschlusses

| EP-Pins | Signal |
|---------|----------------------|
| 1 | CAN1-H |
| 2 | CAN1-L |
| 3 | CAN2-H |
| 4 | CAN2-L |
| 5 | CAN3-H |
| 6 | CAN3-L |
| 7 | CAN4-H |
| 8 | CAN4-L |
| Schirm | CAN1-4 GND = Gehäuse |

Tabelle 3.25.: Pinbelegung der 4xCAN-Anschlüsse

Hinweis: Da der Erweiterungsstecker nur 8 Pins hat, werden alle CAN-GND (von den isolierten CAN-Modulen) mit dem Schirm des M12-Steckers verbunden, der auch Gehäuse-GND ist. Die Schnittstellen sind dann also nicht mehr isoliert!

¹**Hinweis:** An jedem Ende des CAN-Busses ist eine 120-Ω-Terminierung obligatorisch

Spezifikation des IBIS-Anschlusses (Option I)

Der IBIS-Anschluss ist wie folgt spezifiziert:

| Funktion | Spezifikation |
|----------------------------------|---|
| Protokoll | IBIS-Wagenbus nach VDV300 und VDV301 |
| Gerätetyp | IBIS-Peripheriegerät nach VDV300 und VDV301 |
| Geschwindigkeit | 1200 Baud |
| Galvanische Trennung vom Gehäuse | 1500 V _{DC} |
| Max. Kabellänge | 100 m |
| Kabelabschirmung | nicht erforderlich |

Tabelle 3.26.: Spezifikation des IBIS-Anschlusses

| EP-Pins | Signal |
|---------|---------------------------------|
| 1/5 | WBSD (Signalruf/Aufrufbus) |
| 2/6 | WBMS (GND-Ruf/Aufrufbus) |
| 3/7 | WBED (Signalantwort/Antwortbus) |
| 4/8 | WBME (GND-Antwort/Antwortbus) |

Tabelle 3.27.: Pinbelegung der IBIS-Anschlüsse (EP1/EP2)

Spezifikation des isolierten 5-Draht-RS-232-Anschlusses (Option Sb)

Der isolierte 5-Draht-RS-232-Anschluss ist wie folgt spezifiziert (Fettdruck zeigt Standardkonfiguration an):

| Funktion | Spezifikation |
|----------------------------------|---|
| Protokoll | 5-Draht-RS-232: GND, TXD, RXD |
| Baudrate | 600, 1 200, 2 400, 4 800, 9 600, 19 200, 38 400, 57 600, 115 200 , 230 400, 460 800, 921 600 |
| Datenbits | 7 bit, 8 bit |
| Parität | keine , ungerade, gerade |
| Stopbits | 1 , 2 |
| Software-Datenflusssteuerung | keine , XON/XOFF |
| Hardware-Datenflusssteuerung | keine |
| Galvanische Trennung vom Gehäuse | 1500 V _{DC} |
| Max. Kabellänge | 10 m |
| Kabelabschirmung | Obligatorisch |

Tabelle 3.28.: Spezifikation des isolierten RS-232-Anschlusses

| EP-Pins | Signal |
|---------|--------|
| 1 | GND |
| 2 | TxD |
| 3 | RxD |
| 4 | – |
| 5 | CTS |
| 6 | RTS |
| 7 | – |
| 8 | – |

Tabelle 3.29.: Pinbelegung der RS-232-Portsignale (EP1/EP2)

Spezifikation des isolierten RS-485-Anschlusses (Option Sa)

Der RS-485-Anschluss ist wie folgt spezifiziert (Fettdruck zeigt Standardkonfiguration an):

| Funktion | Spezifikation |
|-------------------------------------|--|
| Protokoll | 3-Draht-RS-485 (GND, A, B) |
| Baudrate | 600, 1 200, 2 400, 4 800, 9 600, 19 200, 38 400, 57 600, 115 200 , 230 400, 460 800 |
| Datenbits | 7 bit, 8 bit |
| Parität | keine , ungerade, gerade |
| Stopbits | 1 , 2 |
| Software-Datenflusssteuerung | keine , XON/XOFF |
| Hardware-Datenflusssteuerung | keine |
| Galvanische Trennung vom Gehäuse | 1500 V _{DC} |
| Interne Bus-Terminierung | keine |
| Max. Kabellänge | 10 m |
| Kabelabschirmung | Obligatorisch |
| Kabeltyp | Twisted Pair |
| Max. Anzahl Transceiver auf dem Bus | 256 |
| Max. Anzahl Knoten | 256 |

Tabelle 3.30.: Spezifikation des RS-485-Anschlusses

| EP-Pins | Signal |
|---------|--|
| 1/5 | GND |
| 2/6 | TxD ⁻ /RxD ⁻ (A) |
| 3/7 | TxD ⁺ /RxD ⁺ (B) |
| 4/8 | – |

Tabelle 3.31.: Pinbelegung der RS-485-Portsignale (EP1/EP2)

Spezifikation für Audio-PTT (Option Ap)

Audio-PTT (push to talk) hat folgende Spezifikation gemeinsam:

| Funktion | Spezifikation |
|----------------------------|---|
| Isolierung vom Gehäuse/GND | funktionell (max. 100 V _{DC}) |
| Max. Kabellänge | 30 m |
| Kabelabschirmung | Obligatorisch |

Tabelle 3.32.: Gemeinsame PTT-Spezifikation

Das Audiosignal ist wie folgt spezifiziert:

| Funktion | Spezifikation |
|------------------------------|--|
| Anzahl Anschlüsse | 1x Line In/1x Line Out |
| Eingangsreferenzpegel 0 dBFS | Signalpegel 1,9 V _{pp} |
| Eingangsimpedanz | 21 kΩ |
| Eingangsbandbreite | 100 Hz- 15 kHz |
| Ausgangsspannung @ 0 dBFS | 600 Ω, Signalpegel 3.7 V _{pp} |
| Ausgangsbandbreite | 300 Hz- 4 kHz |

Tabelle 3.33.: Spezifikation des Audio-Anschlusses

Das digitale Eingangssignal ist wie folgt spezifiziert:

| Funktion | Spezifikation |
|---|----------------------|
| Anzahl Anschlüsse | 1x digitaler Eingang |
| Max. Eingangsspannung | 60 V _{DC} |
| Max. Eingangsstrom | 2 mA |
| Verpolungsschutz | Ja |
| Min. Spannung für Level 1 (eingestellt) | 7,2 V _{DC} |
| Max. Spannung für Stufe 0 (nicht eingestellt) | 5,0 V _{DC} |

Tabelle 3.34.: Spezifikation des digitalen Eingangs

Hinweis: Eine negative Eingangsspannung wird nicht erkannt.

Das digitale Ausgangssignal ist wie folgt spezifiziert:

| Funktion | Spezifikation |
|----------------------------------|---|
| Anzahl Anschlüsse | 1x digitaler Ausgang (NO) |
| Max. Dauerausgangsstrom | 1 A |
| Max. Ausgangsspannung, schaltend | 60 V _{DC} , 42 V _{AC} (V _{rms}) |
| Max. Schaltleistung | 60 W |

Tabelle 3.35.: Spezifikation des digitalen Ausgangs

| Pin | Signal |
|-----|---------------|
| 1 | Line IN + |
| 2 | Line IN – |
| 3 | Digital IN + |
| 4 | Digital OUT + |
| 5 | Digital OUT – |
| 6 | Digital IN – |
| 7 | Line OUT + |
| 8 | Line OUT – |

Tabelle 3.36.: Pinbelegung des Audio-PTT-Steckers

Digitale Ein- und Ausgänge (Option 2D)

Die isolierten Ein- und Ausgänge sind alle wie folgt spezifiziert:

| Funktion | Spezifikation |
|----------------------------|----------------------|
| Isolierung vom Gehäuse/GND | 1500 V _{DC} |
| Max. Kabellänge | 30 m |
| Kabelabschirmung | nicht erforderlich |

Tabelle 3.37.: Gemeinsame Spezifikation für die digitalen Ein- und Ausgänge

Das digitale Eingangssignal ist wie folgt spezifiziert:

| Funktion | Spezifikation |
|---|---------------------|
| Anzahl Anschlüsse | 2 |
| Max. Eingangsspannung | 60 V _{DC} |
| Max. Eingangsstrom | 2 mA |
| Verpolungsschutz | Ja |
| Min. Spannung für Level 1 (eingestellt) | 7,2 V _{DC} |
| Max. Spannung für Stufe 0 (nicht eingestellt) | 5,0 V _{DC} |

Tabelle 3.38.: Spezifikation des nicht isolierten Digitalanschlusses

Hinweis: Negative Eingangsspannungen werden nicht erkannt.

Das digitale Ausgangssignal ist wie folgt spezifiziert:

| Funktion | Spezifikation |
|----------------------------------|---|
| Anzahl Anschlüsse | 1xNO/1xNC |
| Max. Dauerausgangsstrom | 1 A |
| Max. Ausgangsspannung, schaltend | 60 V _{DC} , 42 V _{AC} (V _{rms}) |
| Max. Schaltleistung | 60 W |

Tabelle 3.39.: Spezifikation des isolierten digitalen Ausgangs

| EP-Pins | Signal |
|---------|---------------------------|
| 1 | DI1+ |
| 2 | DI1- |
| 3 | DI2+ |
| 4 | DI2- |
| 5 | DO1: Stromlos offen |
| 6 | DO1: Stromlos offen |
| 7 | DO2: Stromlos geschlossen |
| 8 | DO2: Stromlos geschlossen |

Tabelle 3.40.: Pinbelegung der Variante mit zwei digitalen Ein-/Ausgängen

Hinweis: Auf Anfrage: 1xDIn, 1xDOut

3.5. Datenspeicherung (Option Dx)

Der integrierte Massenspeicher arbeitet unabhängig von den Routerfunktionen und ist für Kundenanwendungen wie Datenerfassung oder Fahrgastunterhaltung vorgesehen. Auf den Speicher kann über das SDK zugegriffen werden. Weitere Einzelheiten finden Sie im SDK-API-Handbuch, Abschnitt 2.2.

Folgende Optionen stehen zur Verfügung:

| Option | Kapazität |
|--------|-----------|
| Da | 32 GB |
| Db | 64 GB |
| Dc | 128 GB |
| Dd | 256 GB |
| De | 512 GB |
| Df | 1 TB |

Tabelle 3.41.: Speicherspezifikationen

4. Installation

Der NB2810 ist für die Montage auf einer Arbeitsplatte oder an einer Wand (Nur für die Montage in Höhen kleiner gleich 2 m geeignet) vorgesehen, die Installationsanweisungen für dieses Gerät müssen befolgt werden,

<https://www.netmodule.com/support/downloads/zeichnungen>.

Bitte beachten Sie die Sicherheitshinweise in Kapitel 2 und die Umgebungsbedingungen in Kapitel 3.3.

Vor der Installation des NB2810-Routers sind die folgenden Vorsichtsmaßnahmen zu treffen:

- Direkte Sonneneinstrahlung vermeiden
- Das Gerät vor Feuchtigkeit, Dampf und aggressiven Flüssigkeiten schützen
- Für eine ausreichende Luftzirkulation um das Gerät herum sorgen
- Das Gerät ist nur für den Gebrauch im Innenbereich geeignet



Vorsicht: NetModule-Router sind nicht für den Vertrieb an Endverbraucher bestimmt. Das Gerät darf nur durch zertifiziertes Personal installiert und in Betrieb genommen werden.

4.1. Installation von Micro-SIM-Karten(3FF)

Es können bis zu vier Micro-SIM-Karten (3FF) in einen NB2810-Router eingesetzt werden. Eine SIM-Karte als Multiformat-Karte, sogenannte 3-in-1-Karte (All-in-One SIM oder Triple-SIM) mit dem Format 2FF, 3FF und 4FF werden nicht unterstützt.

SIM-Karten können durch Einschieben in einen der dafür vorgesehenen Steckplätze an der Vorderseite eingesetzt werden. Sie müssen die SIM-Karte mit einer kleinen Büroklammer (oder ähnlichem) eindrücken, bis sie einrastet. Um die SIM-Karte zu entfernen, müssen Sie auf dieselbe Weise erneut die Karte eindrücken. Die SIM-Karte federt dann zurück und kann entnommen werden.

SIM-Karten können einem beliebigen Modem im System zugeordnet werden. Es ist auch möglich, eine SIM-Karte während des Betriebs einem anderen Modem zuzuordnen, zum Beispiel, wenn Sie unter bestimmten Bedingungen einen anderen Anbieter nutzen möchten. Ein SIM-Wechsel dauert jedoch in der Regel etwa 10-20 Sekunden, was (z.B. beim Hochfahren) bei sinnvoll installierten SIMs umgangen werden kann. Wenn Sie nur eine einzige SIM-Karte und ein Modem verwenden, sollte die Karte vorzugsweise in SIM 1 eingesetzt werden. Für Systeme, die zwei Modems mit zwei SIMs parallel nutzen sollen, empfehlen wir, **MOB 1** der SIM 1, **MOB 2** der SIM 2 zuzuordnen und so weiter.

Weitere Informationen zur SIM-Konfiguration finden Sie im Kapitel 5.3.3.



Vorsicht: Nach einem SIM-Wechsel muss die SIM-Abdeckung des NB2810-Routers wieder montiert und verschraubt werden, um die Schutzart IP40 weiter zu gewährleisten.

4.2. Installation der GSM-/UMTS-/LTE-Antennen

NetModule-Router arbeiten im Mobilfunknetz nur dann effizient, wenn ein gutes Signal vorhanden ist. Eine Stummelantenne ist für die meisten Anwendungen ausreichend. Jedoch kann es unter Umständen notwendig sein, externe Antennen mit Verlängerungskabel zu verwenden, um einen besseren Standort mit einem ausreichenden Signal zu erreichen. Im Zweifelsfall nehmen Sie bitte Kontakt mit uns auf. Wir helfen Ihnen gern, die beste Antennenkonfiguration für Ihre Anwendung zu finden.

Beachten Sie, dass durch Faradaysche Käfige wie große Metallflächen (Aufzüge, Maschinengehäuse usw.), engmaschige Eisenkonstruktionen und Ähnliches verursachte Effekte den Signalempfang erheblich verschlechtern können.

Die folgende Tabelle zeigt, wie die LTE-/UMTS-Antennen angeschlossen werden. Im Allgemeinen verwenden LTE-Antennen sowohl den Haupt- als auch den Hilfsanschluss, während UMTS nur den Hauptanschluss benötigt.

| Antennenanschluss | Typ |
|-------------------|--------|
| MOB 1 A1 | Haupt- |
| MOB 1 A2 | Hilfs- |
| MOB 2 A3 | Haupt- |
| MOB 2 A4 | Hilfs- |
| MOB 3 A6 | Haupt- |
| MOB 3 A7 | Hilfs- |
| MOB 4 A9 | Haupt- |
| MOB 4 A10 | Hilfs- |

Tabelle 4.1.: Typen von LTE-/UMTS-Antennenanschlüssen

**Vorsicht:**

Bei der Installation der Antenne unbedingt zu beachten, Kapitel [2](#)

4.3. Installation der WLAN-Antennen

Die folgende Tabelle zeigt, wie die WLAN-Antennen angeschlossen werden. Die Anzahl der angeschlossenen Antennen kann per Software konfiguriert werden. Wenn nur eine Antenne verwendet wird, muss diese am Hauptanschluss angeschlossen sein. Für eine vielseitigere Ausrichtung (und damit einen besseren Durchsatz und eine bessere Abdeckung) empfehlen wir jedoch dringend die Verwendung von zwei Antennen.

| Antennenanschluss | Typ |
|-------------------|--------|
| WLAN 1 A9 | Haupt- |
| WLAN 1 A10 | Hilfs- |
| WLAN 2 A6 | Haupt- |

| Antennenanschluss | Typ |
|-------------------|--------|
| WLAN 2 A7 | Hilfs- |

Tabelle 4.2.: Typen von WLAN-Antennenanschlüssen



Vorsicht:

Bei der Installation der Antenne unbedingt zu beachten, Kapitel [2](#)

4.4. Installation der GNSS-Antenne

Die GNSS-Antenne muss an den Anschluss **GNSS** angeschlossen werden. Ob die Antenne eine aktive oder passive GNSS-Antenne ist, muss in der Software konfiguriert werden. Wir empfehlen eine aktive GNSS-Antenne für eine hochgenaue GNSS-Ortung.

**Vorsicht:**

Bei der Installation der Antenne unbedingt zu beachten, Kapitel [2](#)

4.5. Installation des lokalen Netzwerks (LAN)

Bis zu zwei 10/100/1000-Mbit/s-Ethernet-Geräte können direkt an den Router angeschlossen werden. Weitere Geräte können über einen zusätzlichen Ethernet-Switch angeschlossen werden. Vergewissern Sie sich, dass der Stecker richtig in den Anschluss **ETH** eingestellt ist und dauerhaft fest sitzt, da es sonst zu sporadischen Verbindungsabbrüchen im Betrieb kommen kann. Die Verbindungs-LED Link/Act leuchtet, sobald das Gerät synchronisiert ist. Wenn nicht, muss möglicherweise eine andere Verbindungseinstellung konfiguriert werden, wie beschrieben in Kapitel [5.3.2](#). Standardmäßig ist der Router als DHCP-Server konfiguriert und hat die IP-Adresse 192.168.1.1.

**Vorsicht:**

Es darf nur ein geschirmtes Ethernet-Kabel verwendet werden.

4.6. Installation des Netzteils und verzögertes Ausschalten

Der Router kann über eine externe Spannungsquelle mit einer Spannung zwischen 12 V_{DC} und 48 V_{DC} versorgt werden. Er ist mit einem zertifizierten Netzteil (CE-konform oder gleichwertig) mit strombegrenztem SELV-Ausgangskreis zu verwenden. Der Router ist nun bereit für die Inbetriebnahme.

Wenn keine verzögerte Abschaltung erforderlich ist, schließen Sie die Versorgungsspannung sowohl an IGN als auch an V+ an. Bei Verwendung der Funktion "Verzögertes Ausschalten" muss die V+ direkt mit dem Batteriestromkreis und IGN mit dem Zündstromkreis des Fahrzeugs verbunden. Mit dieser Funktion schaltet sich der Router nach einer definierten Zeit (per SW konfigurierbar) nach Ausschalten des Fahrzeugs ab, anstatt sofort herunterzufahren.



Vorsicht: Die folgenden Punkte sind unbedingt zu beachten:

- Es dürfen für die NetModule-Router nur CE-konforme Netzteile mit strombegrenztem SELV-Ausgangskreis verwendet werden.
- Ein Netzteil der Leistungsklasse 3 (PS3) (mit 100 W oder mehr) darf nur unter der Bedingung verwendet werden, dass eine Kabelzugentlastung am Stromkabel zum Router angebracht ist. Eine solche Kabelzugentlastung stellt sicher, dass die Leiter am Schraubanschluss des Routers nicht unterbrochen werden (z. B. wenn sich der Router im Störfall im Kabel verwickeln würde). Die Kabelzugentlastung muss einer Zugkraft von 30 N (bei einem Routergewicht von bis zu 1 kg) resp. 60 N (bei einem Routergewicht von bis zu 4 kg) standhalten, die auf das Kabel des Routers ausgeübt wird.

4.7. Installation der Audio-Schnittstelle

Die Audioschnittstelle (Line Out) ist an der Erweiterung PTT (Option Ap) und an der Erweiterung Audio (Option A) verfügbar.



Vorsicht:

Gefahr von Hörschäden: Vermeiden Sie die Verwendung von Ohr- oder Kopfhörern bei hoher Lautstärke oder über einen längeren Zeitraum.

5. Konfiguration

In den folgenden Kapiteln finden Sie Informationen zum Einrichten des Routers und zur Konfiguration der Funktionen der Systemsoftware 4.6.0.107.



NetModule liefert regelmäßig aktualisierte Router-Software mit neuen Funktionen, Fehlerbehebungen und geschlossenen Sicherheitslücken aus. Bitte halten Sie die Router-Software immer auf dem neuesten Stand.

<ftp://share.netmodule.com/router/public/system-software/>

5.1. Erste Schritte

NetModule-Router können über die webbasierten Konfigurationsoberfläche, dem Web Manager, einfach eingerichtet werden. Der Web Manager wird von den neuesten Webbrowsern unterstützt. Beachten Sie, dass JavaScript aktiviert sein muss.

Jede über den Web Manager übermittelte Konfigurationsänderung wird sofort auf das System angewendet, wenn Sie auf **Apply** klicken. Bei der Konfiguration von Subsystemen, die mehrere Schritte erfordern (z. B. WLAN), können Sie mit **Continue** alle Einstellungen vorübergehend speichern und zu einem späteren Zeitpunkt anwenden. Bitte beachten Sie, dass diese Einstellungen beim Abmelden verloren gehen, wenn sie nicht ausdrücklich übernommen werden.

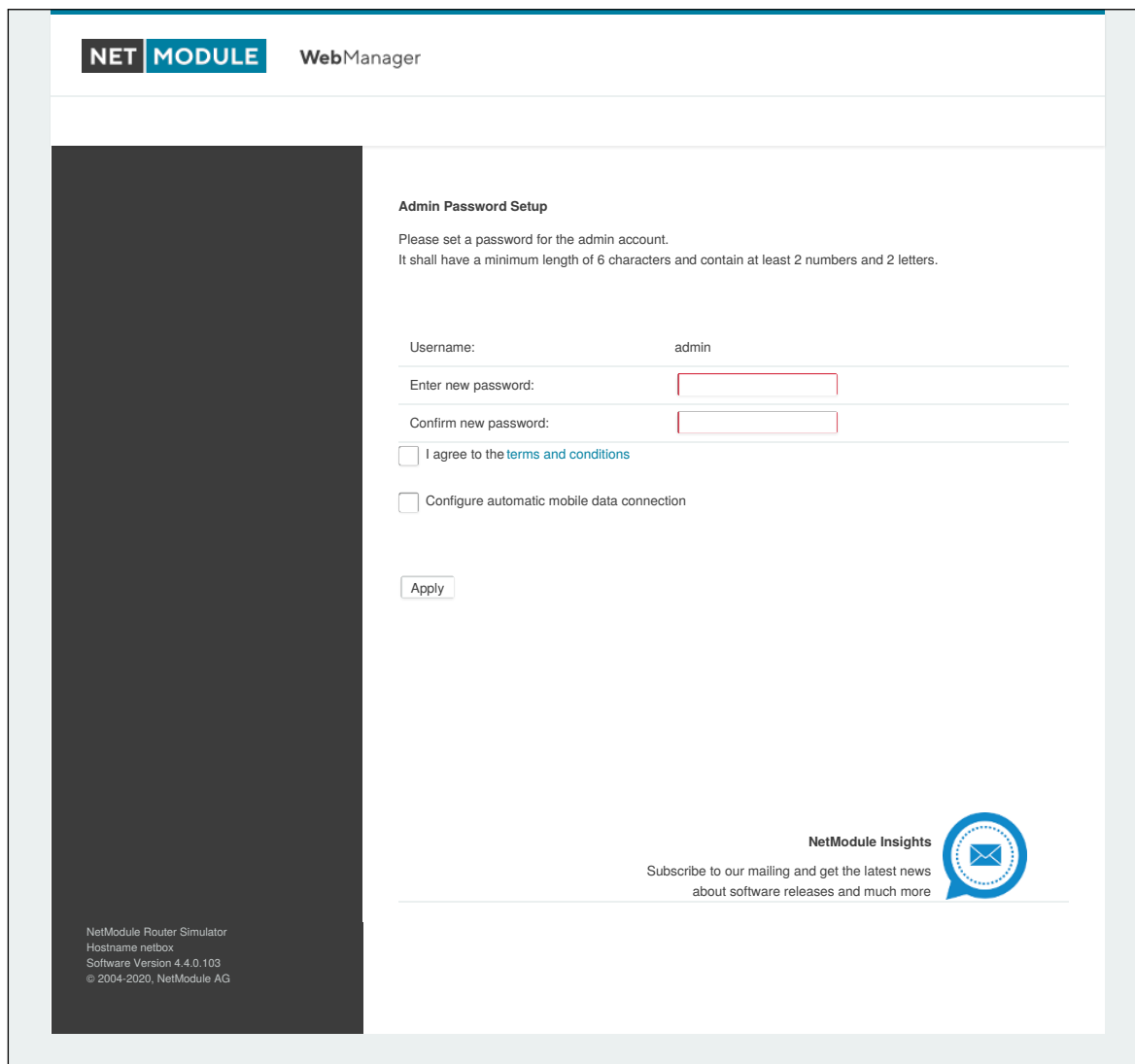
Sie können Konfigurationsdateien auch über SNMP, SSH, HTTP oder USB hochladen, wenn Sie eine größere Anzahl von Routern einsetzen möchten. Fortgeschrittene Benutzer können auch die Befehlszeile (CLI) verwenden und Konfigurationsparameter direkt einstellen.

Die IP-Adresse von Ethernet 1 lautet 192.168.1.1 und DHCP ist auf der Schnittstelle standardmäßig aktiviert. Sie müssen zum Einrichten Ihrer ersten Web Manager-Sitzung die folgenden Schritte durchführen:

1. Verbinden Sie den Ethernet-Anschluss des Computers über ein abgeschirmtes CAT6-Kabel mit M12-Stecker mit dem ETH1-Anschluss (Gigabit Ethernet) des Routers.
2. Falls noch nicht aktiviert, aktivieren Sie DHCP an der Ethernet-Schnittstelle des Computers, damit automatisch eine IP-Adresse vom Router bezogen werden kann. Es dauert in der Regel einen Moment, bis der PC die entsprechenden Parameter (IP-Adresse, Subnetzmaske, Standard-Gateway, Namensserver) erhalten hat. Sie können den Fortschritt verfolgen, indem Sie einen Blick in die Systemsteuerung (Netzwerk) werfen und überprüfen, ob der PC seine IP-Adresse korrekt bezogen hat; sie liegt im Bereich 192.168.1.100 bis 192.168.1.199.
3. Laden Sie im Webbrowser die Startseite unter der IP-Adresse des Routers (die URL lautet <http://192.168.1.1>).
4. Befolgen Sie die Anweisungen des Web Managers zum Konfigurieren des Routers. Die meisten Menüs sind selbsterklärend. Weitere Details finden Sie in den folgenden Kapiteln.

5.1.1. Erster Zugang

Im Auslieferungszustand werden Sie zur Eingabe eines neuen Admin-Passworts aufgefordert. Bitte wählen Sie ein Passwort, das sowohl leicht zu merken als auch robust gegen so genannte Wörterbuchangriffe ist (z. B. eines, das Zahlen, Buchstaben und Satzzeichen enthält). Das Passwort muss mindestens 6 Zeichen lang sein. Es muss mindestens 2 Zahlen und 2 Buchstaben enthalten.



NET MODULE WebManager

Admin Password Setup

Please set a password for the admin account.
It shall have a minimum length of 6 characters and contain at least 2 numbers and 2 letters.

Username: admin

Enter new password:

Confirm new password:

I agree to the [terms and conditions](#)

Configure automatic mobile data connection

Apply

NetModule Insights
Subscribe to our mailing and get the latest news about software releases and much more

NetModule Router Simulator
Hostname netbox
Software Version 4.4.0.103
© 2004-2020, NetModule AG

Abbildung 5.1.: Erste Anmeldung

Bitte beachten Sie, dass das Admin-Passwort auch für den Root-Benutzer angewendet wird, mit dem über die serielle Konsole, Telnet, SSH auf das Gerät zugegriffen oder der Bootloader aufgerufen werden kann. Sie können auch zusätzliche Benutzer konfigurieren, die nur Zugriff auf die Übersichtsseite oder zum Abrufen von Statusinformationen haben, aber keine Konfigurationsparameter ändern können.

Eine Reihe von Diensten (USB Autorun, CLI-PHP) ist im Auslieferungszustand standardmäßig aktiviert; sie werden deaktiviert, sobald das Admin-Passwort gesetzt wurde. Sie können anschließend in den entsprechenden Abschnitten wieder aktiviert werden. Auf andere Dienste (SSH, Telnet, Konsole) kann im Auslieferungszustand durch Angabe eines leeren Passworts oder ohne Passwort zugegriffen werden.

Die Passphrase für den Zugriff auf private Schlüssel wird mit einer zufälligen Zeichenfolge vorbelegt. Sie kann wie in Kapitel 5.8.8 beschrieben geändert werden.

5.1.2. Automatische Konfiguration einer Mobilfunkverbindung

Wenn eine SIM-Karte mit deaktivierter PIN in den ersten SIM-Slot eingelegt wird und die Option 'Configure automatic mobile data connection' ausgewählt wird, versucht der Router automatisch die korrekten Zugangsdaten aus einer internen Datenbank einzustellen und eine Datenverbindung zum Mobilfunknetz aufzubauen. Diese Funktion hängt stark von der verwendeten SIM-Karte und den verfügbaren Mobilfunknetzen ab.

Diese Option ist nur verfügbar, sofern ein Mobilfunk-Modul verbaut ist.

5.1.3. Zurücksetzen

Folgende Maßnahmen können Sie ergreifen, falls der Router falsch konfiguriert wurde und nicht mehr erreichbar ist:

1. Zurücksetzen auf Werkseinstellungen: Ein Zurücksetzen auf die Werkseinstellungen leiten Sie ein mit dem Befehl `factory-reset` oder aber durch Drücken des Reset-Tasters. Um diesen Taster zu drücken, benötigen Sie eine schmale Nadel oder Büroklammer, die Sie in die kleine Öffnung rechts neben dem Steckplatz für SIM 4 stecken. Der Taster muss bis zu 5 Sekunden gedrückt gehalten werden, bis alle LEDs aufleuchten.
2. Anmeldung bei der seriellen Konsole: Es ist auch möglich, sich über die serielle Schnittstelle beim System anzumelden. Dazu benötigen Sie ein Terminalemulatorprogramm (z. B. PuTTY oder HyperTerminal) und eine RS232-Verbindung (115200 8N1) über die serielle Schnittstelle Ihres lokalen PC. Dort werden dann auch die Kernel-Meldungen beim Booten angezeigt.
3. Systemwiederherstellung (Recovery-Image): In schwerwiegenden Fällen können wir auf Wunsch ein Recovery-Image zur Verfügung stellen, das per TFTP in den RAM geladen und ausgeführt wird. Es handelt sich um ein minimales System-Image, mit dem Sie ein Software-Update durchführen und andere Änderungen vornehmen können. Es besteht aus zwei Dateien namens `recovery-image` und `recovery-dtb`. Diese müssen im Stammverzeichnis eines TFTP-Servers abgelegt werden (verbunden über LAN1 mit der Adresse 192.168.1.254). Das Recovery-Image kann über eine serielle Verbindung vom Bootloader aus gestartet werden. Sie müssen dabei den Bootvorgang stoppen, indem Sie die Taste `s` drücken und damit den Bootloader aufrufen. Anschließend können Sie dann mit dem Befehl `run recovery` das Image laden und das System starten, auf das Sie anschließend über HTTP/SSH/Telnet und die IP-Adresse 192.168.1.1 zugreifen können. Dieser Vorgang kann auch eingeleitet werden, indem Sie den Reset-Taster länger als 15 Sekunden gedrückt halten.

5.2. STARTSEITE

Auf dieser Seite finden Sie eine Statusübersicht der aktivierten Funktionen und Verbindungen.

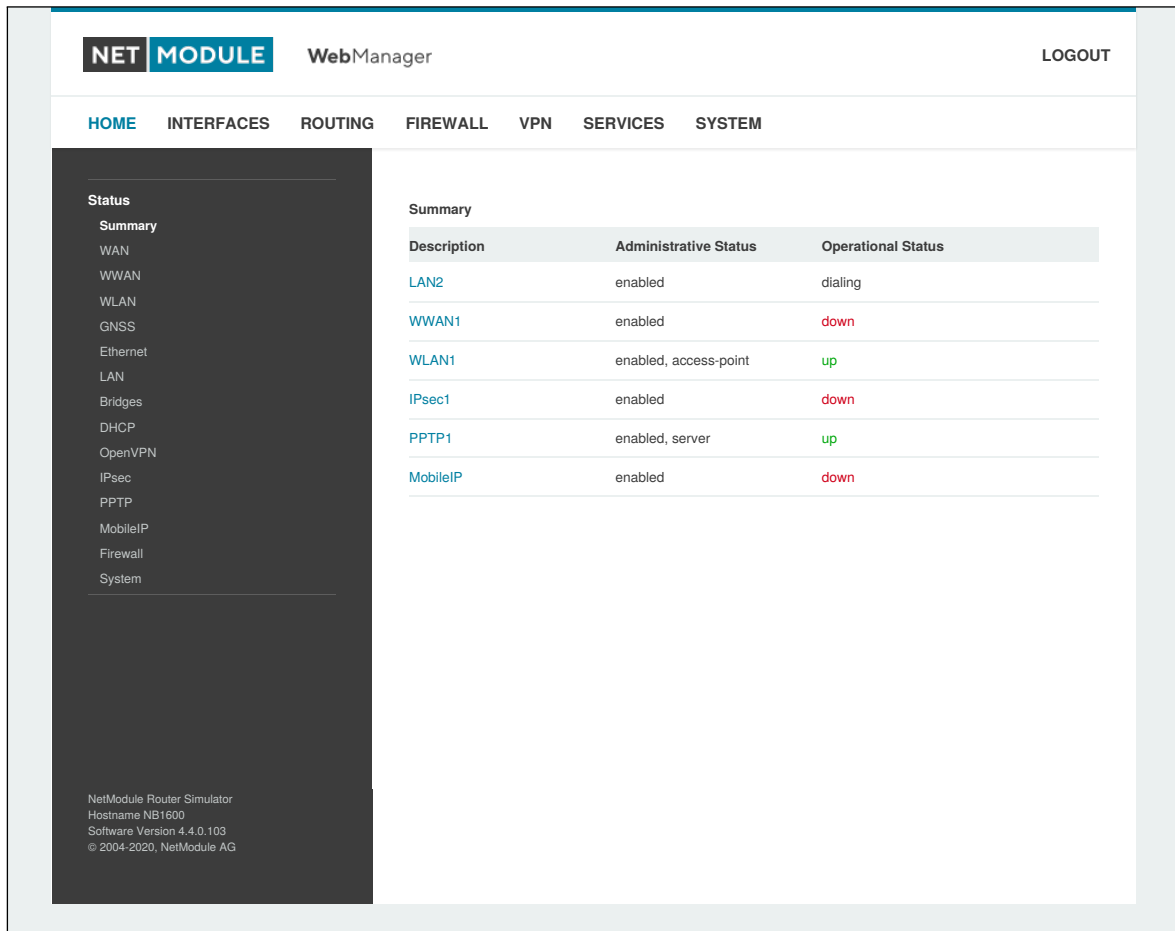


Abbildung 5.2.: Startbildschirm

Zusammenfassung (Summary)

Auf dieser Seite finden Sie eine kurze Zusammenfassung über den Verwaltungs- und Betriebsstatus der Schnittstellen des Routers.

WAN

Auf dieser Seite finden Sie Details zu allen aktivierten Wide Area Network- (WAN-) Verbindungen (z. B. die IP-Adressen, Netzwerkinformationen, Signalstärken usw.) Die Angaben zur Menge der heruntergeladenen/hochgeladenen Daten werden im nichtflüchtigen Speicher gespeichert und sind somit nach einem Neustart des Systems weiterhin vorhanden.

Die Zähler können zurückgesetzt werden, indem Sie auf *Reset* klicken.

WWAN

Auf dieser Seite finden Sie Informationen über Modems und deren Netzwerkstatus.



WLAN

Auf dieser Seite finden Sie Details zu den aktivierten WLAN-Schnittstellen im Access-Point-Modus. Dazu gehören die SSID, IP- und MAC-Adresse und die aktuell verwendete Frequenz und Sendeleistung der Schnittstelle sowie die Liste der zugehörigen Stationen.

GNSS

Auf dieser Seite werden die Positionsstatuswerte, wie z. B. Breitengrad/Längengrad, die sichtbaren Satelliten und weitere Details zu den verwendeten Satelliten angezeigt.

Ethernet

Auf dieser Seite finden Sie Informationen über die Ethernet-Schnittstellen und deren Netzwerkstatus.

LAN

Auf dieser Seite finden Sie Informationen über die LAN-Schnittstellen und das Netzwerkumfeld.

Bridges

Auf dieser Seite finden Sie Informationen zu konfigurierten virtuellen Bridge-Geräten.

Bluetooth

Auf dieser Seite finden Sie Informationen zu Bluetooth-Schnittstellen.

DHCP

Auf dieser Seite finden Sie Details zu allen aktivierten DHCP-Diensten, einschließlich einer Liste der ausgegebenen DHCP-Adressvergaben.

OpenVPN

Auf dieser Seite finden Sie Informationen zum Status des OpenVPN-Tunnels.

IPSec

Auf dieser Seite finden Sie Informationen zum Status des IPSec-Tunnels.

PPTP

Auf dieser Seite finden Sie Informationen zum Status des PPTP-Tunnels.

GRE

Auf dieser Seite finden Sie Informationen zum Status des GRE-Tunnels.

L2TP

Auf dieser Seite finden Sie Informationen zum Status des L2TP-Tunnels.

MobileIP

Auf dieser Seite finden Sie Informationen zu mobilen IP-Verbindungen.

Firewall

Auf dieser Seite finden Sie Informationen zu Firewall-Regeln und die dazugehörigen Statistiken. Sie kann zur Fehlersuche im Umfeld der Firewall genutzt werden.

QoS

Auf dieser Seite finden Sie Informationen zu den verwendeten QoS-Warteschlangen.

**BGP**

Auf dieser Seite finden Sie Informationen über das Border-Gateway-Protokoll.

OSPF

Auf dieser Seite finden Sie Informationen zum OSPF-Routing-Protokoll (Open Shortest Path First).

DynDNS

Auf dieser Seite finden Sie Informationen zu Dynamic DNS.

Systemstatus

Die Systemstatusseite zeigt verschiedene Detailinformationen zum NB2810-Router, darunter Systemdaten, Informationen über installierte und aktivierte Module und Informationen zur Softwareversion.

SDK

In diesem Abschnitt werden alle Webseiten aufgelistet, die von SDK-Skripten erzeugt wurden.

5.3. SCHNITTSTELLEN

5.3.1. WAN

Verbindungsverwaltung

Abhängig vom Hardwaremodell können WAN-Verbindungen entweder als Wireless Wide Area Network (WWAN), Wireless LAN (WLAN), Ethernet oder PPP over Ethernet (PPPoE) definiert sein. Eine WAN-Verbindung muss konfiguriert und aktiviert sein, damit sie auf dieser Seite erscheint.

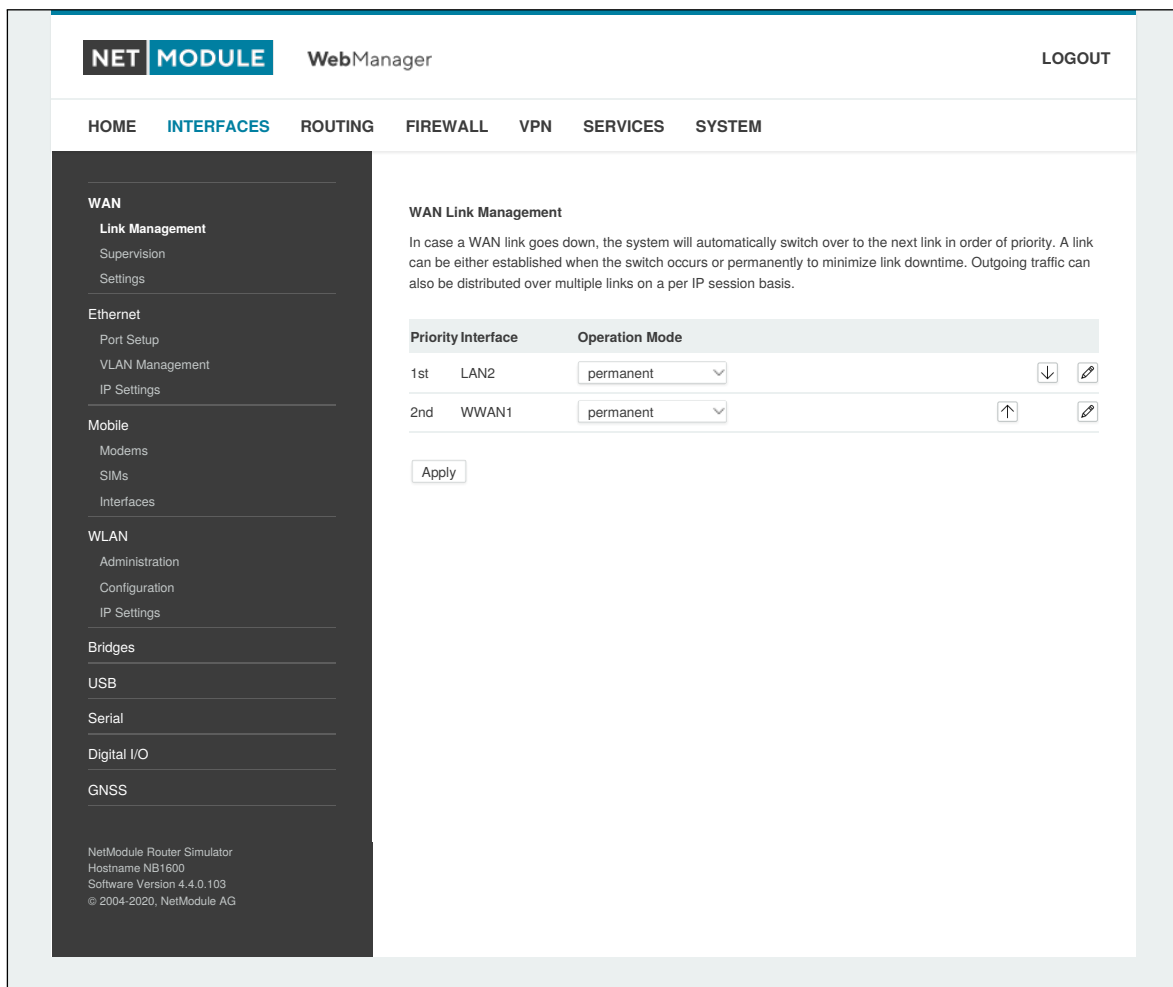


Abbildung 5.3.: WAN-Verbindungen

Generell wird eine Verbindung nur dann angewählt bzw. als vorhanden deklariert, wenn die folgenden Voraussetzungen erfüllt sind:

| Bedingung | WWAN | WLAN | ETH | PPPoE |
|--|------|------|-----|-------|
| Modem ist registriert | X | | | |
| Registriert mit gültigem Diensttyp | X | | | |
| Gültiger SIM-Status | X | | | |
| Ausreichende Signalstärke | X | X | | |
| Client ist zugeordnet | | X | | |
| Client ist authentifiziert | | X | | |
| Gültige DHCP-Adresse ist abgerufen | X | X | X | X |
| Verbindung ist aufgebaut und besitzt Adresse | X | X | X | X |
| Ping-Prüfung erfolgreich | X | X | X | X |

In diesem Menü können Sie den WAN-Verbindungen Prioritäten zuordnen. Die erfolgreich hergestellte Verbindung mit der höchsten Priorität wird der so genannte `hotlink`. Dies ist die Standardroute für ausgehende Pakete.

Wenn eine Verbindung ausfällt, schaltet das System automatisch auf die nächste Verbindung in der Prioritätenliste um. Sie können jede Verbindung so konfigurieren, dass sie entweder beim Umschalten oder permanent hergestellt wird, und so die Ausfallzeit der Verbindung minimieren.

| Parameter | WAN-Verbindungsprioritäten |
|--------------|--|
| 1st priority | Die primäre Verbindung, die verwendet wird, wann immer möglichist. |
| 2nd priority | Die erste Fallback-Verbindung; sie kann dauerhaft aktiviert sein oder angewählt werden, sobald Verbindung 1 ausfällt. |
| 3rd priority | Die zweite Fallback-Verbindung; sie kann dauerhaft aktiviert sein oder angewählt werden, sobald Verbindung 2 ausfällt. |
| 4th priority | Die dritte Fallback-Verbindung; sie kann dauerhaft aktiviert sein oder angewählt werden, sobald Verbindung 3 ausfällt. |

Verbindungen werden regelmäßig getestet. Sie werden in den Ruhezustand versetzt, falls es nicht möglich war, sie innerhalb einer bestimmten Zeit herzustellen. Daher kann es vorkommen, dass permanente Verbindungen im Hintergrund angewählt werden und im Erfolgsfall Ersatzverbindungen mit niedrigerer Priorität wieder ersetzen. Für den Fall, dass sich konkurrierende Verbindungen die gleichen Ressourcen teilen (z. B. im Dual-SIM-Betrieb), können Sie einen Zeitraum definieren, nach dem ein aktiver Hotlink zwangsweise heruntergefahren wird, um die Verbindung mit höherer Priorität wieder anwählbar zu machen.

Wir empfehlen die Betriebsart `permanent` für WAN-Verbindungen im Allgemeinen. Bei getaktet abgerechneten Mobilfunktarifen z. B. ist jedoch der Modus `switchover` möglicherweise sinnvoll. Im Modus `distributed` wird der ausgehende Datenverkehr basierend auf der relativen Last auf mehrere WAN-Verbindungen verteilt.



Vorsicht:

Es können gleichzeitig WWAN-Verbindungen bestehen, die sich eine gemeinsame Ressource teilen, z. B. ein WWAN-Modul mit SIM-Karten verschiedener Anbieter. In diesem Fall ist es nicht möglich, herauszufinden, ob die Verbindung mit der höheren Priorität verfügbar ist, ohne die Verbindung mit der niedrigen Priorität zu unterbrechen. Daher verhält sich eine solche Verbindung wie eine `switchover`-Verbindung, selbst bei Konfiguration als `permanent`.

Bei mobilen Verbindungen ist es weiterhin möglich, die WAN-Adresse an einen lokalen Host weiterzuleiten (auch als Drop-In oder IP-Pass-Through bezeichnet). Insbesondere erhält der erste DHCP-Client die öffentliche IP-Adresse. In diesem Fall verhält sich das System mehr oder weniger wie ein Modem, was bei Firewall-Problemen hilfreich sein kann. Nach der Einrichtung kann der Web Manager unter Verwendung der WAN-Adresse über Port 8080, aber über die LAN1-Schnittstelle weiterhin über Port 80 erreicht werden.

| Parameter | Betriebsmodi für WAN-Verbindungen |
|----------------------------|---|
| <code>disabled</code> | Die Verbindung ist deaktiviert. |
| <code>permanent</code> | Die Verbindung wird dauerhaft hergestellt. |
| <code>on switchover</code> | Die Verbindung wird bei einer Umschaltung hergestellt. Sie wird angewählt, wenn vorherige Verbindungen fehlgeschlagen sind. |
| <code>distributed</code> | Die Verbindung gehört zu einer Lastverteilungsgruppe. |

| Parameter | WAN-Verbindungseinstellungen |
|--|--|
| <code>Operation mode</code> | Der Betriebsmodus der Verbindung |
| <code>Weight</code> | Die Lastverteilung einer verteilten Verbindung |
| <code>Switch-back</code> | Legt die Rückschaltbedingung einer Switchover-Verbindung fest und die Zeit, nach der ein aktiver Hotlink getrennt wird |
| <code>Bridging interface</code> ¹ | Bei einem WLAN-Client die LAN-Schnittstelle, zu der die WAN-Verbindung gebrückt werden soll. |

NetModule-Router unterstützen die Funktion IP-Weiterleitung (IP Pass-Through oder Drop-In-Modus). Wenn sie aktiviert ist, wird die WAN-Adresse an den ersten DHCP-Client der angegebenen LAN-Schnittstelle durchgereicht. Da die Ethernet-basierte Kommunikation zusätzliche Adressen erfordert, wird ein geeignetes Subnetz gewählt, um mit dem LAN-Host zu kommunizieren. Für den Fall, dass sich dieses Subnetzes mit anderen Adressen des WAN-Netzes überschneiden, können Sie optional das vom Betreiber vorgegebene Netz angeben, um Adresskonflikte zu vermeiden.

¹Diese Option erfordert einen Access Point, der ein Frame-Format mit vier Adressen unterstützt.

| Parameter | Einstellungen der IP-Weiterleitung |
|-----------------|---|
| IP Pass-through | Aktiviert oder deaktiviert die IP-Weiterleitung |
| Interface | Legt die Schnittstelle fest, auf der die Adresse weitergeleitet werden soll |
| WAN network | Legt das WAN-Netzwerk fest |
| WAN netmask | Legt die WAN-Netzmaske fest |

Überwachung

Die Erkennung von Netzwerkausfällen auf Verbindungsebene kann durchgeführt werden, indem für jede Verbindung Pings an autorisierende Hosts gesendet werden. Eine Verbindung wird als ausgefallen deklariert, wenn alle Versuche fehlgeschlagen sind - als aktiv nur dann, wenn mindestens ein Host erreicht werden kann.

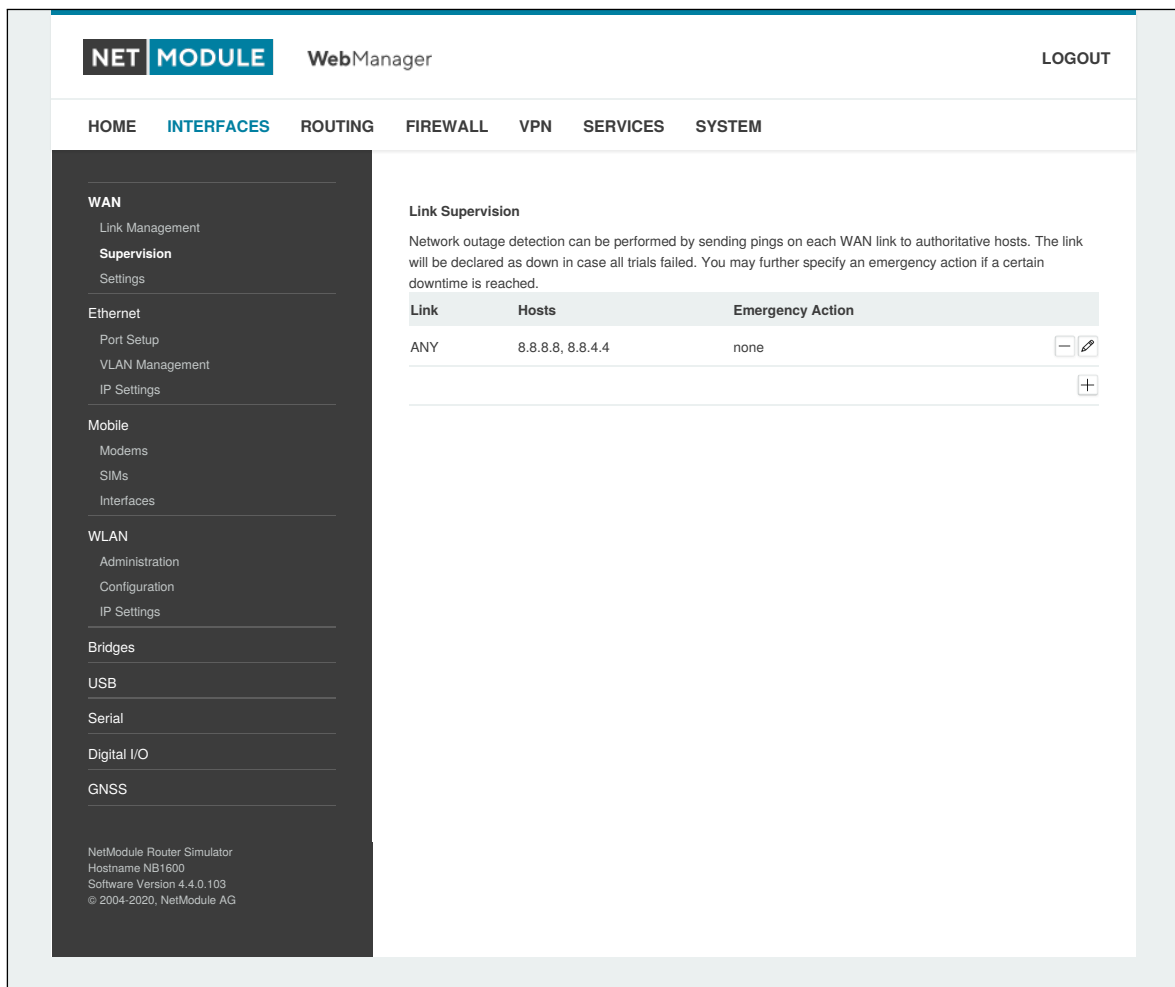


Abbildung 5.4.: Verbindungsüberwachung

| Parameter | Überwachungseinstellungen |
|------------------------------|--|
| Link | Die zu überwachende WAN-Verbindung (kann ANY sein) |
| Mode | Legt fest, ob die Verbindung nur überwacht werden soll, wenn sie aktiv ist (z. B. bei Verwendung eines VPN-Tunnels) oder ob die Konnektivität auch beim Verbindungsaufbau überprüft werden soll (Standard) |
| Primary host | Der zu überwachende primäre Host |
| Secondary host | Der zu überwachende sekundäre Host (optional) |
| Ping timeout | Die Zeit in Millisekunden, die eine Antwort auf einen einzelnen Ping dauern kann. Bei langsamen und trägen Verbindungen (z. B. 2G-Verbindungen) sollten Sie diesen Wert erhöhen. |
| Ping interval | Das Intervall in Sekunden, in dem Pings auf den einzelnen Schnittstellen gesendet werden |
| Retry interval | Das Intervall in Sekunden, in dem Pings erneut gesendet werden, wenn ein erster Ping fehlgeschlagen ist |
| Max. number of failed trials | Die maximale Anzahl der fehlgeschlagenen Ping-Versuche, nach der die Verbindung als ausgefallen deklariert wird |
| Emergency action | Die nach Erreichen der maximalen Ausfallzeit zu ergreifende Notfallmaßnahme. Bei <code>reboot</code> würde einen Neustart des gesamten Systems durchgeführt, während <code>restart link services</code> alle verbindungsbezogenen Anwendungen neu startet; das Modem wird ebenfalls zurückgesetzt. |

WAN-Einstellungen

Auf dieser Seite können Sie WAN-spezifische Einstellungen wie die maximale Segmentgröße (MSS) konfigurieren. Die maximale Segmentgröße entspricht der größten Datenmenge (in Byte), die der Router in einem einzelnen, nicht fragmentierten TCP-Segment verarbeiten kann. Um unerwünschte Nebenwirkungen zu vermeiden, darf die Anzahl der Bytes im Datensegment und in den Headern nicht mehr als die maximale Größe einer Übertragungseinheit (MTU) betragen. Die MTU kann für jede Schnittstelle separat konfiguriert werden und entspricht der maximal übertragbaren Paketgröße.

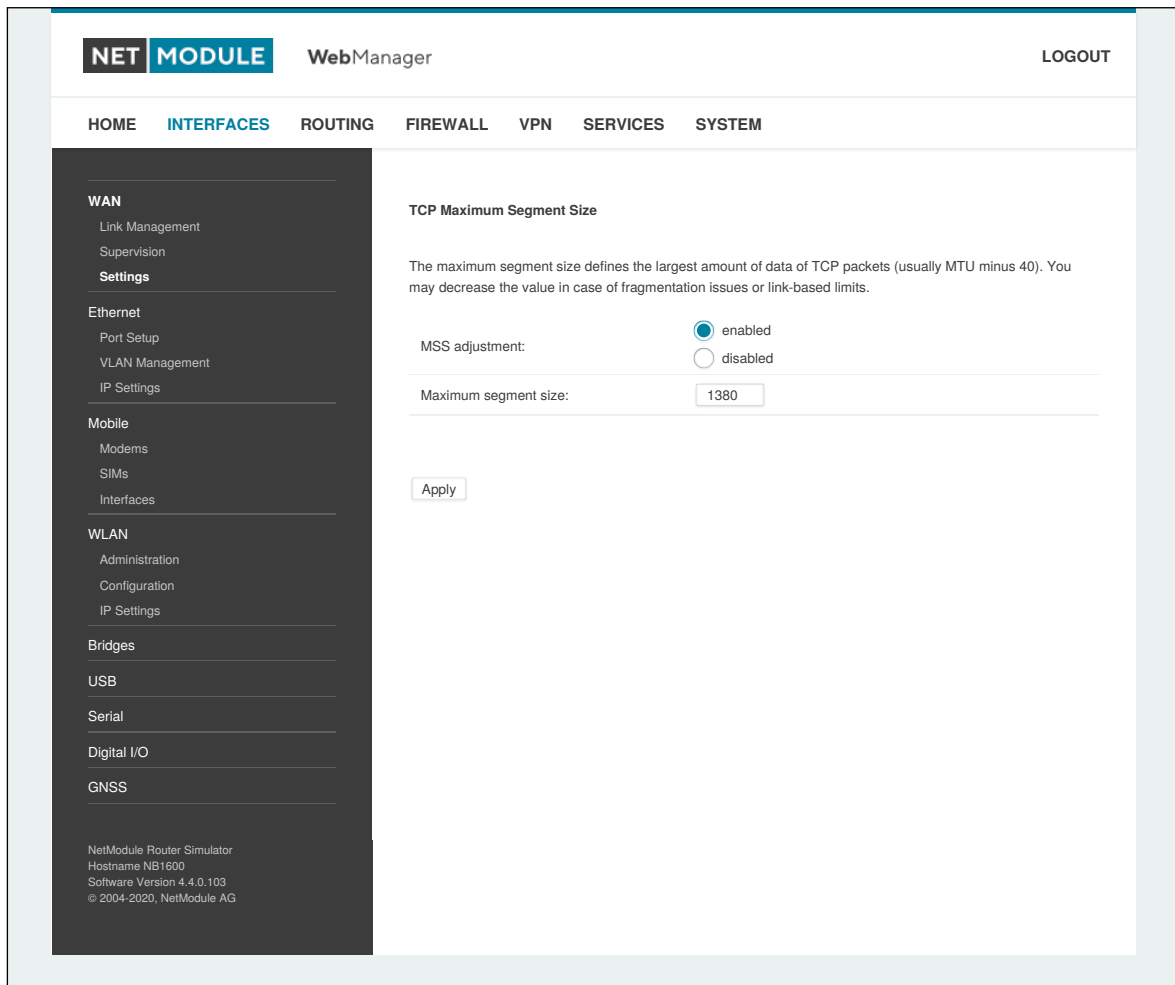


Abbildung 5.5.: WAN-Einstellungen

| Parameter | TCP-MSS-Einstellungen |
|----------------------|--|
| MSS adjustment | Aktiviert oder deaktiviert die MSS-Einstellung auf WAN-Schnittstellen. |
| Maximum segment size | Maximale Anzahl von Bytes in einem TCP-Datensegment. |

5.3.2. Ethernet

NB2810-Router werden mit 2 dedizierten Gigabit-Ethernet-Anschlüssen (ETH1 und ETH2) und einem zusätzlichen Erweiterungsanschluss für M12-Steckverbinder ausgeliefert. ETH1 stellt normalerweise die LAN1-Schnittstelle dar, die für das LAN verwendet werden sollte. Andere Schnittstellen können zum Verbinden zu anderen LAN-Segmenten oder zum Konfigurieren einer WAN-Verbindung verwendet werden. Die LAN10-Schnittstelle ist verfügbar, sobald ein vorkonfiguriertes USB-Ethernet-Gerät eingesteckt ist.

Ethernet-Anschlusszuordnung

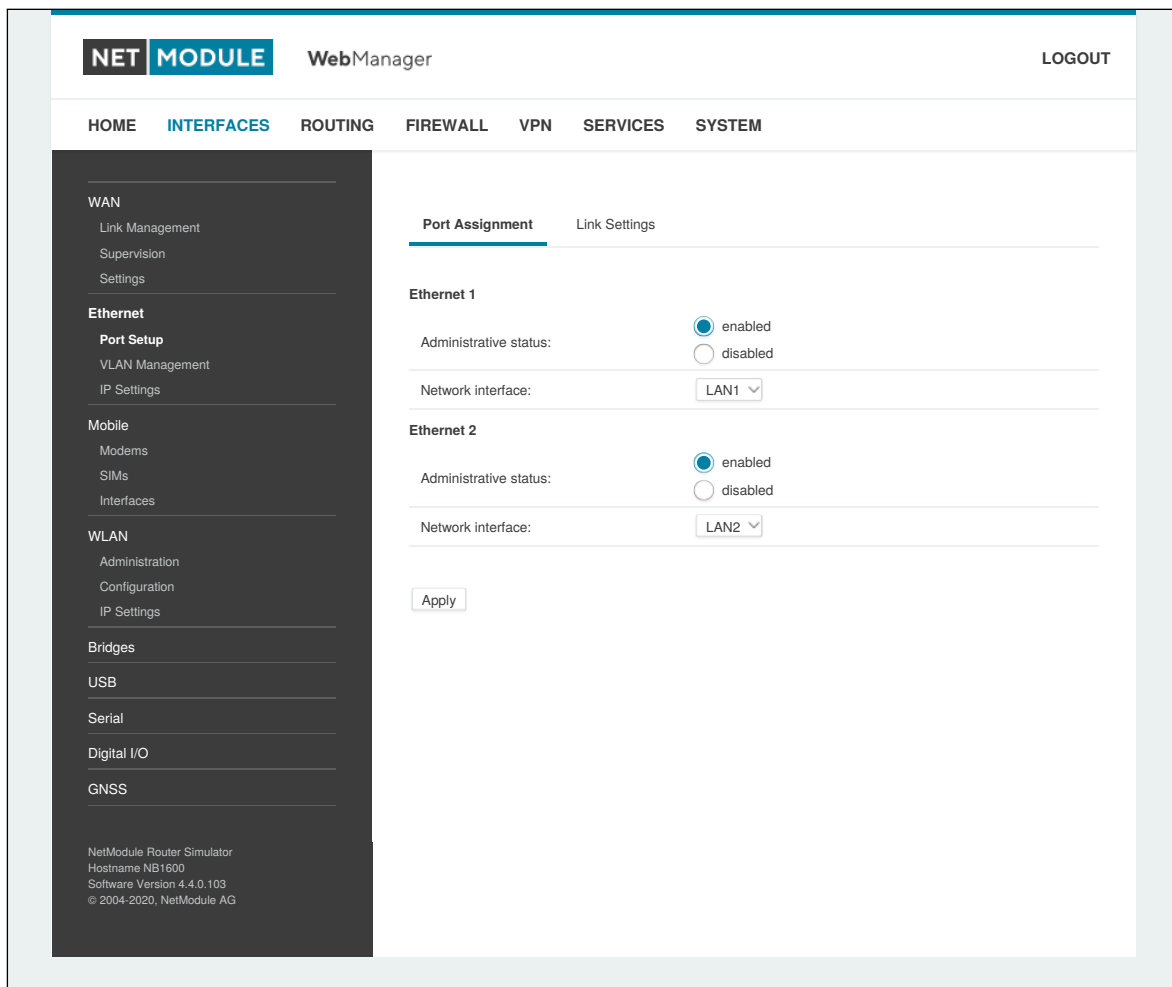


Abbildung 5.6.: Ethernet-Anschlüsse

In diesem Menü können Sie jeden Ethernet-Anschluss einzeln einer LAN-Schnittstelle zuweisen, falls unterschiedliche Subnetze pro Anschluss vorhanden sind oder wenn Sie einen Anschluss als WAN-Schnittstelle verwenden möchten. Sie können derselben Schnittstelle mehreren Anschlüssen zuweisen.

Bitte beachten Sie, dass NB2810-Router keinen Switch, sondern einzelne PHY-Anschlüsse besitzen. Wenn beide Anschlüsse der gleichen LAN-Schnittstelle zugewiesen sind, werden die Anschlüsse per Software überbrückt.

Folgende Optionen stehen zur Verfügung:

| Parameter | Einstellungen für die Ethernet-Softbridge |
|-------------------------|--|
| Enable bridge filtering | Wenn aktiviert, gelten die Firewall-Regeln auch für Paketen zwischen den Anschlüssen |
| Enable RSTP | Wenn aktiviert, wird das Rapid Spanning Tree Protocol (IEEE 802.1D-2004) anstelle des Spanning Tree Protocol genutzt |

Einstellungen für die Ethernet-Verbindung

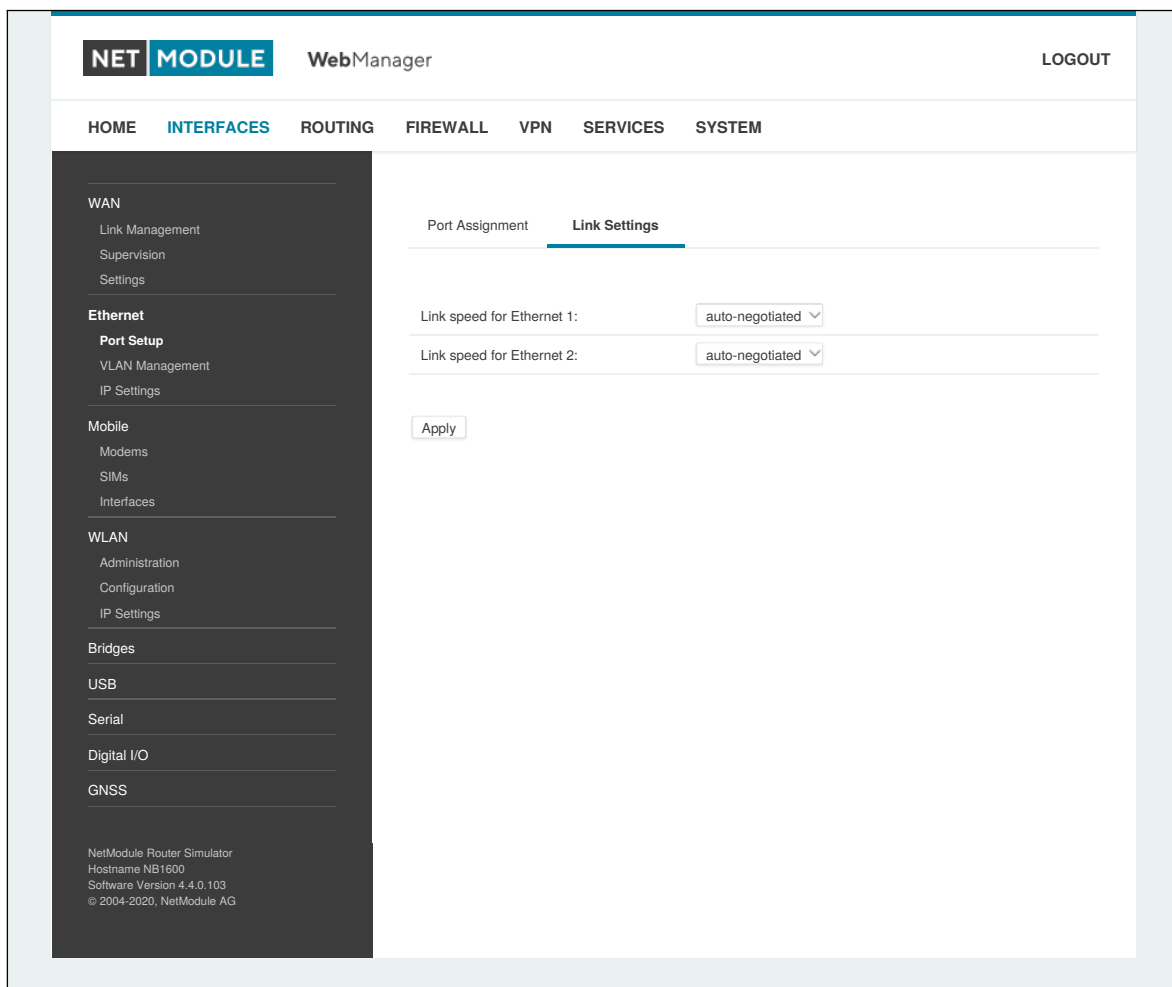


Abbildung 5.7.: Einstellungen für die Ethernet-Verbindung

Die Verbindungsaushandlung kann für jeden Ethernet-Port einzeln konfiguriert werden. Die meisten Geräte unterstützen die automatische Aushandlung, die die Verbindungsgeschwindigkeit automatisch

so konfiguriert, dass sie den Anforderungen der anderen Geräte im Netzwerk entspricht. Bei Verhandlungsproblemen können Sie die Modi manuell zuweisen, aber es muss dabei sichergestellt sein, dass alle Geräte im Netzwerk die gleichen Einstellungen verwenden.

Authentifizierung mittels IEEE 802.1X

NetModule-Router unterstützen eine Port-basierte Authentifizierung nach IEEE 802.1X. Dies kann für jeden Ethernet-Anschluss separat konfiguriert werden.

Folgende Optionen stehen zur Verfügung:

| Parameter | Einstellungen IEEE 802.1X |
|---------------------|--|
| Wired 802.1X status | Wenn aktiviert, authentifiziert der Router sich auf diesem Ethernet-Anschluss mittels IEEE 802.1X |
| EAP type | Das Protokoll mit welchem sich authentifiziert werden soll |
| Anonymous identity | Anonyme Identität für PEAP Authentifizierung |
| Identity | Identität für EAP-TLS oder PEAP Authentifizierung (erforderlich) |
| Password | Passwort für PEAP Authentifizierung (erforderlich) |
| Certificates | Zertifikate für die Authentifizierung mittels EAP-TLS oder PEAP. Zur Konfiguration siehe Kapitel 5.8.8 |

VLAN-Verwaltung

NetModule-Router unterstützen Virtual LAN nach IEEE 802.1Q, mit dem sich virtuelle Schnittstellen auf einer Ethernet-Schnittstelle erstellen lassen. Das VLAN-Protokoll fügt in Ethernet-Frames einen zusätzlichen Header ein, der eine VLAN-Kennung (VLAN-ID) trägt, die zur Verteilung der Pakete auf die zugehörigen virtuellen Schnittstellen verwendet wird. Alle Pakete ohne Kennung (Tagging) sowie Pakete mit einer nicht zugewiesenen ID werden an die native Schnittstelle weitergeleitet.

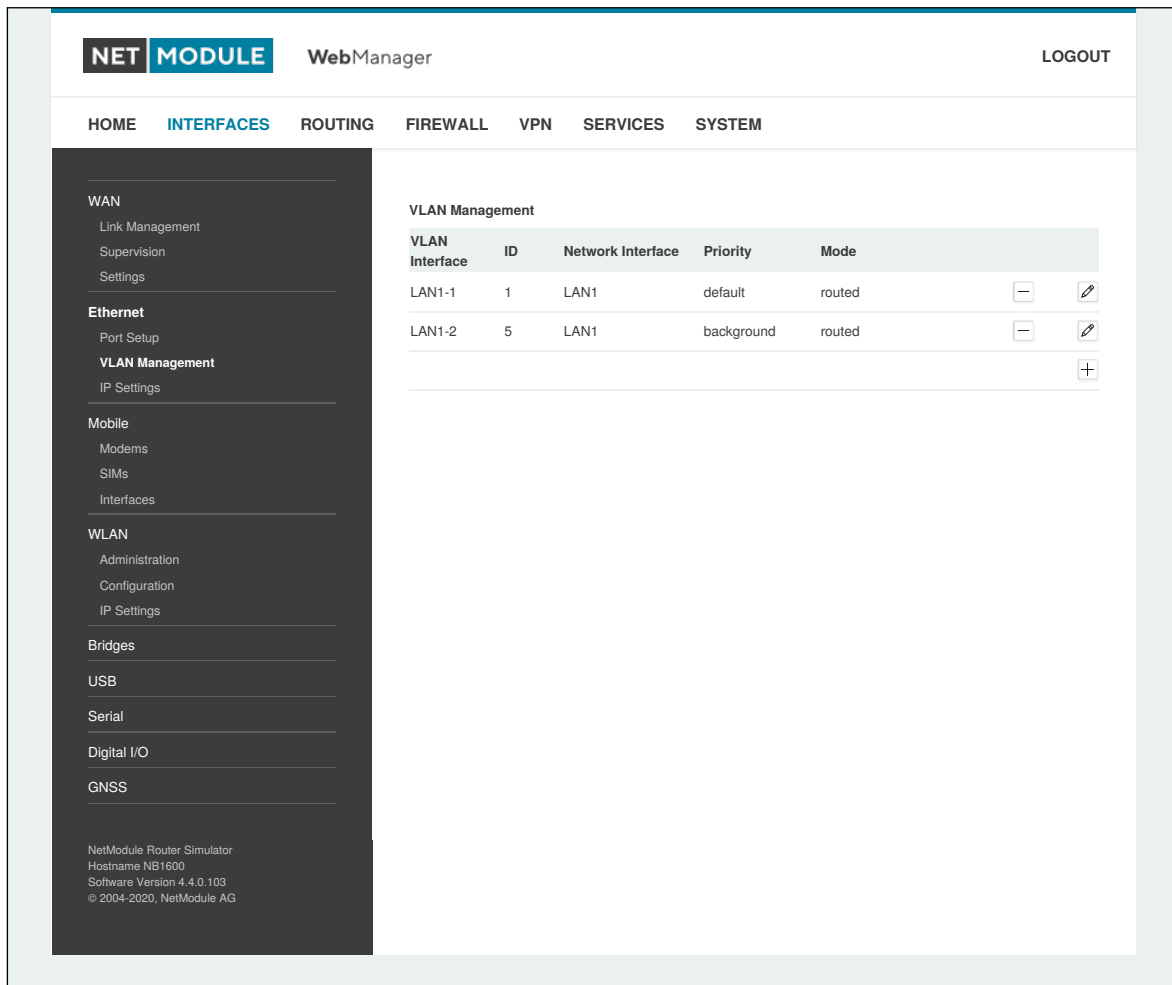


Abbildung 5.8.: VLAN-Verwaltung

Um ein eindeutiges Subnetz zu bilden, muss die Netzwerkschnittstelle eines Remote-LAN-Hosts mit der gleichen VLAN-ID konfiguriert sein, die auf dem Router definiert ist. Außerdem führt 802.1P ein Prioritätsfeld ein, das die Paketplanung im TCP/IP-Stack beeinflusst.

Es gibt die folgenden Prioritätsstufen (von der niedrigsten zur höchsten):

| Parameter | VLAN-Prioritätsstufen |
|-----------|---|
| 0 | Hintergrund (Background) |
| 1 | Best Effort |
| 2 | Excellent Effort |
| 3 | Kritische Anwendungen (Critical Applications) |
| 4 | Video (< 100 ms Verzögerung/Jitter) |
| 5 | Sprache (< 10 ms Verzögerung/Jitter) |
| 6 | Internetwork Control |
| 7 | Network Control |

IP-Einstellungen

Auf dieser Seite können Sie die IP-Adressierung für die LAN/WAN-Ethernet-Schnittstellen konfigurieren.

| Parameter | LAN-IP-Einstellungen |
|-----------|---|
| Mode | Legt fest, ob diese Schnittstelle als LAN- oder WAN-Schnittstelle verwendet wird. |
| MTU | Maximale Übertragungseinheit für die Schnittstelle. Wenn angegeben, gibt sie die maximale Größe eines Pakets an, das auf der Schnittstelle übertragen wird. |

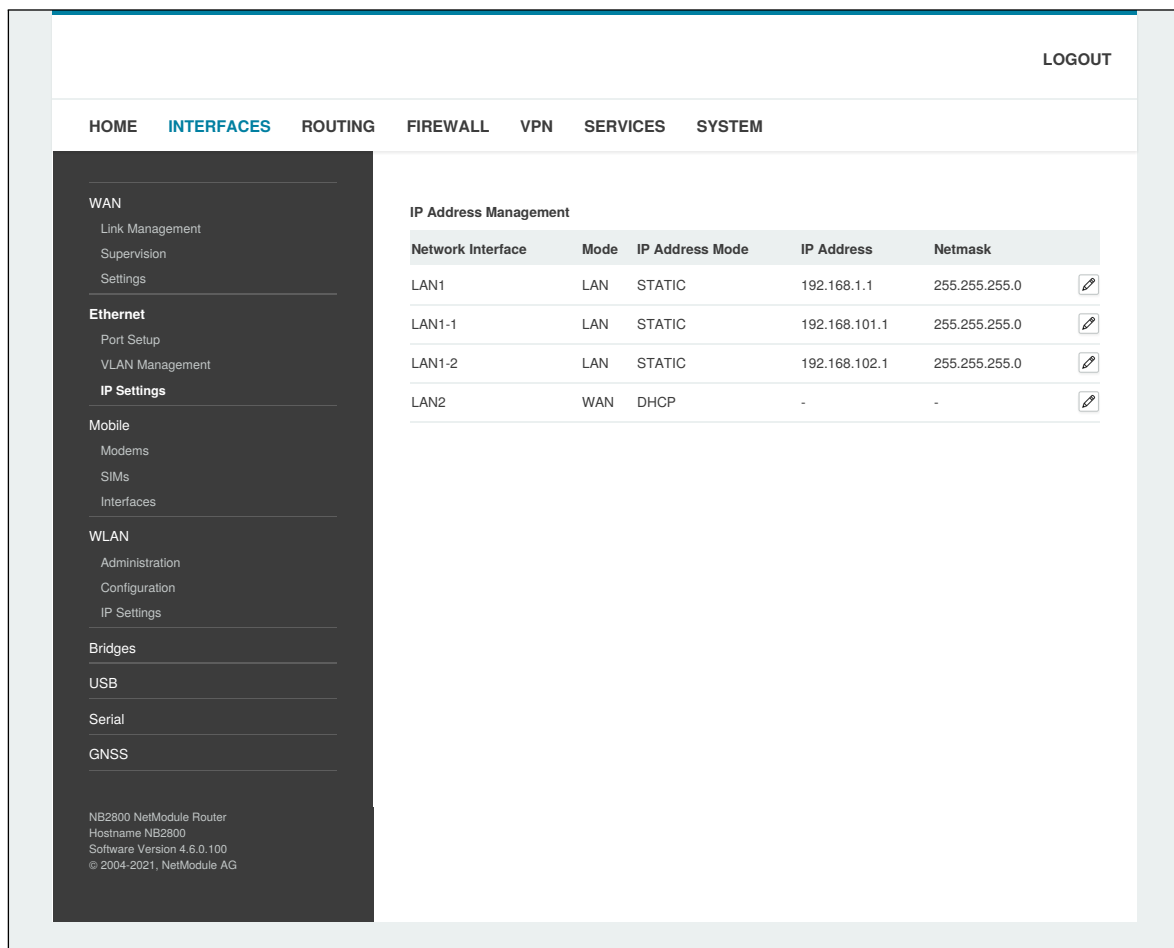


Abbildung 5.9.: IP Einstellungen - Übersicht

LAN-Modus

Im LAN-Modus kann die Schnittstelle mit den folgenden Einstellungen konfiguriert werden:

| Parameter | LAN-IP-Einstellungen |
|------------------|--|
| IP address | Die Adresse der IP-Schnittstelle |
| Netmask | Die Netzmaske für diese Schnittstelle |
| Alias IP address | Zusätzliche Alias-IP-Schnittstellenadresse |
| Alias Netmask | Zusätzliche Alias-Netzmaske für diese Schnittstelle |
| MAC | Benutzerdefinierte MAC Adresse (nicht für VLANs möglich) |

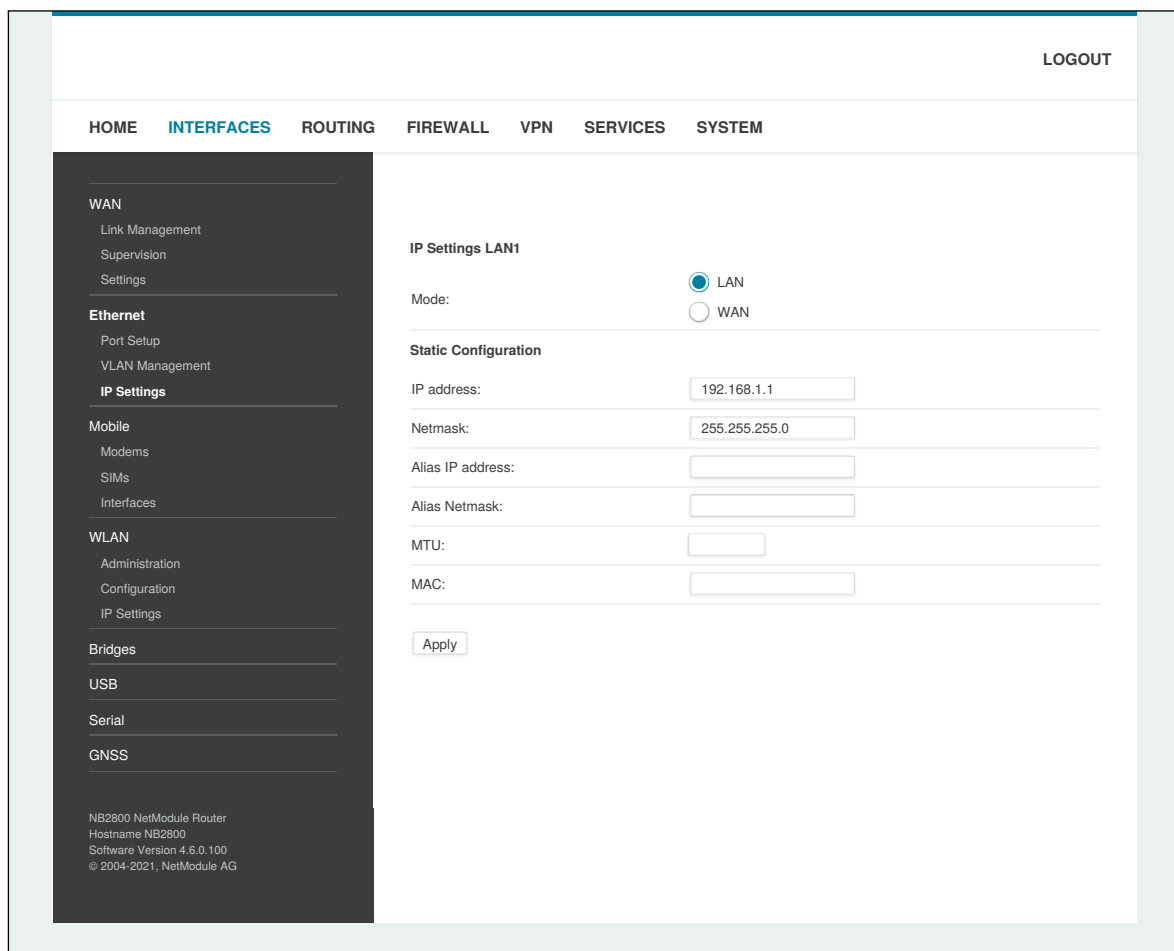


Abbildung 5.10.: IP Einstellungen - LAN Schnittstelle

WAN-Modus

WAN Schnittstellen unterstützen zwei IP Versionen, die wie folgt konfiguriert werden können:

| Parameter | Beschreibung |
|------------|---|
| IPv4 | Ausschließlich Internet Protokoll Version 4 |
| IPv6 | Ausschließlich Internet Protokoll Version 6 |
| Dual-Stack | Internet Protokoll Version 4 sowie Version 6 parallel |

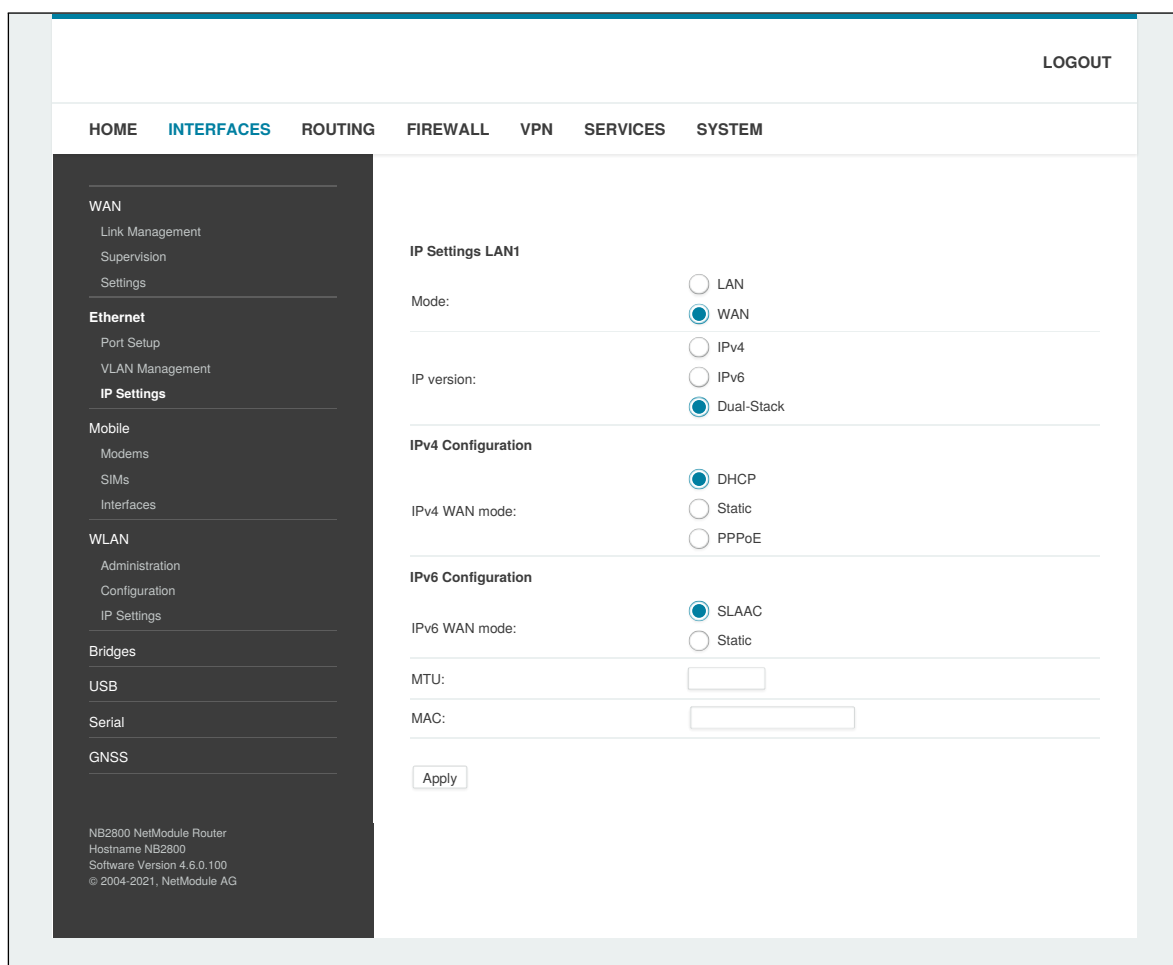


Abbildung 5.11.: IP Einstellungen - WAN Schnittstelle

Abhängig von der konfigurierten IP Version können weitere Einstellung vorgenommen werden. Diese unterscheiden sich je nach ausgewählter IP Version.

IPv4 Einstellungen

Die IPv4 Adressen können in den folgenden Modi konfiguriert werden:

| Parameter | IPv4 WAN Modus |
|-----------|---|
| DHCP | Beim Betrieb als DHCP-Client ist keine weitere Konfiguration erforderlich, da alle IP-bezogenen Einstellungen (Adresse, Subnetz, Gateway, DNS-Server) von einem DHCP-Server im Netzwerk abgerufen werden. |
| Static | Lässt Sie statische Werte definieren. Bei der Zuweisung eindeutiger IP-Adressen ist jedoch Vorsicht geboten, da dies zu IP-Konflikten im Netzwerk führen kann. |
| PPPoE | PPPoE wird üblicherweise für die Kommunikation mit einem anderen WAN-Zugangsgerät (z. B. einem DSL-Modem) verwendet. Es stehen die folgenden Einstellungen zur Verfügung |

IPv4-PPPoE Einstellungen

Es stehen die folgenden Einstellungen zur Verfügung:

| Parameter | PPPoE-Konfiguration |
|--------------------------|---|
| User name | PPPoE-Benutzername zur Authentifizierung am Zugangsgerät |
| Password | PPPoE-Passwort zur Authentifizierung am Zugangsgerät |
| Service name | Legt den Dienstnamenssatz des Zugriffskonzentrators fest. Kann leer bleiben, es sei denn, es laufen mehrere Dienste im selben physischen Netzwerk und Sie müssen angeben, mit welchem Sie eine Verbindung herstellen möchten. |
| Access concentrator name | Der Name des Zugriffskonzentrators (wenn nicht angegeben, stellt der PPPoE-Client eine Verbindung zu einem beliebigen Zugriffskonzentrator her) |

IPv6 Einstellungen

Die IPv6 Adressen können in den folgenden Modi konfiguriert werden:

| Parameter | Beschreibung |
|-----------|--|
| SLAAC | Alle IP-bezogenen Einstellungen (Adresse, Prefix, Routen, DNS-Server) werden durch das Neighbor-Discovery-Protocol mittels IPv6 stateless-address-autoconfiguration bezogen. |
| Static | Lässt Sie statische Werte definieren. Bei der Zuweisung eindeutiger IP-Adressen ist jedoch Vorsicht geboten, da dies zu IP-Konflikten im Netzwerk führen kann. Es kann ausschließlich eine globale Adresse gesetzt werden. Die link-lokale Adresse wird automatisch anhand der Router MAC Adresse generiert. |

DNS Server

Sofern alle genutzten IP Versionen auf `Static` gestellt sind, können hier schnittstellenspezifische Nameserver angegeben werden. Wie Sie globale DNS-Server konfigurieren, und somit die schnittstellenspezifischen DNS-Server überschreiben können, erfahren Sie in Kapitel [5.7.3](#).

5.3.3. Mobile Kommunikation

Modem-Konfiguration

Auf dieser Seite finden Sie die verfügbaren WWAN-Modems. Sie können bei Bedarf deaktiviert werden.

Abfrage

Auf dieser Seite können Sie Hayes-AT-Befehle an das Modem senden. Neben dem 3GPP-konformen AT-Befehlssatz können weitere modemspezifische Befehle nutzbar sein, über die wir auf Wunsch informieren. Einige Modems unterstützen auch das Ausführen von USSD-Anforderungen (Unstructured Supplementary Service Data), z. B. zum Abfragen des verfügbaren Guthabens eines Prepaid-Kontos.

SIM-Karten

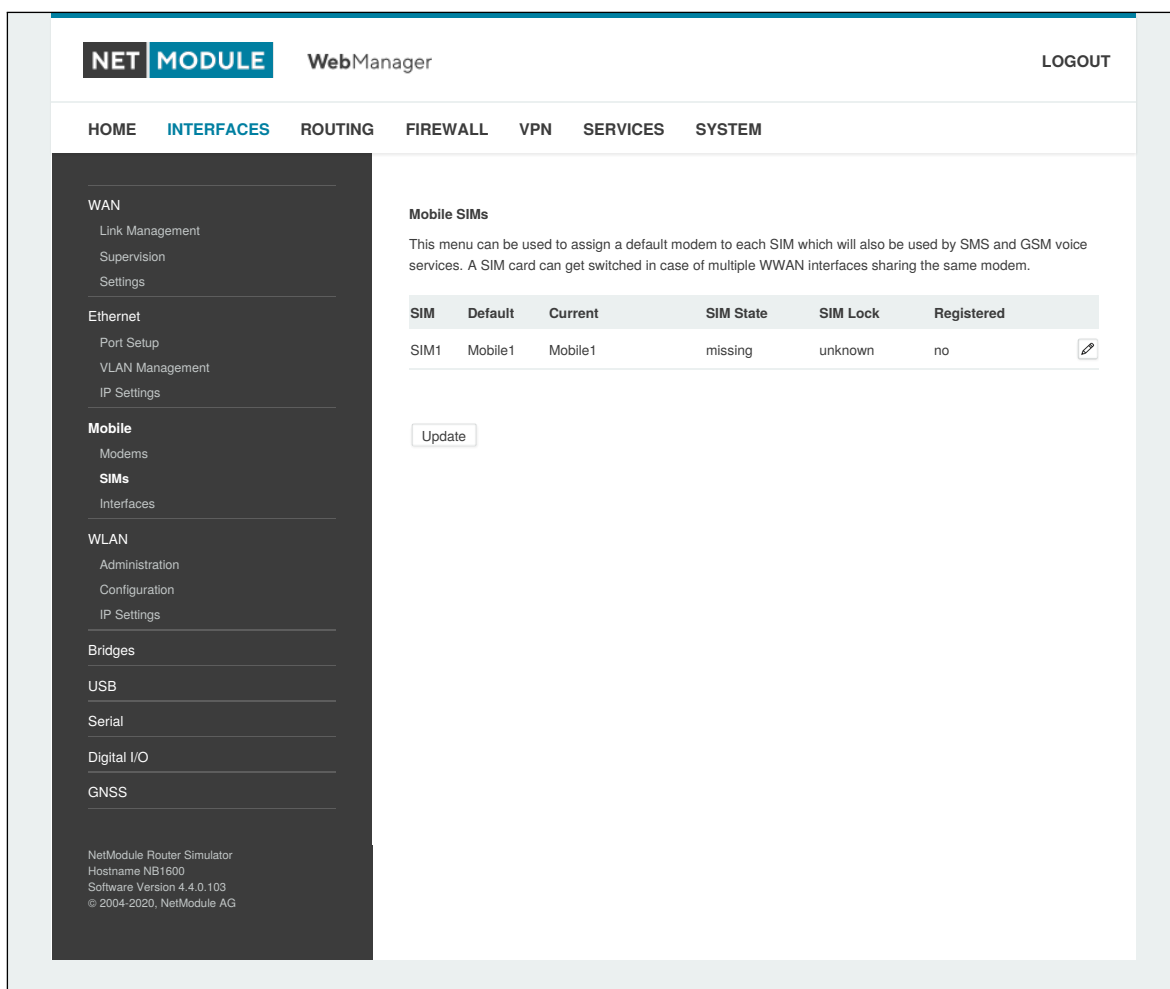


Abbildung 5.12.: SIM-Karten

Auf dieser Seite finden Sie einen Überblick über die verfügbaren SIM-Karten, die ihnen zugeordneten Modems und deren aktuellen Status. Nachdem eine SIM-Karte eingelegt, einem Modem zugewiesen und erfolgreich entsperrt wurde, sollte sich die Karte im Zustand `ready` befinden, und der Status der Netzwerkregistrierung sollte sich auf `registered` ändern. Falls nicht, überprüfen Sie bitte die PIN. Bitte bedenken Sie, dass die Anmeldung in einem Netzwerk in der Regel einige Zeit in Anspruch nimmt und von der Signalstärke und möglichen Funkstörungen beeinflusst wird. Sie können auch mit der Schaltfläche `Update` jederzeit die PIN-Entsperrung neu starten und einen weiteren Registrierungsversuch auslösen.

Unter Umständen (z. B. wenn das Modem zwischen Basisstationen hin- und herwechselt) kann es erforderlich sein, einen bestimmten Dienstyp einzustellen oder einen festen Betreiber zuzuweisen. Die Liste der umliegenden Betreiber erhalten Sie, indem Sie einen Netzwerkscan starten (dies kann bis zu 60 Sekunden dauern). Weitere Details erhalten Sie durch direkte Abfrage des Modems; einen entsprechenden Befehlssatz stellen wir auf Anfrage zur Verfügung.

Konfiguration

Eine SIM-Karte ist in der Regel einem Standardmodem zugeordnet; dies kann aber auch geändert werden, z. B. wenn Sie zwei WWAN-Schnittstellen mit einem Modem, aber unterschiedlichen SIM-Karten einrichten.

Besondere Vorsicht ist geboten, wenn andere Dienste (z. B. SMS oder Sprache) auf diesem Modem betrieben werden, da ein SIM-Wechsel natürlich der Betrieb beeinflusst.

Es stehen die folgenden Einstellungen zur Verfügung:

| Parameter | WWAN-SIM-Konfiguration |
|-------------------|--|
| PIN code | Der PIN-Code zum Entsperren der SIM-Karte |
| PUK code | Der PUK-Code zum Entsperren der SIM-Karte (optional) |
| Default modem | Das dieser SIM-Karte zugewiesene Standardmodem |
| Preferred service | Der bevorzugte Dienst, der mit dieser SIM-Karte verwendet werden soll. Denken Sie daran, dass der Linkmanager diese Festlegung bei abweichenden Einstellungen möglicherweise überschreibt. Standardmäßig wird <code>automatic</code> verwendet; in Gebieten mit anderen, störenden Basisstationen können Sie einen bestimmten Typ erzwingen (z. B. nur 3G), um ein Hin- und Herwechseln zwischen den Basisstationen in der Umgebung zu verhindern. |
| Registration mode | Der gewählte Registrierungsmodus |
| Network selection | Legt fest, welches Netzwerk ausgewählt werden soll. Die Auswahl kann an eine bestimmte Provider ID (PLMN) gebunden werden, der durch Ausführen eines Netzwerkskans ermittelt werden kann. |

eSIM/eUICC

**Vorsicht:**

Beachten Sie, dass eUICC-Profilen NICHT von einem zurücksetzen auf Werkseinstellungen betroffen sind. Um ein eUICC-Profil von einem Gerät zu entfernen, müssen Sie es vor dem Zurücksetzen auf die Werkseinstellungen manuell entfernen.

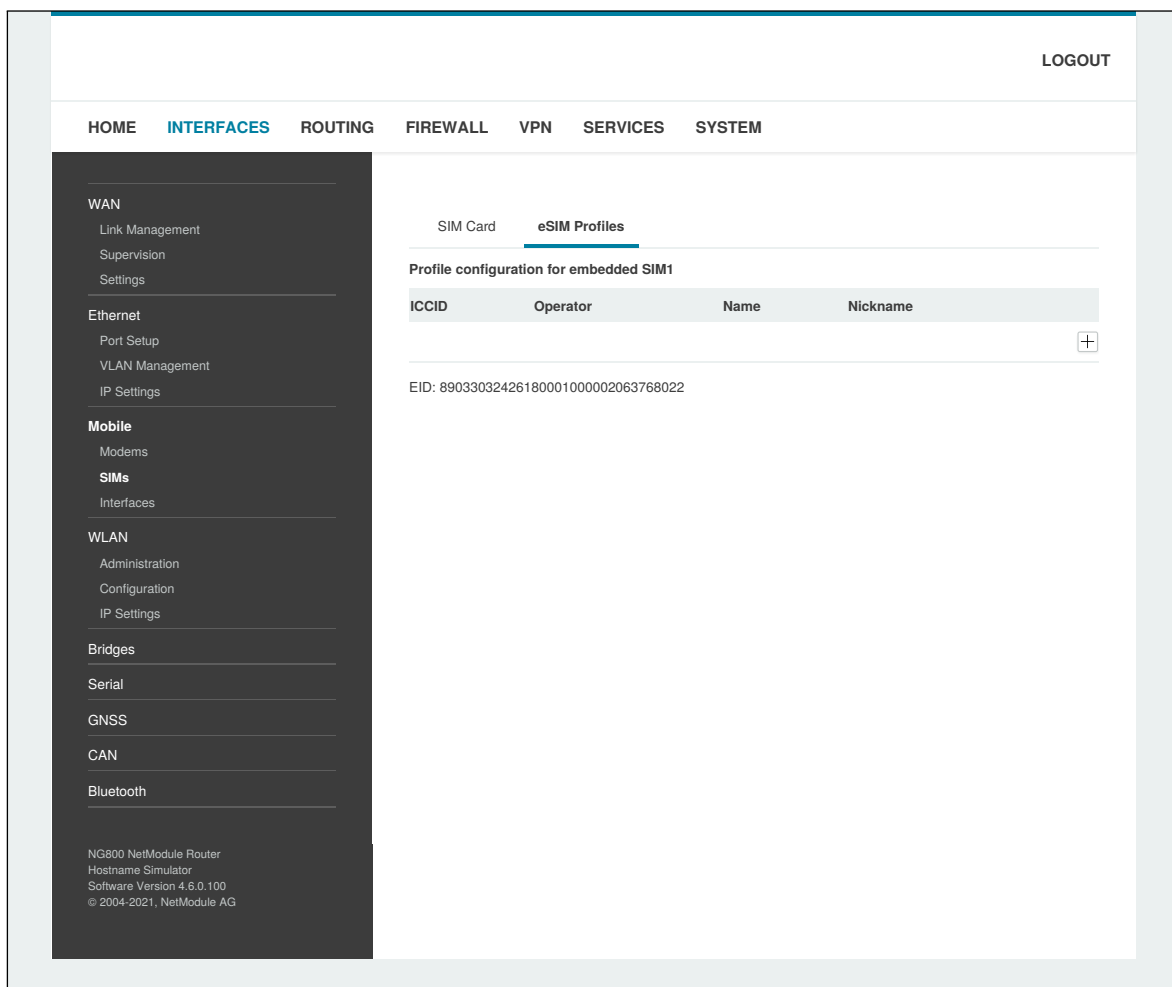


Abbildung 5.13.: eSIM-Profilen

Ausgewählte Routermodelle enthalten eine eUICC (Embedded Universal Integrated Circuit Card), mit der Sie eSIM-Profilen aus dem Internet auf den Router herunterladen können, anstatt eine physische SIM-Karte in den Router einlegen zu müssen. Die zu installierenden eSIM-Profilen müssen der GSMA RSP Technical Specification SGP.22 entsprechen. Dies sind die gleichen eSIM-Profilen, die von aktuellen Mobiltelefonen verwendet werden. Profilen nach der älteren GSMA-Spezifikation SGP.02 werden nicht unterstützt.

eSIM-Profilen können auf der Registerkarte eSIM Profilen der Konfigurationsseite für die mobile Kommunikation verwaltet werden. Auf dieser Seite können Sie alle installierten eSIM-Profilen anzeigen sowie eSIM-Profilen installieren, aktivieren, deaktivieren und löschen. Sie können auch jedem Profil einen gut zu merkenden eigenen Namen zuordnen.

Die eUICC kann bis zu ca. 7 eSIM-Profilen speichern, abhängig von der Größe der Profile. Es kann jeweils nur eines dieser Profile aktiv sein.

Um neue eSIM-Profilen zu installieren, müssen Sie zunächst eine IP-Verbindung zum Internet herstellen, damit der Router das Profil vom Server des Mobilfunkbetreibers herunterladen kann.

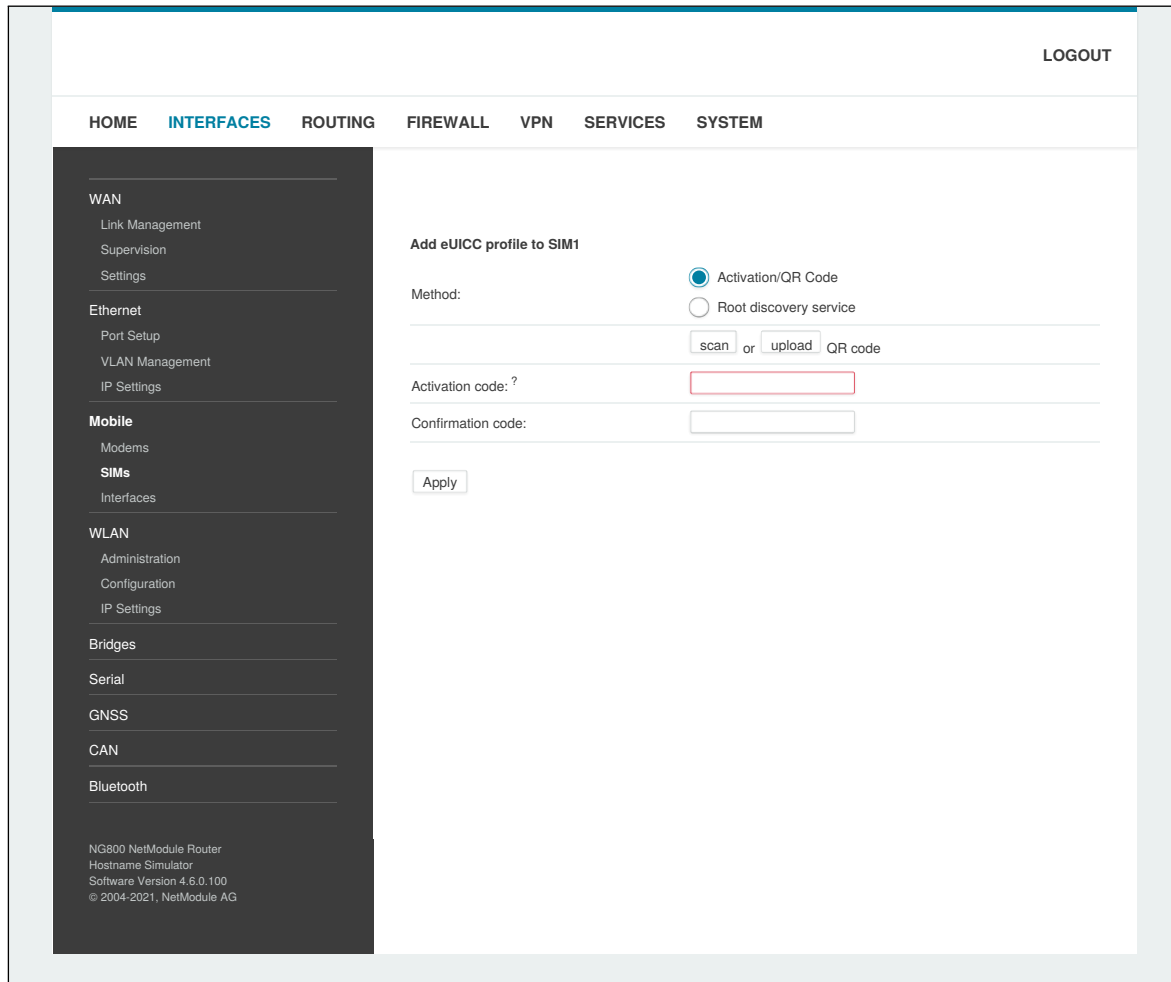


Abbildung 5.14.: eUICC-Profil hinzufügen

Die folgenden zwei Möglichkeiten zur Installation von eSIM-Profilen werden unterstützt und können auf der Konfigurationsseite für eSIM-Profilen ausgewählt werden:

1. Vom Netzbetreiber bereitgestellter QR-Code

Bei dieser Methode laden Sie das eSIM-Profil herunter, indem Sie vom Mobilfunkbetreiber einen QR-Code erhalten, der die Informationen über das zu installierende eSIM-Profil enthält. Wenn das Gerät, mit dem Sie auf die Konfigurationsschnittstelle des Routers zugreifen, eine Kamera besitzt, können Sie den QR-Code mit der Kamera scannen. Ansonsten können Sie auch eine Bilddatei des QR-Codes hochladen. Alternativ ist es möglich, den Inhalt des QR-Codes manuell in das entsprechende Eingabefeld einzutragen.

2. GSMA Root Discovery Service

Bei dieser Methode müssen Sie die EID - eine eindeutige Nummer, die die eUICC des Routers iden-

tifiziert - beim Mobilfunkbetreiber angeben. Die EID wird auf der Konfigurationsseite der eSIM-Profil angezeigt. Der Betreiber erstellt dann das eSIM-Profil für den Router auf seinen Bereitstellungsservern. Anschließend können Sie mit dem GSMA Root Discovery Service das eSIM-Profil abrufen, ohne zusätzliche Informationen für den Download angeben zu müssen.

Hinweis: Die meisten Mobilfunknetzbetreiber erlauben nur einen einmaligen Download eines eSIM-Profiles. Wenn Sie also das Profil einmal herunterladen und danach löschen, können Sie das gleiche Profil kein zweites Mal herunterladen. In diesem Fall müssten Sie beim Betreiber ein neues eSIM-Profil anfordern.

WWAN-Schnittstellen

Auf dieser Seite können Sie die WWAN-Module verwalten. Die resultierende Verbindung wird automatisch als WAN-Verbindung angezeigt, sobald eine Schnittstelle hinzugefügt wurde. In Kapitel 5.3.1 erfahren Sie Näheres zur Verwaltung.

Die Mobil-LED blinkt während des Verbindungsaufbaus und leuchtet dann dauerhaft, sobald die Verbindung steht. Näheres erfahren Sie im Kapitel 5.8.7. Konsultieren zur Fehlersuche Sie die Systemprotokolldateien, falls die Verbindung nicht hergestellt wurde.

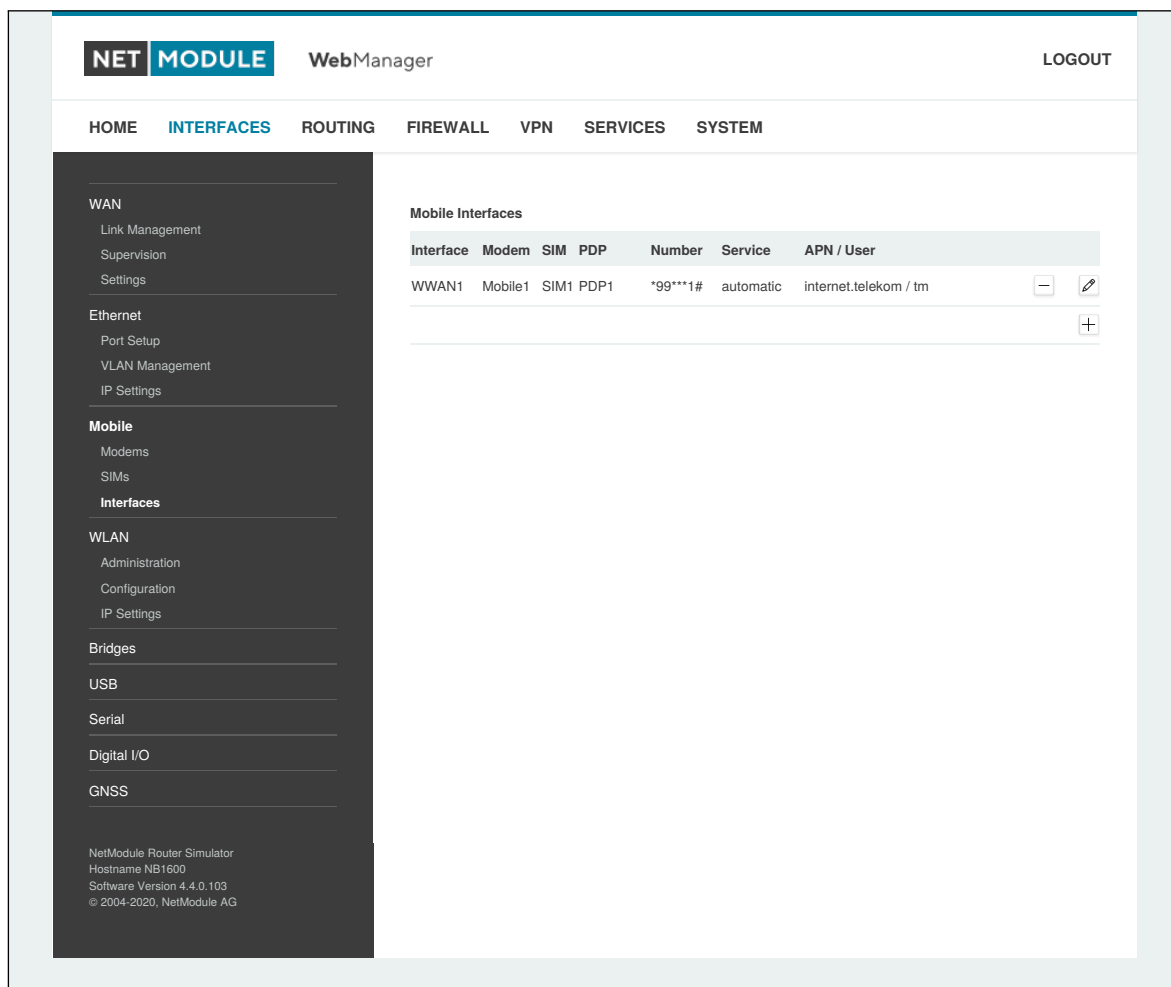


Abbildung 5.15.: WWAN-Schnittstellen

Die folgenden mobilen Einstellungen sind erforderlich:



| Parameter | WWAN-Mobil-Parameter |
|--------------|--|
| Modem | Das Modem, das für diese WWAN-Schnittstelle verwendet wird |
| SIM | Die SIM-Karte, die für diese WWAN-Schnittstelle verwendet wird |
| Service type | Der erforderliche Dienstyp |

Diese Einstellungen ersetzen die allgemeinen SIM-Einstellungen, sobald die Verbindung angewählt wird.

In der Regel werden die Verbindungseinstellungen automatisch ermittelt, sobald sich das Modem angemeldet hat und der Netzbetreiber in unserer Datenbank gefunden wurde. Andernfalls ist es erforderlich, die folgenden Einstellungen manuell zu konfigurieren:

| Parameter | WWAN-Verbindungsparameter |
|-------------------|--|
| Phone number | Die zu wählende Rufnummer. Bei 3G+-Verbindungen ist dies üblicherweise *99***1#. Bei leitungsvermittelten 2G-Verbindungen können Sie die zu wählende Festnetzrufnummer im internationalen Format eingeben (z. B. +49xx). |
| Access point name | Der Name des verwendete Access Points (APN) |
| IP version | Die genutzte IP Version. Dual-stack erlaubt den parallelen Betrieb von IPv4 und IPv6. Beachten Sie, dass die Unterstützten IP Versionen von Ihrem Provider abhängig sind. |
| Authentication | Das verwendete Authentifizierungsschema; wenn erforderlich, kann dies PAP oder CHAP sein |
| Username | Der für die Authentifizierung verwendete Benutzername |
| Password | Das für die Authentifizierung verwendete Passwort |

Darüber hinaus stehen die folgenden erweiterten Einstellungen zur Verfügung:

| Parameter | Erweiterte WAN-Parameter |
|--------------------------|--|
| Required signal strength | Legt eine minimale erforderliche Signalstärke fest, bevor die Verbindung gewählt wird |
| Home network only | Legt fest, ob die Verbindung nur gewählt werden darf, wenn sie in einem Heimnetzwerk angemeldet ist |
| Negotiate DNS | Legt fest, ob die DNS-Aushandlung durchgeführt werden soll und die abgerufenen Nameserver auf dem System angewendet werden sollen |
| Call to ISDN | Muss aktiviert sein, wenn 2G-Verbindungen mit einem ISDN-Modem kommunizieren |
| Header compression | Aktiviert oder deaktiviert die 3GPP-Header-Komprimierung, was unter Umständen die TCP/IP-Leistung bei langsamen seriellen Verbindungen verbessert. Dies muss vom Betreiber unterstützt werden. |
| Data compression | Aktiviert oder deaktiviert die 3GPP-Datenkomprimierung, die die Paketgröße verringert, um den Durchsatz zu verbessern. Dies muss vom Betreiber unterstützt werden. |
| Client address | Gibt eine feste Client-IP-Adresse an, falls vom Betreiber zugewiesen |
| MTU | Maximale Größe einer Übertragungseinheit für die Schnittstelle. |

5.3.4. WLAN

WLAN-Verwaltung

Falls der Router mit einem WLAN-Modul ausgeliefert wird, können Sie ihn entweder als `client`, `access point`, `mesh point` oder für bestimmte Dualmodi (`dual modes`) konfigurieren. In der Betriebsart `client` kann er eine zusätzliche WAN-Verbindung schaffen, die z. B. als Backup-Verbindung genutzt werden kann. Als Access Point kann er eine weitere LAN-Schnittstelle schaffen, entweder gebrückt zur Ethernet-basierten LAN-Schnittstelle oder zur Schaffung einer eigenständigen IP-Schnittstelle, die in gleicher Weise wie ein Ethernet-LAN für Routing-Zwecke und die Bereitstellung von Diensten (z. B. DHCP/DNS/NTP) verwendet werden kann. In der Betriebsart `mesh point` kann er ein drahtloses Mesh-Netzwerk aufspannen und damit Backhaul-Konnektivität mit dynamischer Pfadauswahl bereitstellen. In der Betriebsart `dual mode` ist es möglich, einen Access Point oder Client oder Mesh-Point- und Access-Point-Funktionen auf demselben Funkmodul bereitzustellen.

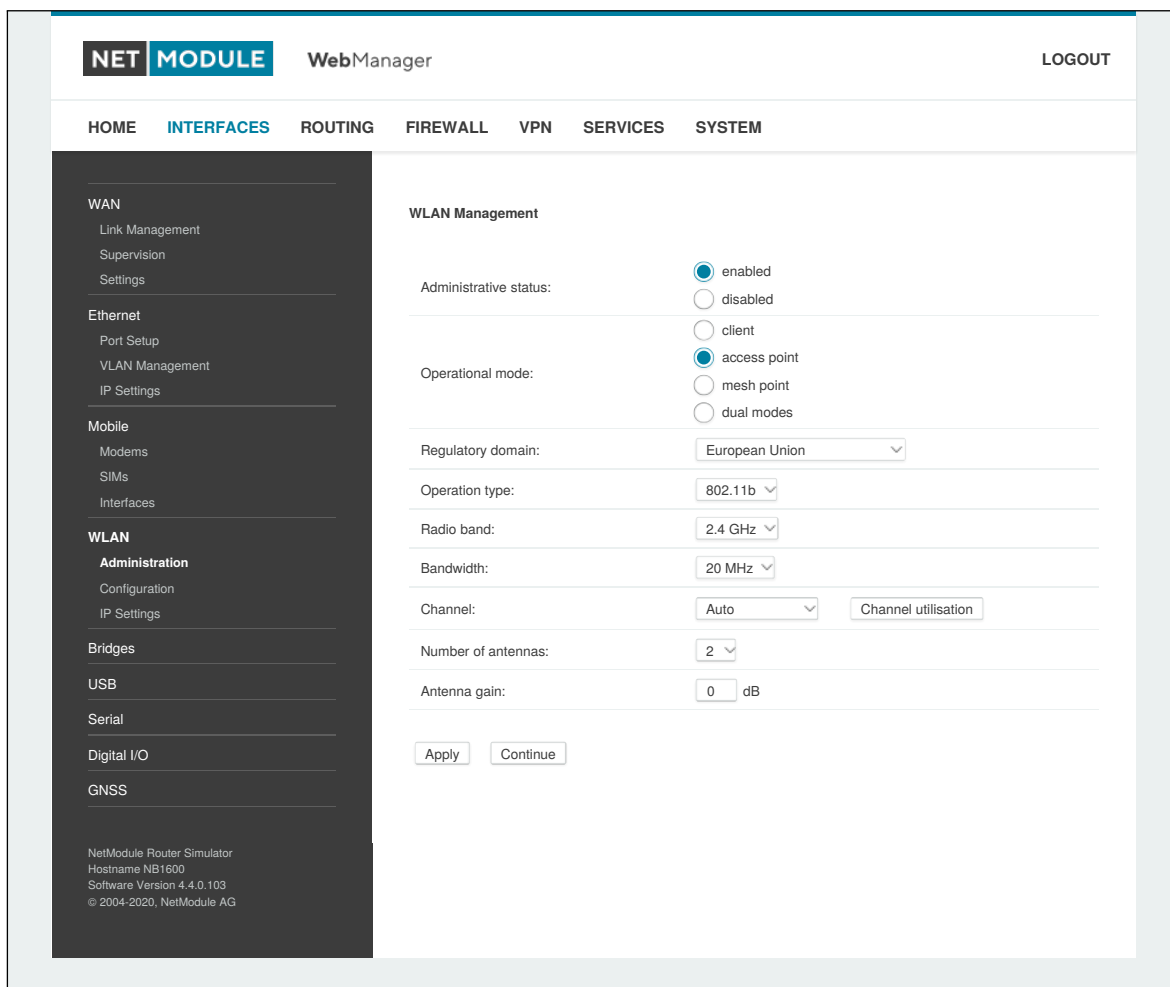


Abbildung 5.16.: WLAN-Verwaltung

Wenn der Verwaltungsstatus auf `disabled` gesetzt ist, wird das Modul ausgeschaltet, um den Gesamtstromverbrauch zu reduzieren. Für eine bessere Abdeckung und einen höheren Durchsatz empfehlen wir generell die Verwendung von zwei Antennen. Eine zweite Antenne ist unbedingt erforderlich, wenn Sie höhere Durchsatzraten wie bei 802.11n erreichen wollen.

Ein WLAN- client und ein mesh point werden automatisch zu einer WAN-Verbindung. Zur Verwaltung siehe Kapitel 5.3.1.

Konfigurierbare Parameter für access-point, client mesh point und ggf. dual mode:

| Parameter | WLAN-Verwaltung |
|------------------------|---|
| Regulatory Domain | Gibt das Land an, in dem der Router betrieben wird |
| Number of antennas | Gibt die Anzahl der angeschlossenen Antennen an |
| Antenna gain | Gibt den Antennengewinn für die angeschlossenen Antennen an. Den korrekten Wert entnehmen Sie dem Datenblatt der Antenne. |
| Tx. Power | Gibt die maximale Sendeleistung in dBm an. |
| Disable low data rates | Sticky Clients vermeiden, indem Sie niedrige Datenraten deaktiviert werden. |



Warnung

Bitte beachten Sie, dass unzulässige Parameter gegen die Konformitätsvorschriften verstoßen können.

In den Betriebsarten access point oder dual modestehen die folgenden weiteren Einstellungen zur Verfügung:

| Parameter | WLAN-Verwaltung |
|------------------------|---|
| Operation type | Legt die IEEE 802.11-Betriebsart fest |
| Radio band | Wählt das Funkband aus, das für Verbindungen verwendet werden soll - je nach Modul 2,4 oder 5 GHz |
| Outdoor | Zeigt die 5-GHz-Außenbereichskanäle an |
| Bandwidth | Legt die Betriebsart für die Kanalbandbreite fest |
| Channel | Legt den zu verwendenden Kanal fest |
| enable client tracking | Aktiviert die Verfolgung nicht zugeordneter Clients |
| Short Guard Interval | Aktiviert ein kürzeres Schutzintervall (Short Guard Interval, GI) |

In der Betriebsart clientstehen die folgenden weiteren Einstellungen zur Verfügung:

| Parameter | WLAN-Verwaltung |
|---------------|---|
| Scan channels | Legt fest, ob alle unterstützten Kanäle gescannt werden sollen oder nur benutzerdefinierte Kanäle |
| 2.4 GHz | Legt die Kanäle fest, die im 2,4-GHz-Band gescannt werden sollen |
| 5 GHz | Legt die Kanäle fest, die im 5-GHz-Band gescannt werden sollen |

Die verfügbaren Betriebsarten sind:

| Standard | Frequenzen | Bandbreite | Datenrate |
|----------|------------|--------------|--------------|
| 802.11a | 5 GHz | 20 MHz | 54 Mbit/s |
| 802.11b | 2,4 GHz | 20 MHz | 11 Mbit/s |
| 802.11g | 2,4 GHz | 20 MHz | 54 Mbit/s |
| 802.11n | 2,4/5 GHz | 20/40 MHz | 300 Mbit/s |
| 802.11ac | 5 GHz | 20/40/80 MHz | 866,7 Mbit/s |

Tabelle 5.24.: IEEE 802.11-WLAN-Normen

In der Betriebsart `mesh point` stehen die folgenden weiteren Einstellungen zur Verfügung:

| Parameter | Verwaltung des WLAN Mesh Point |
|------------|---|
| Radio band | Wählt das Funkband aus, das für Verbindungen verwendet werden soll - je nach Modul 2,4 oder 5 GHz |
| Channel | Legt den zu verwendenden Kanal fest |

Hinweis: NetModule Router mit 802.11n und 802.11ac unterstützen 2x2 MIMO

Vor dem Einrichten eines Access Points ist es sinnvoll, einen Netzwerksan durchzuführen, um eine Liste der benachbarten WLAN-Netzwerke zu erhalten und dann den am wenigsten störenden Kanal zu wählen. Bitte beachten Sie, dass zwei ausreichend nutzbare Kanäle erforderlich sind, um mit 802.11n bei einer Bandbreite von 40 MHz einen guten Durchsatz zu erzielen.

WLAN-Konfiguration

In der Betriebsart `client` ist es möglich, eine Verbindung zu einem oder mehreren entfernten Zugangspunkten herzustellen. Das System schaltet auf das nächste Netzwerk in der Liste um, wenn eines ausfällt, und kehrt zum Netzwerk mit der höchsten Priorität zurück, sobald es wieder verfügbar ist.

Sie können einen WLAN-Netzwerksan durchführen und die Einstellungen direkt aus den gefundenen Informationen auswählen. Die Authentifizierungsdaten müssen beim Betreiber des entfernten Access Points in Erfahrung gebracht werden.

| Parameter | Konfiguration des WLAN-Clients |
|---------------|--|
| SSID | Der Netzwerkname (als SSID bezeichnet) |
| Security mode | Der gewählte Sicherheitsmodus |
| WPA mode | Die gewählte Verschlüsselungsmethode. WPA3 sollte gegenüber WPA2 und WPA1 bevorzugt werden |
| WPA cipher | Die zu verwendende WPA-Verschlüsselung; standardmäßig werden beide verwendet (TKIP und CCMP) |
| Identity | Die für WPA-RADIUS und WPA-EAP-TLS verwendete Identität |

| Parameter | Konfiguration des WLAN-Clients |
|--------------------------|---|
| Passphrase | Die Passphrase, die für die Authentifizierung mit WPA-Personal verwendet wird, ansonsten die Schlüsselpassphrase für WPA-EAP-TLS |
| Force PMF | Aktiviert geschützte Verwaltungsframes (Protected Management Frames) |
| Enable fast transition | Aktiviert in der Betriebsart Client schnelle Roaming-Fähigkeiten über Fast Basic Service Set Transition. Nur nutzbar, wenn auch der Access Point diese Funktion unterstützt |
| Required signal strength | Erforderliche Signalstärke zum Herstellen der Verbindung |

Der `client` führt Hintergrundscans für das Roaming innerhalb eines Extended Service Set durch. Die Hintergrundscans basieren auf der aktuellen Signalstärke.

| Parameter | Parameter für die WLAN-Client-Hintergrundscans |
|----------------|---|
| Threshold | Die Signalstärke in dBm, ab der das lange bzw. kurze Zeitintervall gerechnet werden soll |
| Long interval | Die Zeit in Sekunden, nach der ein Hintergrundscan durchgeführt werden soll, nachdem die Signalstärke über den angegebenen Schwellenwert steigt |
| Short interval | Die Zeit in Sekunden, nach der ein Hintergrundscan durchgeführt werden soll, nachdem die Signalstärke unter den angegebenen Schwellenwert fällt |

In der Betriebsart `access point` können Sie bis zu 8 SSIDs erstellen, von denen jede ihre eigene Netzwerkkonfiguration besitzt. Die Netzwerke können einzeln mit einer LAN-Schnittstelle verbunden (gebrückt) oder im Routing-Modus als dedizierte Schnittstelle betrieben werden.

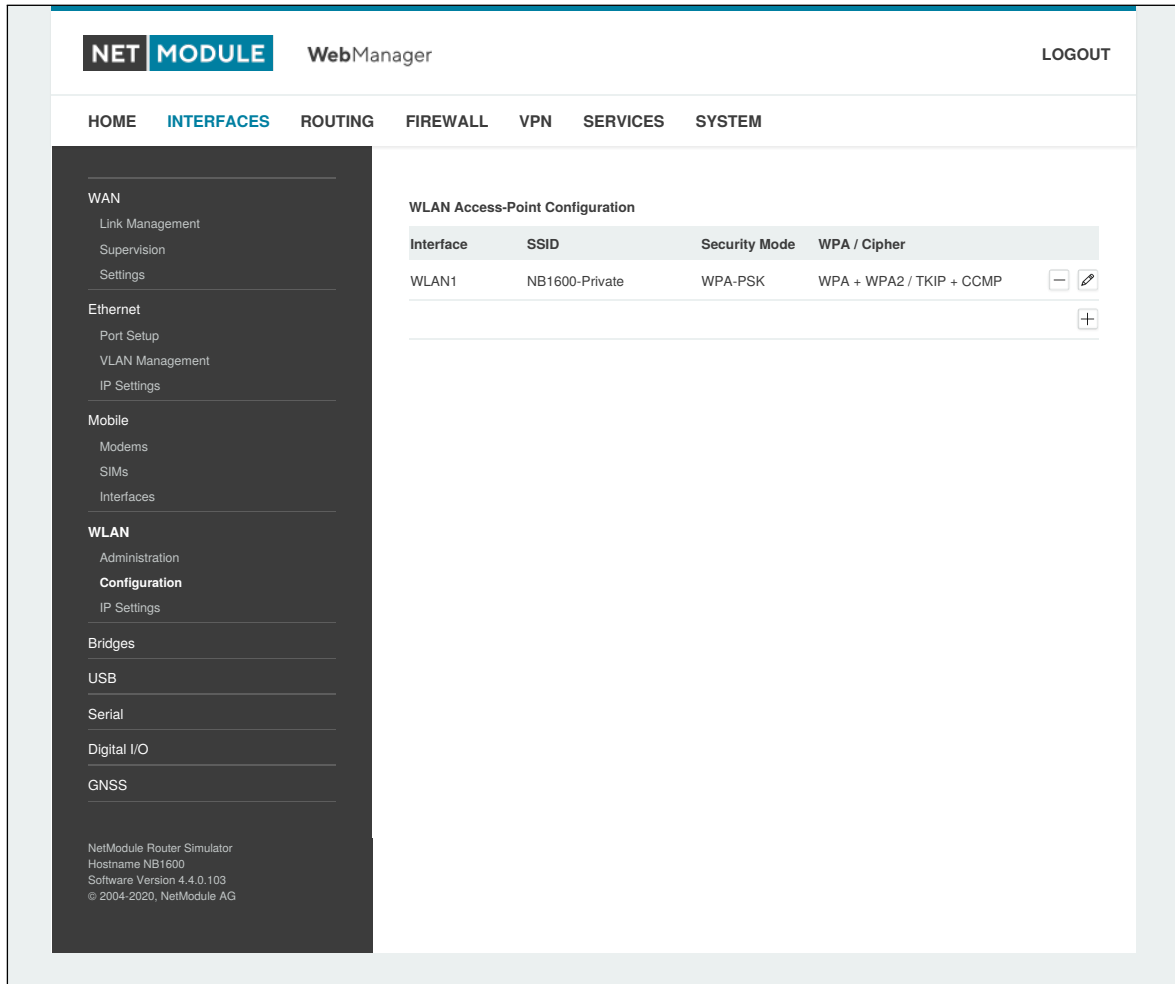


Abbildung 5.17.: WLAN-Konfiguration

In diesem Abschnitt können Sie sicherheitsrelevante Einstellungen konfigurieren.

| Parameter | Konfiguration des WLAN-Access-Point |
|--|---|
| SSID | Der Netzwerkname (als SSID bezeichnet) |
| Security mode | Der gewählte Sicherheitsmodus |
| WPA mode | Die gewählte Verschlüsselungsmethode. WPA3 + WPA2 im gemischten Modus sollten bevorzugt werden |
| WPA cipher | Die zu verwendende WPA-Verschlüsselung; standardmäßig werden beide verwendet (TKIP und CCMP) |
| Passphrase | Die Passphrase, die für die Authentifizierung mit WPA-Personal verwendet wird. |
| Force PMF | Aktiviert geschützte Verwaltungsframes (Protected Management Frames) |
| Hide SSID | Der Netzwerkname (SSID) wird verborgen |
| Isolate clients | Deaktiviert die direkte Kommunikation zwischen Clients |
| Band steering master | Die WLAN-Schnittstelle, zu der der Client geleitet werden soll |
| Opportunistic Wireless Encryption transition | Die WLAN-Schnittstelle, zu der der Client von einer unverschlüsselten WLAN-Schnittstelle zu einer mit OWE verschlüsselten WLAN-Schnittstelle geleitet werden soll |
| Accounting | Legt das Abrechnungsprofil fest |

Es gibt für die Sicherheit die folgenden Konfigurationsmöglichkeiten:

| Parameter | WLAN-Sicherheitsmodi |
|----------------|--|
| Off | SSID ist deaktiviert |
| None | Keine Authentifizierung, offenes WLAN |
| WEP | WEP (wird heute nicht mehr empfohlen) |
| WPA-Personal | WPA-Personal (TKIP, CCMP), bietet eine passwortbasierte Authentifizierung |
| WPA-Enterprise | WPA-Enterprise im Access-Point-Modus; kann zur Authentifizierung gegenüber einem entfernten RADIUS-Server verwendet werden. Zur Konfiguration siehe Kapitel 5.8.2 |
| WPA-RADIUS | EAP-PEAP/MSCHAPv2 im Access-Point-Modus; kann zur Authentifizierung gegenüber einem entfernten RADIUS-Server verwendet werden. Zur Konfiguration siehe Kapitel 5.8.2 |
| WPA-TLS | EAP-TLS im Client-Modus; dient zur Authentifizierung über Zertifikate. Zur Konfiguration siehe Kapitel 5.8.8 |
| OWE | Opportunistic Wireless Encryption alias Enhanced OPEN bietet verschlüsseltes WLAN ohne eine Authentifizierung |

In der Betriebsart `mesh point` ist es möglich, eine Verbindung zu einem oder mehreren entfernten Mesh Points innerhalb des Mesh-Netzwerks herzustellen. Das System meldet sich automatisch beim WLAN an und verbindet sich mit den anderen Mesh-Partnern mit der gleichen ID und denselben Zugangsdaten.

Die Authentifizierungsdaten müssen beim Betreiber des entfernten Mesh-Networks in Erfahrung gebracht werden.

| Parameter | Konfiguration von WLAN Mesh Points |
|---------------------------|--|
| MESHID | Der Netzwerkname (als MESHID bezeichnet) |
| Security mode | Der gewählte Sicherheitsmodus |
| enable gate announcements | Aktiviert Gate-Ankündigungen für das Mesh-Netzwerk |

Es gibt für die Sicherheit die folgenden Konfigurationsmöglichkeiten:

| Parameter | WLAN-Mesh-Point-Sicherheitsmodi |
|-----------|---|
| Off | MESHID ist deaktiviert |
| None | Keine Authentifizierung, offenes WLAN |
| SAE | SAE (Simultaneous Authentication of Equals) ist ein sicheres passwortbasiertes Protokoll zur Authentifizierung und zum Erstellen von Schlüsseln |

WLAN-IP-Einstellungen

In diesem Abschnitt können Sie die TCP/IP-Einstellungen des WLAN-Netzwerks konfigurieren. Eine Schnittstelle für die Betriebsarten `client` und `mesh point` kann über DHCP oder mit einer statisch konfigurierten Adresse und einem Standard-Gateway betrieben werden.

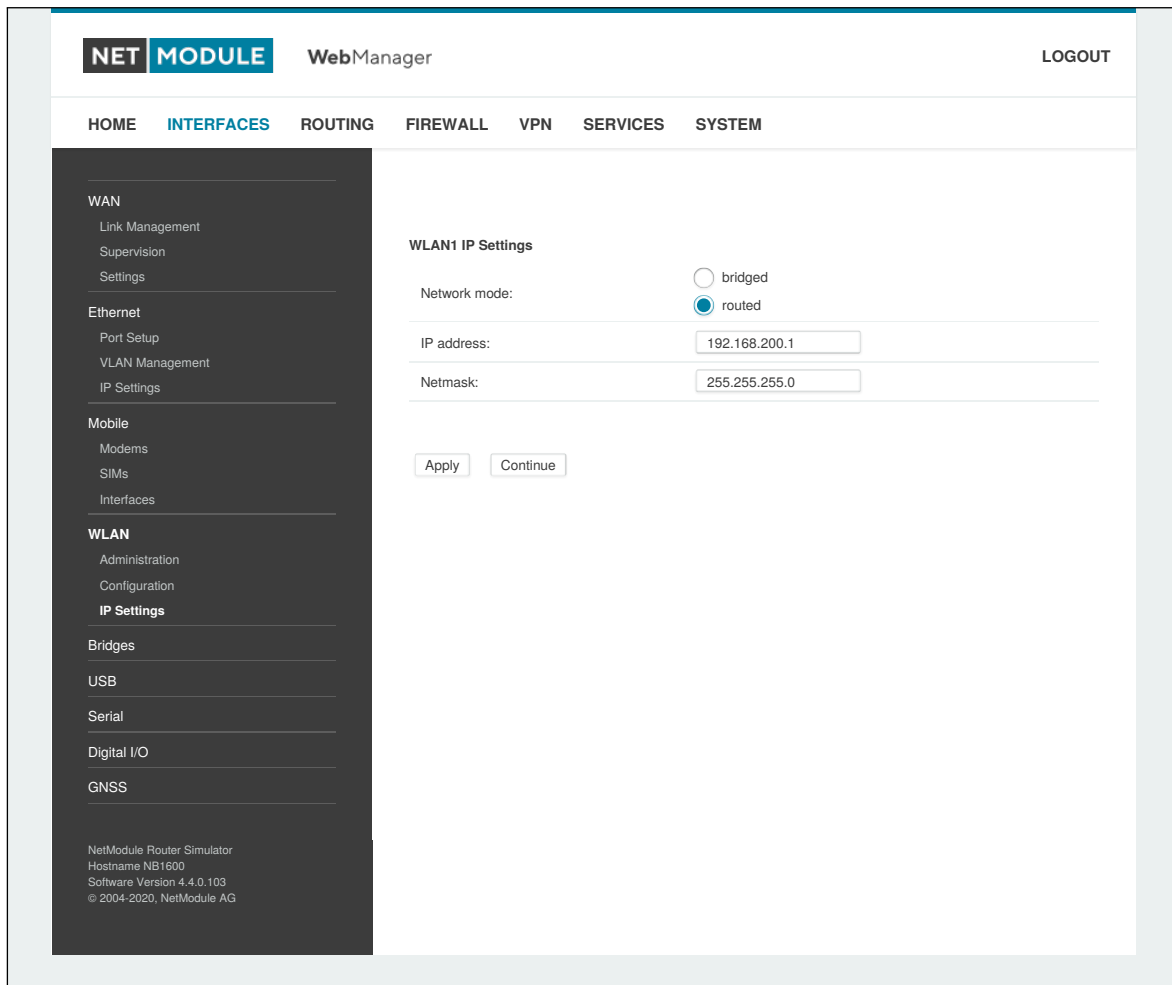


Abbildung 5.18.: WLAN-IP-Konfiguration

Die Netzwerke der Access Points können per Bridge mit jeder LAN-Schnittstelle verbunden (gebrückt) werden, damit WLAN-Clients und Ethernet-Hosts im gleichen Subnetz arbeiten können. Bei mehreren SSIDs empfehlen wir jedoch dringend, getrennte Schnittstellen im Routing-Modus einzurichten, um unerwünschte Zugriffe und Datenverkehr zwischen den Schnittstellen zu unterbinden. Der entsprechende DHCP-Server für jedes Netzwerk kann anschließend konfiguriert werden, siehe Kapitel 5.7.2.

| Parameter | WLAN-IP-Einstellungen |
|--------------------|--|
| Network mode | Legt fest, ob die Schnittstelle gebrückt oder im Routing-Modus betrieben werden soll |
| Bridge interface | Wenn gebrückt, die LAN-Schnittstelle, mit der das WLAN-Netzwerk gebrückt werden soll |
| IP address/netmask | Im Routing-Modus die IP-Adresse und Netzmaske für dieses WLAN-Netzwerk |

Die folgende Funktion kann konfiguriert werden, wenn die WLAN-Schnittstelle gebrückt ist

| Parameter | WLAN-Brückenfunktionen |
|-----------------|--|
| 4addr frame | Aktiviert das Frame-Format mit vier Adressen (erforderlich für gebückte Verbindungen) |
| IAPP | Aktiviert die Funktion Inter-Access Point Protocol |
| Pre-auth | Aktiviert den Vorauthentifizierungsmechanismus für Roaming-Clients (falls vom Client unterstützt). Pre-auth wird nur mit WPA2-Enterprise mit CCMP unterstützt. |
| Fast transition | Aktiviert schnelle Roaming-Fähigkeiten (FT) über Fast Basic Service Set Transition, falls vom Client unterstützt |

Es stehen für FT die folgenden Einstellungen zur Verfügung:

| Parameter | WLAN-Brückenfunktionen |
|------------------------------|--|
| Mobility domain | Die Mobilitätsdomäne des FT-Netzwerks |
| Preshared key | Die PSK für das FT-Netzwerk |
| Fast transition clients only | Wenn aktiviert, akzeptiert der Access Point nur Clients, die FT unterstützen |

5.3.5. Software-Bridges

Software-Bridges können Layer-2-Geräte wie OpenVPN TAP, GRE oder WLAN-Schnittstellen zu überbrücken, ohne dass eine physische LAN-Schnittstelle erforderlich ist.

Bridge-Einstellungen

Auf dieser Seite können Sie Software-Bridges aktivieren/deaktivieren.

Es bestehen die folgenden Konfigurationsmöglichkeiten:

| Parameter | Bridge-Einstellungen |
|-----------------------|--|
| Administrative status | Aktiviert oder deaktiviert die Bridge-Schnittstelle. Wenn Sie eine Schnittstelle zum lokalen System benötigen, müssen Sie eine IP-Adresse für das lokale Gerät definieren. |
| IP Address | IP-Adresse der lokalen Schnittstelle (nur verfügbar, wenn Aktiviert mit lokaler Schnittstelle"gewählt wurde) |
| Netmask | Netzmaske der lokalen Schnittstelle (nur verfügbar, wenn Aktiviert mit lokaler Schnittstelle"gewählt wurde) |
| MTU | Optional: Maximale Größe einer Übertragungseinheit der lokalen Schnittstelle (nur verfügbar, wenn Aktiviert mit lokaler Schnittstelle"gewählt wurde" |

5.3.6. USB

NetModule-Router werden mit einem Standard-USB-Host-Anschluss geliefert, an den ein Speicher-, Netzwerk- oder serielles USB-Gerät angeschlossen werden kann. Eine Liste der unterstützten Geräte erhalten Sie auf Anfrage vom Technischen Support.

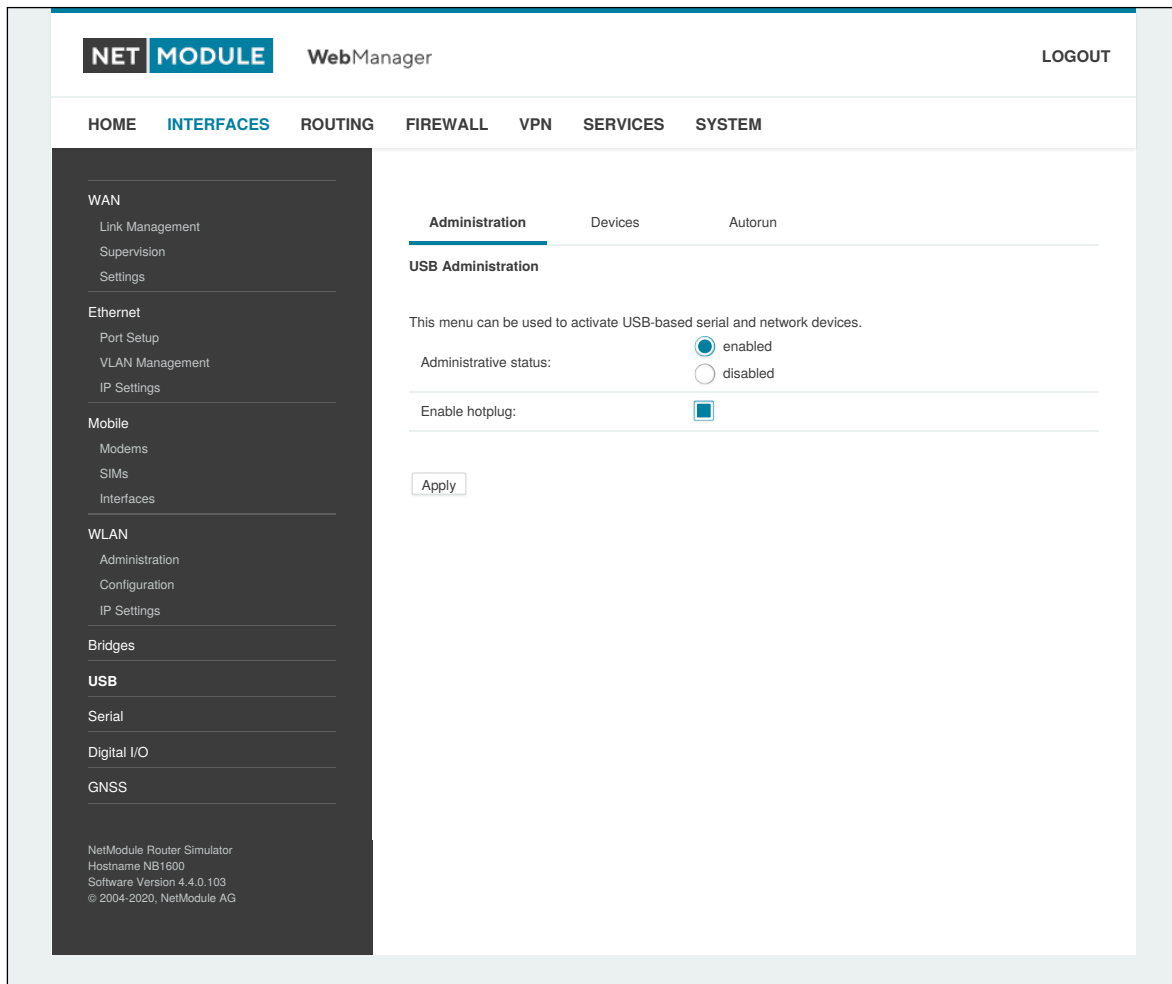


Abbildung 5.19.: USB-Verwaltung

USB-Verwaltung

| Parameter | USB-Verwaltung |
|-----------------------|--|
| Administrative status | Legt fest, ob Geräte erkannt werden sollen |
| Enable hotplug | Legt fest, ob Geräte beim Einstecken im laufenden Betrieb erkannt werden oder nur beim Bootvorgang |

USB-Geräte

Diese Seite zeigt die aktuell angeschlossenen Geräte an. Hier können Sie ein bestimmtes Gerät basierend auf seiner Hersteller- und Produkt-ID aktivieren. Nur aktivierte Geräte werden vom System erkannt und können zusätzliche Anschlüsse und Schnittstellen bereitstellen.

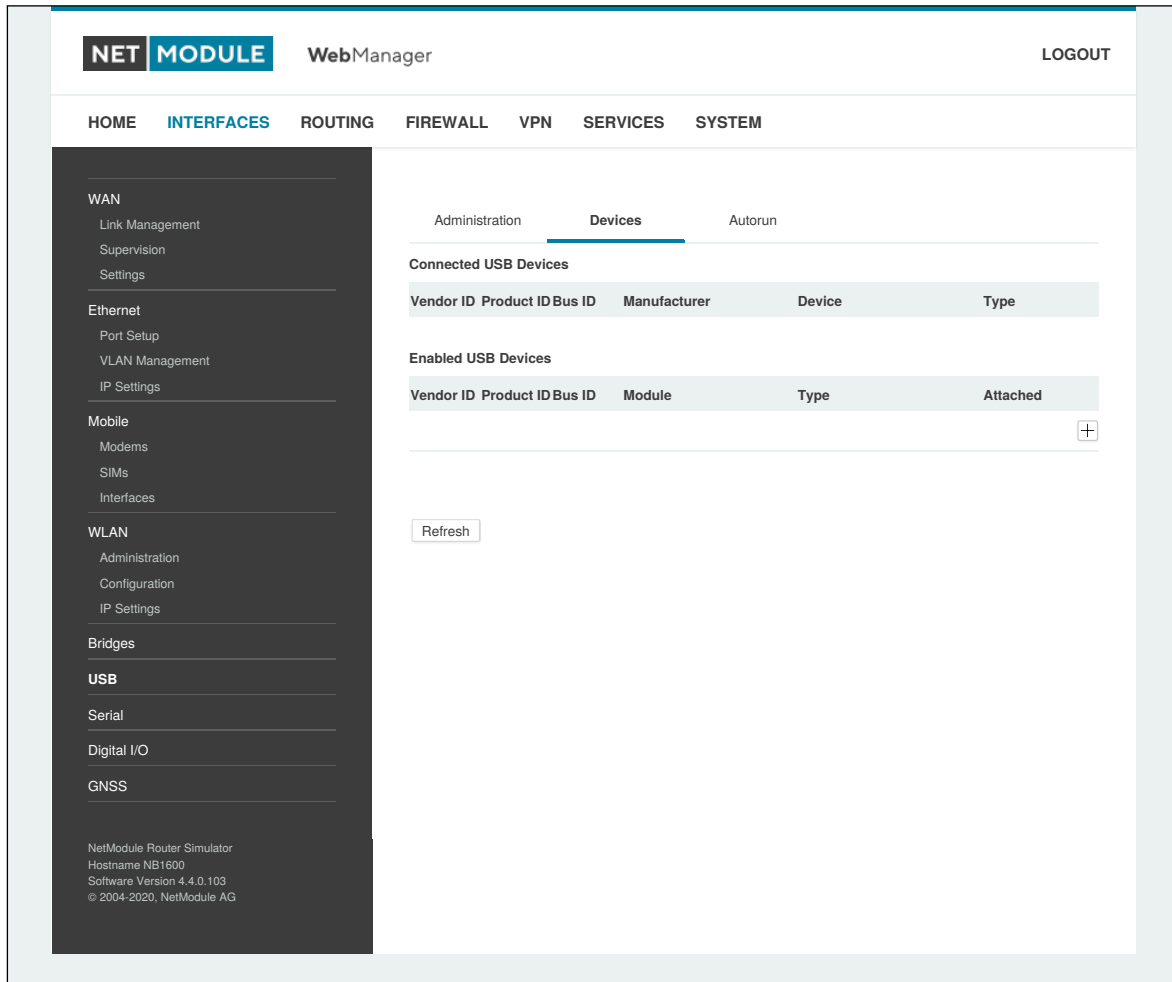


Abbildung 5.20.: USB-Geräteverwaltung

| Parameter | USB-Geräte |
|------------|--|
| Vendor ID | Die Herstellerkennung (Vendor ID) des USB-Geräts |
| Product ID | Die Produktkennung (Product ID) des USB-Geräts |
| Module | Das USB-Modul und der Typ des Treibers, der für dieses Gerät verwendet werden soll |

Kennungen ID muss in hexadezimaler Schreibweise angegeben werden, Wildcards werden unterstützt (z. B. AB[0-1][2-3] oder AB*). Ein USB-Netzwerkgerät wird als LAN10 bezeichnet.

5.3.7. Serial

Auf dieser Seite können Sie die seriellen Schnittstellen verwalten. Eine serielle Schnittstelle kann verwendet werden von:

| Parameter | Verwendung der seriellen Schnittstelle |
|----------------|--|
| none | Die serielle Schnittstelle wird nicht verwendet |
| login console | Über die serielle Schnittstelle wird eine Konsole geöffnet, auf die von einem Client mit seriellm Terminal von der Gegenseite aus zugegriffen werden kann. Sie bietet hilfreiche Start- und Kernel-Meldungen und erzeugt eine Anmeldeshell, über die sich Benutzer beim System anmelden können. Wenn mehr als eine serielle Schnittstelle vorhanden ist, kann jeweils eine serielle Schnittstelle als Anmeldekonsole konfiguriert werden. |
| device server | Die serielle Schnittstelle wird über einen TCP/IP-Port freigegeben und kann zur Implementierung eines seriellen/IP-Gateways verwendet werden. |
| modem bridge | Überbrückt die serielle Schnittstelle zum Modem TTY eines integrierten WWAN-Modems. |
| modem emulator | Emuliert ein klassisches mit AT-Befehlen gesteuertes Modem auf der seriellen Schnittstelle. Nähere Informationen finden Sie unter http://wiki.netmodule.com/app-notes/hayes-modem-at-simulator . |
| SDK | Die serielle Schnittstelle wird für SDK-Skripte reserviert. |

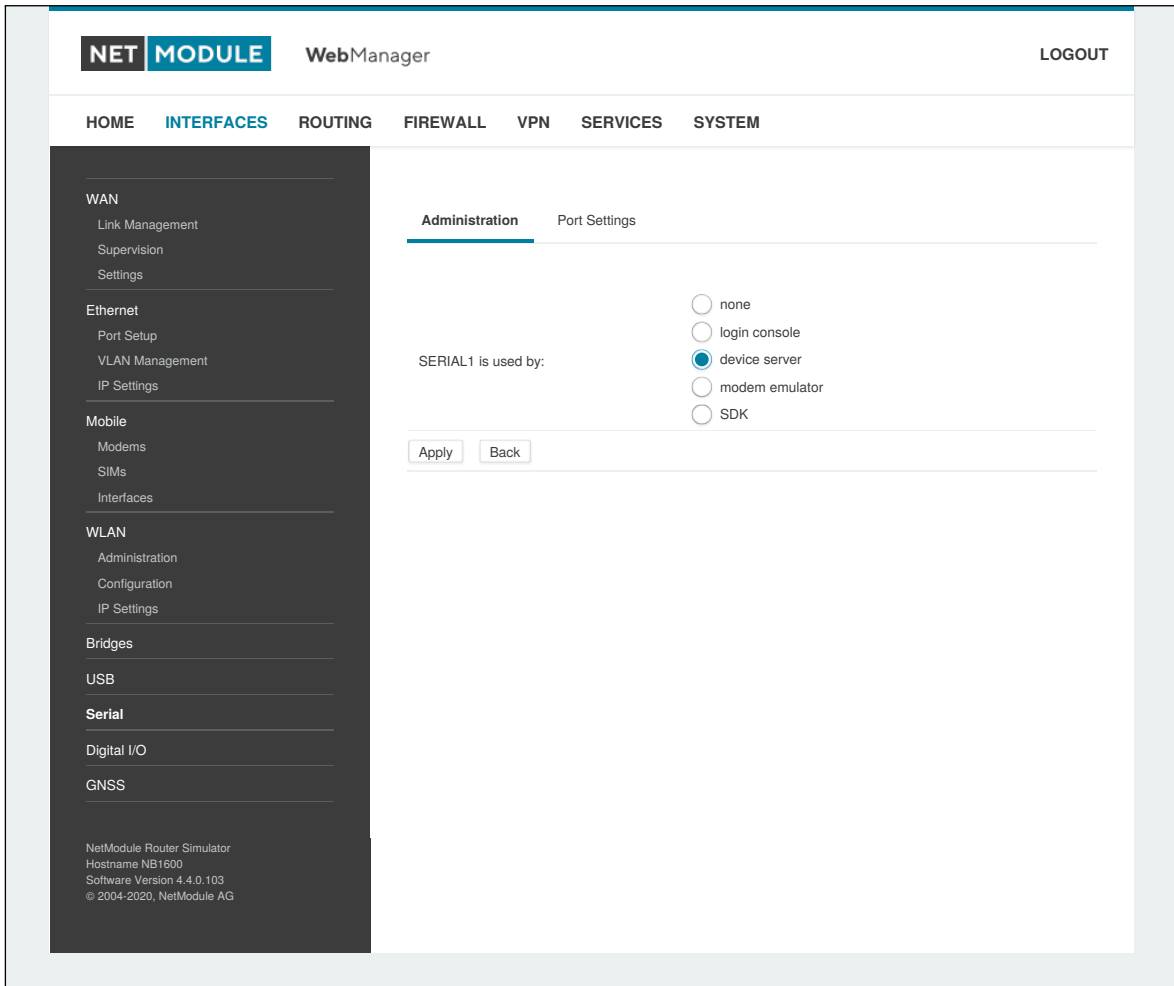


Abbildung 5.21.: Verwaltung der seriellen Schnittstelle

Beim Betrieb eines Geräteservers sind die folgenden Einstellungen verfügbar:

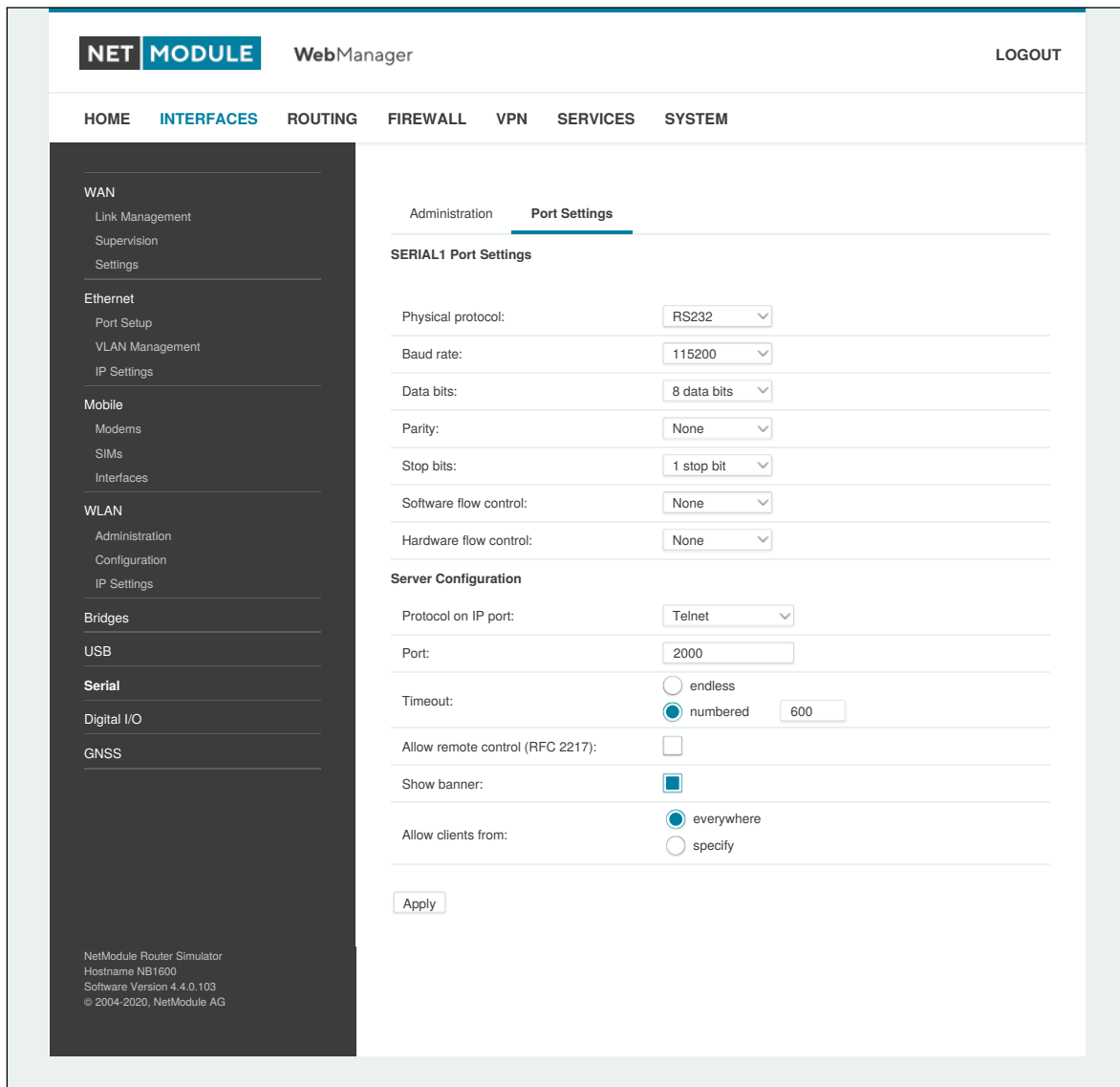


Abbildung 5.22.: Einstellungen der seriellen Schnittstelle

| Parameter | Einstellungen der seriellen Schnittstelle |
|-------------------|---|
| Physical protocol | Wählt das gewünschte physikalische Protokoll auf der seriellen Schnittstelle |
| Baud rate | Gibt die Geschwindigkeit an, mit der die serielle Schnittstelle betrieben wird |
| Data bits | Gibt die Anzahl der Datenbits an, die in jedem Frame enthalten sind |
| Parity | Gibt die Parität an, die für jeden gesendeten oder empfangenen Frame verwendet wird |

| Parameter | Einstellungen der seriellen Schnittstelle |
|-----------------------|---|
| Stop bits | Legt die Anzahl der Stoppbits fest, die verwendet werden, um das Ende eines Frames anzuzeigen |
| Software flow control | Legt die Software-Datenflusssteuerung für die serielle Schnittstelle fest; XOFF sendet ein Stoppsymbol, XON ein Startsymbol an die Gegenstelle, um die eingehenden Daten zu steuern |
| Hardware flow control | Sie können die RTS/CTS-Hardware-Datenflusssteuerung aktivieren, sodass die RTS- und CTS-Leitungen zur Steuerung des Datenflusses verwendet werden können |
| Protocol on TCP/IP | Sie können die IP-Protokolle Telnet oder TCP raw für den Geräteserver wählen. |
| Port | Der TCP-Port für den Geräteserver |
| Timeout | Das Zeitlimit, bis ein Client als nicht mehr verbunden betrachtet wird |

| Parameter | Server-Einstellungen |
|----------------------|---|
| Protocol on IP port | Legt das IP-Protokoll fest (TCP oder Telnet) |
| Port | Legt den TCP-Port fest, auf dem der Server erreichbar sein soll |
| Timeout | Zeit (in Sekunden) bis zum Trennen der Verbindung, wenn auf dem Anschluss keine Aktivität verzeichnet wird Ein Wert von 0 deaktiviert diese Funktion. |
| Allow remote control | Lässt die (nach RFC 2217) der seriellen Schnittstelle zu |
| Show banner | Zeigt ein Banner an, wenn Clients eine Verbindung herstellen |
| Stop bits | Legt die Anzahl der Stoppbits fest, die verwendet werden, um das Ende eines Frames anzuzeigen |
| Allow clients from | Legt fest, welche Clients eine Verbindung zum Server herstellen dürfen |

Bitte beachten Sie, dass der Geräteserver keine Authentifizierung oder Verschlüsselung bietet und Clients von überall aus eine Verbindung herstellen können. Ziehen Sie in Erwägung, den Zugriff auf ein begrenztes Netzwerk/einen bestimmten Host zu beschränken oder Pakete mit Hilfe der Firewall zu blockieren.

Wenn die serielle Schnittstelle als AT-Modem-Emulator betrieben wird, stehen die folgenden Einstellungen zur Verfügung:

| Parameter | Einstellungen der seriellen Schnittstelle |
|-------------------|--|
| Physical protocol | Wählt das gewünschte physikalische Protokoll auf der seriellen Schnittstelle |
| Baud rate | Gibt die Geschwindigkeit an, mit der die serielle Schnittstelle betrieben wird |



| Parameter | Einstellungen der seriellen Schnittstelle |
|-----------------------|--|
| Hardware flow control | Sie können die RTS/CTS-Hardware-Datenflusssteuerung aktivieren, sodass die RTS- und CTS-Leitungen zur Steuerung des Datenflusses verwendet werden können |

| Parameter | Eingehende Verbindungen über Telnet |
|-----------|-------------------------------------|
| Port | Der TCP-Port für den Geräteserver |

| Parameter | Telefonbucheinträge |
|------------|--|
| Number | Rufnummer, die einen Alias erhalten soll |
| IP address | IP-Adresse, die der Nummer zugewiesen wird |
| Port | Anschlussbezeichnung (Port) der IP-Adresse |

5.3.8. Audio

Audio-Verwaltung

Auf dieser Seite können Sie das Audiomodul vorkonfigurieren. Sie kann später auch für das Sprach-Gateway verwendet werden.

Es bestehen die folgenden Konfigurationsmöglichkeiten:

| Parameter | Audio-Einstellungen |
|--------------|---------------------------------|
| Volume level | Standardlautstärke für Line-Out |

Audio Testing

Auf dieser Seite können Sie ein Audio-Sample abspielen oder aufnehmen. Für den Wiedergabetest können Sie eine WAV-Datei (2-Kanal, 44100 Hz, 16 Bit) hochladen.

5.3.9. GNSS

Konfiguration

Auf dieser Seite können Sie die im System vorhandenen GNSS-Module aktivieren oder deaktivieren und den Daemon konfigurieren, der einen gemeinsamen Zugriff auf die Empfänger ohne Konflikte oder Datenverluste ermöglicht.

Es antwortet auf Abfragen in einem Format, das wesentlich einfacher zu parsen ist als das direkt vom GNSS-Gerät ausgegebene NMEA-0183-Format.

Wir verwenden derzeit den Berlios-GPS-Daemon (Version 3.15), der das neue JSON-Format unterstützt. Unter <http://www.catb.org/gpsd/> finden Sie weitere Informationen darüber, wie Sie beliebige Clients per Fernzugriff mit dem Daemon verbinden können. Die Positionswerte können auch über die Kommandozeile abgefragt und in SDK-Skripten verwendet werden.

| Parameter | Konfiguration des GNSS-Moduls |
|-----------------------|---|
| Administrative status | Aktiviert oder deaktiviert das GNSS-Modul |
| Operation mode | Die Betriebsart, entweder Standalone oder Assisted (A-GPS) |
| Antenna type | Der Typ der angeschlossenen GPS-Antenne, entweder passiv oder aktiv mit 3 Volt gespeist |
| Accuracy | Der GNSS-Empfänger vergleicht die berechnete Positionsgenauigkeit auf Basis auf den Satelliteninformationen und vergleicht sie mit dieser Genauigkeitsschwelle in Metern. Wenn die berechnete Positionsgenauigkeit höher als die Genauigkeitsschwelle ist, wird die Position gemeldet. Stellen Sie diesen Parameter auf einen höheren Schwellenwert ein, wenn der GNSS-Empfänger keinen Positionsfix meldet oder wenn es zu lange dauert, einen solche Positionsfix zu berechnen. Dies kann der Fall sein, wenn keine freie Sicht zur GNSS-Antenne besteht, z. B. in Tunneln oder neben hohen Gebäuden oder Bäumen. |
| Fix frame interval | Die Zeit, die zwischen Positionsfixes gewartet wird |

Wenn das GNSS-Modul AssistNow unterstützt und `operation mode` auf `assisted` gesetzt ist, stehen die folgenden Einstellungen zur Verfügung:

| Parameter | GPS-Konfiguration mit GNSS Assisted |
|---------------|-------------------------------------|
| Primary URL | Die primäre AssistNow-URL |
| Secondary URL | Die sekundäre AssistNow-URL |



Informationen zu AssistNow: Wenn Sie viele Geräte unterwegs haben, die den AssistNow-Dienst nutzen, sollten Sie in Erwägung ziehen, ein eigenes AssistNow-Token zu erstellen, und zwar unter <http://www.u-blox.com>. Wenn zu viele Anfragen pro Zeiteinheit eintreffen, funktioniert der Dienst möglicherweise nicht wie erwartet. Bei weiteren Fragen wenden Sie sich bitte an unseren Support.

| Parameter | Konfiguration des GNSS-Servers |
|--------------------|--|
| Server port | Der TCP-Anschluss, auf dem der Daemon auf eingehende Verbindungen wartet |
| Allow clients from | Legt fest, von wo aus sich Clients verbinden können; mögliche Werte sind <code>everywhere</code> oder ein bestimmtes Netzwerk |
| Clients start mode | Legt fest, wie die Datenübertragung erfolgt, wenn ein Client eine Verbindung herstellt. Möglich ist <code>on request</code> , was typischerweise erfordert, dass ein <code>R</code> gesendet wird. Die Daten werden sofort gesendet, wenn der Modus <code>raw</code> aktiv ist, wobei dann NMEA-Frames ausgeliefert werden, oder <code>super-raw</code> , wobei die Originaldaten des GPS-Empfängers ausgeliefert werden. Wenn der Client das JSON-Format unterstützt (d. h. eine neuere <code>libgps</code> verwendet), kann auch der Modus <code>json mode</code> festgelegt werden. |

Überlegen Sie, ob Sie nicht den Zugriff auf den Server-Anschluss beschränken sollten, entweder durch Angabe eines dedizierten Client-Netzwerks oder durch eine Firewall-Regel.



Informationen zu Dead Reckoning: Wenn Sie ein Gerät haben, das Dead Reckoning unterstützt, finden Sie weitere Informationen in der Installationsanleitung für GNSS Dead Reckoning, oder Sie kontaktieren unseren Support.

Position

Auf dieser Seite finden Sie weitere Informationen zu sichtbaren Satelliten und den erhaltenen Werten:

| Parameter | GNSS-Information |
|-----------------------|--|
| Latitude | Die geografische Koordinate, die die Nord-Süd-Position angibt |
| Longitude | Die geografische Koordinate, die die Ost-West-Position angibt |
| Altitude | Die Höhe über dem Meeresspiegel des aktuellen Standorts |
| Satellites in view | Die Anzahl der sichtbaren Satelliten, wie in GPGSV-Frames angegeben |
| Geschwindigkeit: | Die horizontale und vertikale Geschwindigkeit in Metern pro Sekunde, wie in den GPRMC-Frames angegeben |
| Satellites used | Die Anzahl der Satelliten, die für die Berechnung der Position verwendet werden, wie in den GPGGA-Frames angegeben |
| Dilution of precision | Die Verringerung der Genauigkeit (DOP bzw. GDOP), wie in den GPGSA-Frames angegeben |

Darüber gibt es zu jedem Satelliten die folgenden Detailangaben:

| Parameter | GNSS-Satelliteninformationen |
|-----------|--|
| PRN | Der PRN-Code des Satelliten (auch als Satelliten-ID oder -Kennung bezeichnet), wie in den GPGSA-Frames angegeben |
| Elevation | Die Winkelhöhe (vertikaler Winkel der Schüsselausrichtung) in Grad, wie in den GPGSV-Frames angegeben |
| Azimuth | Der Azimut (Drehung um die vertikale Achse) in Grad, wie in den GPGSV-Frames angegeben |
| SNR | Das SNR (Signal-Rausch-Verhältnis), oft auch als Signalstärke bezeichnet |

Bitte beachten Sie, dass die Werte so angezeigt werden, wie sie vom Daemon berechnet wurden; ihre Genauigkeit ist möglicherweise nur ungefähr.

Überwachung

| Parameter | GNSS-Überwachung |
|-----------------------|--|
| Administrative status | Aktiviert oder deaktiviert die GNSS-Überwachung |
| Mode | Legt fest, ob der NMEA-Stream oder die GPS-Positionsfixes überwacht werden sollen |
| Max. downtime | Die Zeitspanne ohne gültigen NMEA-Stream oder GPS-Positionsfix, nach der eine Notfallaktion erfolgt. |



| Parameter | GNSS-Überwachung |
|------------------|---|
| Emergency action | <p>Die entsprechende Notfallaktion. Sie können entweder nur den Server neu starten lassen, wodurch auch die GPS-Funktion auf dem Modul neu initialisiert wird, oder in schwierigen Fällen das Modul zurücksetzen.</p> <p>Bitte beachten Sie, dass dies Auswirkungen auf laufende WWAN/SMS-Dienste haben kann.</p> |

5.4. ROUTING

5.4.1. Statisches Routing

In diesem Menü werden alle Routing-Einträge des Systems angezeigt. Sie werden normalerweise durch ein Adresse-Netzmaske-Paar gebildet (dargestellt in IPv4-Dezimalpunktschreibweise), die das Ziel eines Pakets angeben. Die Pakete können entweder an ein Gateway oder an eine Schnittstelle oder an beide adressiert werden. Wenn die Schnittstelle auf ANY eingestellt ist, wählt das System die Routenschnittstelle automatisch aus, abhängig vom am besten passenden Netzwerk, das für eine Schnittstelle konfiguriert ist.

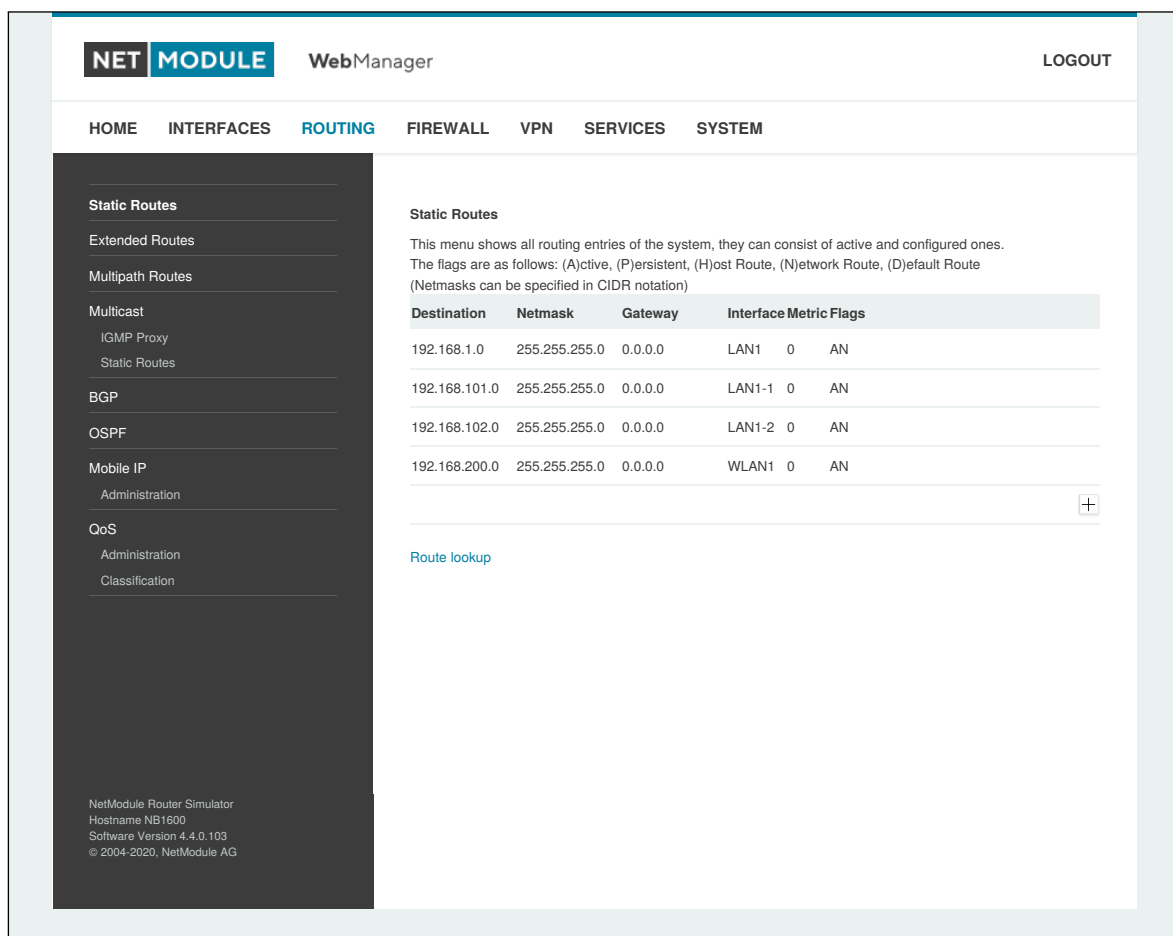


Abbildung 5.23.: Statisches Routing

Im Allgemeinen haben Hostrouten Vorrang vor Netzwerkrouen und Netzwerkrouen Vorrang vor Standardrouen. Zusätzlich kann die Priorität einer Route bestimmt werden; ein Paket geht in die Richtung mit dem niedrigsten Routenmesswert, falls ein Ziel mehreren Routen entspricht.

Netzmasken können in CIDR-Notation angegeben werden (d. h. /24 wird interpretiert als 255.255.255.0).

| Parameter | Konfiguration des statischen Routing |
|-------------|---|
| Destination | Die Zieladresse eines Pakets |
| Netmask | Die Netzmaske, die in Kombination mit dem Ziel das zu adressierende Netzwerk definiert. Ein einzelner Host kann durch eine Netzmaske von 255.255.255.255 angegeben werden; eine Standardroute entspricht 0.0.0.0. |
| Gateway | Der nächste Hop, der als Gateway für dieses Netzwerk fungiert (kann bei Peer-to-Peer-Verbindungen weggelassen werden) |
| Interface | Die Netzwerkschnittstelle, auf der ein Paket übertragen wird, um das dahinterliegende Gateway oder Netzwerk zu erreichen |
| Metric | Routenmesswert der Schnittstelle (Standardwert 0); je höher der Wert, desto ungünstiger die Route |
| Flags | (A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route |

Die Flags haben folgende Bedeutung:

| Flag | Beschreibung |
|------|---|
| A | Die Route wird als aktiv betrachtet; sie kann inaktiv sein, wenn die Schnittstelle für diese Route noch nicht fertig aktiviert ist. |
| P | Die Route ist persistent, d. h. es handelt sich um eine konfigurierte Route; ansonsten entspricht sie einer Schnittstellenroute. |
| H | Die Route ist eine Host-Route; typischerweise ist die Netzmaske auf 255.255.255.255 gesetzt. |
| N | Die Route ist eine Netzwerkroute, bestehend aus einer Adresse und einer Netzmaske, die das zu adressierende Subnetz bildet. |
| D | Die Route ist eine Standard-Route; Adresse und Netzmaske sind auf 0.0.0.0 gesetzt und passen somit zu jedem Paket. |

Tabelle 5.52.: Statische Routen-Flags

5.4.2. Erweitertes Routing

Mit dem erweiterten Routing können richtlinienbasierte Routen genutzt werden; sie haben in der Regel Vorrang vor statischen Routen.

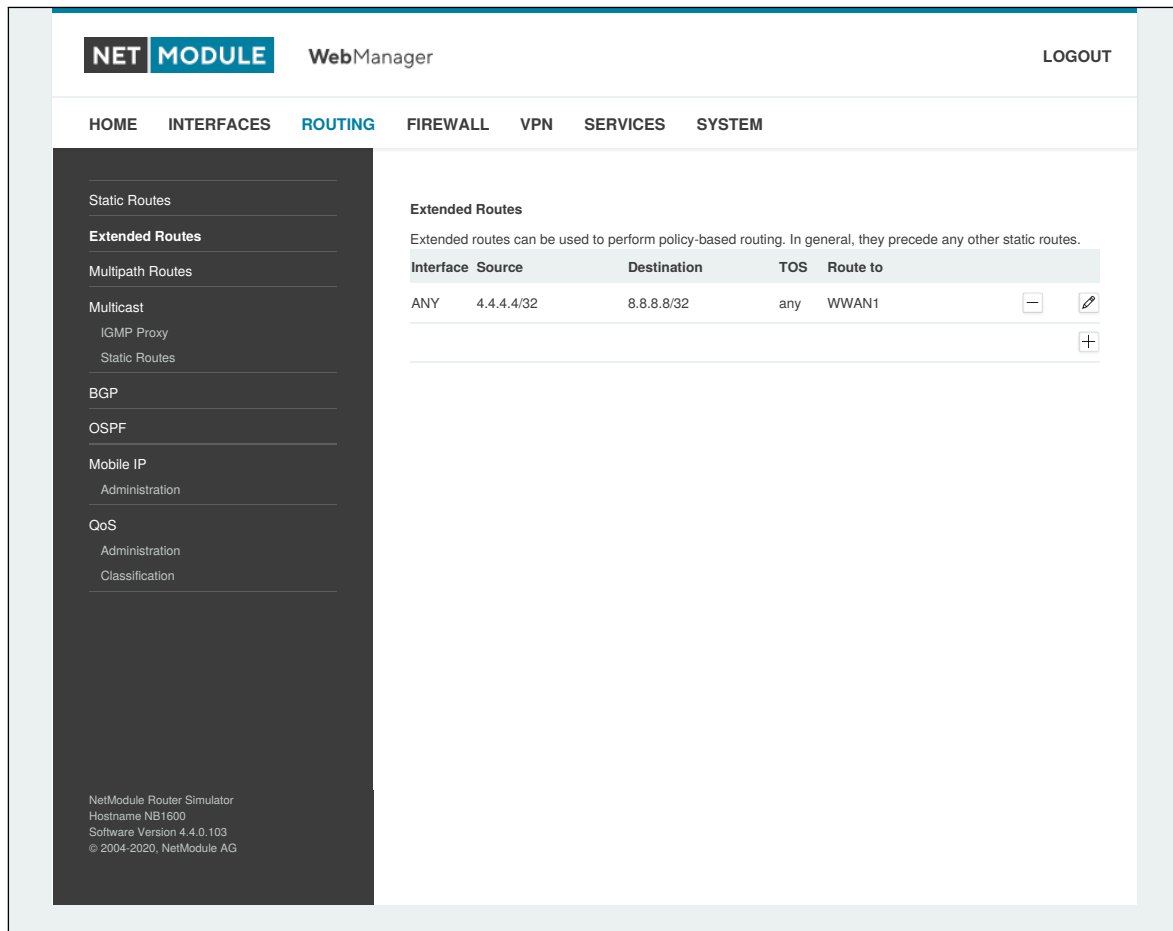


Abbildung 5.24.: Erweitertes Routing

Im Gegensatz zu statischen Routen können erweiterte Routen nicht nur eine Zieladresse/Netzmaske, sondern auch eine Quelladresse/Netzmaske, die eingehenden Schnittstelle und den Dienstyp (TOS) der Pakete enthalten.

| Parameter | Konfiguration des erweiterten Routing |
|---------------------|---|
| Source address | Die Quelladresse eines Pakets |
| Source netmask | Die Quelladressmaske eines Pakets |
| Destination address | Die Zieladresse eines Pakets |
| Destination netmask | Die Zieladressmaske eines Pakets |
| Incoming interface | Die Schnittstelle, über die das Paket in das System gelangt |
| Type of service | Der TOS-Wert im Header des Pakets |
| Route to | Legt die Zielschnittstelle oder das Zielgateway an, an die das Paket weitergeleitet werden soll |



| Parameter | Konfiguration des erweiterten Routing |
|-----------------|---|
| discard if down | Pakete verwerfen, wenn die angegebene Schnittstelle ausgefallen ist |

5.4.3. Multipath-Routing

Multipath-Routen führen eine gewichtete IP-Sitzungsverteilung für bestimmte Subnetze über mehrere Schnittstellen durch.

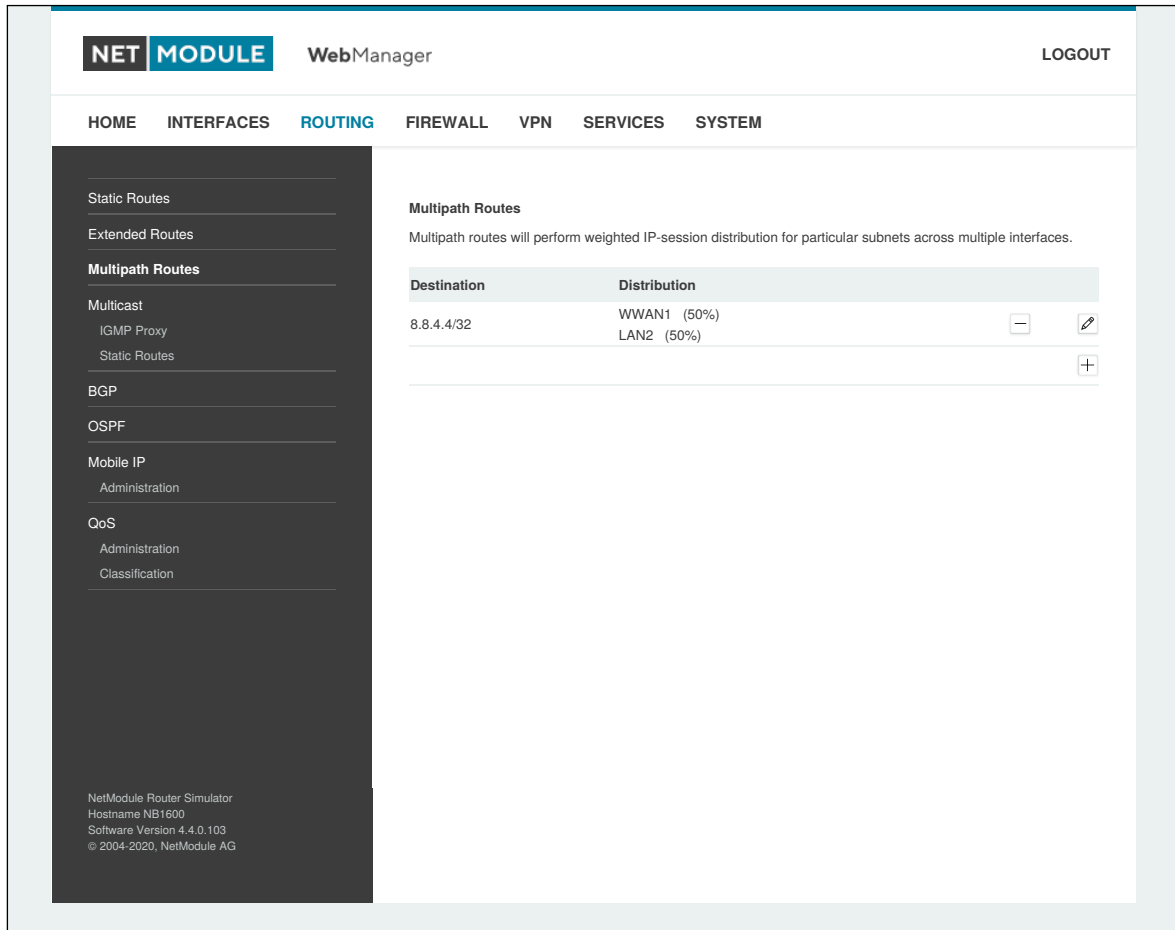


Abbildung 5.25.: Multipath-Routing

Für die Einrichtung des Multipath-Routings müssen mindestens zwei Schnittstellen definiert sein. Weitere Schnittstellen können mit dem Pluszeichen hinzugefügt werden.

| Parameter | Multipath-Routen hinzufügen |
|------------------------|--|
| Target network/netmask | Definiert das Zielnetzwerk, für das Multipath-Routing angewendet werden soll |
| Interface | Wählt die Schnittstelle für einen Pfad aus |
| Weight | Last der konkreten Schnittstelle im Verhältnis zu den anderen |
| NextHop | Überschreibt das Standard-Gateway dieser Schnittstelle |

5.4.4. Multicast-Routing

Multicast ist die Zustellung von IP-Paketen einer Quelle an mehrere Empfänger. Die Empfänger senden Multicast-Nachrichten um sich für eine Multicast-Gruppe anzumelden und erhalten dann die Daten in Form von Multicast-Paketen. Die Multicast-Nachrichten werden also von der Paketsenke and die Paketquelle gesendet.

Multicast-Routing (MCR) dient der gezielten weiterleitung von Multicast-Paketen von einem Netzwerk in ein Anderes.



Achtung:

Da Multicast zur Verteilung von Nachrichten an mehrere Empfänger innerhalb eines einzelnen Netzwerkes eingesetzt wird, ist es üblich, dass Programme, die Testdaten hierfür generieren, die TTL von Multicast-Paketen auf 1 setzen, um zu verhindern, dass diese in andere Netze übermittelt werden. Sollen Pakete von einem Netz in ein anderes geroutet werden, so muss sichergestellt werden, dass die TTL der versendeten Pakete größer als 1 ist.

Multicast-Routing (MCR) kann von einem Daemon konfiguriert und verwaltet werden. Es kann jeweils nur ein MCR-Daemon verwendet werden.

NetModule-Router werden mit zwei verschiedenen MCR-Daemons ausgeliefert; die Auswahl richtet sich nach den vorhandenen Abhängigkeiten im System

| Parameter | Verwaltungsstatus |
|---------------|---|
| IGMP proxy | Weiterleitung von Multicast-Nachrichten, die auf einer bestimmten Schnittstelle dynamisch erkannt werden, an eine andere Schnittstelle |
| static routes | Liste der MCR-Regeln zur Weiterleitung von Nachrichten einer bestimmten Quelle und Gruppe von einer bestimmten Schnittstelle zu einer anderen |
| disabled | Deaktiviert das Routing von Multicast-Nachrichten |

IGMP proxy

IGMP-Proxy, der Multicast-Gruppen auf einer bestimmten Schnittstelle verwalten kann und eingehende Multicast-Pakete in Richtung der Downstream-Schnittstellen verteilen kann, an denen Hosts Multicast-Gruppen beigetreten sind.

| Parameter | Einstellungen für Multicast-Routing |
|--------------------|--|
| Incoming interface | Legt die Upstream-Schnittstelle fest, auf der Hosts Multicast-Gruppen beitreten können und auf der Multicast-Pakete ankommen |
| Sender network | Legt die Netzwerkadresse der Multicast-Quelle fest |
| Sender netmask | Legt die Netzmaske der Multicast-Quelle fest |
| Distribute to | Legt die Downstream-Schnittstellen fest, an die Multicast-Pakete weitergeleitet werden sollen |

Statisches Routing

Leitet Multicast-Pakete je nach Ursprung und Gruppe in unterschiedliche Richtungen, basierend auf vorgegebenen MCR-Regeln:

| Parameter | Einstellungen für statisches Multicast-Routing |
|--------------------|---|
| Group | IP-Adresse der MCR-Gruppe |
| Source | IP der Paketquelle |
| Incoming interface | Schnittstelle zum Netz der Quelle der Multicast-Pakete |
| Outgoing interface | Schnittstelle an die Multicast-Pakete weitergeleitet werden |

5.4.5. BGP

Auf der allgemeinen BGP-Registerkarte (BGP General Settings) können Peerings des NetModule Routers mit anderen Routern eingerichtet werden, die das Border Gateway Protocol (BGP) beherrschen.

| Parameter | Allgemeine BGP-Einstellungen |
|--------------------------------|--|
| Administrative status | Legt fest, ob das BGP-Routingprotokoll aktiv ist |
| AS number | Die Nummer des autonomen Systems (AS), zu dem der NetModule-Router gehört (1-4294967295) |
| Redistribute connected routes | Routen an Netzwerke umverteilen, die direkt mit dem NetModule-Router verbunden sind |
| Redistribute local routes | Umverteilen von Routen entsprechend der eigenen Routing-Tabelle des NetModule-Routers |
| Redistribute OSPF routes | Legt fest, dass über das OSPF-Routingprotokoll erlernte Routen weitergeleitet werden |
| Disable when redundancy backup | Deaktiviert das BGP, wenn der Router durch das VRRP-Redundanzprotokoll in den Slave-Modus versetzt wird |
| Keepalive timer | Die Zeit in Sekunden, nach dem eine Keepalive-Nachricht gesendet wird |
| Holddown timer | Die Zeit in Sekunden, die der Router auf eintreffende BGP-Nachrichten wartet, bis er annimmt, dass der Nachbar ausgefallen ist |

Auf der Registerkarte BGP Neighbors werden alle BGP-Router konfiguriert, zu denen eine Peer-Verbindung aufgebaut werden soll (Nachbarn).

| Parameter | BGP-Nachbarn |
|------------|--|
| IP address | IP-Adresse des Peer-Routers |
| As number | Nummer des Peer-Routers im autonomen System (1-4294967295) |
| Password | Passwort für die Authentifizierung beim Peer-Router. Wenn das Passwort leer ist, wird die Authentifizierung deaktiviert. |
| Multihop | Ermöglicht mehrere Hops zwischen diesem Router und dem Peer-Router, ohne dass der Peer direkt verbunden sein muss. |
| Weight | Gibt die Standardlast für die Nachbarroute an |

Auf der Netzwerk-Registerkarte (BGP Networks) können IP-Netzwerkpräfixe hinzugefügt werden, die über BGP verteilt werden sollen, und zwar zusätzlich zu den Netzwerken, die aus anderen Quellen verteilt werden, wie auf der Registerkarte Allgemein definiert.



| Parameter | BGP-Netzwerke |
|---------------|--|
| Prefix | Präfix des zu verteilenden Netzwerks |
| Prefix length | Länge des Präfixes des zu verteilenden Netzwerks |

5.4.6. OSPF

Im OSPF-Menü können Sie den NetModule-Router zu einem Netzwerk von OSPF-Routern hinzufügen.

| Parameter | Allgemeine OSPF-Einstellungen |
|--------------------------------|---|
| Administrative status | Legt fest, ob das OSPF-Routingprotokoll aktiv ist |
| Router ID | Die Router-ID ist eine eindeutige Identität für den NetModule-Router. Wenn keine Router-ID angegeben ist, wählt das System automatisch die höchste IP-Adresse als Router-ID aus |
| Redistribute connected routes | Routen an Netzwerke umverteilen, die direkt mit dem NetModule-Router verbunden sind |
| Redistribute local routes | Umverteilen von Routen entsprechend der eigenen Routing-Tabelle des NetModule-Routers |
| Redistribute BGP routes | Legt fest, dass über das BGP-Routingprotokoll erlernte Routen weitergeleitet werden |
| Redistribute default route | Verteilt die Standardroute des Routers weiter |
| Disable when redundancy backup | Deaktiviert das OSPF, wenn der Router durch das VRRP-Redundanzprotokoll in den Slave-Modus versetzt wird |

Auf der Schnittstellen-Registerkarte werden OSPF-spezifische Einstellungen für die IP-Schnittstellen des Routers festgelegt. Wenn für eine bestimmte Schnittstelle keine Einstellungen definiert sind, werden die Standardeinstellungen verwendet.

| Parameter | OSPF-Schnittstellen |
|----------------|---|
| Interface | Name der Schnittstelle, für die Einstellungen definiert werden sollen |
| Authentication | Das Authentifizierungsprotokoll, das auf der Schnittstelle zur Authentifizierung von OSPF-Paketen verwendet werden soll |
| Key | Der für die Authentifizierung verwendete Schlüssel |
| Key ID | Die ID des Schlüssels, der für die Authentifizierung verwendet werden soll (1-255) |
| Cost | Die Kosten für das Senden von Paketen über diese Schnittstelle. Wenn die Abgabe fehlt oder gleich 0 ist, werden die OSPF-Standardwerte verwendet. |
| Passive | Legt fest, dass keine OSPF-Pakete auf dieser Schnittstelle versendet werden |

Auf der Netzwerke-Registerkarte wird festgelegt, für welche IP-Netzwerke das OSPF zuständig ist und zu welchem Routing-Bereich sie gehören.



| Parameter | OSPF-Netzwerke |
|---------------|---|
| Prefix | Präfix des Netzwerks |
| Prefix length | Länge des Präfixes |
| Bereich | Routing-Bereich, zu dem diese Schnittstelle gehört (0-65535, 0 bedeutet Backbone) |

5.4.7. Mobile IP

Die Mobile IP (MIP) ermöglicht einen nahtlosen Wechsel zwischen verschiedenen Arten von WAN-Verbindungen (z. B. WWAN/WLAN). Der Befehl `mobile node` ist dabei stets über die gleiche IP-Adresse erreichbar (`home address`), unabhängig von der verwendeten WAN-Verbindung. Effektiv verursacht jeder Wechsel der WAN-Verbindung während des Umschaltvorgangs kurzzeitige Ausfälle, während alle IP-Verbindungen aktiv gehalten werden.

Außerdem unterstützen NetModule-Router auch NAT-Traversal für mobile Knoten, die hinter einer Firewall laufen (und NAT ausführen), wodurch mobile Knoten auch dort von einer Zentrale aus über ihre Home-Adresse erreichbar sind und komplizierte VPNs umgangen werden.

Der `home agent` bewerkstelligt dies durch den Aufbau eines Tunnels (ähnlich einem VPN-Tunnel) zwischen sich selbst und dem `mobile node`. Der Wechsel von WAN-Verbindungen funktioniert so: Der `home agent` wird benachrichtigt, dass die WAN-IP-Adresse (bei MIP als `care-of address` bezeichnet) des `mobile node` sich geändert hat. Der `home agent` verkapselt dann Pakete, die für die Home-Adresse eines `mobile node` bestimmt sind, in einem Umpaket mit der aktuellen `care-of address` des `mobile node` als Zieladresse.

Um Probleme mit Firewalls und privater IP-Adressierung zu vermeiden, wird bei der MIP-Implementierung immer ein Reverse Tunneling eingesetzt, was bedeutet, dass der gesamte Datenverkehr, der von einem `mobile node` gesendet wird, über den Tunnel an den `home agent` weitergeleitet wird statt direkt an den Zielort. Dank dieses Verhaltens kann MIP auch als vereinfachter VPN-Ersatz (ohne Payload-Geheimhaltung) verwendet werden.

Die MIP-Implementierung unterstützt RFC 3344, 5177, 3024 und 3519. Für Anwendungen, die eine große Anzahl von mobilen Knoten erfordern, wurde die Interoperabilität mit der `home agent`-Implementation der Cisco-2900-Serie getestet. Da jedoch NetModule-Router sowohl einen `mobile node` als auch einen `home agent` implementieren, können MIP-Netzwerke mit bis zu 10 mobilen Knoten eingerichtet werden, ohne dass teure Router von Drittanbietern erforderlich sind.

Wenn das MIP als `mobile node` ausgeführt wird, stehen die folgenden Einstellungen zur Verfügung:

| Parameter | Konfiguration von Mobile IP |
|------------------------------|--|
| Primary home agent address | Die Adresse des primären <code>home agent</code> |
| Secondary home agent address | Die Adresse des sekundären <code>home agent</code> . Der mobile Knoten wird versuchen, sich hier anzumelden, wenn der primäre <code>home agent</code> nicht erreichbar ist. |
| Home address | Die permanenten Home-Adresse des <code>mobile node</code> über den der mobile Router jederzeit erreichbar ist. |
| SPI | Der Security Parameter Index (SPI), der den Sicherheitskontext für den mobilen IP-Tunnel zwischen dem <code>mobile node</code> und dem <code>home agent</code> . Auf diese Weise werden mobile Knoten voneinander unterschieden. Daher muss jedem mobilen Knoten ein eindeutiger SPI zugewiesen werden. Dies ist ein 32-Bit-Hexadezimalwert. |



| Parameter | Konfiguration von Mobile IP |
|------------------------|--|
| Authentication type | Der verwendete Authentifizierungsalgorithmus. Dies kann prefix-suffix-md5 (Standard bei MIP) oder hmac-md5 sein. |
| Shared secret | Die Passphrase (Shared Secret), das für die Authentifizierung des <code>mobile node</code> beim <code>home agent</code> genutzt wird. Dies kann ein 128-Bit-Hexadezimalwert oder eine ASCII-Zeichenkette beliebiger Länge sein. |
| Life time | Die Gültigkeitsdauer von Sicherheitszuordnungen in Sekunden. |
| MTU | Die maximale Grösse eines Pakets in Byte, Default Wert 1468 |
| UDP encapsulation | Legt fest, ob die UDP-Kapselung verwendet werden soll. Um NAT-Traversal zu ermöglichen, muss die UDP-Kapselung aktiviert sein. |
| Mobile network address | Gibt optional ein Subnetz an, das an den <code>mobile node</code> weitergeleitet werden soll, Diese Information wird über die Erweiterungen der Netzwerkmobilität (NEMO) an den <code>home agent</code> weitergeleitet. Der <code>home agent</code> kann dann automatisch IP-Routen für das Subnetz über den <code>mobile node</code> hinzufügen. Hinweis: Diese Funktion wird nicht von allen <code>home agent</code> -Implementationen von Drittanbietern unterstützt. |
| Mobile network mask | Die Netzmaske für das optionale geroutete Netzwerk. |

Wenn das MIP als home agent ausgeführt wird, müssen Sie zunächst eine Home-Adresse und eine Netzmaske für den home agent festlegen. Anschließend müssen Sie die Konfiguration für alle mobilen Knoten hinzufügen.

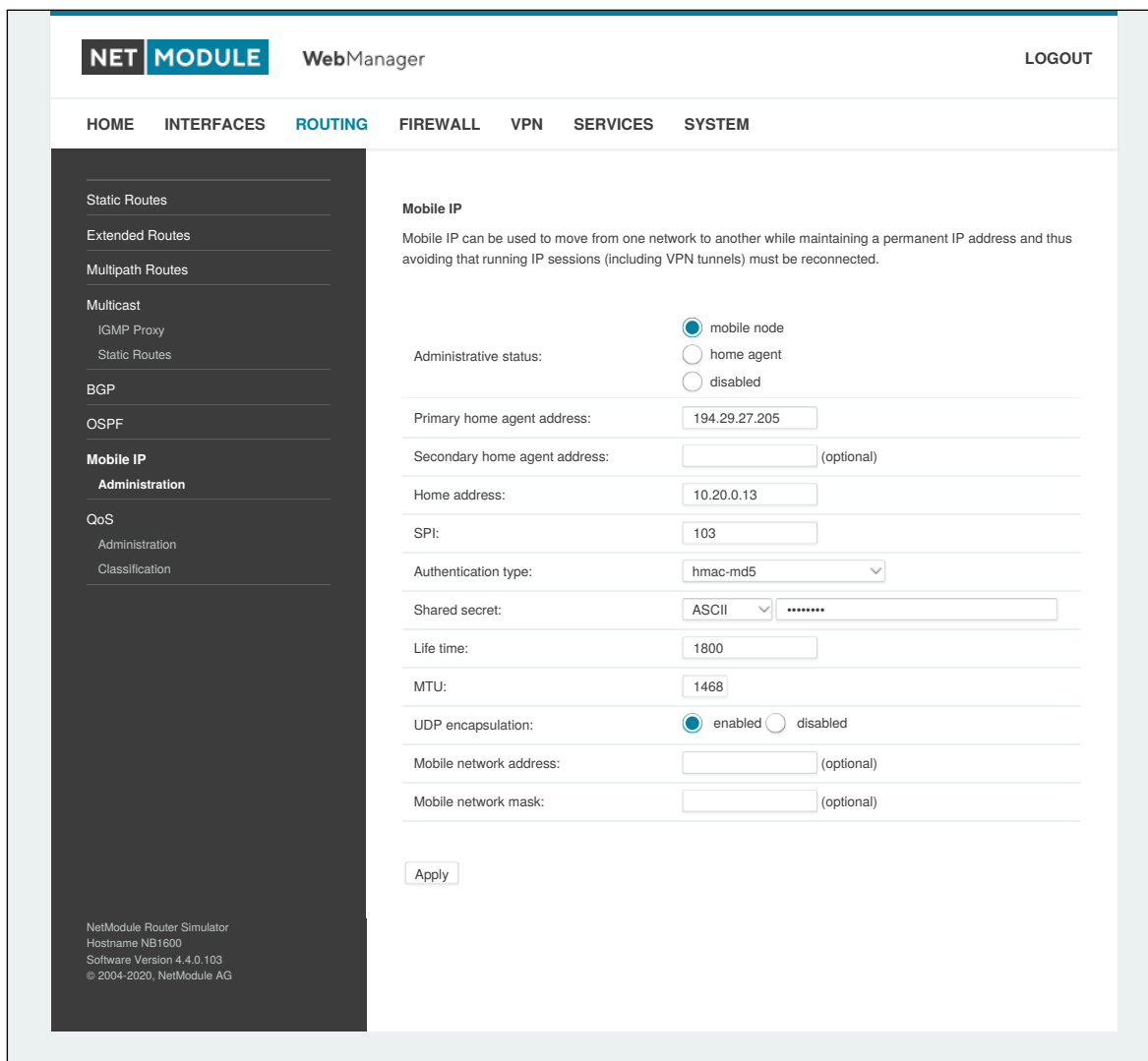


Abbildung 5.26.: Mobile IP

| Parameter | Konfiguration home agent |
|----------------------|--------------------------|
| Home network address | Home network IP Adresse |
| Home network mask | Home network mask |

5.4.8. Quality of Service

NetModule-Router können bestimmte Arten von IP-Datenverkehr priorisieren und ausgestalten (Shaping). Diese ist derzeit auf den Ausgang beschränkt, d. h. es kann nur ausgehender Datenverkehr gestaltet werden.

Die aktuelle QoS-Lösung verwendet SFQ-Klassen (Stochastic Fairness Queuing) in Kombination mit HTB-QDiscs (Hierarchy Token Bucket). Sein Funktionsprinzip lässt sich als Obergrenze des Durchsatzes pro Verbindung und Gestaltung des Datenverkehrs unter Berücksichtigung der angegebenen Warteschlangenprioritäten zusammenfassen. Im Allgemeinen erhält die niedrigste Prioritätsnummer in einer Warteschlange den größten Anteil der verfügbaren Bandbreite.

Bei Bedarf an anderen Klassen- oder qdisc-Algorithmen wenden Sie sich bitte an unser Support-Team, um den besten Ansatz für die betreffende Anwendung zu ermitteln.

QoS-Verwaltung

Auf dieser Seite können Sie QoS aktivieren und deaktivieren.

QoS-Klassifikation

Im Klassifizierungsabschnitt können Sie festlegen, auf welchen WAN-Schnittstellen QoS aktiv sein soll.

| Parameter | QoS-Schnittstellenparameter |
|------------------------|--|
| Interface | Die WAN-Schnittstelle, auf der QoS aktiv sein soll |
| Bandwidth congestion | Die Methode der Bandbreitenüberlastung. Bei der Einstellung <code>auto</code> versucht das System, die Grenzwerte bestmöglich anzuwenden. Es wird jedoch empfohlen, feste Bandbreitenbeschränkungen festzulegen, da diese auch eine Möglichkeit zur Optimierung des QoS-Verhaltens bieten. |
| Downstream bandwidth | Die verfügbare Bandbreite für eingehenden Datenverkehr |
| Upstream bandwidth | Die verfügbare Bandbreite für ausgehenden Datenverkehr |
| IP to ping (primary) | Eine IP, die auf ICMP-Echo-Anfragen antwortet, um die Bandbreite der Verbindung zu ermitteln |
| IP to ping (secondary) | Eine IP, die auf ICMP-Echo-Anfragen antwortet, um die Bandbreite der Verbindung zu ermitteln |

Bei der Definition von Limits sollten Sie zumindest mögliche Bandbreitengrenzen berücksichtigen, da die meisten Shaping- und Queue-Algorithmen nicht korrekt arbeiten, wenn die angegebenen Limits nicht erreicht werden können. Insbesondere WWAN-Schnittstellen, die in einer mobilen Umgebung betrieben werden, leiden oft unter schwankenden Bandbreiten, weshalb eher niedrigere Werte verwendet werden sollten.

Wenn eine Schnittstelle aktiviert wurde, legt das System automatisch die folgenden Warteschlangen an:

| Parameter | QoS-Standardwarteschlangen |
|-----------|--|
| high | Eine Warteschlange mit hoher Priorität, die möglicherweise latenzkritische Dienste (z. B. VoIP) enthält. |
| default | Eine Standardwarteschlange, die alle anderen Dienste verarbeitet |
| low | Eine Warteschlange mit niedriger Priorität, die möglicherweise weniger kritische Dienste enthält, für die Shaping vorgesehen ist |

Es bestehen die folgenden Konfigurationsmöglichkeiten:

| Parameter | QoS Queue Parameters |
|-----------|--|
| Name | Der Name der QoS-Warteschlange |
| Priority | Eine numerische Priorität für die Warteschlange; niedrigere Werte zeigen höhere Prioritäten an |
| Bandwidth | Die maximal mögliche Bandbreite für diese Warteschlange, falls die Gesamtbandbreite aller Warteschlangen die bei den QoS-Schnittstellenparametern eingestellte Upstream-Bandbreite überschreitet |
| Set TOS | Der TOS/DiffServ-Wert, der für abzugleichende Pakete festgelegt werden soll |

Sie können nun die einzelnen Warteschlangen konfigurieren und ihnen beliebige Dienste zuweisen. Es bestehen die folgenden Parameter:

| Parameter | QoS-Dienstparameter |
|------------------|--|
| Interface | Die QoS-Schnittstelle der Warteschlange |
| Queue | Die QoS-Warteschlange, der dieser Dienst zugewiesen werden soll |
| Source | Legt eine Netzwerkadresse und Netzmaske fest, die verwendet wird, um die Quelladresse von Paketen abzugleichen |
| Destination | Legt eine Netzwerkadresse und Netzmaske fest, die verwendet wird, um die Zieladresse von Paketen abzugleichen |
| Protokoll | Legt das Protokoll für Pakete fest, die abgeglichen werden sollen |
| Source Port | Legt den Quellport für Pakete fest, die abgeglichen werden sollen |
| Destination Port | Legt den Zielport für Pakete fest, die abgeglichen werden sollen |
| Type of Service | Legt den TOS/DiffServ-Wert für Pakete fest, die abgeglichen werden sollen |

5.5. FIREWALL

5.5.1. Verwaltung

NetModule-Router verwenden das Linux-Firewall-Framework netfilter/iptables (Näheres siehe <http://www.netfilter.org>), die eine zustandsabhängige Inspektion unterstützt, d. h. gleiche Berechtigungen für vererbte Verbindungen innerhalb einer IP-Sitzung gewährt (z. B. wenn FTP eine Steuer- und Datenverbindung aufbaut).

Auf der Verwaltungsseite können Sie die Firewall aktivieren und deaktivieren. Beim Einschalten kann über eine Tastenkombination ein vordefinierter Satz von Regeln erzeugt werden, die standardmäßig die Administration (über HTTP, HTTPS, SSH oder TELNET) zulassen, aber alle anderen von der WAN-Schnittstelle kommenden Pakete blockieren.

5.5.2. Adress-/Portgruppen

In diesem Menü können Sie Adress- oder Portgruppen bilden, die später für Firewall-Regeln verwendet werden können, um die Anzahl der Regeln zu reduzieren. Wenn auf Adress- oder Portgruppen verwiesen wurde, reicht es für eine Übereinstimmung, wenn eine beliebige der konfigurierten Adress- oder Portgruppen auf das Paket passt.

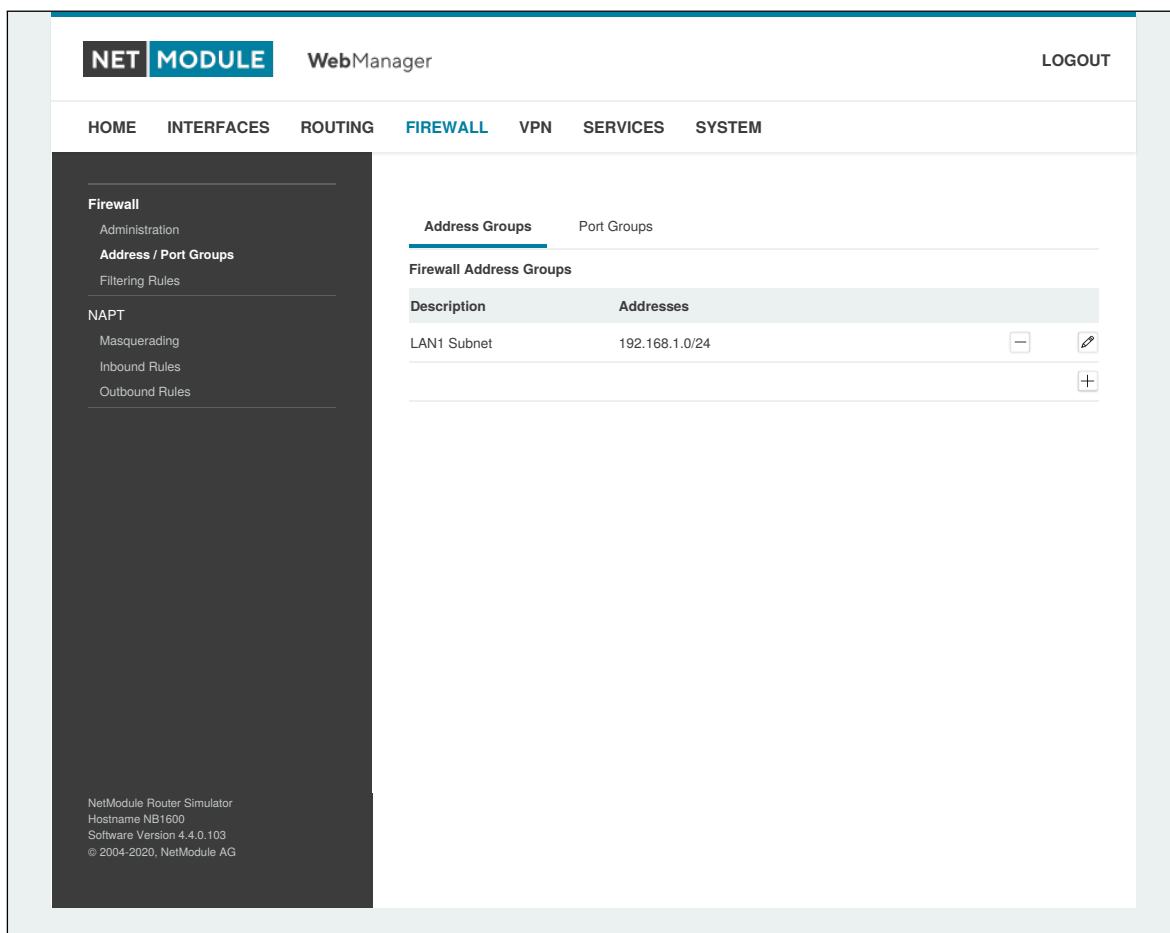


Abbildung 5.27.: Firewall-Gruppen

5.5.3. Regeln

Eine Firewall besteht hauptsächlich aus einer Reihe von Regeln, die festlegen, ob ein bestimmtes Paket den Router passieren darf oder blockiert wird. Die Regeln werden der Reihe nach abgearbeitet, d. h. die Liste wird von oben nach unten durchlaufen, bis eine passende Regel gefunden wird. Pakete, die keiner der konfigurierten Regeln entsprechen, werden zugelassen (ALLOWED).

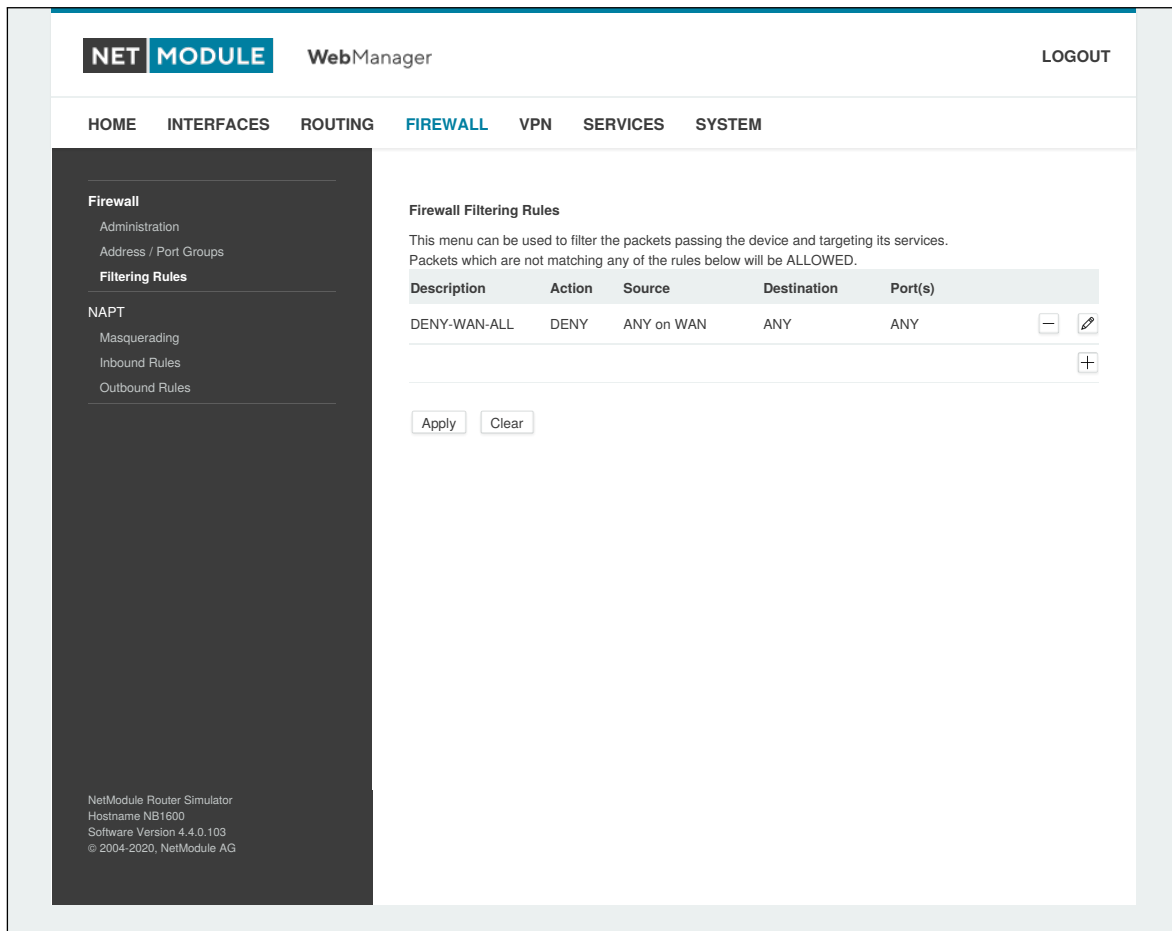


Abbildung 5.28.: Firewall-Regeln

| Parameter | Konfiguration der Firewall-Regeln |
|-------------|--|
| Description | Eine aussagekräftige Beschreibung über den Zweck dieser Regel |
| Action | Legt fest, ob die dieser Regel entsprechenden Pakete blockiert oder zugelassen werden sollen |
| log matches | Legt fest, dass eine Syslog-Meldung ausgegeben wird, wenn die Regel passt |
| Source | Die Quelladresse der übereinstimmenden Pakete; kann beliebig sein oder als Adresse/Netzwerk angegeben werden. Die Auswahl nach Quell-MAC-Adressen ist ebenfalls möglich. |



| Parameter | Konfiguration der Firewall-Regeln |
|--------------------|--|
| Destination | Die Zieladresse der übereinstimmenden Pakete, kann ANY, LOCAL (an das System selbst adressiert) oder durch Adresse/Netzwerk angegeben sein |
| Incoming interface | Die Schnittstelle, an der passende Pakete empfangen werden |
| Outgoing interface | Die Schnittstelle, an der passende Pakete gesendet werden |
| Protocol | Das verwendete IP-Protokoll der passenden Pakete (UDP, TCP, ICMP, ESP, GRE oder OSPF) |

Auf der Statistik Seite können Sie prüfen, ob Pakete angekommen sind, auf die eine oder mehrere Regeln gepasst haben. Sie ist eine praktische Möglichkeit zur Fehlersuche in der Firewall.

5.5.4. NAPT

Auf dieser Seite können Sie die Netzwerkadress- und Portübersetzung (network and port translation, NAPT) für Pakete konfigurieren, die durch das System transportiert werden. NAPT ändert dabei IP-Adressen oder/und TCP/UDP-Ports in passenden IP-Paketen. Diese Verbindungen werden verfolgt, und auch die zurückkehrenden Pakete einer IP-Sitzung werden automatisch angepasst.

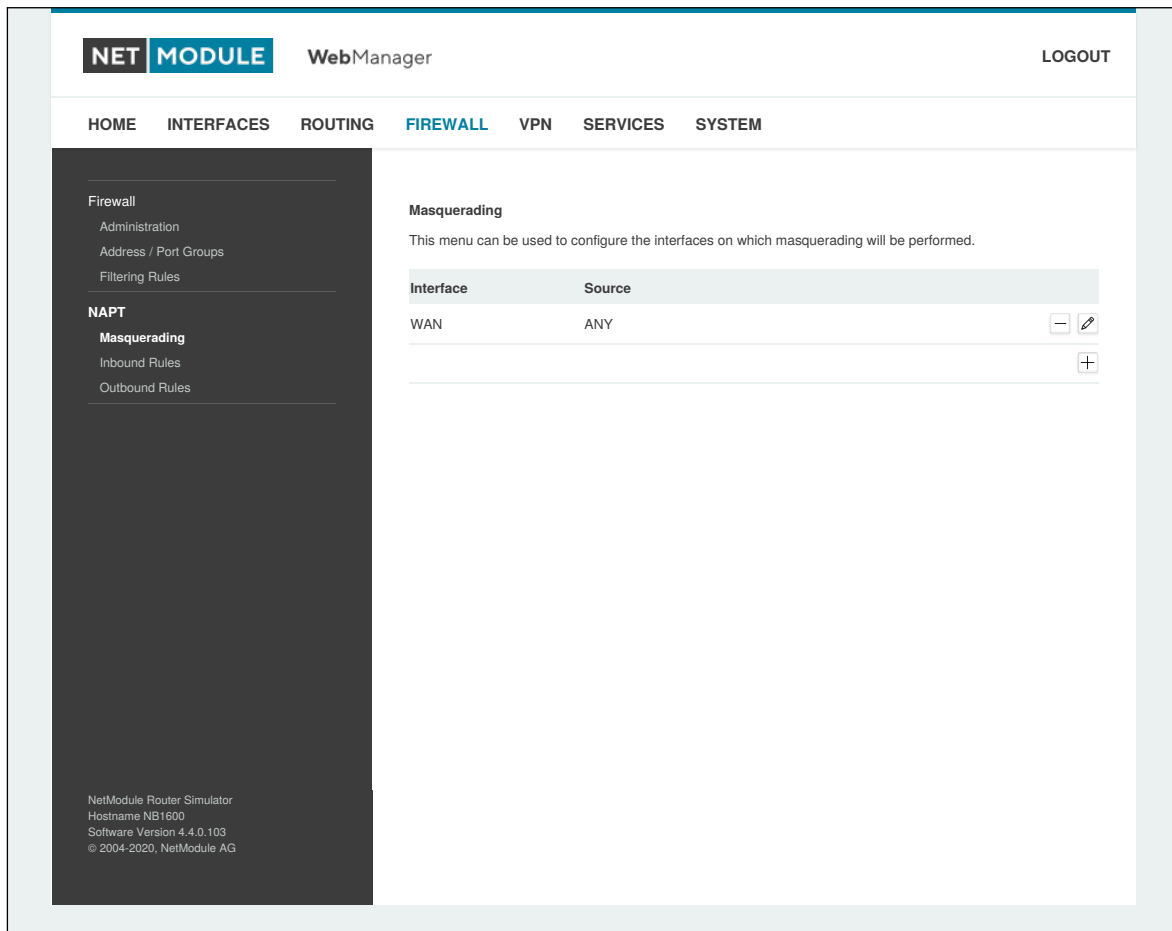


Abbildung 5.29.: Maskierung (Masquerading)

Auf der Verwaltungsseite können Sie die Schnittstellen angeben, auf denen die Maskierung durchgeführt werden soll. NAPT verwendet dabei die Adresse der gewählten Schnittstelle und wählt einen zufälligen Quellport für ausgehende Verbindungen.

NAPT ermöglicht so die Kommunikation zwischen Hosts von einem privaten lokalen Netzwerk zu Hosts im öffentlichen Netzwerk.

| Parameter | Masquerading-Regeln |
|----------------|---|
| Interface | Die Schnittstelle (Ausgang), auf der Verbindungen maskiert werden |
| Source address | Die Quelladresse oder das Netzwerk, von dem passende Pakete maskiert werden |

| Parameter | Masquerading-Regeln |
|----------------|--|
| Source netmask | Die Quellnetzmaske des Netzwerks, aus dem passende Pakete mas-kiert werden |

NAPT-Regeln für eingehende Pakete

Mit Regeln für eingehende Pakete können den Zielbereich von IP-Paketen ändern und z. B. einen Dienst oder Port an einen internen Host weiterleiten. So können Sie diesen Dienst verfügbar machen und über das Internet verfügbar machen. Sie können auch ein 1:1-NAPT-Mapping für einen einzelnen Host einrichten, indem Sie zusätzliche NAPT-Regeln für abgehende Pakete

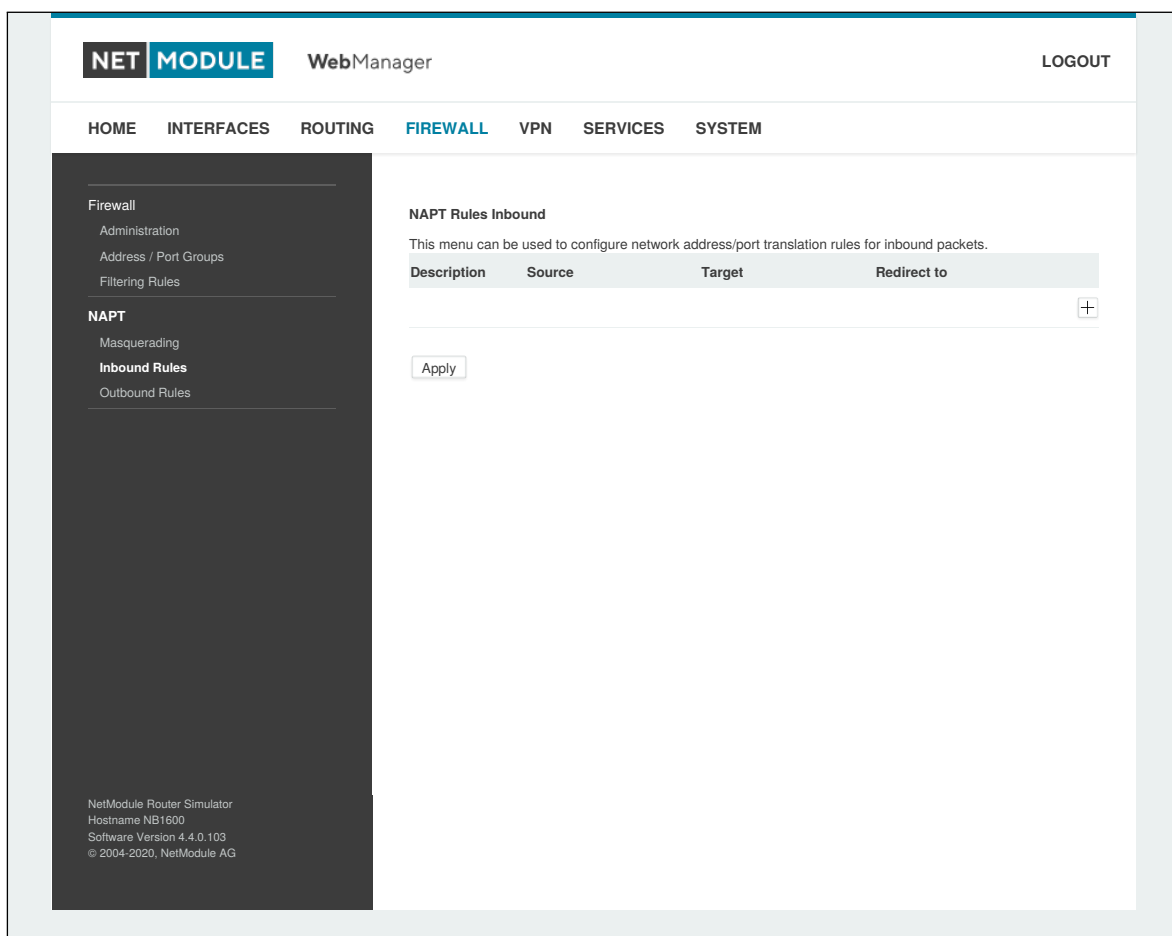


Abbildung 5.30.: NAPT-Regeln für eingehende Pakete

Die Regeln werden der Reihe nach abgearbeitet; die Liste wird von oben nach unten durchlaufen, bis eine passende Regel gefunden wird. Wenn keine passende Regel gefunden wird, wird das Paket unverändert zugelassen.

| Parameter | NAPT-Regeln für eingehende Pakete |
|-------------|---|
| Description | Eine aussagekräftige Beschreibung über den Zweck dieser Regel |

| Parameter | NAPT-Regeln für eingehende Pakete |
|--------------------|---|
| Map | Kontext für diese Regel: Host, Netzwerk oder Port-Bereich - siehe Tabelle unten |
| Incoming interface | Die Schnittstelle, an der passende Pakete empfangen werden |
| Source | Die Quelladresse oder das Netzwerk, von dem passende Pakete maskiert werden |
| Target address | Die Zieladresse der passenden Pakete (optional) |
| Protocol | Das verwendete Protokoll der passenden Pakete |
| Ports | Der verwendete UDP/TCP-Port der passenden Pakete |
| Redirect to | Die Adresse, an die passende Pakete umgeleitet werden sollen |
| Redirect port | Der Port, an den passende Pakete umgeleitet werden sollen |

Wählen Sie den Zuordnungskontext entsprechend den herrschenden Anforderungen aus:

| Parameter | Zuordnungskontext |
|------------|---|
| host | Zieladresse und Port für einen bestimmten Host umschreiben (z. B. 10.0.0.1:8080 → 192.168.1.100:80) |
| network | Zieladresse für ein vollständiges Netzwerk umschreiben (z. B. 10.0.0.0/24 → 192.168.1.0/24) |
| port range | Zieladresse und Port in Abhängigkeit vom Eingangsport umschreiben (z. B. 10.0.0.1:22000-22000 → 192.168.1.0:22). Es gibt keine entsprechende Portbereichsübersetzung in Regeln für abgehende Pakete. Verwenden Sie dort das netzwerkbasierte Mapping. |

NAPT-Regeln für abgehende Pakete

NAPT-Regeln für abgehende Pakete ändern den Quellbereich von IP-Paketen und können verwendet werden, um 1:1-NAPT-Mappings zu erreichen, aber auch, um Pakete an einen bestimmten Dienst umzuleiten.

| Parameter | NAPT-Regeln für abgehende Pakete |
|------------------------|---|
| Description | Eine aussagekräftige Beschreibung über den Zweck dieser Regel |
| Outgoing interface | Die Schnittstelle, von der passende Pakete gesendet werden |
| Target | Die Zieladresse oder das Netzwerk, für das die passenden Pakete bestimmt sind |
| Source address | Die Quelladresse der passenden Pakete (optional) |
| Protocol | Das verwendete Protokoll der passenden Pakete |
| Ports | Der verwendete UDP/TCP-Port der passenden Pakete |
| Rewrite source address | Die Adresse, zu der die Quelladresse passender Pakete umgeschrieben werden soll |



| Parameter | NAPT-Regeln für abgehende Pakete |
|---------------------|---|
| Rewrite source port | Der Port, zu der der Quellport passender Pakete umgeschrieben werden soll |

5.6. VPN

5.6.1. OpenVPN

Verwaltung von OpenVPN

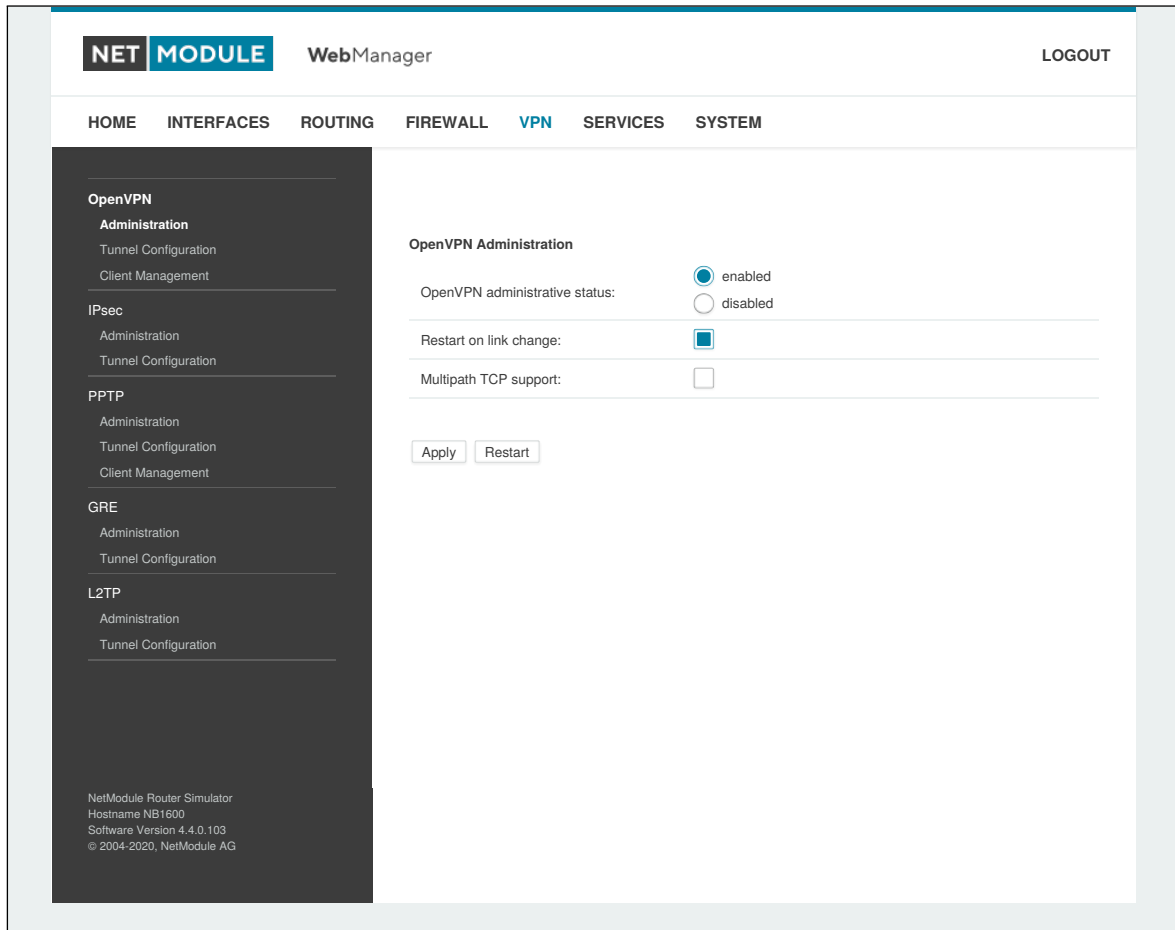


Abbildung 5.31.: Verwaltung von OpenVPN

| Parameter | Verwaltung von OpenVPN |
|------------------------|--|
| Administrative status | Legt fest, ob OpenVPN aktiv ist |
| Restart on link change | Legt fest, ob der OpenVPN-Dämon bei einer Änderung der WAN-Verbindung neu gestartet wird |
| Multipath TCP support | Aktiviert die Multipath-TCP-Unterstützung |

Tunnel-Konfiguration

NetModule-Router unterstützen einen Server-Tunnel und bis zu vier Client-Tunnel. Sie können die Tunnelparameter entweder in der Standardkonfiguration angeben oder eine zuvor erstellte Expertendatei hochladen. In Kapitel 5.6.1 erfahren Sie mehr über das Verwalten von Clients und das Erstellen der Dateien.

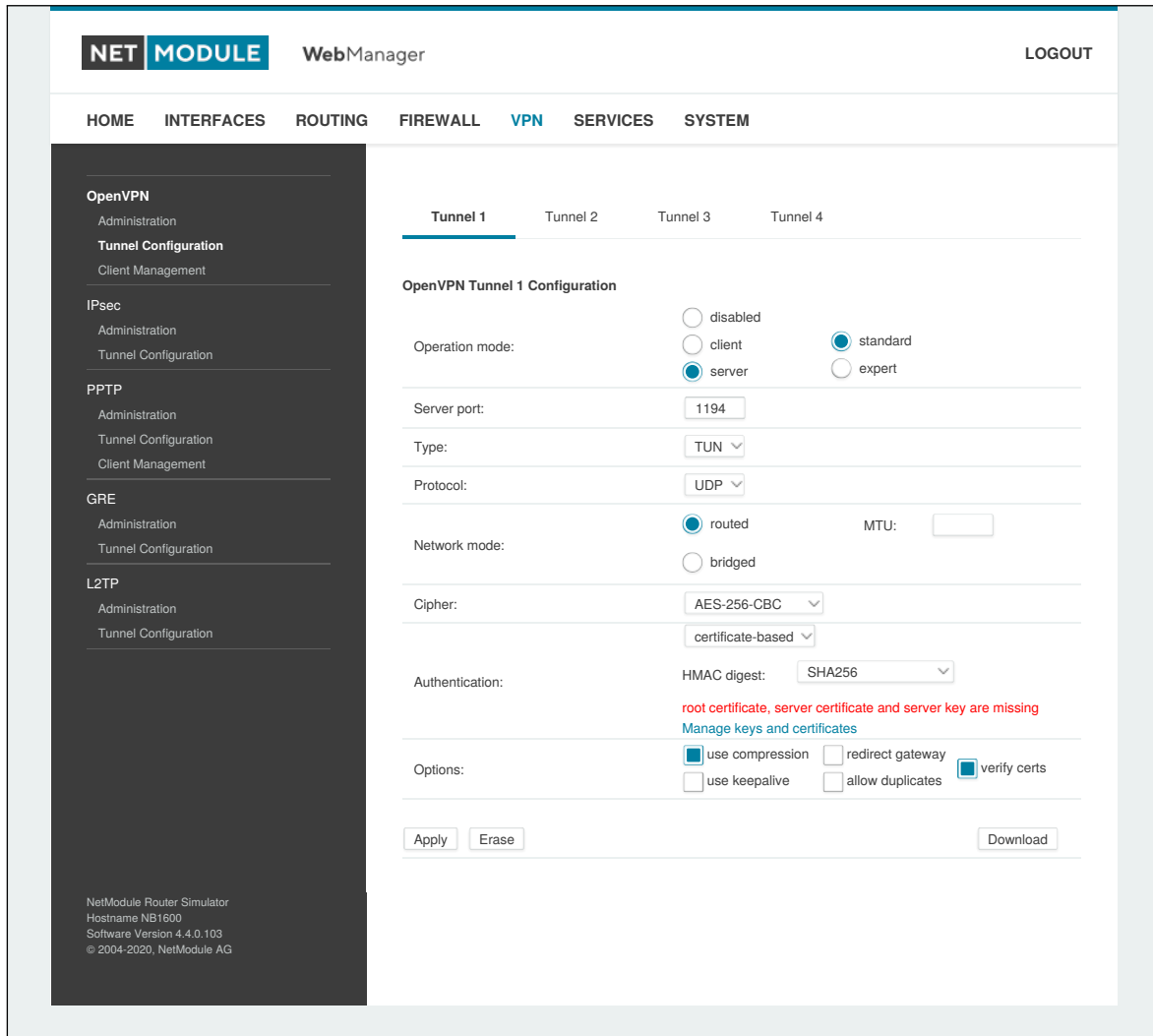


Abbildung 5.32.: Konfiguration von OpenVPN

| Parameter | Konfiguration von OpenVPN |
|----------------|---|
| Operation mode | Legt fest, ob für diesen Tunnel der Client- oder der Server-Modus verwendet wird, sowie ob der Tunnel normal konfiguriert oder ob eine Expertendatei verwendet werden soll. |

Wenn der Tunnel im Clientmodus betrieben wird, stehen die folgenden Einstellungen zur Verfügung:

| Parameter | OpenVPN-Clientkonfiguration |
|----------------|---|
| Peer selection | Legt fest, wie die Gegenstelle ausgewählt werden soll. Sie können einen einzelnen Server konfigurieren, aber auch mehrere, die dann bei Ausfällen entweder nacheinander ("Failover") oder nach Last ("Load Balancing") ausgewählt werden können |
| Server | Die Adresse oder der Hostname des Remote-Servers |
| Port | Der Port des Remote-Servers (standardmäßig 1194) |

Mit den folgenden Einstellungen können Sie einen Tunnel konfigurieren (Client- und Server-Modus):

| Parameter | Konfiguration von OpenVPN |
|----------------|--|
| Interface type | Der Gerätetyp für diesen Tunnel: entweder TUN (typischerweise für geroutete Verbindungen verwendet) oder TAP (erforderlich für gebückte Netzwerke) |
| Protocol | Das Tunnelprotokoll, das für diese Transportverbindung verwendet werden soll |
| Network mode | Legt fest, wie die Pakete weitergeleitet werden sollen, die entweder geroutet oder von/zu einer bestimmten LAN-Schnittstelle gebückt werden können. Bei Bedarf können Sie auch die maximale Größe einer Übertragungseinheit für die Tunnelschnittstelle angeben. |
| MTU | Maximale Größe einer Übertragungseinheit für die Tunnelschnittstelle |
| Encryption | Der geforderte Verschlüsselungsalgorithmus |
| Digest | Der zur Authentifizierung verwendete Digest-Algorithmus |

Die Authentifizierung kann auf folgende Arten erfolgen:

| Parameter | OpenVPN-Authentifizierung |
|-------------------|--|
| certificate-based | Zertifikate und Schlüssel für die Authentifizierung des Tunnels. Achten Sie darauf, dass die richtigen Schlüssel/Zertifikate hochgeladen bzw. erzeugt wurden (siehe Kapitel 5.8.8). |
| credential-based | Zur Authentifizierung werden Benutzername und Passwort verwendet. |
| both | Für den Zugang zum Tunnel werden Zertifikate und Anmeldeinformationen benötigt. |
| none | Tunnel erfordert keine Authentifizierung (nicht empfohlen) |

Es stehen die folgenden weiteren Optionen zur Verfügung:

| Parameter | OpenVPN-Optionen |
|------------------|---|
| use compression | Legt fest, ob die LZO-Paketkomprimierung aktiv ist |
| use keepalive | Kann verwendet werden, um ein periodisches Keepalive-Paket zu senden, damit der Tunnel trotz Inaktivität aufrechterhalten bleibt |
| redirect gateway | Durch die Umleitung des Gateways werden alle Pakete an den VPN-Tunnel weitergeleitet. Sie müssen sicherstellen, dass wesentliche Dienste (z. B. DNS- oder NTP-Server) am Netzwerk hinter dem Tunnel erreichbar sind. Im Zweifelsfall legen Sie eine zusätzliche statische Route an, die auf die richtige Schnittstelle zeigt. |
| allow duplicates | Ermöglicht mehreren Clients mit demselben Namen die gleichzeitige Verbindung (nur im Server-Modus). |
| verify certs | Überprüft das Zertifikat der Gegenstelle anhand der lokalen CRL (nur im Server-Modus). |
| negotiate DNS | Legt fest, ob das System die Nameserver nutzt, die über den Tunnel ausgehandelt wurden. |

OpenVPN-Expertenkonfiguration (Client)

Die Expertenkonfiguration bietet eine unkomplizierte Möglichkeit, einen Tunnel zu konfigurieren. Hierzu wird ein ZIP-Paket hochgeladen, das die erforderlichen Konfigurations- und optional auch die Schlüssel-/Zertifikatdateien enthält. Ein Client-Tunnel erfordert normalerweise die folgenden Dateien:

| Parameter | Client-Expertendateien |
|-------------|---|
| client.conf | OpenVPN-Konfigurationsdatei. Verfügbare Parameter siehe http://www.openvpn.net |
| ca.crt | Root-Zertifizierungsstellendatei |
| client.crt | Zertifikatsdatei |
| client.key | Datei mit privatem Schlüssel |
| client.p12 | PKCS#12-Datei |
| ta.key | Datei mit dem TLS-Authentifizierungsschlüssel |

Sie können zwar beliebige Dateinamen vergeben, das Suffix der Konfigurationsdatei muss jedoch `.conf` lauten, und alle Dateien, auf die in der Konfigurationsdatei verwiesen wird, müssen korrekte relative Pfadnamen besitzen.

OpenVPN-Expertenkonfiguration (Server)

Ein Server-Tunnel erfordert normalerweise die folgenden Dateien:

| Parameter | Server-Expertendateien |
|-------------|--|
| server.conf | OpenVPN-Konfigurationsdatei |
| ca.crt | Root-Zertifizierungsstellendatei |
| server.crt | Zertifikatsdatei |
| server.key | Datei mit privatem Schlüssel |
| dh1024.pem | Diffie-Hellman-Parameterdatei |
| ccd | Ein Verzeichnis mit clientspezifischen Konfigurationsdateien |

Hinweis: Ein Zertifikat wird erst ab dem Beginn des Gültigkeitszeitraums gültig. Daher muss vor dem Erstellen von Zertifikaten und dem Aufbau einer Tunnelverbindung eine genaue Systemzeit eingestellt werden. Stellen Sie sicher, dass alle NTP-Server erreichbar sind. Für die Verwendung von Hostnamen ist außerdem ein funktionierender DNS-Server erforderlich.

Client-Verwaltung

Sobald der OpenVPN-Server-Tunnel erfolgreich eingerichtet ist, können Sie Clients, die sich mit Ihrem Dienst verbinden, verwalten und aktivieren. Die aktuell verbundenen Clients werden auf dieser Seite angezeigt, einschließlich der Verbindungszeit und der IP-Adresse. Sie können angeschlossene Clients durch Deaktivieren trennen.

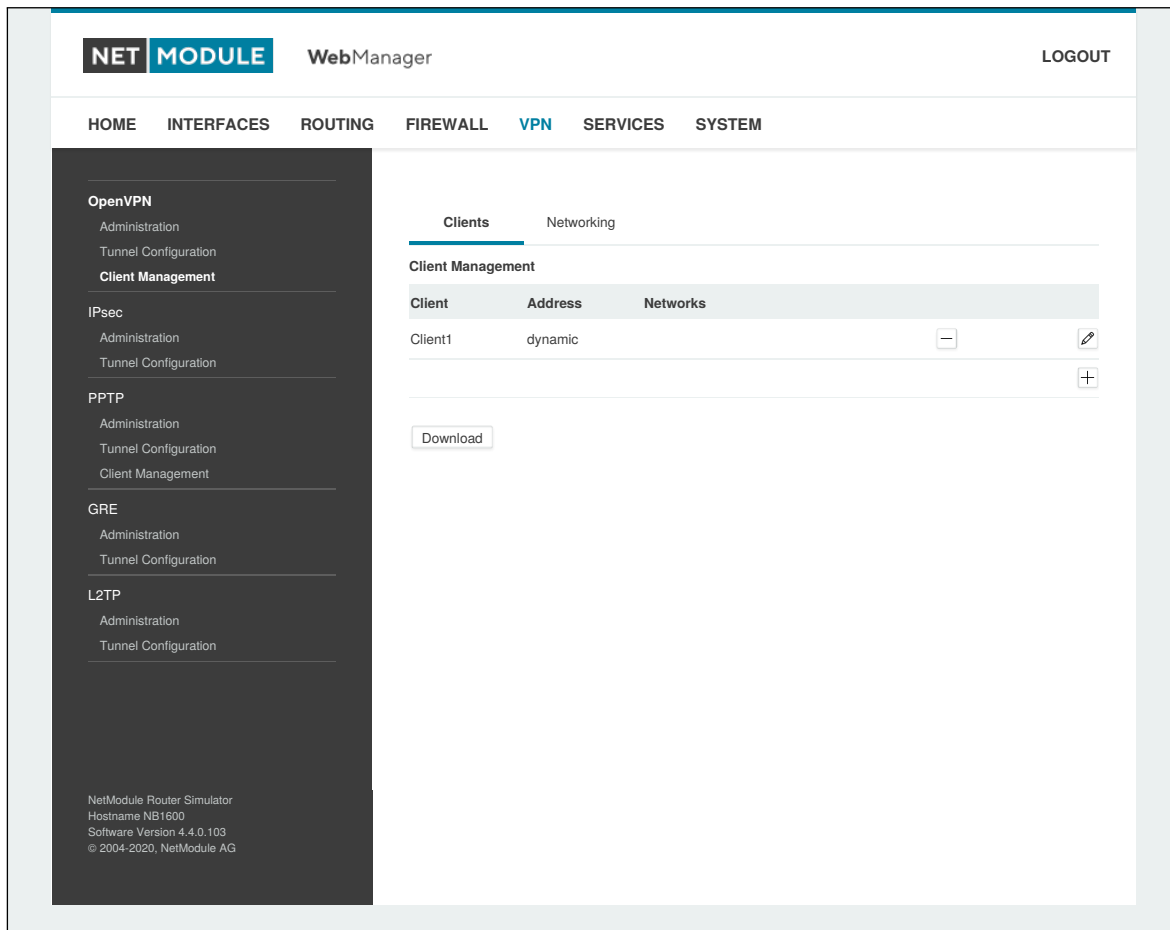


Abbildung 5.33.: OpenVPN-Client-Verwaltung

Im Networking-Abschnitt können Sie für jeden Client eine feste Adresse für den Tunnelendpunkt vergeben. Wenn Sie für einen bestimmten Client eine feste Adresse verwenden wollen, müssen Sie auch für die anderen Clients feste Adressen verwenden.

Sie können das Netzwerk hinter den Clients sowie die Routen angeben, die an jeden Client übergeben werden. Dies kann für Routing-Zwecke nützlich sein, z. B. für den Fall, dass Sie den Verkehr für bestimmte Netzwerke zum Server umleiten möchten. Ein Routing zwischen den Clients ist im Allgemeinen nicht zulässig; Sie können es jedoch bei Bedarf aktivieren.

Schließlich können Sie alle Expertendateien für aktivierte Clients erstellen und herunterladen und damit die Clients einfach bestücken.

Beim Betrieb im Server-Modus mit Zertifikaten ist es möglich, einen bestimmten Client mit einem möglicherweise gestohlenen Client-Zertifikat zu sperren (siehe [5.8.8](#)).

5.6.2. IPsec

IPsec ist eine Protokoll-Suite zur Absicherung der IP-Kommunikation, wobei jedes Paket einer Sitzung authentifiziert und verschlüsselt wird und damit ein sicheres virtuelles privates Netzwerk entsteht.

IPsec enthält verschiedene kryptografische Protokolle und Chiffren für den Schlüsselaustausch und die Datenverschlüsselung und gilt unter Sicherheitsgesichtspunkten als eines der stärksten VPN-Technologien. IPsec verwendet die folgenden Mechanismen:

| Mechanismus | Beschreibung |
|-------------|---|
| AH | Authentication Headers (AH) bieten verbindungslose Integrität, Authentifizierung der Datenquelle IP-Datagramme und gewährleisten Schutz vor Replay-Angriffen. |
| ESP | Encapsulating Security Payloads (ESP) bieten Vertraulichkeit, Authentifizierung der Datenquelle, verbindungslose Integrität, einen Anti-Replay-Dienst und begrenzte Vertraulichkeit des Datenverkehrs. |
| SA | Security Associations (SA) bieten einen sicheren Kanal und ein Bündel von Algorithmen, die die notwendigen Parameter für den Betrieb der AH- und/oder ESP-Operationen bereitstellen. Das ISAKMP (Internet Security Association Key Management Protocol) ist ein Framework für den authentifizierten Schlüsselaustausch. |

Das Aushandeln von Schlüsseln für die Verschlüsselung und Authentifizierung erfolgt im Allgemeinen über das Internet Key Exchange-Protokoll (IKE), das aus zwei Phasen besteht:

| Phase | Beschreibung |
|-------------|--|
| IKE phase 1 | IKE authentifiziert in dieser Phase die Gegenstelle für eine sichere ISAKMP-Zuordnung. Dies kann in den Modi <code>main</code> oder <code>aggressive</code> erfolgen. Im Modus <code>main</code> arbeitet das Protokoll mit dem Diffie-Hellman-Schlüsselaustausch und die Authentifizierung wird immer mit dem ausgehandelten Schlüssel verschlüsselt. Im Modus <code>aggressive</code> werden nur Hashes des Pre-Shared Key verwendet. Dieser Modus stellt daher einen weniger sicheren Mechanismus dar und sollte generell vermieden werden sollte, da er anfällig für Wörterbuchangriffe ist. |
| IKE phase 2 | IKE handelt abschließend IPsec-SA-Parameter und -Schlüssel aus (SA: Security Association) und richtet in den Gegenstellen passende IPsec-SAs ein, die später für AH/ESP benötigt werden. |

Verwaltung

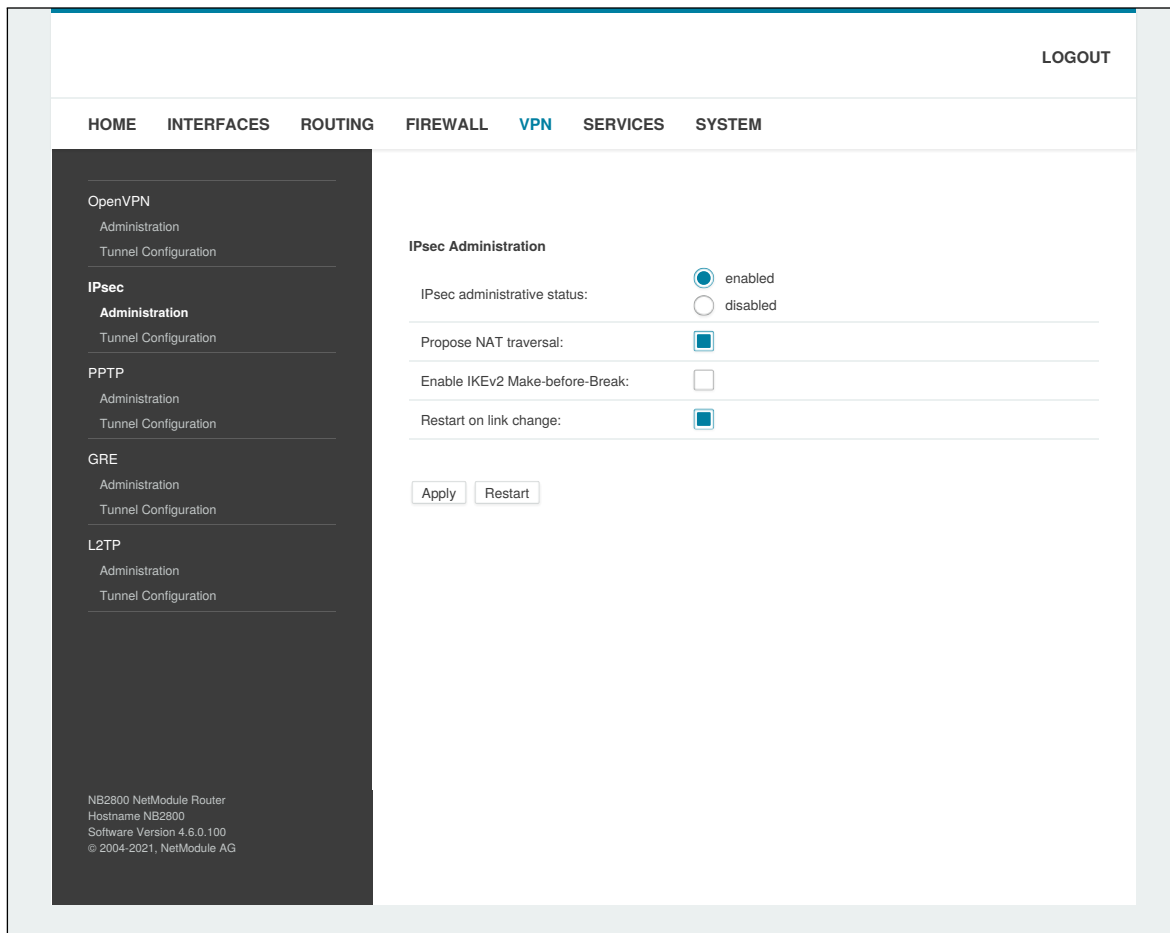


Abbildung 5.34.: IPsec-Verwaltung

Auf dieser Seite können Sie IPsec aktivieren/deaktivieren. Sie können zusätzlich auch angeben, ob die Optionen NAT-Traversal und IKEv2 Make-before-Break verwendet werden sollen.

NAT-Traversal wird hauptsächlich für Verbindungen verwendet, die einen Transportweg durchlaufen, bei dem ein Router die IP-Adresse/Port von Paketen verändert. Es kapselt Pakete in UDP und bedingt daher einen gewissen Overhead, der beim Ausführen über kleine MTU-Schnittstellen berücksichtigt werden muss.

Hinweis: Bei Ausführung von NAT-Traversal verwendet IKE den UDP-Port 4500 und nicht 500. Dies muss bei der Einrichtung von Firewall-Regeln berücksichtigt werden.

Make-before-Break ist eine IKEv2 Option welche die in regelmäßigen Abständen notwendige Reauthifizierung optimiert, indem erst eine überlappende SA erzeugt wird (=make), bevor die aktuell verwendete SA abgebaut wird (=break). Auf diese Weise wird die Unterbrechung des Datenstroms minimiert. Um diese Option verwenden zu können müssen beide Seiten überlappende SAs unterstützen.

Konfiguration

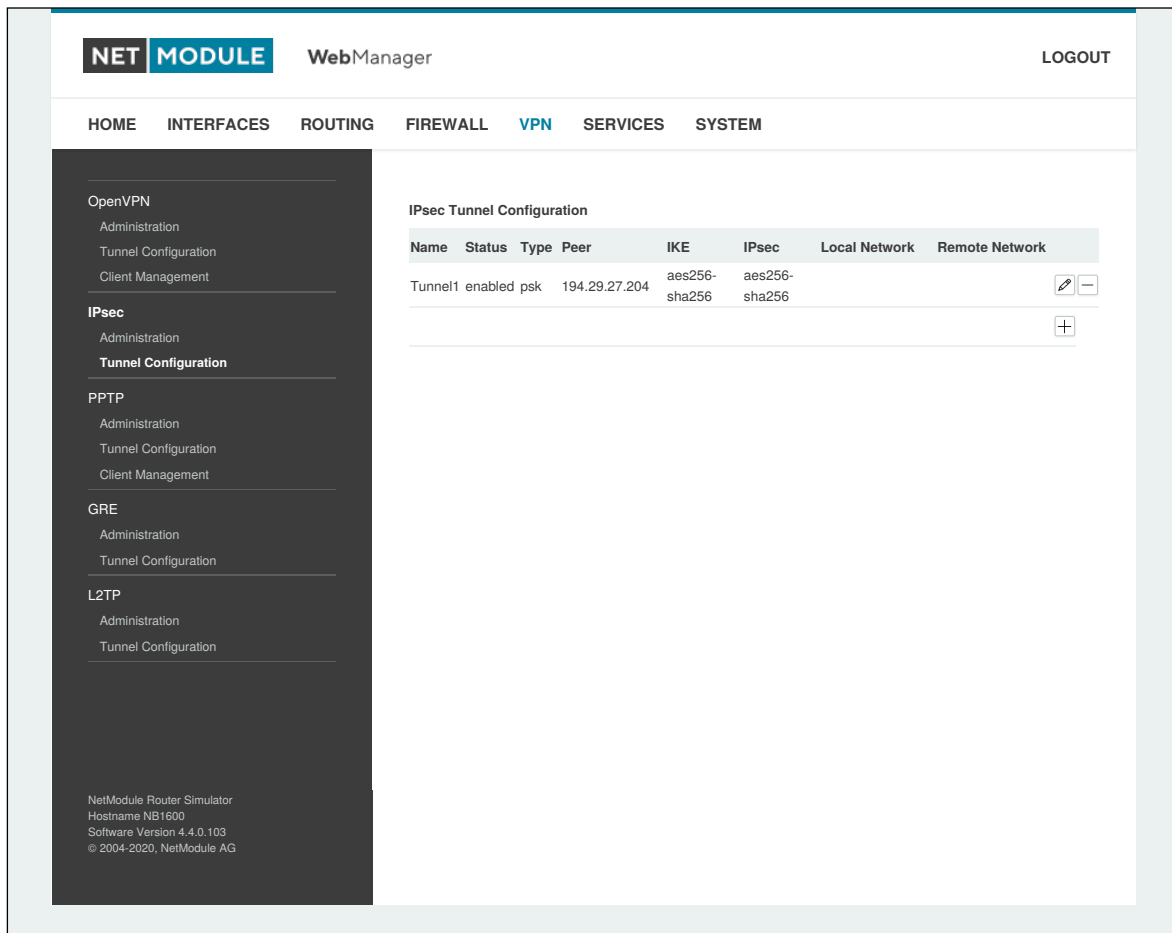


Abbildung 5.35.: IPsec-Konfiguration

Allgemeines

Zum Einrichten des Tunnels müssen Sie zunächst die folgenden Parameter konfigurieren:

| Parameter | Allgemeine IPsec-Einstellungen |
|-------------|---|
| Local IP | Die IP-Adresse der lokalen Schnittstelle. 0.0.0.0 lässt eine beliebige IP-Adresse zu. |
| Remote peer | IP-Adresse oder Hostname der Remote-IPsec-Gegenstelle. 0.0.0.0 macht die Nutzung als Responder für Road-Warrior-Clients möglich. |
| DPD Status | Legt fest, ob ausgefallene Gegenstellen erkannt werden sollen (Dead Peer Detection, siehe RFC 3706). DPD erkennt alle unterbrochenen IPsec-Verbindungen, insbesondere den ISAKMP-Tunnel, und aktualisiert die entsprechenden SAs (Security Associations) und SPIs (Security Payload Identifier) für einen schnelleren Wiederaufbau des Tunnels. |

| Parameter | Allgemeine IPsec-Einstellungen |
|-------------------|--|
| Detection cycle | Die Zeit (in Sekunden) zwischen DPD-Keepalive-Paketen, die für diese Verbindung gesendet werden (Standard 30 Sekunden) |
| Failure threshold | Anzahl der unbeantworteten DPD-Anfragen, nach der die IPsec-Gegenstelle als ausgefallen gilt (der Router versucht dann automatisch, eine unterbrochene Verbindung wieder aufzubauen) |
| Action | Die Aktion, die ausgeführt werden soll, wenn eine Gegenstelle die Verbindung trennt. Mögliche Aktionen sind das Löschen, Halten oder der Neustart der Gegenstelle. |

IKE-Authentifizierung

NetModule-Router unterstützen die IKE-Authentifizierung über Pre-Shared Keys (PSK) oder Zertifikate innerhalb einer Public-Key-Infrastruktur. Die erweiterte Authentifizierung (XAUTH) nutzt eine RADIUS-ähnliche Authentifizierung und für die Zugriffskontrolle auf Benutzerebene über IPsec verwendet werden.

Für die Nutzung von PSK sind folgende Einstellungen erforderlich:

| Parameter | IPsec-IKE-Authentifizierungseinstellungen |
|----------------|---|
| PSK | Der Pre-Shared Key, der zur Authentifizierung bei der Gegenstelle verwendet wird |
| Local ID Type | Die Art der Identifizierung für die lokale ID. Es gibt folgende Möglichkeiten: FQDN, Benutzername>@FQDN oder IP-Adresse |
| Local ID | Der lokale ID-Wert |
| Remote ID Type | Die Art der Identifizierung für die lokale ID |
| Remote ID | Der Remote-ID-Wert |

Bei der Verwendung von Zertifikaten müssten Sie die Betriebsart angeben. Beim Betrieb als PKI-Client (Initiator) können Sie im Bereich Zertifikate einen Certificate Signing Request (CSR) erstellen, der bei Ihrer Zertifizierungsstelle eingereicht und anschließend in den Router importiert werden muss. Im PKI-Server-Modus (Konzentrator) stellt der Router die Zertifizierungsstelle dar und stellt die Zertifikate für Gegenstellen aus; diese sind widerruflich.

Bei Verwendung von XAUTH stehen die folgenden Einstellungen zur Verfügung:

| Parameter | IPsec-XAUTH-Einstellungen |
|----------------|----------------------------------|
| User name | Der Name des XAUTH-Benutzers |
| User password | Das Passwort des XAUTH-Benutzers |
| Group name | Die Gruppen-ID |
| Group password | Die Gruppenpassphrase |

IKE Proposal

In diesem Abschnitt können Sie die Einstellungen der Phase 1 konfigurieren:

| Parameter | IPsec-IKE-Vorschlagseinstellungen |
|--------------------------|--|
| Negotiation mode | Legt den Verhandlungsmodus fest. Vorzugsweise sollte der Modus <code>main</code> verwendet werden, aber der Modus <code>aggressive</code> könnte in Verbindung mit dynamischen Endpunktadressen sinnvoll sein. |
| Encryption algorithm | Die gewählte IKE-Verschlüsselungsmethode (empfohlen wird AES256) |
| Authentication algorithm | Die gewählte IKE-Authentifizierungsmethode (SHA1 sollte gegenüber MD5 bevorzugt werden) |
| IKE Diffie-Hellman Group | Die IKE-Diffie-Hellman-Gruppe |
| SA life time | Die Gültigkeitsdauerdauer von Security Associations (SA) |
| Pseudo-random function | Pseudozufallszahlen-Algorithmen, die optional verwendet werden können. |

IKE-Vorschläge (Proposals)

In diesem Abschnitt können Sie die Einstellungen der Phase 2 konfigurieren:

| Parameter | Einstellungen für IPsec-Vorschläge |
|-------------------------------|--|
| Encapsulation mode | Der gewählte Kapselungsmodus (Tunnel oder Transport) |
| IPsec protocol | Das gewählte IPsec-Protokoll aus (AH oder ESP) |
| Encryption algorithm | Die gewählte IKE-Verschlüsselungsmethode (empfohlen wird AES256) |
| Authentication algorithm | Die gewählte IKE-Authentifizierungsmethode (SHA1 sollte gegenüber MD5 bevorzugt werden) |
| SA life time | Die Gültigkeitsdauerdauer von Security Associations (SA) |
| Perfect forward secrecy (PFS) | Legt fest, ob Perfect Forward Secrecy (PFS) verwendet wird. Diese Funktion erhöht die Sicherheit, da PFS Eindringen in das Schlüsselaustauschprotokoll vermeidet und die Kompromittierung früherer Schlüssel verhindert. |
| Force encapsulation | Erzwingt die UDP-Kapselung für ESP-Pakete, auch wenn keine NAT-Situation erkannt wird. |

Netzwerke

Bei der Erstellung von Security Associations (SA) Sicherheitsassoziationen behält IPsec die gerouteten Netzwerke innerhalb des Tunnels im Auge. Pakete werden nur übertragen, wenn eine gültige SA mit passendem Quell- und Zielnetz vorliegt. Daher müssen Sie möglicherweise die Netzwerke neben

den Endpunkten in den folgenden Einstellungen angeben:

| Parameter | IPsec-Netzwerkeinstellungen |
|---------------|---|
| Local network | Die Adresse des lokalen Netzwerks |
| Local netmask | Die Netzmaske des lokalen Netzwerks |
| Peer network | Die Adresse des Remote-Netzwerks hinter der Gegenstelle |
| Peer netmask | Die Netzmaske des Remote-Netzwerks hinter der Gegenstelle |
| NAT address | Optional können Sie NAT (Masquerading) für Pakete anwenden, die aus einem anderen lokalen Netzwerk stammen. Die NAT-Adresse muss sich in dem Netzwerk befinden, das zuvor als lokales Netzwerk angegeben wurde. Sollte NAT address aktiviert, jedoch keine Adresse festgelegt werden, so wird der Router versuchen, automatisch eine geeignete Adresse zu finden (nicht empfohlen). |

Client-Verwaltung

Sobald der IPsec-Tunnel erfolgreich eingerichtet ist, können Sie Clients, die sich mit dem Dienst verbinden, verwalten und aktivieren. Sie können Expertendateien für aktivierte Clients erstellen und herunterladen und damit die Clients einfach bestücken.

5.6.3. PPTP

Das Point-to-Point Tunneling Protocol (PPTP) ist eine Methode zur Implementierung von virtuellen privaten Netzwerken zwischen zwei Hosts. PPTP ist einfach zu konfigurieren und unter den Servern von Microsoft-Dial-up-Netzwerken (DUN) weit verbreitet. Aufgrund seiner schwachen Verschlüsselungsalgorithmen wird es heutzutage als unsicher angesehen, bietet aber dennoch eine einfache Möglichkeit, Tunnel einzurichten.

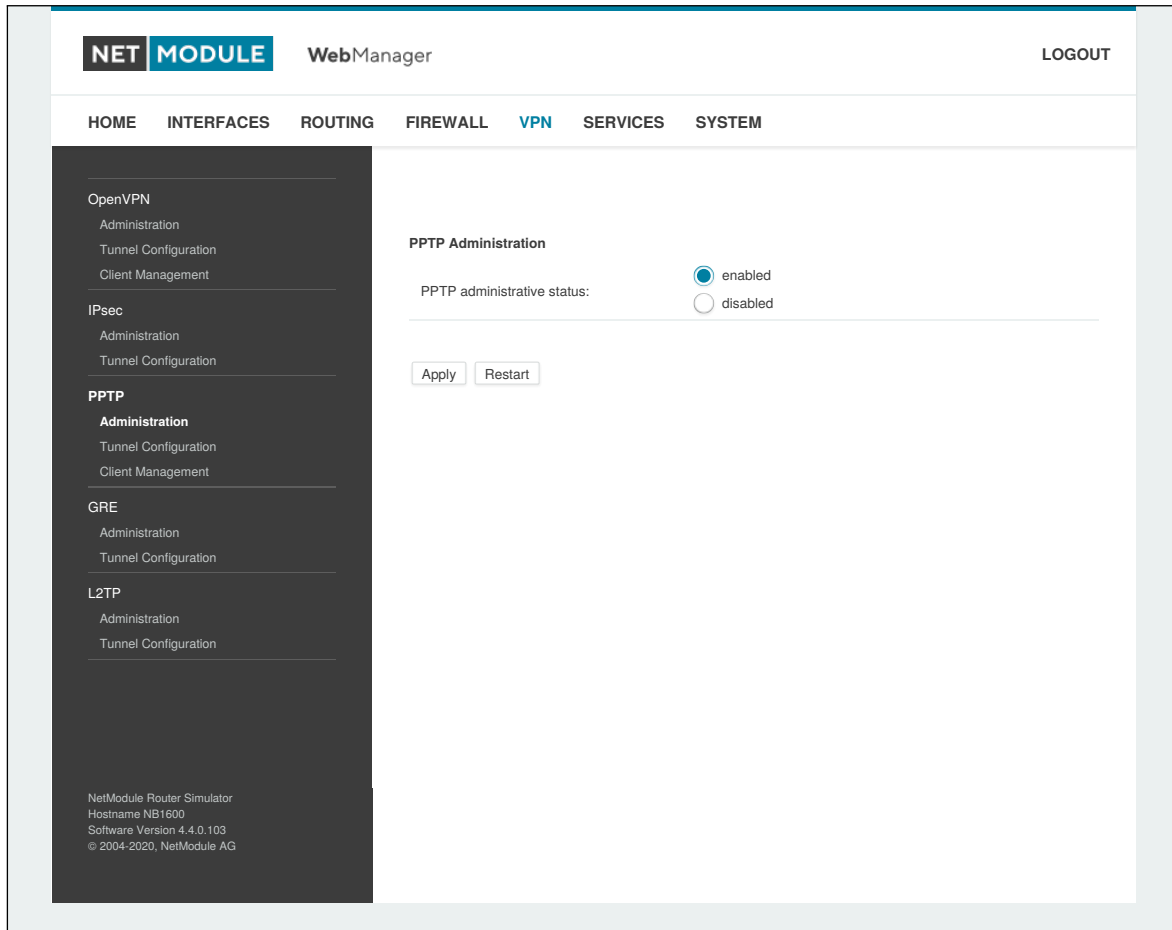


Abbildung 5.36.: PPTP-Verwaltung

Beim Einrichten eines PPTP-Tunnels müssten Sie zwischen den Betriebsarten Server und Client wählen. Für einen Client-Tunnel müssen die folgenden Einstellungen festgelegt werden:

| Parameter | PPTP-Client-Einstellungen |
|----------------|---|
| Server address | Die Adresse des Remote-Servers |
| Username | Der für die Authentifizierung verwendete Benutzername |
| Password | Das zur Authentifizierung verwendete Passwort |

Hinweis: Beim Einrichten von Clients mit festen Adressen werden Benutzername und Passwort nicht verwendet.

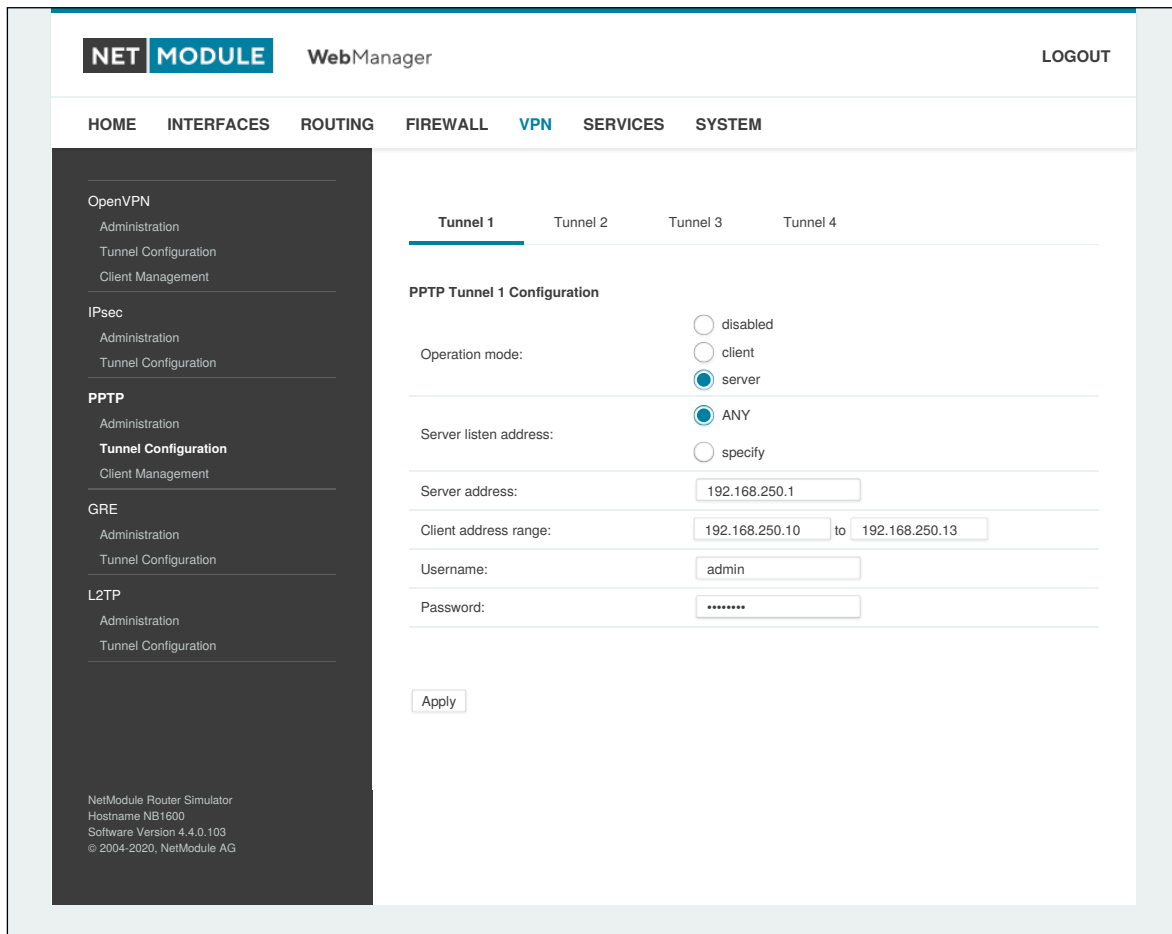


Abbildung 5.37.: Konfiguration eines PPTP-Tunnels

Für einen Server-Tunnel sind die folgenden Einstellungen erforderlich:

| Parameter | PPTP-Servereinstellungen |
|----------------------|--|
| Listen address | Legt fest, auf welcher IP-Adresse eingehende Client-Anfragen erwartet werden |
| Server address | Die Serveradresse innerhalb des Tunnels |
| Client address range | Legt einen Bereich fest, aus dem den Clients IP-Adressen zugewiesen werden |

PPTP-Client-Verwaltung

Auf dieser Seite müssen die PPTP-Clients für einen Server-Tunnel konfiguriert werden. Hierzu werden Benutzername und Passwort benötigt. Den Clients kann eine feste IP-Adresse zugewiesen werden, über die beliebige Routen auf einen dedizierten Tunnel geleitet werden können.

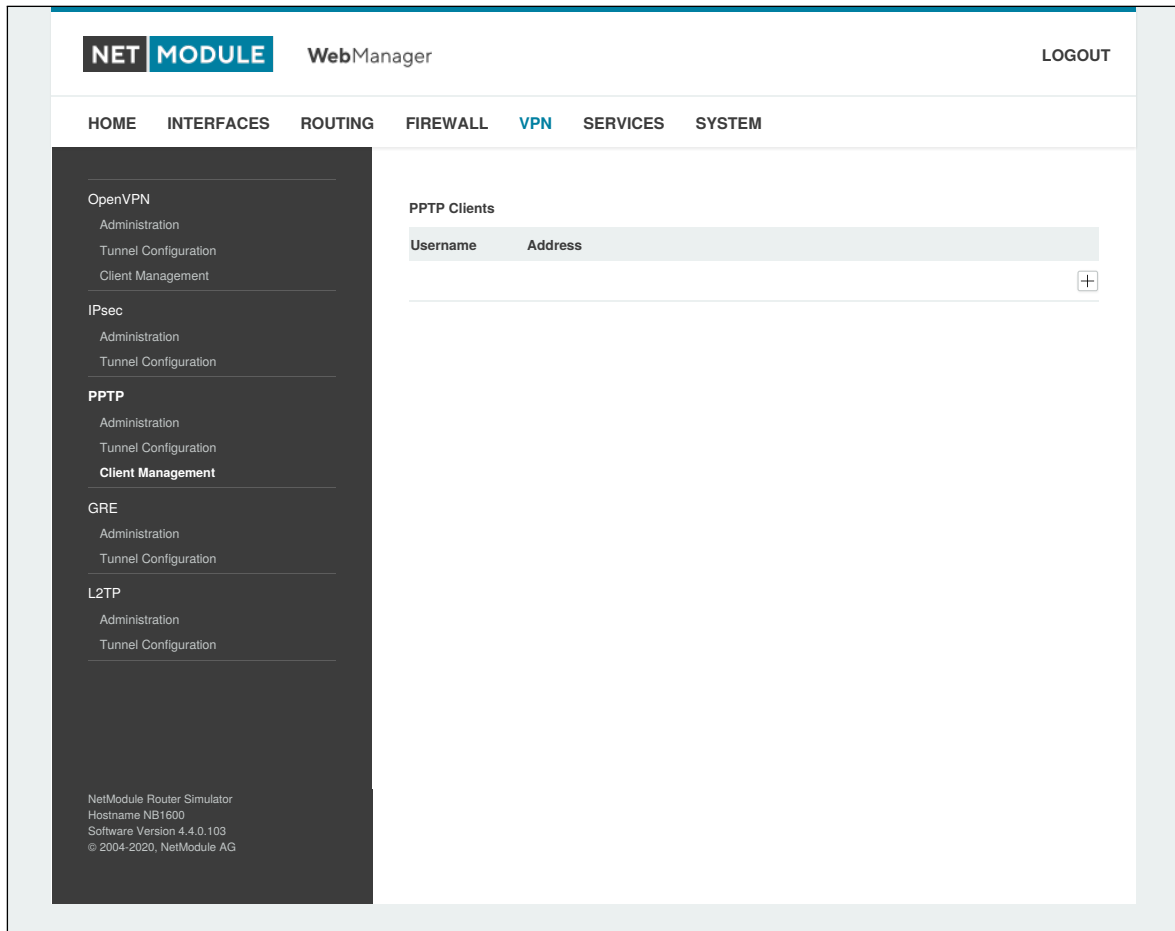


Abbildung 5.38.: PPTP-Client-Verwaltung

5.6.4. GRE

Generic Routing Encapsulation (GRE) ist ein Tunneling-Protokoll, das eine Vielzahl von Netzwerkschichtprotokollen in virtuelle Punkt-zu-Punkt-Verbindungen über IP einkapseln kann. GRE ist in RFC 1701, 1702 und 2784 definiert. Es bietet weder Verschlüsselung noch Autorisierung, kann jedoch auf Adressbasis für Tunneling-Zwecke zusätzlich zu anderen VPN-Techniken (z. B. IPSec) verwendet werden.

Zum Einrichten eines Tunnels sind die folgenden Parameter erforderlich:

| Parameter | GRE-Konfiguration |
|----------------------|--|
| Local address | Die IP-Adresse, die als Absender der GRE-Pakete genutzt wird (optional) |
| Peer address | Die IP-Adresse der Remote-Gegenstelle |
| Interface | Der Gerätetyp für diesen Tunnel |
| Local tunnel address | Die lokale IP-Adresse des Tunnels |
| Local tunnel netmask | Die lokale Netzmaske des Tunnels |
| Remote network | Die Remote-Netzwerkadresse des Tunnels |
| Remote netmask | Die Remote-Subnetzmaske des Tunnels |
| Tunnel key | Ein GRE-Tunnel-Schlüssel ermöglicht es dem Remote-Server, GRE-Pakete von verschiedenen Kommunikationspartnern voneinander zu unterscheiden |

Normalerweise darf die lokale Tunneladresse/Netzmaske nicht mit anderen Schnittstellenadressen in Konflikt geraten. Das entfernte Netzwerk/die entfernte Netzmaske ergibt einen zusätzlichen Routeneintrag, damit gesteuert werden kann, welche Pakete eingekapselt und über den Tunnel übertragen werden sollen.

5.6.5. L2TP (Layer-2-Tunneling-Protokoll)

Das Layer-2-Tunneling-Protokoll ist ein Tunneling-Protokoll, das weder Verschlüsselung noch Vertraulichkeit unterstützt. Es verlässt sich auf ein Verschlüsselungsprotokoll, das es innerhalb des Tunnels durchläuft, um Vertraulichkeit zu gewährleisten.

Zum Einrichten eines Tunnels sind die folgenden Parameter erforderlich:

| Parameter | L2TP-Konfiguration |
|--------------------|---|
| Transport protocol | Das zu verwendende Transportprotokoll |
| Local IP | Die lokale IP-Adresse des Tunnels |
| Remote IP | Die Remote-IP-Adresse des Tunnels |
| Local port | Die lokale Port-Adresse des Tunnels |
| Remote port | Die Remote-Port-Adresse des Tunnels |
| Local tunnel ID | Die lokale Tunnel-ID identifiziert den Tunnel, in dem die Sitzung erstellt wird |
| Remote tunnel ID | Die Remote-Tunnel-ID identifiziert den von der Gegenstelle zugewiesenen Tunnel |
| Local Session ID | Die lokale Session-ID identifiziert die zu erstellende Sitzung |
| Remote Session ID | Die Remote-Session-ID identifiziert die von der Gegenstelle zugewiesene Sitzung |
| Local Cookie | Setzt einen optionalen Cookie-Wert, der der Sitzung zugewiesen wird |
| Remote Cookie | Setzt einen optionalen oberen Cookie-Wert, der der Sitzung zugewiesen wird |
| MTU | Maximale Größe einer Übertragungseinheit für die Tunnelschnittstelle |
| Bridge interface | Die Schnittstelle, mit der die Host-Schnittstelle gebrückt werden soll |

5.6.6. Einwahl (Dial-In)

Auf dieser Seite können Sie den Einwahlserver konfigurieren, um Point-to-Point- (PPP-) Datenverbindungen über Mobilfunk (GSM) anbieten zu können. Hierfür würde man in der Regel 2G als erforderlichen Dienstyp angeben, sodass sich das Modem nur bei GSM anmelden kann. Eine gleichzeitige Verwendung ausgehender WWAN-Schnittstellen und Einwahlverbindungen ist natürlich nicht möglich.

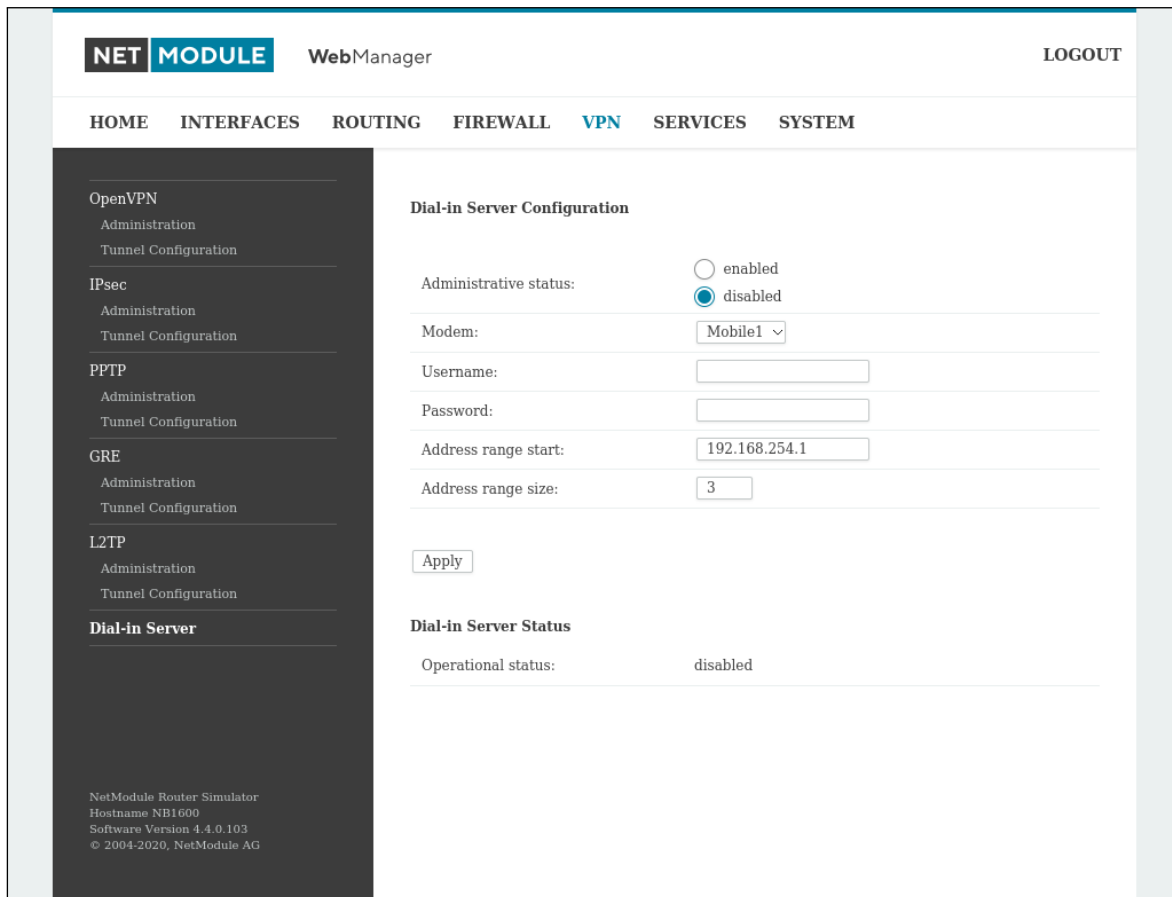


Abbildung 5.39.: Einwahlserver-Einstellungen

Es stehen die folgenden Einstellungen zur Verfügung:

| Parameter | Einwahlserver-Konfiguration |
|-----------------------|--|
| Administrative status | Legt fest, ob eingehende Anrufe angenommen werden sollen |
| Modem | Legt das Modem fest, über das Anrufe eingehen können |
| User | Legt den Benutzernamen für die eingehende PPP-Verbindung fest |
| Password | Legt das Passwort für die eingehende PPP-Verbindung fest |
| Address range start | Beginn des IP-Adressbereichs, der den anrufenden Clients zugewiesen wird |
| Address range size | Anzahl der Adressen für den Client-IP-Adressbereich |



Ganz generell wird von Einwahlverbindungen abgeraten. Da sie als GSM-Sprachanrufe implementiert sind, zeichnen sie sich durch Unzuverlässigkeit und sehr geringe Bandbreite aus.

5.7. DIENSTE

5.7.1. SDK

NetModule-Router werden mit einem Software Development Kit (SDK) ausgeliefert. Mit seiner Hilfe können Sie einfach und schnell kundenspezifische Funktionen und Anwendungen implementieren. Das SDK umfasst die folgenden Komponenten:

1. Einen SDK-Host, der die Laufzeitumgebung (die sogenannte Sandbox) definiert, d. h. den Zugriff auf die Systemressourcen (z. B. Arbeitsspeicher, Speicher und CPU) kontrolliert und damit für die benötigte Skalierbarkeit sorgt
2. Eine Interpretersprache namens `arena`, eine einfache, für eingebettete Systeme optimierte Skriptsprache, die eine ANSI-C-ähnliche Syntax verwendet, aber zusätzlich Ausnahmen, automatische Speicherverwaltung und Laufzeitpolymorphismus unterstützt
3. Eine NetModule-spezifische Anwendungs-Programmierschnittstelle (API) mit einem umfassenden Satz von Funktionen für den Zugriff auf Hardware-Schnittstellen (z. B. digitale IO-Ports, GPS, externe Speichermedien, serielle Schnittstellen), aber auch für die Abfrage von Systemstatus-Parametern, das Versenden von E-Mail- oder SMS-Nachrichten oder die Konfiguration des Routers

Wer einige Erfahrung mit der Programmiersprache C hat, wird eine Umgebung vorfinden, in die man sich leicht einarbeiten kann. Sie können uns jedoch gerne über support@netmodule.com kontaktieren - wir unterstützen Sie gerne dabei, ein Programm für Ihr spezielles Problem zu finden.

Sprachelemente

Die Skripting-Sprache `arena` umfasst eine breite Palette von POSIX-Funktionen (wie `printf` oder `open`) und bietet zusammen mit maßgeschneiderten API-Funktionen eine einfache Plattform für das Erstellen von Anwendungen aller Art, die Geräte oder Dienste mit dem Router verbinden.

Ein kurzes Beispiel:

```
/* We are going to eavesdrop on the first serial port
 * and turn on lights via a digital I/O output port,
 * otherwise we'd have to send a short message.
 */

for (attempts = 0; attempts < 3; attempts++) {
    if (nb_serial_read("serial0") == "Klopf klopf!") {
        nb_serial_write("serial0", "Wer ist da?");

        if (nb_serial_read("serial0") == "Weihnachtsmann") {
            printf("Hurra!\n");
            nb_dio_set("out1", 1);
        }
    }
}
nb_sms_send("+123456789", "Diesmal keine Geschenke:")
```

Eine Reihe von Beispielskripten kann direkt vom Router heruntergeladen werden. Eine Liste finden Sie im Anhang. Das Handbuch kann abgerufen werden von der [NetModule-Supportseite](#). Es enthält eine detaillierte Einführung in die Sprache, einschließlich einer Beschreibung aller Funktionen.

API-Funktionen des SDK

Mit den derzeit verfügbaren API-Funktionen können Sie die folgenden Aufgaben lösen:

1. SMS senden/abrufen
2. E-Mail senden
3. Vom seriellen Gerät lesen und dorthin schreiben
4. Digitale Ein-/Ausgänge steuern
5. TCP/UDP-Server ausführen
6. IP/TCP/UDP-Clients ausführen
7. Auf Dateien von eingebundenen Medien (z. B. einem USB-Stick) zugreifen
8. Statusinformationen vom System abrufen
9. Konfigurationsparameter abrufen oder setzen
10. Ins Systemprotokoll schreiben
11. Dateien über HTTP/FTP übertragen
12. Konfigurations-/Software-Updates durchführen
13. Die LED steuern
14. Systemereignisse abrufen, Dienste neu starten oder System neu starten
15. Nach Netzwerken in Reichweite suchen
16. Eigene Webseiten erstellen
17. Sprachsteuerungsfunktionen nutzen
18. SNMP-Funktionen nutzen
19. CAN-Socket-Funktionen nutzen
20. Verschiedene netzwerkbezogene Funktionen nutzen
21. Andere systembezogene Funktionen nutzen

Das SDK-API-Handbuch (das vom Router heruntergeladen werden kann) gibt einen Überblick, erklärt aber auch alle Funktionen im Detail.

Hinweis: Für einige Funktionen müssen die entsprechenden Dienste (z. B. E-Mail, SMS) oder Schnittstellen (z. B. CAN) vor der Nutzung im SDK richtig konfiguriert werden.

Wir widmen uns zuerst der sehr mächtigen API-Funktion `nb_status`. Mit ihr können die Statuswerte des Routers auf die gleiche Weise abgefragt werden, wie sie mit der CLI angezeigt werden. Sie liefert eine Struktur von Variablen für einen bestimmten Abschnitt zurück (eine Liste der verfügbaren Abschnitte erhalten Sie mit `cli status -h`).

Mit der Funktion `dump` können Sie sich den Inhalt der zurückgegebenen Struktur ausgeben lassen:

```
/* dump current location */  
dump(nb_status("location"));
```

Das Skript erzeugt dann eine Ausgabe wie diese:

```
struct(8): {  
  .LOCATION_STREET      = string[11]: "Bahnhofquai"  
  .LOCATION_CITY        = string[10]: "Zurich"  
  .LOCATION_COUNTRY_CODE = string[2]: "ch"  
  .LOCATION_COUNTRY     = string[11]: "Switzerland"  
  .LOCATION_POSTCODE    = string[4]: "8001"  
  .LOCATION_STATE       = string[6]: "Zurich"  
  .LOCATION_LATITUDE    = string[9]: "47.3778058"  
  .LOCATION_LONGITUDE   = string[8]: "8.5412757"  
}
```

In Kombination mit der Funktion `nb_config_set` kann bei Statusänderungen eine Neukonfiguration beliebiger Teile des Systems gestartet werden. Mögliche Abschnitte und Parameter können Sie wieder mit der CLI abfragen:

```
~ $ cli get -c wanlink.0  
cli get -c wanlink.0  
Konfigurationsentitäten anzeigen (wie "wanlink.0"):
```

| | | |
|--------------------------------|-----------------------------------|-------------------------------|
| <code>wanlink.0.mode</code> | <code>wanlink.0.multipath</code> | <code>wanlink.0.name</code> |
| <code>wanlink.0.options</code> | <code>wanlink.0.passthru</code> | <code>wanlink.0.prio</code> |
| <code>wanlink.0.suspend</code> | <code>wanlink.0.switchback</code> | <code>wanlink.0.weight</code> |

Wenn Sie mit der CLI im interaktiven Modus ausführen, können Sie die möglichen Konfigurationsparameter mit der Taste `TABULATOR` auch schrittweise durchblättern.

Hier ist ein Beispiel, wie man diese Funktionen nutzen könnte:

```
/* Aktuellen Ort finden und 2. WAN-Verbindung aktivieren */  
  
location = nb_status("location");  
if (location) {  
    city = struct_get(location, "LOCATION_CITY");  
  
    if (city == "Wonderland") {  
        for (led = 0; led < 5; led++) {  
            nb_led_set(led, LED_BLINK_FAST|LED_COLOR_RED);  
        }  
    } else {  
        printf("You'll never walk alone in %s ...\n", city);  
        nb_config_set("wanlink.1.mode=1");  
    }  
}
```

Arbeiten mit dem SDK

Im Zusammenhang mit dem SDK sprechen wir von Skripten und Triggern, aus denen sich die diversen Jobs zusammensetzen.

Ein `arena`-Skript kann auf den Router hochgeladen oder mit Hilfe spezieller Benutzerkonfigurationspakete importiert werden. Sie können das Skript auch direkt im Web Manager bearbeiten oder eines der mitgelieferten Beispiele auswählen. Außerdem steht auf dem Router ein Testbereich zur Verfügung, in dem Sie Ihre Syntax überprüfen oder Testläufe durchführen können.

Nach dem Hochladen müssen Sie einen Trigger angeben, d. h. dem Router mitteilen, wann das Skript ausgeführt werden soll. Trigger können entweder zeitbasiert sein (z. B. "jeden Montag") oder durch eines der vordefinierten Systemereignisse ausgelöst werden (z. B. wan-up), wie beschrieben im Kapitel 5.7.7. Mit einem Skript und einem Trigger können Sie einen SDK-Job einrichten. Das Ereignis `test` ist in der Regel eine gute Möglichkeit, zu überprüfen, ob der Job ordnungsgemäß läuft. Der Admin-Bereich bietet außerdem Möglichkeiten zur Fehlerbehebung und zur Kontrolle laufender Jobs.

Der SDK-Host (`sdkhost`) entspricht dem Daemon, der die Skripte und ihre Aktionen verwaltet und Schäden am System verhindert. Er begrenzt CPU- und Speicherressourcen für die Ausführung von Skripten und stellt außerdem einen vordefinierten Teil des verfügbaren Speicherplatzes auf dem Speichergerät zur Verfügung. Sie können den Speicherplatz mit einem externen USB-Speicher oder (je nach Modell) mit weiterem Flash-Speicher erweitern. Dateien, die auf `/tmp` geschrieben werden, werden im Speicher gehalten und nach einem Neustart des Skripts wieder gelöscht. Da Ihre Skripte in der Sandbox laufen, haben Sie keinen Zugriff auf Systemtools (wie `ifconfig`).

Verwaltung

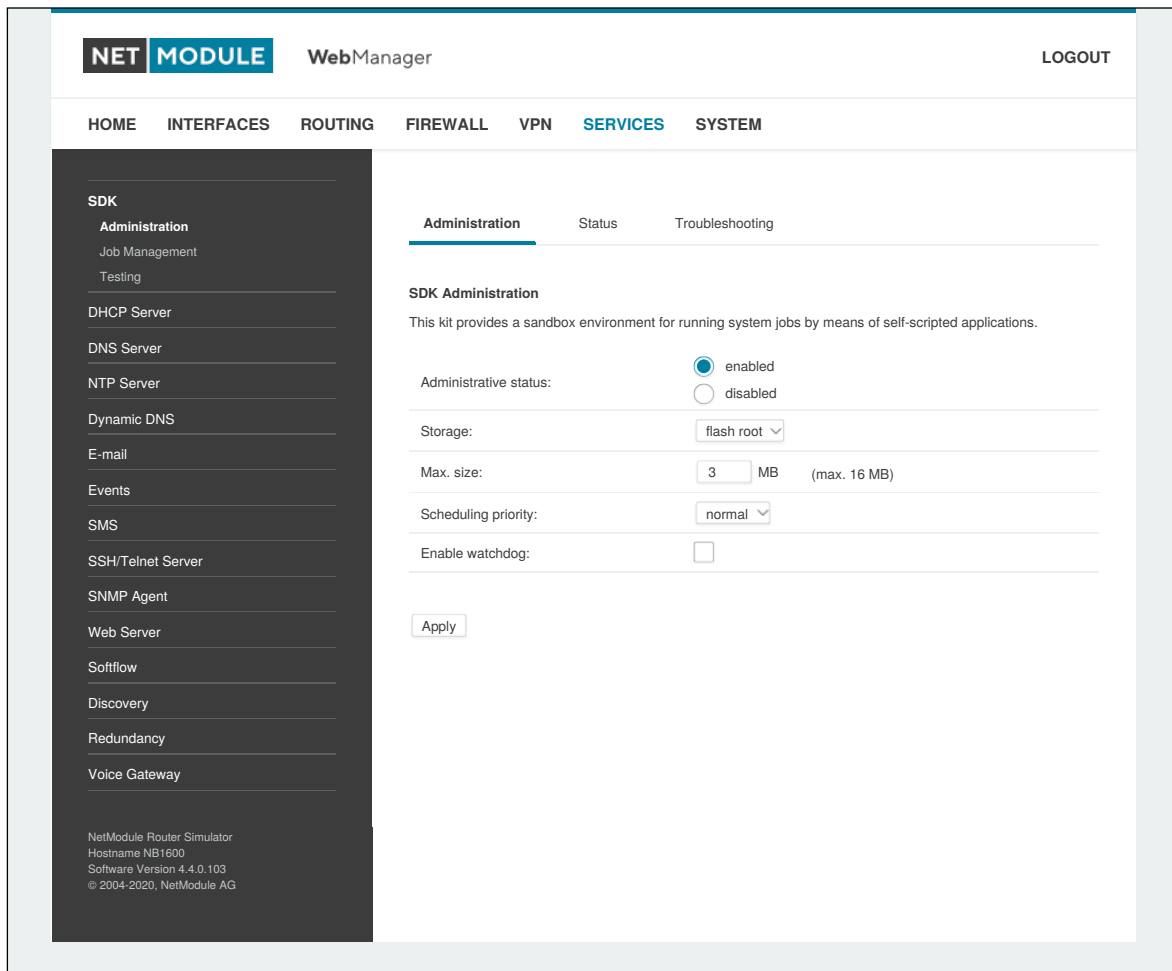


Abbildung 5.40.: SDK-Verwaltung

Auf dieser Seite können Sie den SDK-Host steuern und die folgenden Einstellungen vornehmen:

| Parameter | SDK-Verwaltungseinstellungen |
|-----------------------|---|
| Administrative status | Legt fest, ob SDK-Skripte ausgeführt werden sollen oder nicht |
| Storage | Das Speichergerät, auf dem die Sandbox gespeichert werden soll (siehe Kapitel 5.8.1) |
| Max. size | Den maximalen Platz (in MB), die Skripte auf dem Speichergerät nutzen können |
| Scheduling priority | Legt die Prozesspriorität des sdkhost fest. Höhere Prioritäten beschleunigen die Ausführung der Skripte, niedrigere haben geringere Auswirkungen auf das Hostsystem |
| Enable watchdog | Aktiviert die Watchdog-Überwachung für jedes Skript. Sie bewirkt einen Neustart des Systems, wenn das Skript nicht reagiert oder mit einem Exit-Code ungleich Null gestoppt wird. |

Die Statusseite informiert über den aktuellen Status des SDK. Sie liefert eine Übersicht über alle abgeschlossenen Jobs. Sie können dort auch einen laufenden Job stoppen und die Skriptaussgabe im Bereich Fehlerbehebung einsehen, wo Sie auch Links zum Herunterladen der Handbücher und Beispiele finden.

Job-Verwaltung

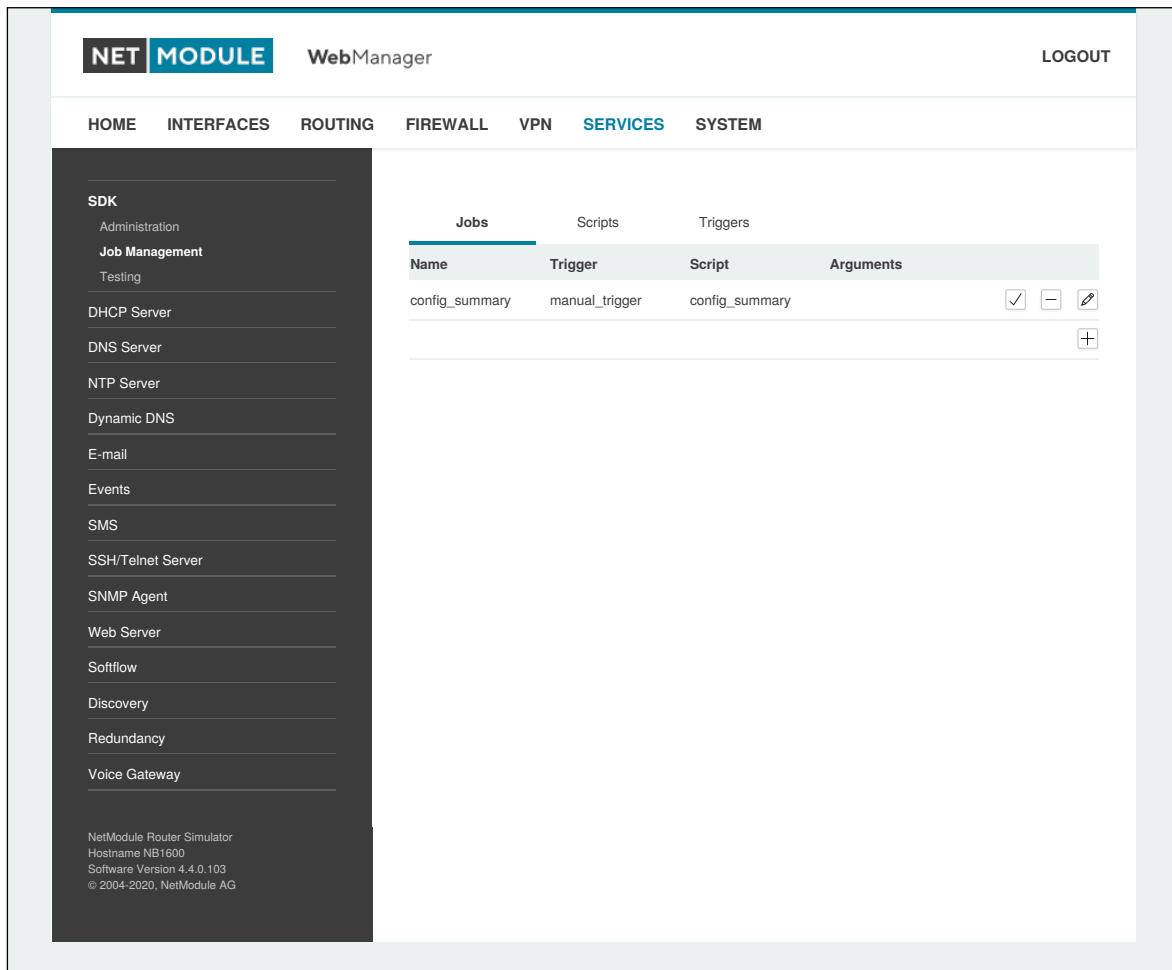


Abbildung 5.41.: SDK-Jobs

Auf dieser Seite können Sie Skripte, Trigger und Jobs einrichten. In der Regel ist es sinnvoll, zunächst einen Trigger zu erstellen, der sich aus den folgenden Parametern zusammensetzt:

| Parameter | SDK-Triggerparameter |
|-----------|--|
| Name | Ein aussagekräftiger Name zur Identifizierung des Triggers |
| Type | Der Typ des Triggers - zeitbasiert oder ereignisbasiert |
| Bedingung | Legt die Zeitbedingung für zeitbasierte Trigger fest (z. B. stündlich) |
| Timespec | Der Zeitpunkt, der zusammen mit der Bedingung die Zeit(en) angibt, zu denen der Trigger ausgelöst wird |
| Event | Das Systemereignis, bei dem der Trigger ausgelöst werden soll |

Sie können nun Ihr persönliches Skript hinzufügen, für das Sie die folgenden Parameter anwenden:

| Parameter | SDK-Skriptparameter |
|-------------|---|
| Name | Ein aussagekräftiger Name zur Identifizierung des Skripts |
| Description | Eine Beschreibung des Skripts (optional) |
| Arguments | Ein Satz von Argumenten, die an das Skript übergeben werden (unterstützt Quoting) (optional) |
| Action | Sie können ein Skript bearbeiten, es hochladen oder eines der Beispielskripte oder ein bereits hochgeladenes Skript auswählen |

Als nächstes können Sie einen Job einrichten, der mit den folgenden Parametern erstellt werden kann:

| Parameter | SDK-Jobparameter |
|-----------|--|
| Name | Ein aussagekräftiger Name zur Identifizierung des Jobs |
| Trigger | Legt den Trigger fest, der den Job starten soll |
| Script | Legt das auszuführende Skript fest |
| Arguments | Definiert Argumente, die an das Skript übergeben werden (unterstützt Quoting); sie werden den Argumenten vorangestellt, die Sie eventuell zuvor selbst dem Skript zugewiesen haben |

Sie können jeden konfigurierten Job direkt auslösen, was zu Testzwecken hilfreich sein kann.

Seiten

Alle programmierten SDK-Seiten werden hier angezeigt.

SDK-Tests

Die Testseite enthält einen Editor und ein Eingabefeld für optionale Argumente, mit denen Sie Testläufe Ihres Skripts durchführen oder bestimmte Teile davon testen oder eine ganze Datei hochladen können. Hinweis Sie müssen die Argumente eventuell in Anführungszeichen setzen, da sie sonst durch Leerzeichen getrennt werden.

```
/* arguments: 'Schnick Schnack "S c h n u c k"'
for (i = 0; i < argc; i++) {
    printf("argv%d: %s\n", i, argv[i]);
}

/* generates:
*     argv0: Skriptname
*     argv1: Schnick
*     argv2: Schnack
*     argv3: S c h n u c k
*/
```

Bei Syntaxfehlern gibt arena normalerweise Fehlermeldungen wie die folgende aus (mit Angabe der Zeile und der Position, an der der Parsing-Fehler auftrat):

```
/scripts/testrun:2:10:FATAL: parse error, unexpected $, expecting ';''
```

SDK-Beispielanwendung

Als Einführung können Sie eine Beispielanwendung durchgehen - ein SMS-Steuerungsskript, das die Fernsteuerung von Kurznachrichten implementiert und den Systemstatus zum Absender zurückgeben kann. Der Quellcode ist im Anhang enthalten.

Nach der Aktivierung können Sie eine Nachricht an die mit einer SIM-Karte/einem Modem verbundene Telefonnummer senden. In der Regel muss in der ersten Zeile ein Passwort und in der zweiten Zeile ein Befehl angegeben werden, z. B.:

```
admin01
status
```

Wir empfehlen dringend, eine Authentifizierung zu verwenden, um unbeabsichtigte Zugriffe zu vermeiden. Sie können dies jedoch mit `noauth` als Argument deaktivieren und so die erste Zeile mit dem Passwort überspringen. Wenn Sie sich das Skript genauer ansehen, werden Sie feststellen, dass Sie auch die Liste der zulässigen Absender einschränken können. Bitte prüfen Sie das Systemprotokoll, um eventuelle Probleme zu beheben.

Die folgenden Befehle werden unterstützt:

| Befehl | Action |
|--------------|---|
| status | Beantwortet eine Nachricht an den Absender mit einer kurzen Systemübersicht |
| connect | Aktiviert die erste auf dem System konfigurierte WAN-Verbindung |
| disconnect | Deaktiviert die erste auf dem System konfigurierte WAN-Verbindung |
| reboot | Leitet einen Neustart des Systems ein |
| output 1 on | Aktiviert den ersten digitalen Ausgang |
| output 1 off | Deaktiviert den ersten digitalen Ausgang |
| output 2 on | Aktiviert den zweiten digitalen Ausgang |
| output 2 off | Deaktiviert den zweiten digitalen Ausgang |

Tabelle 5.100.: SMS-Steuerbefehle

Die Antwort auf den status-Befehl sieht typischerweise so aus:

```
System: NB2700 hostname (00:11:22:AA:BB:CC)
WAN1: WWAN1 is up (10.0.0.1, Mobile1, UMTS, -83 dBm, LAI 12345)
GPS: lat 47.377894, lon 8.540055, alt 282.200
OVPN: client on tun0 is up (10.0.8.4)
DIO: IN1=off, IN2=off, OUT1=on, OUT2=off
```

5.7.2. DHCP-Server

In diesem Abschnitt kann der DHCP-Dienst (Dynamic Host Configuration Protocol) für jede LAN-Schnittstelle individuell konfiguriert werden, der den Hosts im lokalen Netzwerk dynamische IP-Adressen zuweist. Sie können die Statusseite mit einer Übersicht über ausgehandelte Client-Adressen einsehen.

Hier tauchen auch die WLAN-Schnittstellen (für alle SSIDs) auf, falls Sie jeweils einen Access Point konfiguriert haben.

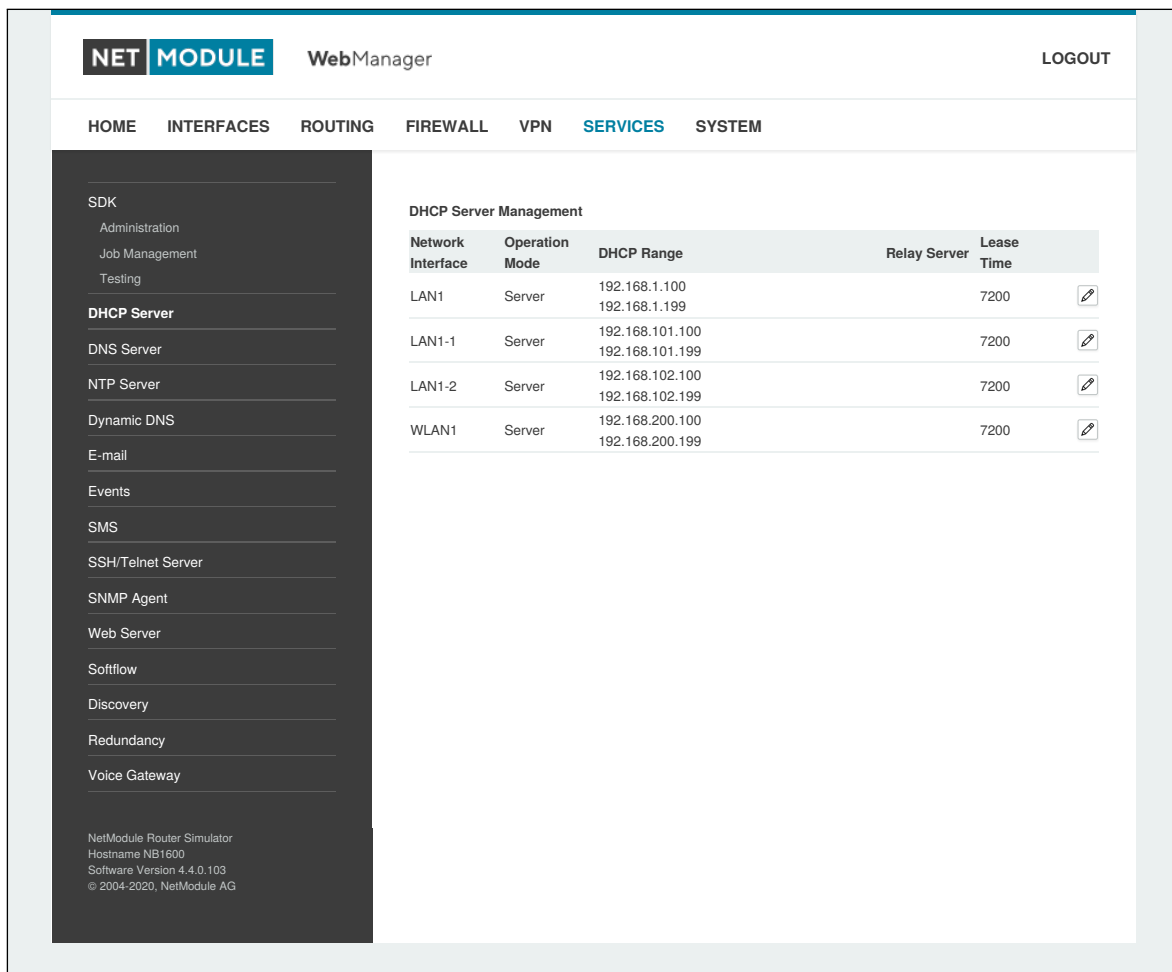


Abbildung 5.42.: DHCP-Server

Es stehen die folgenden Einstellungen für die jeweilige Schnittstelle zur Verfügung:

| Parameter | DHCP-Verwaltungseinstellungen |
|----------------|---|
| Operation mode | Legt den DHCP-Modus fest: server, relay, disabled |

| Parameter | DHCP-Servereinstellungen |
|-------------------------|---|
| First lease address | Die erste Adresse aus dem Bereich der IP-Adressen, die an Hosts vergeben werden |
| Last lease address | Die letzte Adresse aus diesem Bereich |
| Lease duration | Zeit in Sekunden, für die eine Vergabe gültig sein soll, bis er erneut angefordert werden muss |
| Persistent leases | Aktiviert die Speicherung einer Vergabe und Erneuerung durch den Router auch nach einem Neustart. Dies kann sicherstellen, dass einem bestimmten Host immer dieselbe IP-Adresse zugewiesen wird. |
| DHCP options | Standardmäßig vergibt der DHCP die Schnittstellenadresse als Standard-Gateway und die Adressen des aktuellen DNS-Servers, wenn nicht anders konfiguriert. Sie können hier feste Adressen angeben. |
| Only allow static hosts | Alle Anfragen, die von nicht-statischen Hosts kommen, werden ignoriert. |

| Parameter | DHCP-Relay-Einstellungen |
|------------------------|---------------------------------|
| Primary relay server | Der primäre DHCP-Relay-Server |
| Secondary relay server | Der sekundäre DHCP-Relay-Server |

Es ist auch möglich, bestimmte Adressen für bestimmte Clients zu vergeben.

| Parameter | DHCP-Einstellungen für statische Hosts |
|---------------|--|
| IP address | Die vergebene IP-Adresse |
| Identified by | Legt fest, nach welchen Kriterien der Client identifiziert werden soll |
| MAC address | Die MAC-Adresse des Clients |
| hostname | Die Client-ID (DHCP-Option 61) |
| port | Der Ethernet-Port, an dem die DHCP-Anforderung empfangen wird |

5.7.3. DNS-Server

Der DNS-Server kann DNS-Anfragen an Server im Netz weiterleiten, die z. B. bei der Herstellung der WAN-Verbindung ausgehandelt wurden. Indem man DNS-Anfragen an den Router weiterleitet, kann man den ausgehenden DNS-Verkehr reduzieren, da er bereits aufgelöste Namen zwischenspeichert. Sie können den DNS-Server auch für die Vergabe fester Adressen für bestimmte Hosts nutzen.

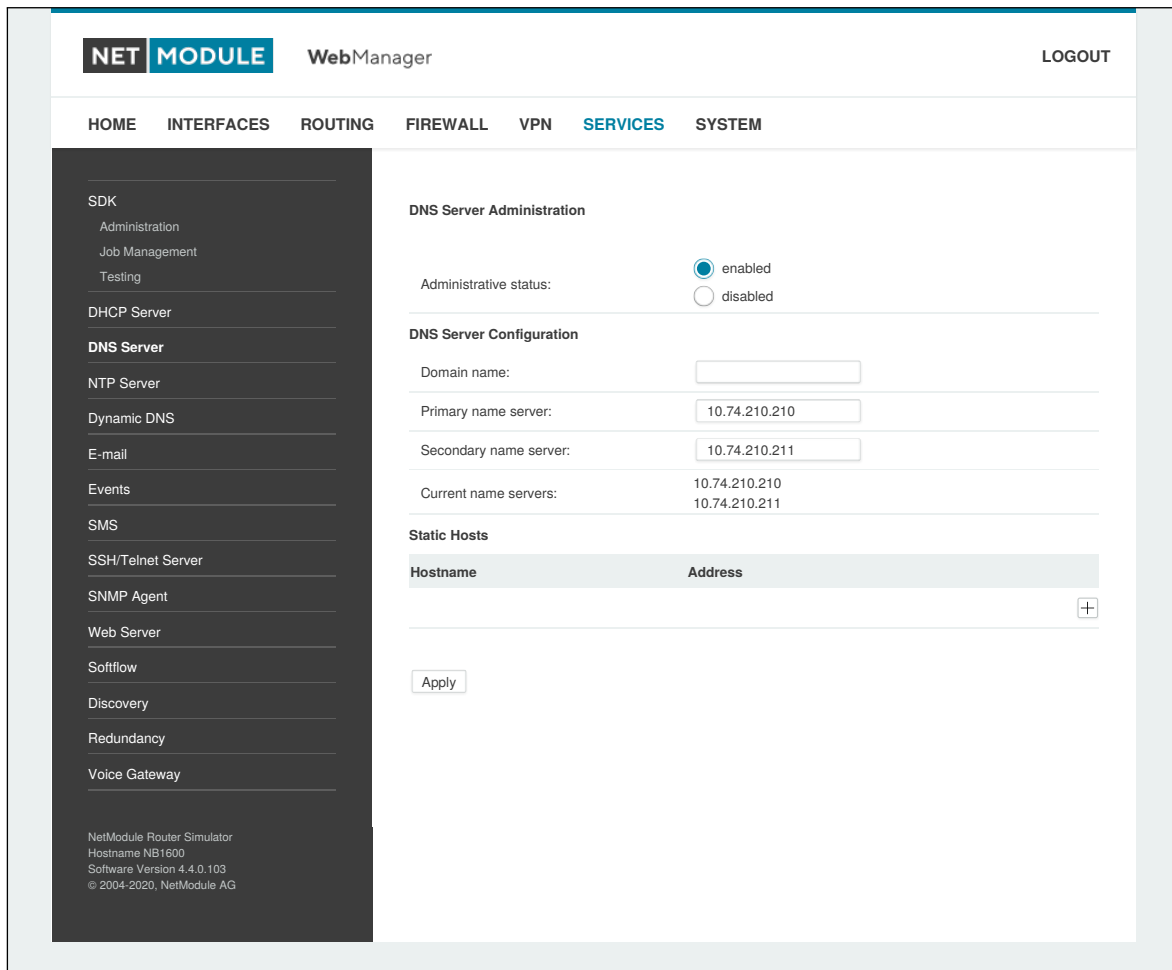


Abbildung 5.43.: DNS-Server

Es stehen die folgenden Einstellungen zur Verfügung:

| Parameter | DNS-Servereinstellungen |
|-----------------------|--|
| Administrative status | Legt fest, ob der DNS-Server aktiviert ist |
| Domain name | Der Domainname, der für die Suche nach Kurznamen verwendet wird |
| Primary name server | Der standardmäßige primäre Nameserver, der anstelle der ausgehandelten Nameserver verwendet wird |
| Secondary name server | Der standardmäßige sekundäre Nameserver, der anstelle der ausgehandelten Nameserver verwendet wird |



Sie können außerdem statische Hosts konfigurieren, um feste IP-Adressen für verschiedene Hostnamen bereitzustellen.

| Parameter | DNS-Einstellungen für statische Hosts |
|-----------|---------------------------------------|
| Address | Die IP-Adresse des statischen Hosts |
| Hostname | Der Hostname des statischen Hosts |

Denken Sie daran, DNS-Lookups lokaler Hosts auf die Adresse des Routers zu verweisen.

5.7.4. NTP-Server

In diesem Abschnitt können Sie die NTP-Serverfunktion (Network Time Protocol) individuell konfigurieren.

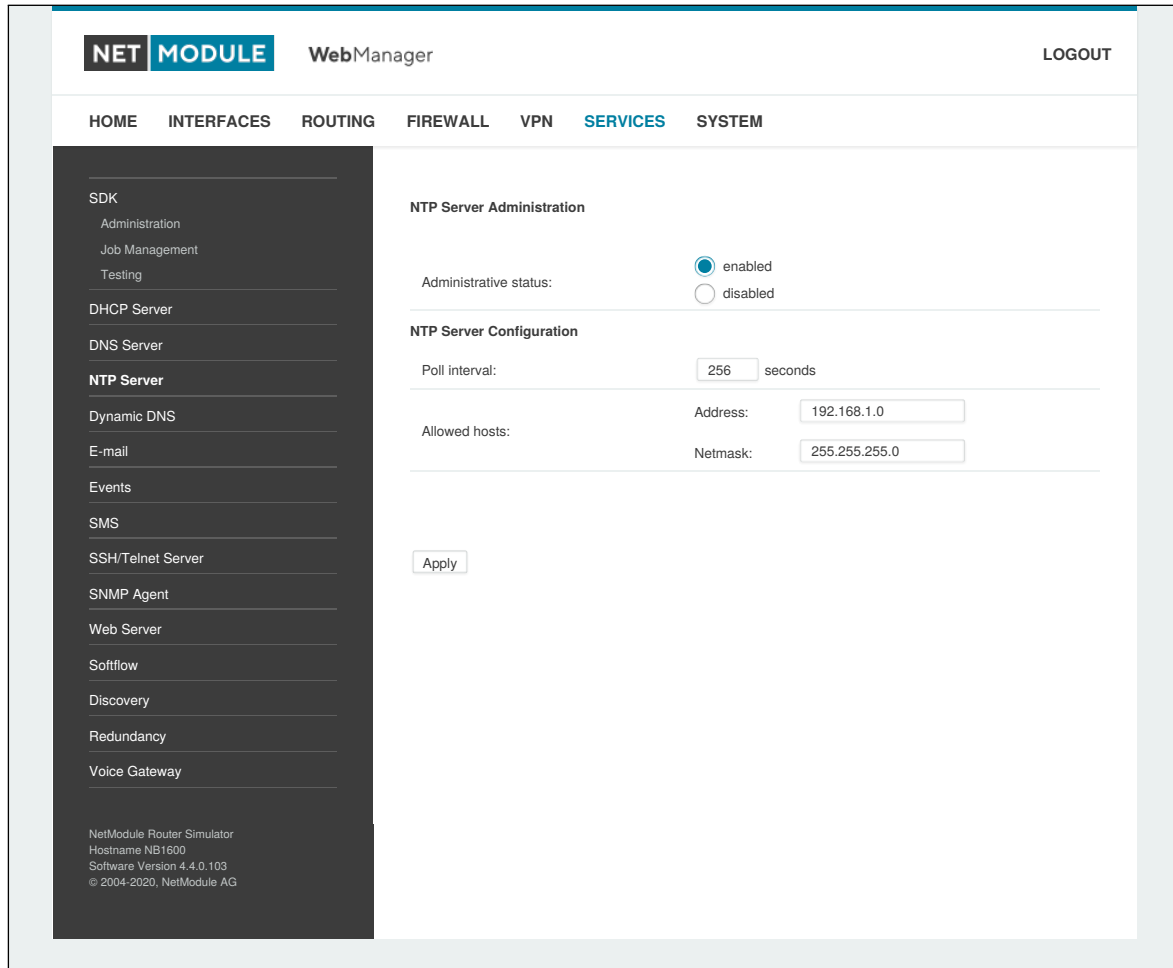


Abbildung 5.44.: NTP-Server

Es stehen die folgenden Einstellungen für die jeweilige Schnittstelle zur Verfügung:

| Parameter | NTP-Servereinstellungen |
|-----------------------|--|
| Administrative status | Legt fest, ob der NTP-Server aktiviert ist |
| Poll interval | Definiert das Abfrageintervall (64..2048 Sekunden) für die Synchronisation der Zeit mit den Hauptzeitservern |
| Allowed hosts | Legt den IP-Adressbereich fest, aus dem der NTP-Server abgefragt werden darf |

Zum Einstellen der Systemzeit des Geräts siehe Kapitel [5.8.1](#).

5.7.5. Dynamic DNS

Mit dem Dynamic-DNS-Client können Sie einem oder mehreren DynDNS-Anbietern die aktuelle IP-Adresse Ihres Systems mitteilen. Diese Adresse kann von der aktuellen Hotlink-Schnittstelle oder der Ausgangsschnittstelle abgeleitet werden, die für die Kontaktaufnahme mit dem Server verwendet wird. Unterstützt wird außerdem der CheckIP-Dienst bei dyndns.org, um die aktuelle Internetadresse zu erhalten, was in NAT-Szenarien nützlich sein kann.

Der DynDNS-Client wird immer dann aktiviert, wenn eine WAN- oder VPN-Verbindung aufgebaut wird.

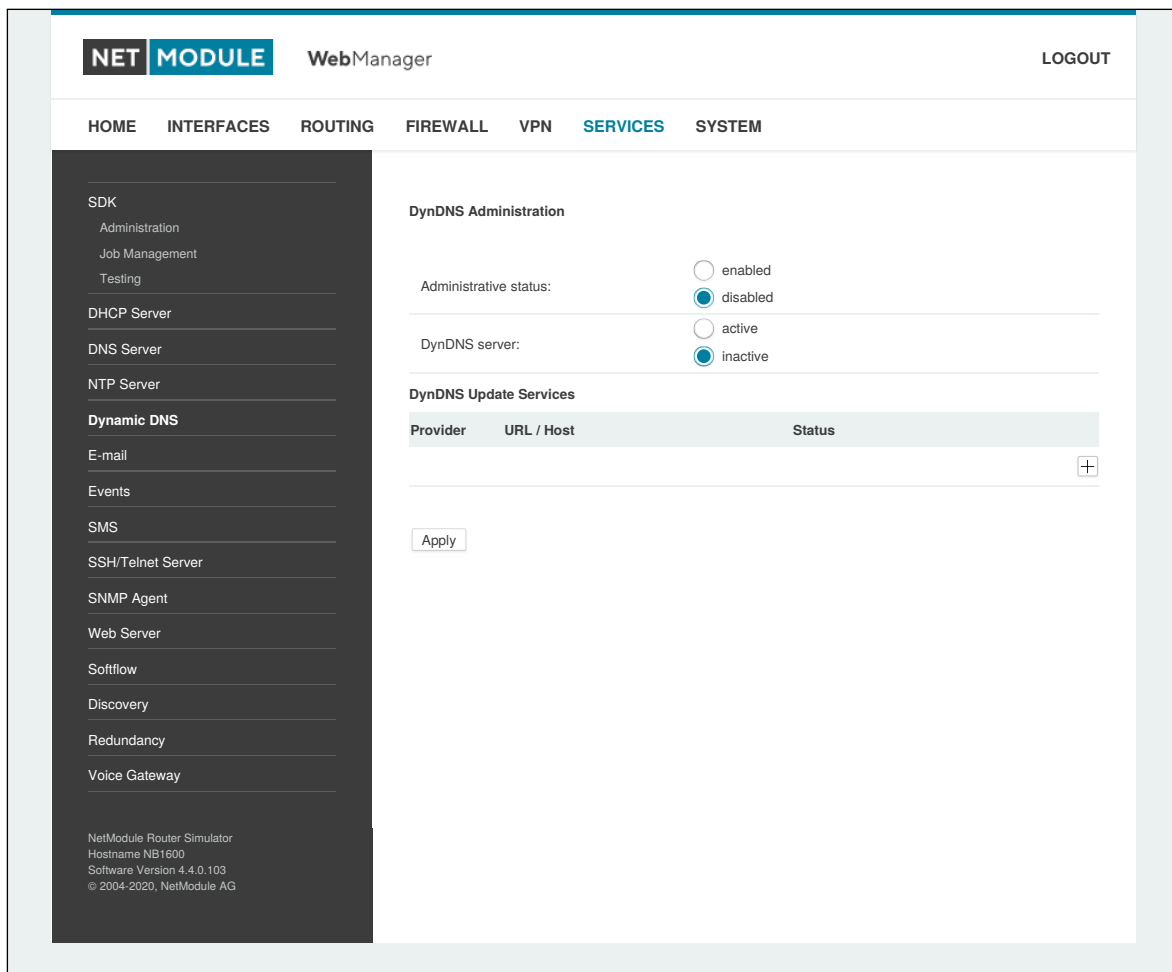


Abbildung 5.45.: Einstellungen für Dynamic DNS

Es werden eine Reihe gängiger DynDNS-Betreiber unterstützt, aber auch benutzerdefinierte Update-URLs sind möglich.

Hinweis: Der NetModule-Router kann auch selbstständig als DynDNS-Server arbeiten, sofern die Hosts auf den DNS-Dienst des Routers verweisen..

Außerdem werden das GnuDIP-Protokoll und RFC2136-ähnliche dynamische DNS-Updates unterstützt. Letztere ist in der Regel durch einen TSIG-Schlüssel gesichert.

Ein DynDNS-Dienst kann die folgenden Parameter verarbeiten:

| Parameter | Einstellungen für Dynamic DNS |
|-----------------|--|
| Provider | Sie können einen der aufgelisteten Anbieter wählen oder eine eigene URL angeben |
| Dynamic address | Legt fest, ob die Adresse aus dem Hotlink oder über einen externen Dienst bezogen wird |
| Hostname | Der vom DynDNS-Dienst bereitgestellte Hostname (z. B. my-box.dyndns.org) |
| Port | Der HTTP-Port des Dienstes (normalerweise 80) |
| Username | Der zur Authentifizierung beim Dienst verwendete Benutzername |
| Password | Das zur Authentifizierung verwendete Passwort |
| Protokoll | Das zur Authentifizierung verwendete Protokoll (HTTP, HTTPS) |
| Server address | Die Adresse des Servers, der aktualisiert werden soll |
| Server port | Der Port des Servers, der aktualisiert werden soll |
| TSIG key name | Der Name des TSIG-Schlüssels, der Updates durchführen darf |
| TSIG key | Der in base64 codierte TSIG-Schlüssel |

5.7.6. E-Mail

Mit dem E-Mail-Client können Sie bei bestimmten Ereignissen oder über SDK-Skripte Benachrichtigungen an eine bestimmte E-Mail-Adresse senden.

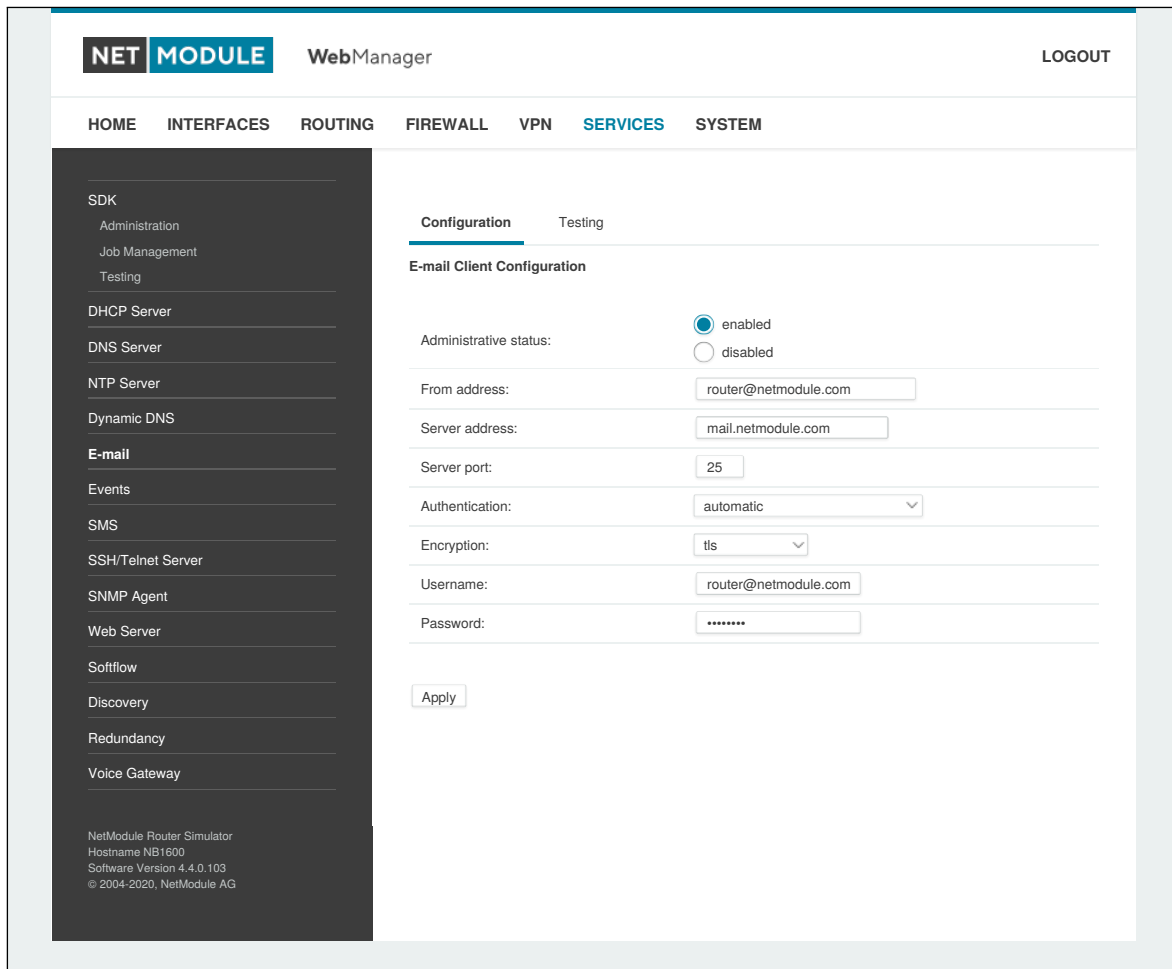


Abbildung 5.46.: E-Mail-Einstellungen

E-Mail kann mit den folgenden Einstellungen aktiviert werden.

| Parameter | Einstellungen des E-Mail-Clients |
|-----------------------|--|
| E-mail client status | Verwaltungsstatus des E-Mail-Clients |
| From e-mail address | E-Mail-Adresse des Absenders |
| Server address | Adresse des SMTP-Servers |
| Server port | SMTP-Server-Port (typischerweise 25) |
| Authentication method | Legt die Authentifizierungsmethode fest, die zur Authentifizierung gegenüber dem SMTP-Server verwendet werden soll |
| Encryption | Legt die Art der Verschlüsselung fest. Mögliche Werte: STARTTLS, none |



| Parameter | Einstellungen des E-Mail-Clients |
|-----------|--|
| Username | Für die Authentifizierung verwendeter Benutzername |
| Password | Passwort, das zur Authentifizierung verwendetet wird |

5.7.7. Ereignismanager

Mit dem Ereignismanager können Sie Remote-Systeme über Systemereignisse informieren. Benachrichtigungen können per E-Mail, SMS oder SNMP-Traps gesendet werden.

| Parameter | Einstellungen für Ereignisbenachrichtigungen |
|----------------|--|
| E-Mail address | Die E-Mail-Adresse, an die die Benachrichtigung gesendet werden soll (E-Mail-Client muss aktiviert sein) |
| Phone number | Die Rufnummer, an die die Benachrichtigung gesendet werden soll (SMS-Dienst muss aktiviert sein) |
| SNMP host | Der SNMP-Host oder die SNMP-Adresse, an die der Trap gesendet werden soll |
| SNMP port | Der Port des entfernten SNMP-Dienstes |
| Username | Der Benutzername für den Zugriff auf den entfernten SNMP-Dienst |
| Password | Das Passwort für den Zugriff auf den entfernten SNMP-Dienst |
| Authentication | Der Authentifizierungsalgorithmus für den Zugriff auf den entfernten SNMP-Dienst (MD5 oder SHA) |
| Encryption | Der Verschlüsselungsalgorithmus für den Zugriff auf den entfernten SNMP-Dienst (DES oder SHA) |
| Engine ID | Die Engine-ID des entfernten SNMP-Dienstes |

Die Meldungen enthalten eine von Ihnen erstellte Beschreibung und eine kurze Systeminformation. Eine Liste aller Systemereignisse finden Sie in Anhang [A.2](#).

5.7.8. SMS

Verwaltung

NetModule-Router können Kurznachrichten (SMS) empfangen oder senden, wenn dies vom SIM-Anbieter freigegeben wurde.

Nachrichten werden von dem Modem empfangen/gesendet, das einer SIM-Karte zugewiesen wurde, daher wird ein richtig konfiguriertes SMS-fähiges Standardmodem benötigt. Siehe Kapitel [5.3.3](#).

Hinweis: Das System wechselt möglicherweise die SIM-Karte, wenn sich mehrere WWAN-Schnittstellen eine SIM-Karte teilen. Daher kann es vorkommen, dass ein anderes Modem für die Kommunikation verwendet wird oder, wenn die SIM-Karte nicht zugewiesen ist, ein Vorgang sogar gestoppt wird.

Hinweis: Modems können sich möglicherweise für das Roaming in fremden Netzen registrieren, in denen möglicherweise andere Gebühren anfallen. Sie können im Abschnitt Mobile SIM manuell ein vorgegebenes Netz zuweisen (per PLMN) (siehe Kapitel [5.3.3](#)).

Ob Mitteilungen versendet werden, hängt stark vom Registrierungszustand des Modems ab und davon, ob der bereitgestellte SMS-Center-Dienst funktioniert - anderenfalls kann der Versand fehlschlagen. Mit dem Ereignis `sms-report-received` lässt sich herausfinden, ob eine Nachricht erfolgreich gesendet wurde.

Empfangene Nachrichten werden von den SIM-Karten kopiert und vorübergehend auf dem Router gespeichert, wo sie aber beim Neustart des Systems gelöscht werden. Ziehen Sie daher in Betracht, ein SDK-Skript zu nutzen, wenn Sie Nachrichten bearbeiten oder kopieren möchten.

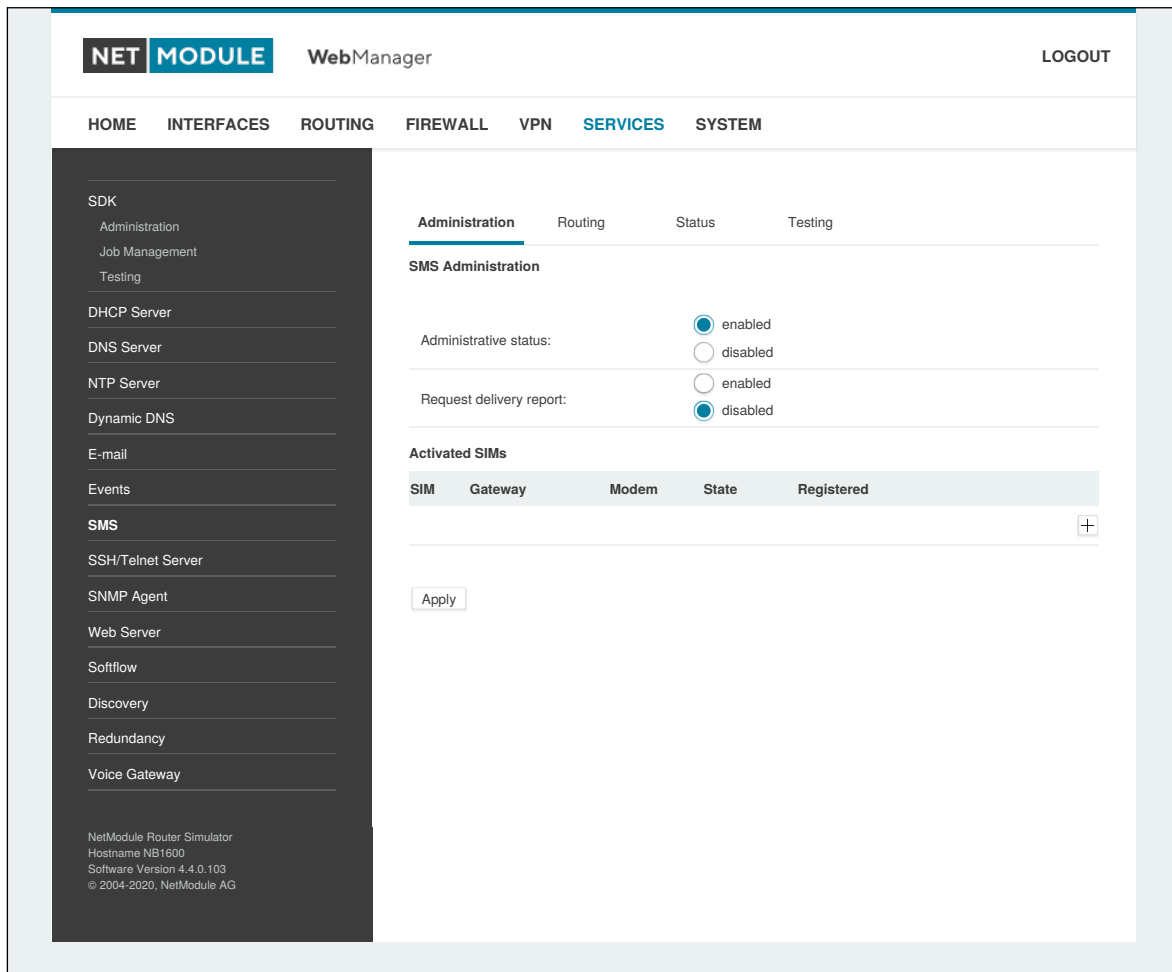


Abbildung 5.47.: SMS-Konfiguration

Auf dieser Seite können Sie den SMS-Dienst aktivieren und festlegen, über welche SIM-Karte er ausgeführt werden soll. SIMs-Karten werden anhand ihrer IMEI-Nummer unterschieden. Ihre Statistiken sind nicht-flüchtige.

| Parameter | SIM-Konfiguration für SMS |
|-------------|--|
| SMS gateway | Nummer des Servicecenters für den Versand von SMS-Kurznachrichten. Sie wird in der Regel automatisch der SIM-Karte entnommen, aber Sie können hier eine andere, feste Nummer definieren. |

Routing und Filtern

Bei SMS-Routing können Sie Regeln festlegen, die immer dann angewendet werden, wenn eine Nachricht gesendet wird. Zum einen können Sie sie an ein freigegebenes Modem weiterleiten. Für eine bestimmte Nummer können Sie z. B. erzwingen, dass Nachrichten über eine spezielle SIM-Karte gesendet werden. Rufnummern können in Form von regulären Ausdrücken angegeben werden. Einige Beispiele:

| Number | Ergebnis |
|-----------|---|
| +12345678 | Eine konkrete Rufnummer |
| +1* | Eine beliebige Rufnummer, beginnend mit +1 |
| +1*9 | Eine beliebige Rufnummer, beginnend mit +1 und endend mit 9 |
| + [12]* | Eine beliebige Rufnummer, beginnend mit +1 oder 2 |

Tabelle 5.112.: Darstellungsweisen von SMS-Rufnummern

Rufnummern müssen im internationalen Format mit gültigem Präfix eingegeben werden.

Darüber hinaus können Sie Regeln definieren, um ausgehende Nachrichten zu verwerfen, z. B. wenn Sie keine teuren Sonderdienste oder Auslandsrufnummern nutzen möchten.

Beide Arten von Regeln bilden eine Liste, die der Reihe nach abgearbeitet wird, wobei ausgehende Nachrichten über das angegebene Modem weitergeleitet oder verworfen werden. Nachrichten, auf die keine der konfigurierten Regeln passt, werden an das erste verfügbare Modem weitergeleitet.

Die Filterfunktion dient als eine Art Firewall, die eingehende Nachrichten entweder verwirft oder zulässt, je nach Modem. Die erstellten Regeln werden der Reihe nach abgearbeitet. Wenn eine Regel passt, wird die eingehende Nachricht entweder verworfen oder weitergeleitet, bevor sie in das System gelangt. Alle Nachrichten, auf die keine der konfigurierten Regeln passt, werden zugelassen.

Status

Auf der Statusseite können Sie den aktuellen Modemstatus abrufen und sich über gesendete oder empfangene Nachrichten informieren. Es steht ein einfacher SMS-Posteingangsläser bereit, mit dem Sie die Nachrichten ansehen oder löschen können. Hinweis: Der Posteingang wird jeweils um Mitternacht gelöscht, wenn er mehr als 512 kB Flash-Speicher nutzt.

SDK-Tests

Auf dieser Seite können Sie testen, ob das Senden von SMS im Allgemeinen oder die Filter-/Routing-Regeln im Besonderen funktionieren. Die maximale Länge pro Nachrichtenteil beträgt 160 Zeichen. Es wird empfohlen, ausschließlich Zeichen aus dem GSM-7-Bit-Alphabet zu verwenden.

5.7.9. SSH-/Telnet-Server

Neben dem Web-Manager können Sie sich auch über die Dienste SSH und Telnet am System anmelden. Gültige Benutzernamen sind *root* und *admin* sowie zusätzliche Benutzer, die im Abschnitt Benutzerkonten erstellt werden können. Hinweis: Eine reguläre System-Shell wird nur für den Benutzer *root* erstellt. Für alle anderen Benutzer wird die CLI gestartet, Während normale Benutzer nur die Statuswerte auslesen können, erhält der Benutzer *admin* die Berechtigung, Änderungen am System vorzunehmen

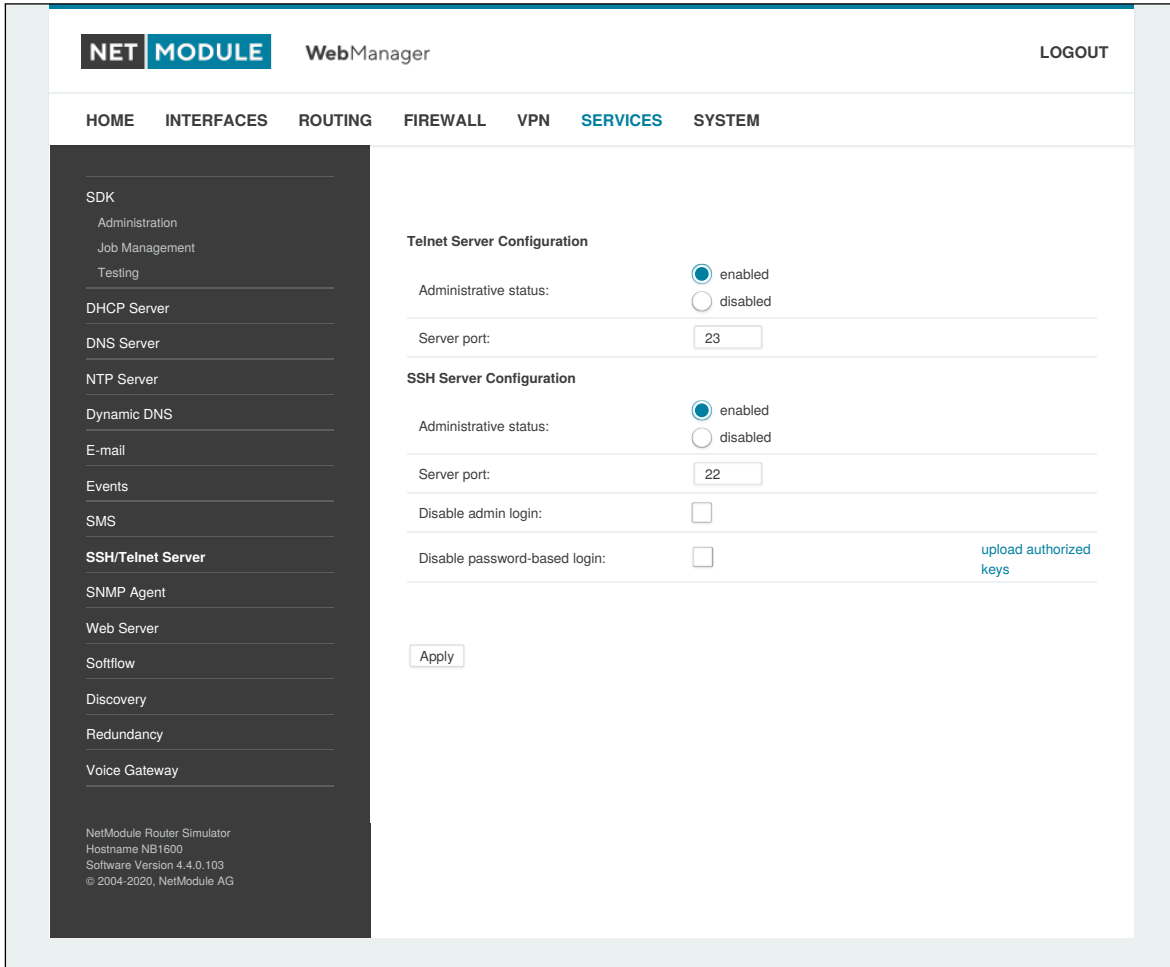


Abbildung 5.48.: SSH- und Telnet-Server

Hinweis: Diese Dienste sind auch über die WAN-Schnittstelle zugänglich. Im Zweifelsfall sollten Sie in Erwägung ziehen, den Zugriff hierauf zu deaktivieren oder einzuschränken, indem Sie entsprechende Firewall-Regeln anwenden.

Die folgenden Parameter stehen zum Einrichten des Telnet-Dienstes zur Verfügung:

| Parameter | Telnet-Server-Einstellungen |
|-----------------------|---|
| Administrative status | Legt fest, ob der Telnet-Dienst aktiviert ist |
| Server port | Der TCP-Port des Dienstes (normalerweise 23) |



Die folgenden Parameter stehen zum Einrichten des SSH-Dienstes zur Verfügung:

| Parameter | SSH-Servereinstellungen |
|------------------------------|--|
| Administrative status | Legt fest, ob der SSH-Dienst aktiviert ist |
| Server port | Der TCP-Port des Dienstes (normalerweise 22) |
| Disable admin login | Anmeldung für Admin-Benutzer deaktivieren |
| Disable password-based login | Wenn diese Einstellung aktiviert ist, müssen sich alle Benutzer mit SSH-Schlüsseln authentifizieren; diese können auf den Router hochgeladen werden. |

5.7.10. SNMP-Agent

NetModule-Router sind mit einem SNMP-Daemon ausgestattet, der grundlegende MIB-Tabellen (z. B. ifTable) sowie zusätzliche Enterprise-MIBs zur Verwaltung mehrerer Systeme unterstützt.

| Parameter | Unterstützte MIBs |
|--------------------------|--|
| .1.3.6.1.2.1 | MIB-II (RFC1213), SNMPv2-MIB (RFC3418) |
| .1.3.6.1.2.1.2.1 | IF-MIB (RFC2863) |
| .1.3.6.1.2.1.4 | IP-MIB (RFC1213) |
| .1.3.6.1.2.1.10.131 | TUNNEL-MIB (RFC4087) |
| .1.3.6.1.2.25 | HOST-RESOURCES-MIB (RFC2790) |
| .1.3.6.1.6.3.10 | SNMP-FRAMEWORK-MIB |
| .1.3.6.1.6.3.11 | SNMPv2-SMI (RFC2578) |
| .1.0.8802.1.1.2 | LLDP-MIB |
| .1.0.8802.1.1.2.1.5.4795 | LLDP-EXT-MED-MIB |
| .1.3.6.1.4.1.31496 | VENDOR-MIB |

Die Hersteller-MIB-Tabellen (VENDOR-MIB) liefern einige zusätzliche Informationen über das System und seine WWAN-, GNSS- und WLAN-Schnittstellen. Auf sie kann über die folgenden OIDs zugegriffen werden:

| Parameter | OID-Zuordnung Hersteller-MIB |
|--------------|------------------------------|
| NBAdminTable | .1.3.6.1.4.1.31496.10.40 |
| NBWwanTable | .1.3.6.1.4.1.31496.10.50 |
| NBGnssTable | .1.3.6.1.4.1.31496.10.51 |
| NBDioTable | .1.3.6.1.4.1.31496.10.53 |
| NBWlanTable | .1.3.6.1.4.1.31496.10.60 |
| NBWanTable | .1.3.6.1.4.1.31496.10.22 |

Sie liefern Ressourcen für die folgenden Aufgaben:

- Gerät neu starten
- Aktualisieren auf eine neue Systemsoftware über FTP/TFTP/HTTP
- Aktualisieren auf eine neue Systemkonfiguration über FTP/TFTP/HTTP
- WWAN/GNSS/WLAN/DIO-Informationen abrufen

Unsere VENDOR-MIB ist im Anhang aufgeführt oder kann direkt vom Router heruntergeladen werden.

SNMP-Konfiguration

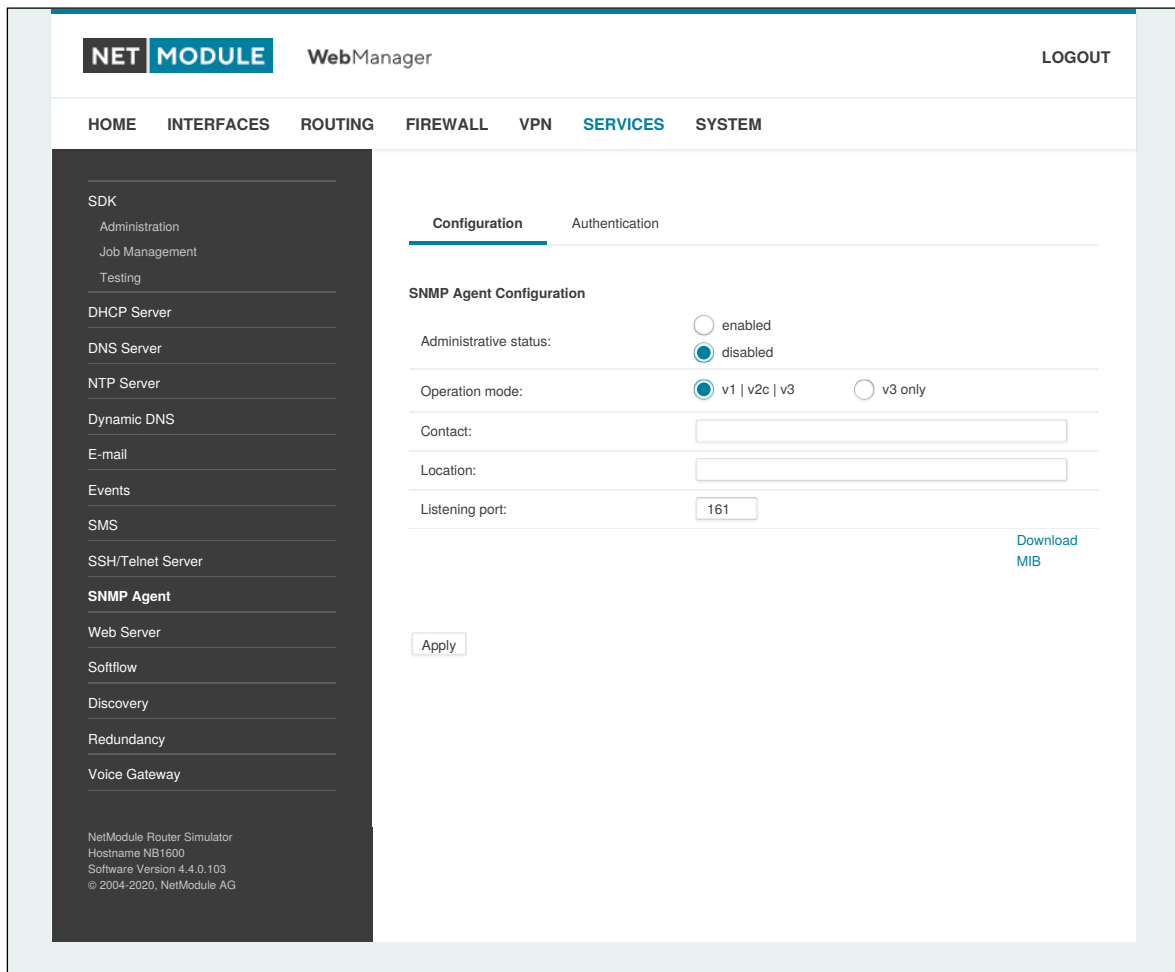


Abbildung 5.49.: SNMP-Agent

Sie können den SMTP-Agenten kann mit den folgenden Parametern konfigurieren:

| Parameter | SNMP-Konfiguration |
|-----------------------|---|
| Administrative status | Legt fest, ob der SNMP-Agent aktiviert ist |
| Operation mode | Legt fest, ob der SMTP-Agent im Kompatibilitätsmodus oder nur für SNMPv3 ausgeführt werden soll |
| Contact | Systembetreuer oder andere Kontaktinformationen |
| Location | Standort des Geräts |
| Listening Port | SNMP-Agent-Anschluss |

Sobald der SNMP-Agent aktiviert ist, können mit SDK-Skripten SNMP-Traps erzeugt werden.

SNMP-Authentifizierung

Beim Betrieb unter SNMPv3 können die folgenden Authentifizierungseinstellungen konfiguriert werden:

| Parameter | SNMPv3-Authentifizierung |
|----------------|--|
| Authentication | Definiert die Authentifizierung (MD5 oder SHA) |
| Encryption | Definiert die zu verwendenden Datenschutzprotokolle (DES oder AES) |

Generell kann der Admin-Benutzer beliebige Werte lesen und schreiben. Allen anderen Systembenutzern wird ein Lesezugriff gewährt.

Auf Grund der Verwendung von passwortbasierter Authentifizierung im SNMP-Standard muss das Passwort eines Anwenders, der sich gegen den SNMP-Server mit seinem Passwort authentifizieren können soll, auf dem Gerät gespeichert werden. Für mehr Informationen zu dem Thema schauen Sie bitte in Kapitel [5.8.2](#).

Es gibt keine Authentifizierung/Verschlüsselung unter SNMPv1/v2c: dies sollte nicht verwendet werden, um irgendwelche Werte zu setzen. Es ist jedoch möglich, Communities und autorisierte Hosts zu definieren, denen administrativer Zugriff gewährt wird.

| Parameter | SNMPv1/v2c-Authentifizierung |
|-----------------|--|
| Read community | Legt den Community-Namen für den Lesezugriff fest |
| Admin community | Legt den Community-Namen für den Admin-Zugang fest |
| Allowed host | Legt den Host fest, von dem der Admin-Zugriff zugelassen ist |

Hinweis: SNMP-Passwörter müssen länger als 8 Zeichen sein. Kürzere Passwörter werden für SNMP verdoppelt (z. B. admin01 wird zu admin01admin01).

Hinweis: Der SNMP-Daemon fragt auch WAN-Schnittstellen an. Es wird daher empfohlen, den Zugriff über die Firewall zu beschränken.

Typische SNMP-Befehle

Das Festlegen von MIB-Werten und das Starten von Erweiterungen ist im Allgemeinen auf den SNMPv3-Administrator beschränkt. Es ist möglich, einen administrativen Host für SNMP v1/2c anzugeben.

Die SNMP-Erweiterungen können wie folgt gelesen und gestartet werden:

Softwareversion des Systems ermitteln:

```
snmpget -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.1.0
```

Kernelversion ermitteln:

```
snmpget -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1
```



1.3.6.1.4.1.31496.10.40.2.0

Seriennummer ermitteln:

```
snmpget -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.3.0
```

Aktuelle Konfigurationsbeschreibung abrufen:

```
snmpget -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.4.0
```

Aktuellen Konfigurations-Hash ermitteln:

```
snmpget -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.5.0
```

Gerät neu starten:

```
snmpset -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.10.0 i 1
```

Konfigurations-Update vornehmen:

```
snmpset -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.11.0 s „http://<Server>/<Verzeichnis>“
```

Sie können TFTP-, HTTP-, HTTPS- und FTP-URLs verwenden (die Angabe eines Benutzernamens/Passworts oder eines Ports wird noch nicht unterstützt).

Bitte beachten Sie, dass Konfigurations-Updates eine Zip-Datei mit dem Namen <Seriennummer>.zip im angegebenen Verzeichnis erwarten.

Status des Konfigurations-Updates abrufen:

```
snmpget -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.12.0
```

Der Rückgabewert kann einer der folgenden sein: succeeded (1), failed (2), inprogress (3), notstarted (4).

Software-Updates vornehmen:

```
snmpset -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.13.0 s „http://<Server>/<Verzeichnis>“
```

Status des Software-Updates abrufen:

```
snmpget -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.14.0
```

Der Rückgabewert kann einer der folgenden sein: succeeded (1), failed (2), inprogress (3), notstarted (4).

Update-Vorgang definieren:

```
snmpset -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.15.0 i 1
```



Standardmäßig ist der Update-Vorgang auf `update (0)` voreingestellt, was nach dem Auslösen zu einer sofortigen Aktualisierung der Software oder Konfiguration führt. Als Vorgang kann auch `store (1)` angegeben werden, wobei dann nur die Software oder das Konfigurationspaket gespeichert wird. Sie kann später mit den folgenden Argumenten aktiviert werden.



Umstellung auf alternative Software:

```
snmpset -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.16.0 i 0
```

Der Rückgabewert kann aus dem Status des Software-Updates abgeleitet werden.

Wechseln zu alternativer Konfiguration:

```
snmpset -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.16.0 i 1
```

Der Rückgabewert kann aus dem Status des Konfigurations-Updates abgeleitet werden.

Aktuelle Konfigurationsbeschreibung abrufen:

```
snmpget -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.17.0
```

Aktuellen Konfigurations-Hash ermitteln:

```
snmpget -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.18.0
```

Version der alternativen Software ermitteln:

```
snmpget -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.19.0
```

Versions-Hash der alternativen Software ermitteln:

```
snmpget -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.20.0
```

Digitales OUT1 einstellen:

```
snmpset -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
.1.3.6.1.4.1.31496.10.53.10.0 i 0  
snmpset -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
.1.3.6.1.4.1.31496.10.53.10.0 i 1
```

Digitales OUT2 einstellen:

```
snmpset -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
.1.3.6.1.4.1.31496.10.53.11.0 i 0  
snmpset -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
.1.3.6.1.4.1.31496.10.53.11.0 i 1
```

Gefundenes Gerät auflisten:

```
snmpget -v 3 -u admin -n -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
.1.0.8802.1.1
```

5.7.11. Let's Encrypt

Dieser Dienst erlaubt es, TLS-Zertifikate für den Web-Server des Routers automatisch über die PKI des Anbieters Let's Encrypt zu erzeugen. Wenn HTTPS eingeschaltet ist, wird das Web-Interface automatisch das Zertifikat von Let's Encrypt verwenden, wenn dieser Dienst eingeschaltet ist. Stellen Sie dazu sicher, dass die folgenden Voraussetzungen erfüllt werden:

- HTTP und HTTPS müssen für den Web-Server eingeschaltet sein und auf den Standard-Ports 80 und 443 laufen.
- Der Router muss über das Internet über den eingestellten Domain-Namen erreichbar sein.

Sobald Let's Encrypt eingeschaltet ist, wird automatisch eine Zertifikatsanfrage für die konfigurierte Domain an den Anbieter gestellt. Außerdem wird einmal pro Tag geprüft, ob das Zertifikat erneuert werden sollte und falls erforderlich ein Zertifikatsupdate durchgeführt.

| Parameter | Let's Encrypt Einstellungen |
|------------------------------|--|
| Enable | Schaltet den Dienst ein oder aus |
| Domain | Domain für die ein Zertifikat angefordert werden soll |
| Certificate state | Zeigt an, ob ein Zertifikat installiert ist |
| Certificate valid not before | Zeitpunkt ab dem das installierte Zertifikat gültig ist |
| Certificate valid not after | Zeitpunkt zu dem das installierte Zertifikat abläuft |
| Renew Certificate | Erlaubt es, das Zertifikatsupdate manuell zu starten. Bitte beachten Sie, dass dies nur möglich ist, wenn ein Zertifikatsupdate ansteht. |
| Delete Certificate | Löscht das installierte Zertifikat. Dies ist nur möglich, wenn der Let's Encrypt Dienst abgeschaltet ist. |

Zur Fehleranalyse kann das Kommando `tail-scripts` im CLI verwendet werden, das den Log des verwendeten ACME-Client enthält. Außerdem findet sich der Log der letzten Zertifikatsanfrage in folgender Datei:

```
/etc/acme/<DOMAIN>/issue.log
```

5.7.12. Webserver

Auf dieser Seite können Sie verschiedene Ports für den Zugriff auf den Web Manager über HTTP/HTTPS konfigurieren. Wir empfehlen dringend, beim Zugriff auf den Webserver über eine WAN-Schnittstelle HTTPS zu verwenden, da die Kommunikation verschlüsselt erfolgt und somit ein Missbrauch des Systems vermieden wird.

Um HTTPS zu aktivieren, müssten Sie im Abschnitt 5.8.8 ein Serverzertifikat hochladen.

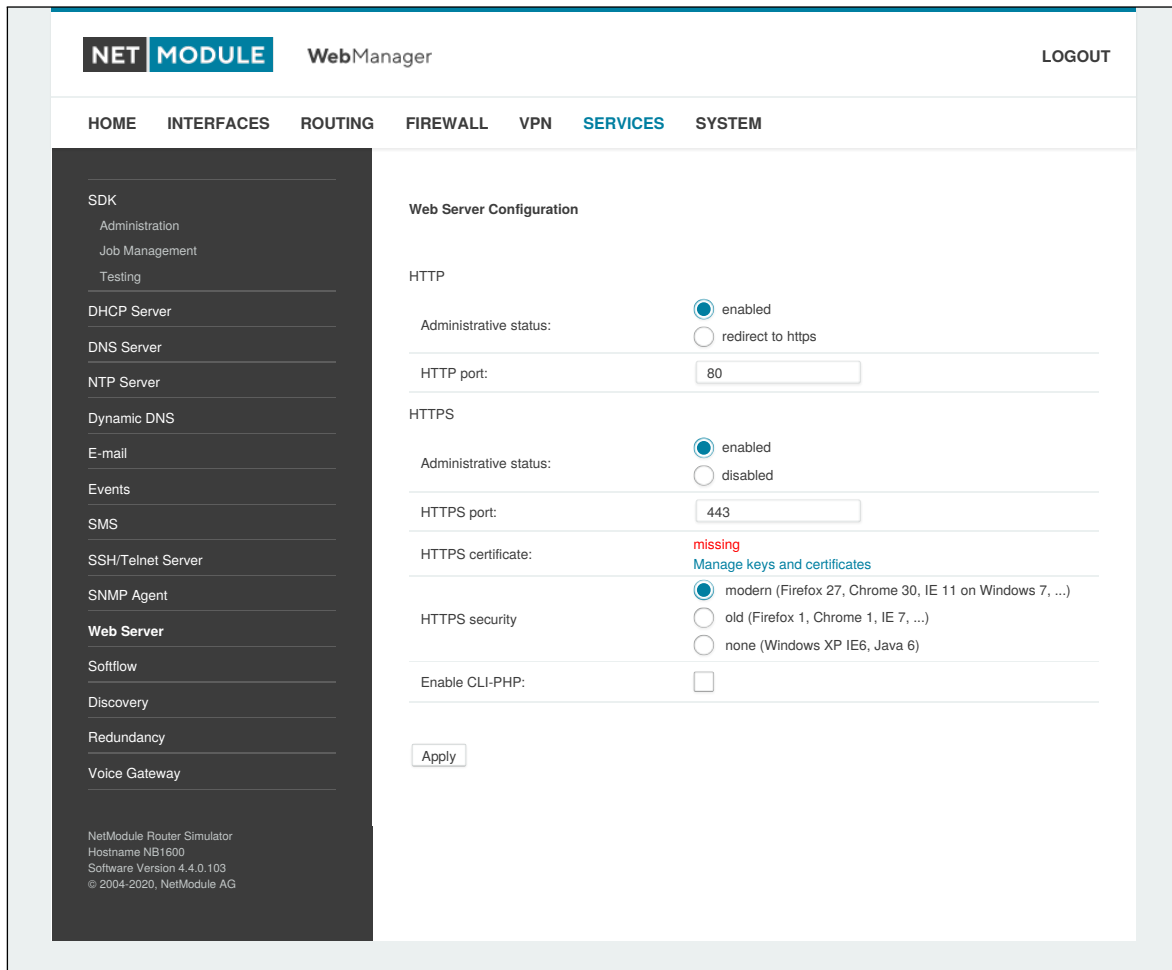


Abbildung 5.50.: Webserver

| Parameter | Webserver-Einstellungen |
|-----------------------|---|
| Administrative Status | Legt fest, ob der Webserver aktiviert ist |
| HTTP port | Webserver-Port für HTTP-Verbindungen |
| HTTPS port | Webserver-Port für HTTPS-Verbindungen |
| Enable CLI-PHP | Aktiviert den CLI-PHP-Dienst (siehe Kapitel ??) |

5.7.13. MQTT Broker

Mit dem MQTT Broker können MQTT-Nachrichten zwischen MQTT-Clients verteilt werden. Richten Sie dazu passende Firewall-Regeln ein, wenn Sie den Zugriff auf den MQTT-Broker einschränken möchten.

Schlüssel und Zertifikate für die TLS-Verschlüsselung werden über Schlüssel und Zertifikate verwaltet (siehe Kapitel [5.8.8](#)).

Der MQTT-Broker-Dienst kann die folgenden Parameter verarbeiten:

| Parameter | Einstellungen für den MQTT Broker |
|-----------------------|--|
| Administrative Status | Legt fest, ob der Dienst aktiviert ist |
| Port | Legt den Netzwerkport fest, auf dem Daten erwartet werden |
| TLS Encryption | Legt fest, ob die TLS-Verschlüsselung für den Dienst aktiviert ist |

5.7.14. Softflow

Auf dieser Seite können Sie den Daemon für die Netzverkehrsanalyse (softflowd) konfiguriert werden, der für den Export von NetFlow-Verkehrsdaten verwendet wird.

| Parameter | Softflow-Einstellungen |
|------------------|--|
| Interface | Schnittstelle, auf der Verkehr erwartet werden soll |
| Host Address | Zieladresse der Verkehrsdaten |
| Port | Port der Zieladresse |
| Protocol Version | Protokollversion der Daten |
| Maximum Flows | Die maximale Anzahl der gleichzeitig zu verfolgenden Verkehrsdaten |
| Track Level | Flow-Elemente, die zur Definition eines Flows verwendet werden |
| Sample Rate | Zeitintervall für die regelmäßige Datenerhebung |

5.7.15. Discovery (Erkennungsprotokolle)

Auf dieser Seite können Sie Erkennungsprotokolle aktivieren, mit denen Sie andere Hosts erkennen und von diesen erkannt werden können.

| Parameter | Erkennungskonfiguration |
|-----------------------|--|
| Administrative status | Der aktuelle Verwaltungsstatus |
| Enabled protocols | Liste der aktivierten Erkennungsprotokolle |

Die folgenden Protokolle werden unterstützt:

| Parameter | Erkennungskonfiguration |
|-----------|---------------------------------|
| LLDP | Link-Layer-Erkennungsprotokoll |
| CDP | Cisco-Erkennungsprotokoll |
| FDP | Foundry-Erkennungsprotokoll |
| SONMP | Nortel-Erkennungsprotokoll |
| EDP | Extreme-Erkennungsprotokoll |
| IRDP | ICMP-Router-Erkennungsprotokoll |

IRDP implementiert RFC1256 und kann auch lokal verbundene Hosts über das Nexthop-Gateway informieren. Alle erkannten Hosts durchlaufen LLDP-MIB und können über SNMP oder CLI/GUI abgefragt werden.

5.7.16. Redundanz (VRRP)

Auf dieser Seite können Sie ein redundantes Paar von NetModule-Routern (oder anderen Systemen) einrichten, die untereinander das Virtual Router Redundancy Protocol (VRRP) ausführen. Ein typisches VRRP-Szenario definiert einen ersten Host in der Rolle des Masters und einen weiteren in der Rolle des Backup-Geräts. Beide definieren eine virtuelle Gateway-IP-Adresse, die über Gratuitous-ARP-Nachrichten bekanntgegeben wird, um den ARP-Cache aller LAN-Hosts zu aktualisieren und so die Pakete entsprechend umzuleiten.

Eine Übernahme erfolgt innerhalb von ca. 3 Sekunden, sobald der Partner nicht mehr erreichbar ist (geprüft über Multicast-Pakete). Dies kann passieren, wenn ein Gerät neu gestartet wird oder die Ethernet-Verbindung ausgefallen ist. Dasselbe gilt, wenn die WAN-Verbindung ausfällt.

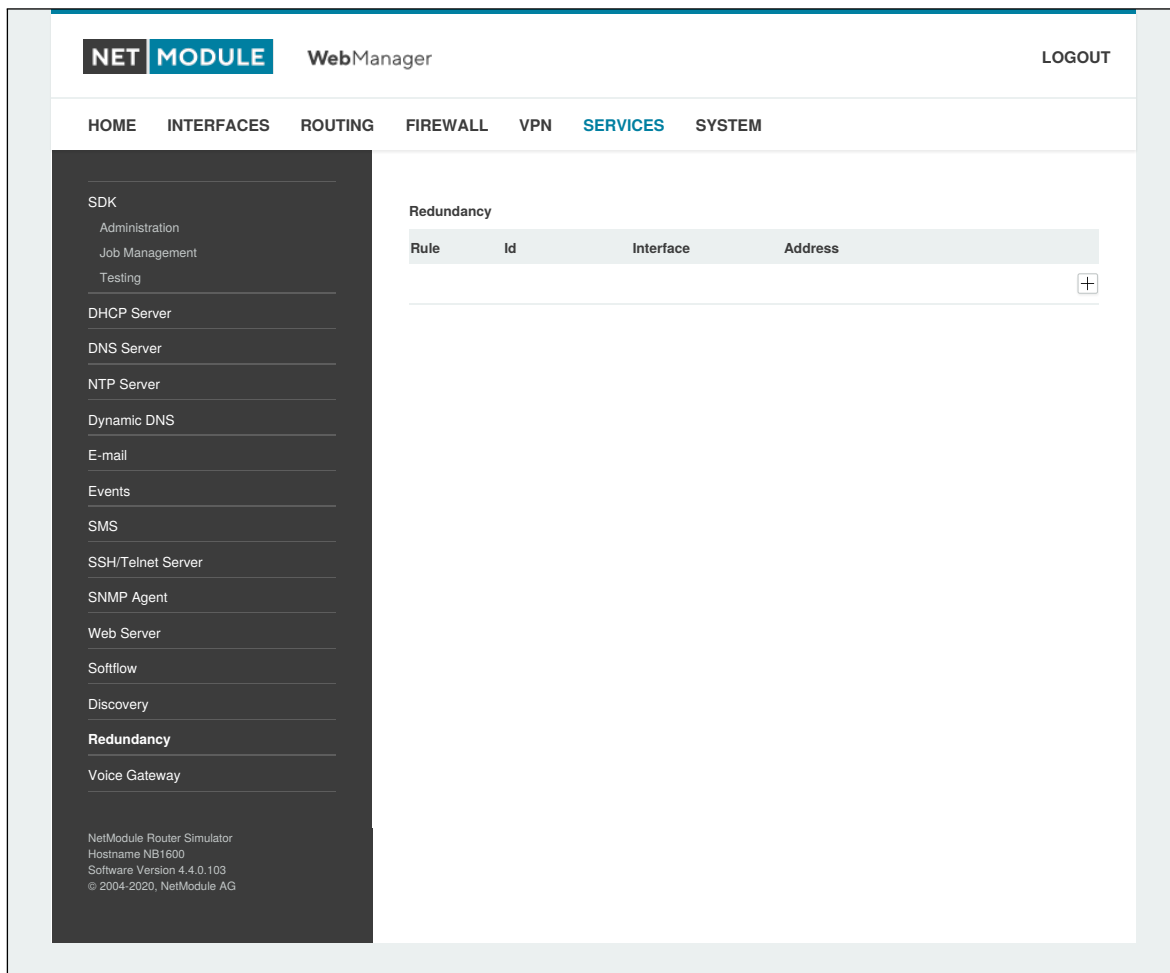


Abbildung 5.51.: VRRP-Konfiguration

Falls DHCP aktiviert wurde, muss die vom Server angebotene DHCP-Gateway-Adresse neu konfiguriert werden und auf die virtuelle Gateway-Adresse zeigen. Um Konflikte zu vermeiden, können Sie DHCP auf dem Backup-Gerät ausschalten oder - noch besser - den DHCP-Vergabebereich auf beide Router aufteilen, um eine doppelte Vergabe zu verhindern.



| Parameter | Redundanzkonfiguration |
|-------------------------|---|
| Administrative status | Der aktuelle Verwaltungsstatus |
| Role | Die zugewiesene Rolle dieses Systems (Master oder Backup) |
| VID | Die ID des virtuellen Routers (es können theoretisch mehrere Instanzen ausgeführt werden) |
| Interface | Schnittstelle, auf der VRRP ausgeführt werden soll |
| Virtual gateway address | Die von den beteiligten Hosts gebildete virtuelle Gateway-Adresse |

Vergeben wird eine Priorität von 100 für den Master und 1 für den Backup-Router. Bitte passen Sie die Priorität Ihres Drittanbietergeräts entsprechend an.

5.7.17. ITxPT

Dies ist eine Integration des ITxPT-Standards v2.0.1. (siehe [ITxPT Onboard Architecture Specifications v2.0.1](#))

Konfiguration

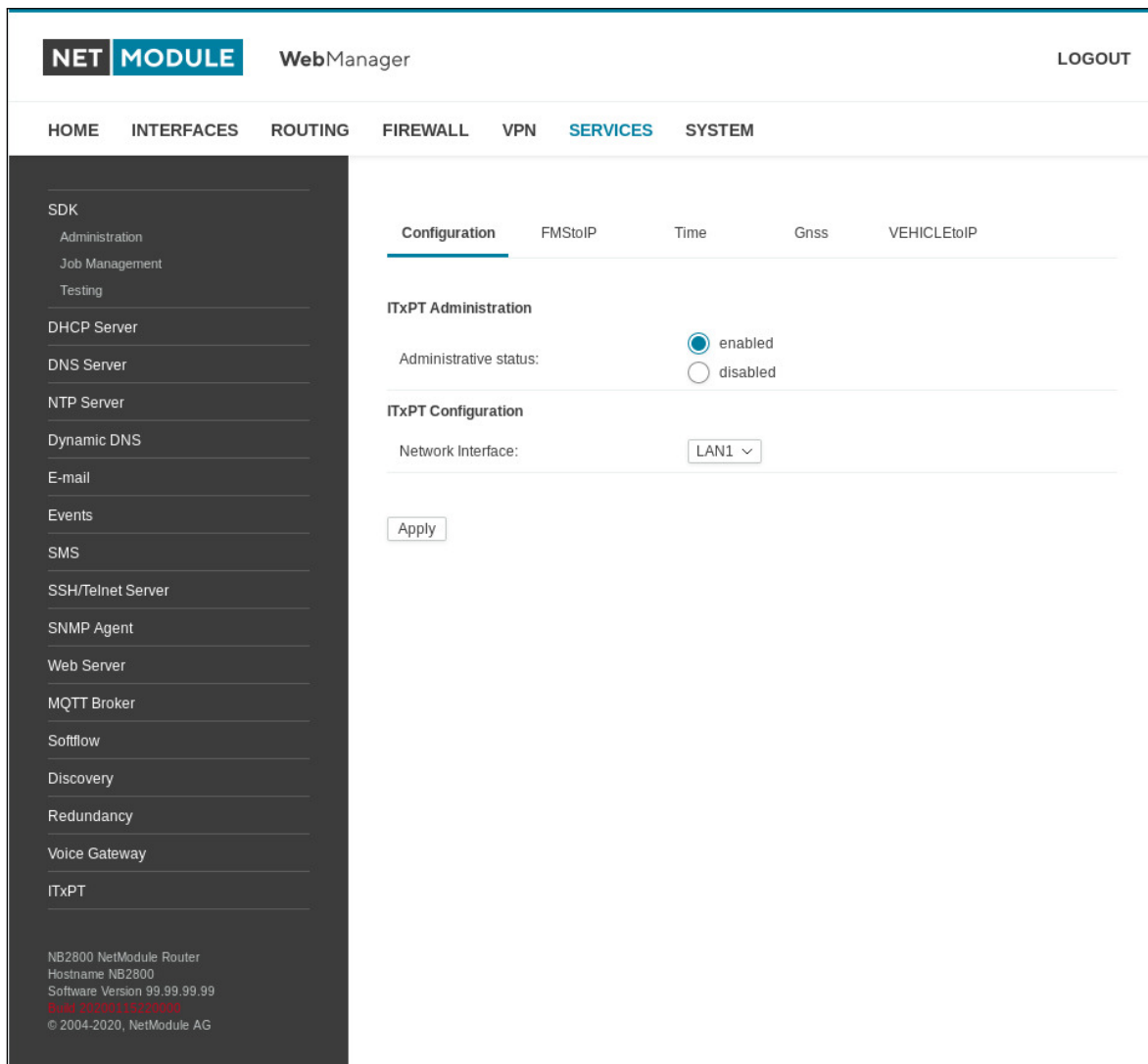


Abbildung 5.52.: ITxPT-Konfiguration

Die folgenden Parameter stehen zum Einrichten zur Verfügung:

| Parameter | ITxPT-Administration |
|-----------------------|--|
| Administrative status | Legt fest, ob die ITxPT-Funktion aktiviert ist. |
| Network Interface | Legt die Netzwerkschnittstelle fest, auf der der Dienst ausgeführt wird. |

Hinweise:

FMS-to-IP

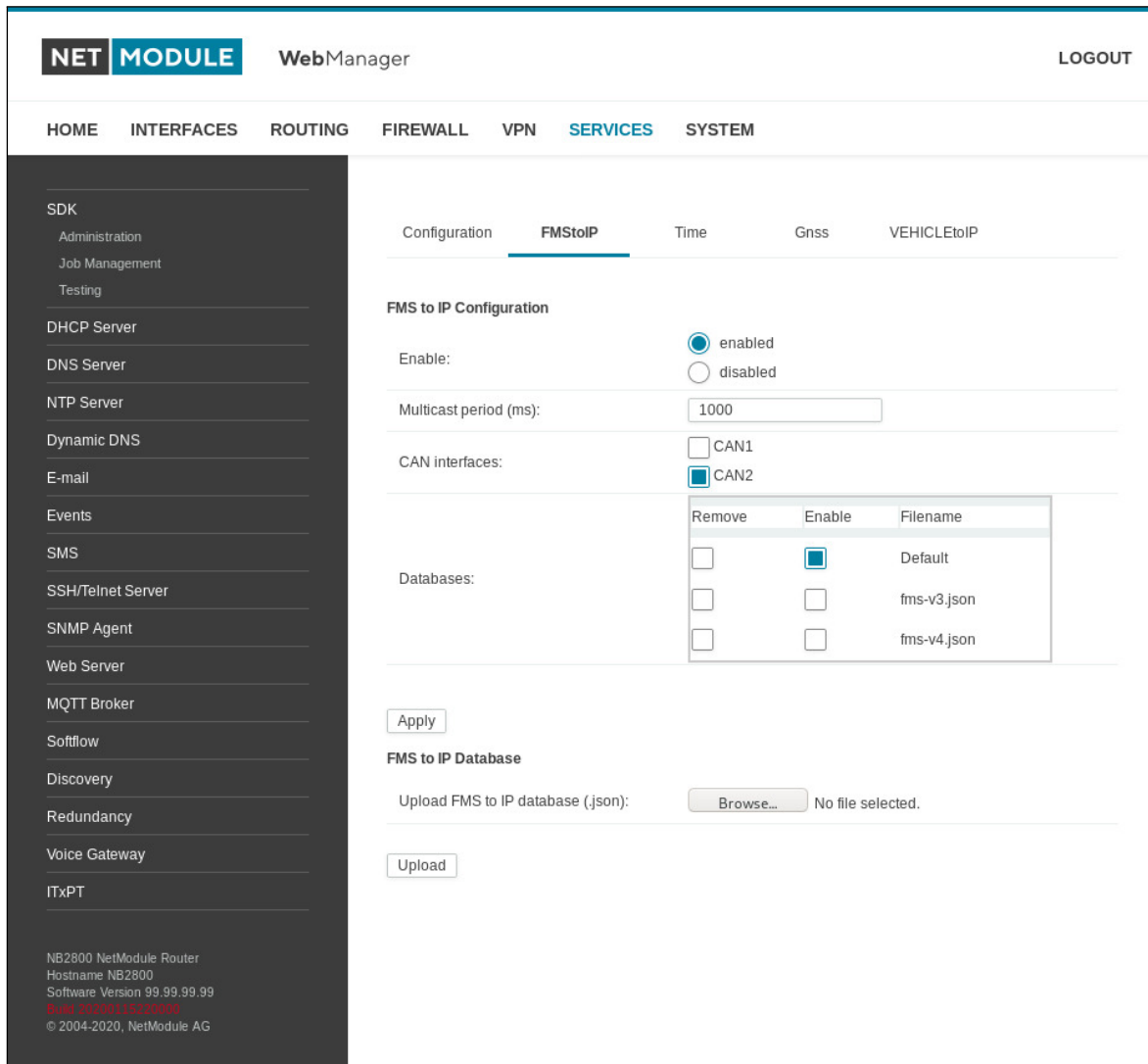


Abbildung 5.53.: ITxPT FMS-to-IP

Auf dieser Seite können Sie FMS-to-IP konfigurieren.

| Parameter | Einstellungen für FMS-to-IP |
|------------------|--|
| Enable | Legt fest, ob FMS-zu-IP aktiviert ist. |
| Multicast period | Legt fest, wie häufig FMS-to-IP-Multicasts gesendet werden. Ein Wert von Null leitet eingehende CAN-Nachrichten sofort um. |
| CAN interfaces | Legt die CAN-Schnittstellen fest, deren Daten verarbeitet werden sollen (Mehrfachauswahl). |
| Databases | Legt die FMS-to-IP-Datenbanken aus, die zur Verarbeitung der CAN-Daten verwendet werden (Mehrfachauswahl). |

FMS-to-IP-Datenbankformat

Es wird das json-Dateiformat verwendet. Die Datenbankdatei beschreibt die eingehenden Datenpakete. Es gibt zwei grundlegende Elemente, die die im FMS-Standard verwendeten Signale beschreiben: die Parameter Group Number (PGN) und die Suspect Parameter Number (SPN). Die PGN besteht aus einem oder mehreren Signalen. Die SPN wird verwendet, um einem Signal einen eindeutigen Bezeichner zu geben. Weitere Informationen finden Sie in der Norm SAE-J1939.

```
[
  {
    "name" : "EBFF",
    "pgn" : 60415,
    "length" : 8,
    "spns" : []
  },
  {
    "name" : "CCVS",
    "pgn" : 65265,
    "length" : 8,
    "spns" :
    [
      {
        "byteSize" : 2,
        "offset" : 1,
        "formatGain" : 0.00390625,
        "formatOffset" : 0,
        "units" : "km/h",
        "name" : "Radgeschwindigkeit",
        "number" : 84,
        "type" : 0
      },
      {
        "bitSize" : 2,
        "bitOffset" : 4,
        "offset" : 3,
        "descriptions" :
        [
          "Pedal oben",
          "Pedal unten"
        ],
        "name" : "Bremsschalter",
        "number" : 597,
        "type" : 1
      }
    ]
  }
]
```


Die Struktur der obersten Ebene ist ein Array. Es enthält PGN-Objekte, die ein PGN mit den folgenden Typen definieren:

PGN-Definition

| Parameter | PGN-Definition |
|-----------|---------------------------------|
| name | Name des PGN. |
| pgn | Die PGN-Nummer als Dezimalzahl. |
| length | Länge der CAN-Nachricht. |
| spns | Array mit SPN-Objekten. |

Das Array spns kann leer bleiben, wenn keine Dekodierung erforderlich ist.

SPN-Definition

Die SPN sind in drei Typen unterteilt: numerisch, Status und String.

| Parameter | Numerische SPN |
|--------------|---|
| byteSize | Umfang der Daten in Byte. |
| offset | Der Offset in den CAN-Daten. |
| formatGain | Der numerische Faktor, der verwendet wird, um den Wert zu erhalten. |
| formatOffset | Der numerische Offset des Wertes. |
| units | Die physikalische Einheit des Wertes. |
| name | Der Name des SPN. |
| number | Die SPN-Nummer. |
| type | 0 -> Numerische SPN. |

| Parameter | Status-SPN |
|--------------|--|
| bitSize | Umfang der Daten in Bit. |
| bitOffset | Der Offset in Bits im Byte. |
| offset | Der Offset in Byte. |
| descriptions | Array, das die Statusbeschreibung enthält. |
| name | Der Name des SPN. |
| number | Die SPN-Nummer. |
| type | 1 -> Status-SPN. |

| Parameter | String-SPN |
|-----------|-------------------|
| name | Der Name des SPN. |
| number | Die SPN-Nummer. |
| type | 2 -> String-SPN. |

ITxPT GNSS

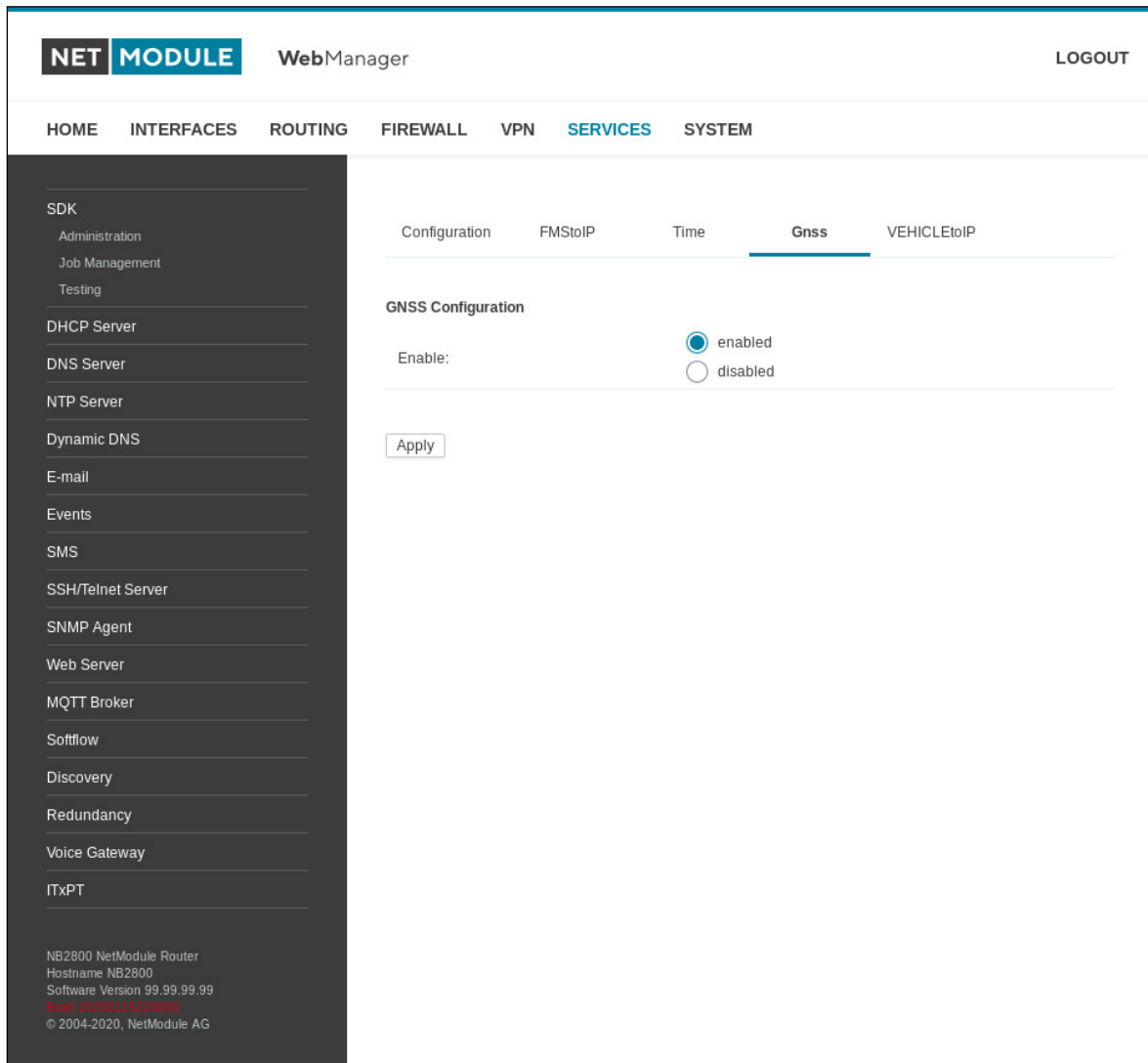


Abbildung 5.54.: ITxPT GNSS

| Parameter | ITxPT GNSS |
|-----------|---|
| Enable | Legt fest, ob der ITxPT GNSS aktiviert ist. |

ITxPT Time

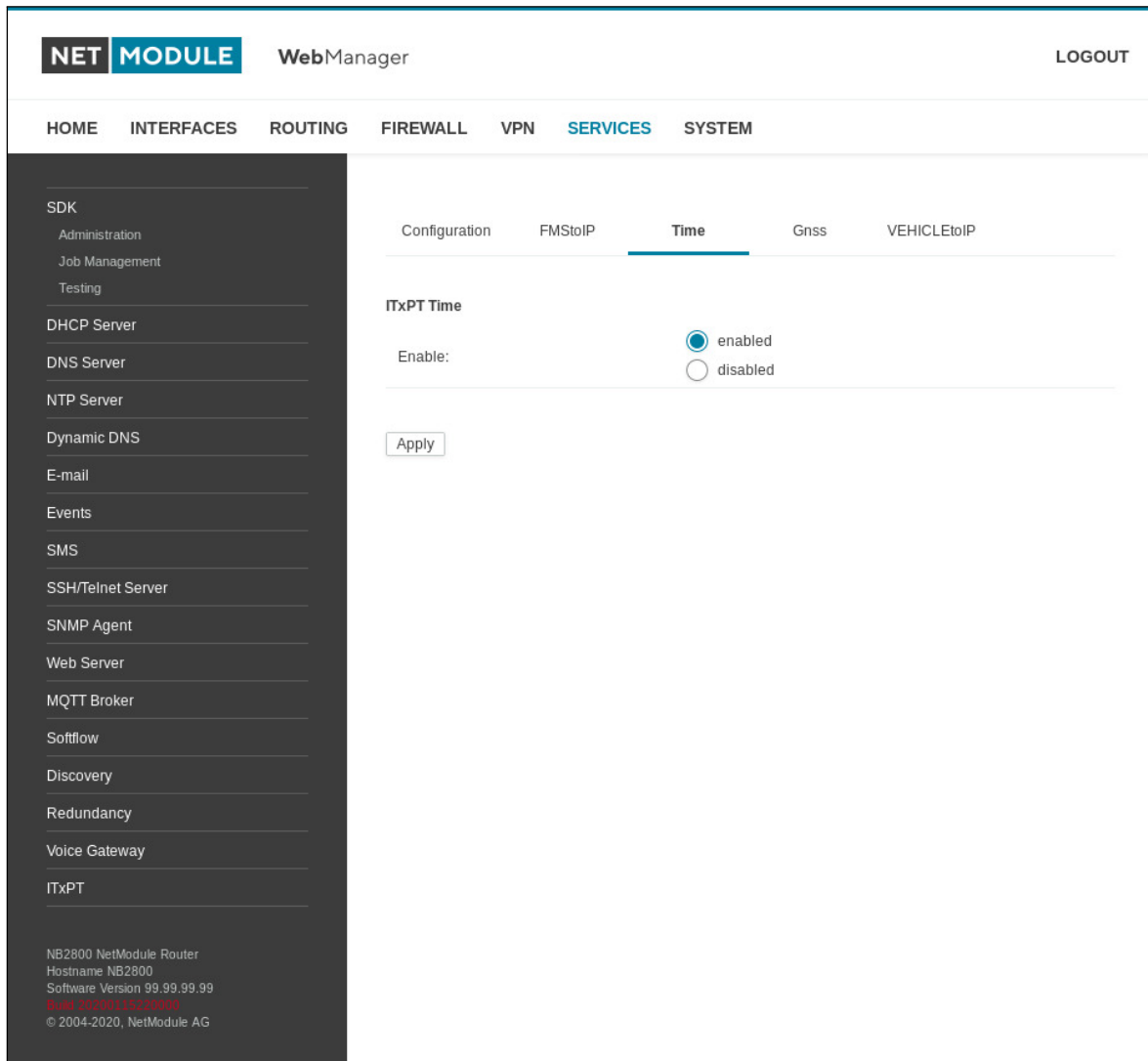


Abbildung 5.55.: ITxPT Time

| Parameter | ITxPT Time |
|-----------|---|
| Enable | Legt fest, ob der ITxPT Time aktiviert ist. |

Vehicle-to-IP

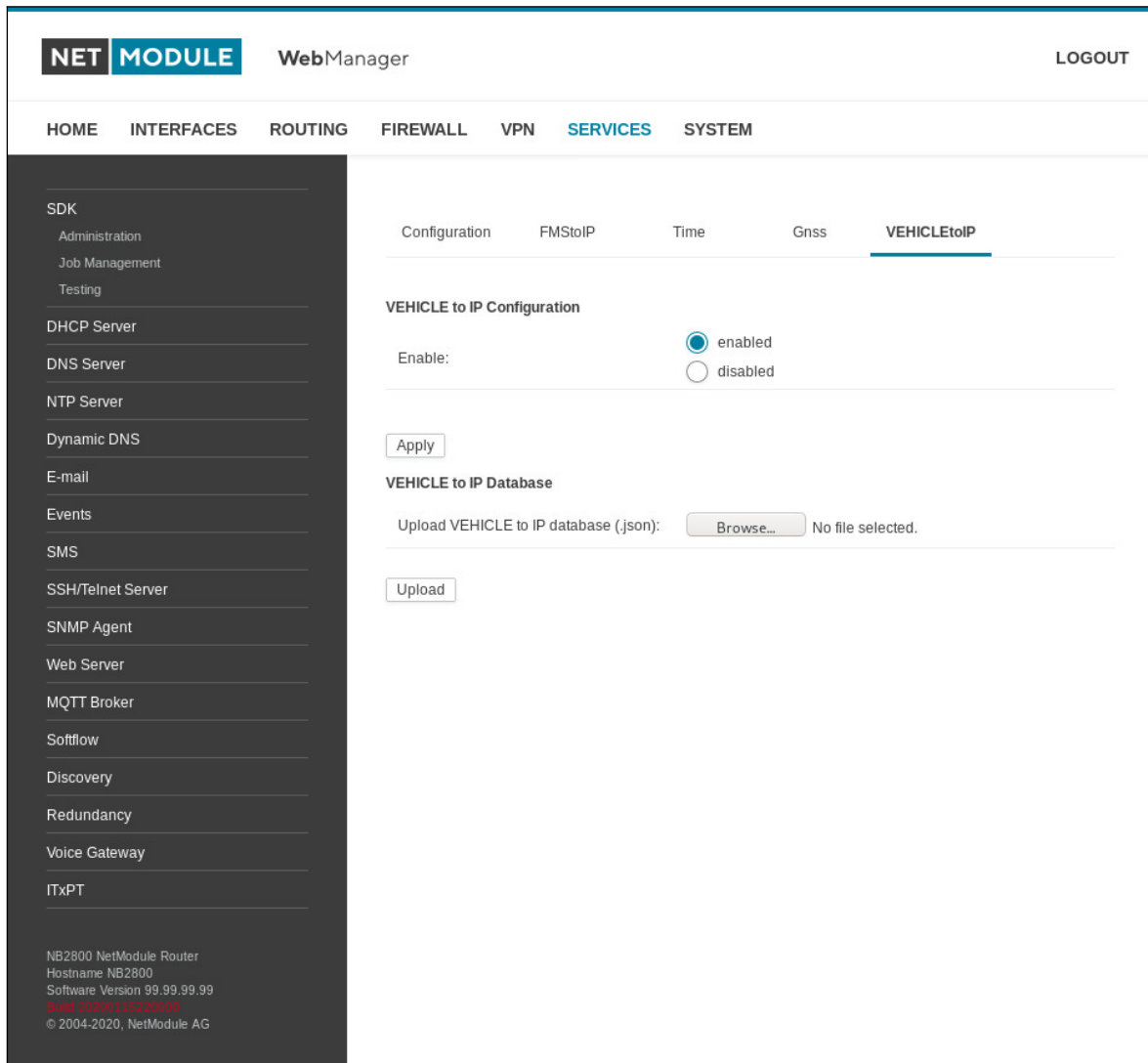


Abbildung 5.56.: ITxPT VEHICLEtoIP

| Parameter | ITxPT VEHICLEtoIP |
|-----------|---|
| Enable | Legt fest, ob ITxPT Vehicle-to-IP aktiviert ist. Um diesen Dienst zu aktivieren, ist eine Vehicle-to-IP-Datenbank erforderlich. |

5.7.18. Voice-Gateway

Wenn die Hardware dies unterstützt, können Sie auf dem Router ein Voice-Gateway einrichten, über das Sie in beiden Richtungen Mobilfunkgespräche mit VoIP-Clients führen können.

Verwaltung

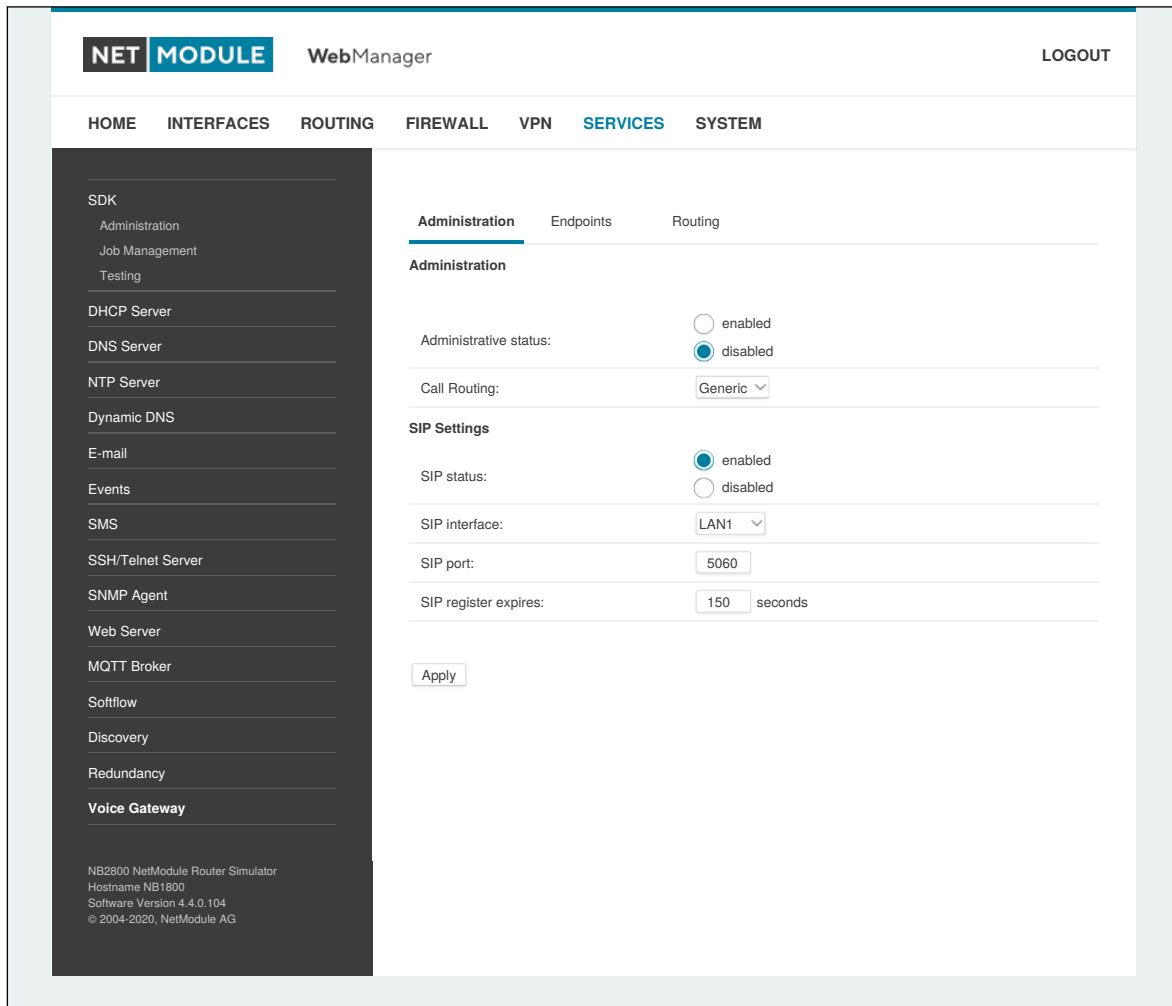


Abbildung 5.57.: Verwaltung des Voice-Gateways

Die folgenden Parameter stehen zum Einrichten zur Verfügung:

| Parameter | Verwaltungseinstellungen für das Voice-Gateway |
|-----------------------|---|
| Administrative status | Legt fest, ob das Gateway aktiviert ist |
| Call routing | Legt fest, wer für das Routing zuständig ist. Wenn hier SDK angegeben wurde, müssten Sie ein Skript installieren (siehe Beispiele), das für das Routing und die Annahme der Anrufe zuständig ist. Andernfalls wird die statische Routing-Konfiguration verwendet. |
| SIP status | Legt fest, ob der SIP-Agent aktiviert ist |

| Parameter | Verwaltungseinstellungen für das Voice-Gateway |
|----------------------|--|
| SIP interface | Legt die Schnittstelle (LAN oder WAN) fest, auf der der SIP-Agent eingehende Anrufe erwartet |
| SIP port | Legt den Port fest, auf dem der SIP-Agent eingehende Anrufe erwartet |
| SIP register expires | Legt das Registrierungsintervall in Sekunden fest |

Falls Sie mehrere WWAN-Schnittstellen betreiben, die sich eine SIM-Karte teilen, beachten Sie, dass das System während des Betriebs die SIM-Karte wechseln kann, was auch zu unterschiedlichen Einstellungen für die Sprachkommunikation führt.

Voice-Endpunkte

Auf dieser Seite können Sie die für die Sprachkommunikation verwendeten Endpunkte aktivieren. Die folgenden Typen werden unterstützt:

| Parameter | Typen von Voice-Endpunkten |
|-------------------|--|
| Voice-Over-Mobile | Endpunkt für GSM/UMTS/LTE-Anrufe (kann für Anrufe zu Mobil- oder Festnetztelefonen verwendet werden) |
| SIP (registrar) | SIP-Endpunkt, der ein bei unserem Registrar registrierter Client sein kann |
| SIP (direct) | Endpunkt für Anrufe, die ohne Registrierung direkt an einen SIP-Agenten weitergeleitet werden |
| SIP (user-agent) | Endpunkt, der als SIP-Benutzeragent gegenüber einem entfernten Registrar agiert |

Je nach Hardware empfehlen wir, das Audioprofil des Modems anzupassen, um ein besseres Klangergebnis zu erzielen. Folgende Optionen stehen zur Verfügung:

| Parameter | Voice-Over-Mobil-Audioprofile |
|-----------|---|
| Handset | Ergibt ein leichtes Echo mit kurzer Verzögerung (unter 16 ms Dispersion). Dieser Modus ist für die Verwendung mit einem günstig gestalteten Mobilteil vorgesehen, bei dem die Echorückflusssdämpfung (Echo Return Loss, ERL) im Allgemeinen hoch ist. Vollduplex-Leistung ist in diesem Modus am einfachsten zu erreichen. |

| Parameter | Voice-Over-Mobil-Audioprofile |
|--------------|--|
| Headset | <p>Ergibt ein moderates Echo mit kurzer Verzögerung (unter 16 ms Dispersion).</p> <p>Dieser Modus ist für den Einsatz in Situationen gedacht, in denen das Echo laut, aber verzögerungsarm sein Es gibt eine Vielzahl von Headsets mit einer Vielzahl von Echo- und Rauschunterdrückungseigenschaften. Obwohl die Echoverzögerung bei allen Headsets typischerweise kurz ist (unter 16 ms), können die Eigenschaften der Echorückflussdämpfung erheblich variieren; sie können dem Entwickler des Mobilteils nicht im Voraus bekannt sein.</p> <p>Dieser Modus ist robuster und aggressiver bei der Echounterdrückung.</p> |
| Speakerphone | <p>Bewältigt Situationen mit lautem Echo und extremer akustischer Verzerrung.</p> <p>Dieser Modus ist für die Verwendung mit einem Fahrzeugkit oder für Freisprechanwendungen mit hoher Lautstärke und hohen Verzerrungen vorgesehen. Das akustische Echo hat in dieser Situation eine negative Echorückflussdämpfung und kann nicht vollständig gelöscht werden. Er arbeitet im Halbduplex-Verfahren und schaltet das gesamte Signal sehr aggressiv stumm, um zu verhindern, dass Echo-signale zu hören sind.</p> |
| Bluetooth | <p>Ergibt ein moderates Echo mit langer Verzögerung (über 64 ms Dispersion).</p> <p>Dieser Modus ist für Bluetooth-Headsets und Fahrzeugkits vorgesehen, die möglicherweise eine digitale Signalverarbeitung vornehmen, was zusätzliche Verzögerungen bewirken könnte.</p> |

| Parameter | Endpunkteinstellungen für Voice-Over-Mobile |
|---------------|---|
| Modem | Legt das Modem fest, das für Voice-over-Mobile-Anrufe verwendet werden soll |
| Audio profile | Legt das Audioprofil des Modems fest |
| Volume level | Legt den Lautstärkepegel des Modems fest (1 = niedrig) |

| Parameter | Endpunkteinstellungen für SIP (registrar) |
|------------|--|
| Subscriber | Teilnehmername für einen sich registrierenden SIP-Client |
| Username | Benutzername für einen sich registrierenden SIP-Client |
| Password | Passwort für einen sich registrierenden SIP-Client |

| Parameter | Endpunkteinstellungen für SIP (direct) |
|------------|---|
| Subscriber | Der Teilnehmer Name des SIP-Agenten |
| Host | Die IP-Adresse des SIP-Agenten |
| Port | Der Port des SIP-Agenten |
| Username | Der Benutzername zur Authentifizierung beim SIP-Agenten |
| Password | Das zur Authentifizierung verwendete Passwort |

| Parameter | Endpunkteinstellungen für SIP (user-agent) |
|------------|---|
| Host | Die IP-Adresse des entfernten SIP-Registrars |
| Port | Der Port des entfernten SIP-Registrars |
| Domain | Der beim Registrar verwendete Domainname |
| Subscriber | Der beim Registrar verwendete Teilnehmername |
| Username | Der Benutzername zur Authentifizierung beim Registrar |
| Password | Das zur Authentifizierung verwendete Passwort |
| Register | Legt fest, ob sich der user-agent beim Registrar anmelden muss |
| Expires | Ablaufzeit in Sekunden, nach der erneut eine Registrierung ausgelöst wird |

Voice-Gateway-Routing

Auf dieser Seite können Sie das generische Voice-Gateway-Routing zwischen Endpunkten konfigurieren.

Erweiterte Routing-Möglichkeiten stellt die SDK-Schnittstelle bereit, die Sprachanrufe je nach Attributen (z. B. Telefonnummer) und anderen System-Statusinformationen versenden kann (z. B. Anzahl/Dauer der Anrufe pro Endpunkt, Registrierungsstatus und so weiter). Mit dem SDK können Sie auch einen Anruf einleiten oder annehmen, seine Lautstärke einstellen oder den Anruf beenden.

Für einfache Szenarien sollte jedoch die generische Methode ausreichend sein. Sie kann wie folgt konfiguriert werden:

| Parameter | Einstellungen für das Voice-Gateway-Routing |
|-------------|--|
| Source | Legt den Quell-Endpunkt fest (d. h. wo der Anruf eingeht) |
| Mode | Die Aktion, die für den Anruf angewendet werden soll: DROP will silently hangup the call, ROUTE will route the call to the specified endpoint. |
| Destination | Legt den Ziel-Endpunkt fest (d. h. wohin der Anruf geleitet wird) |



Clientkonfiguration

Jeder SIP-Client muss so konfiguriert werden, dass er den Router als Registrar/Proxy verwendet.

| Parameter | Konfiguration von X-Lite |
|--------------------|---|
| User ID | SIP-Benutzername, der in from-Headern verwendet wird (d. h. Teilnehmername) |
| Domain | SIP-Domäne, die in from-Headern verwendet wird (optional) |
| Authorization name | Benutzername, der zur Authentifizierung verwendet wird (d. h. der Name des Teilnehmers) |
| Password | Passwort, das zur Authentifizierung verwendetet wird |
| Display name | Name, der auf dem Mobilteil angezeigt werden soll |

5.8. SYSTEM

5.8.1. System

Systemeinstellungen

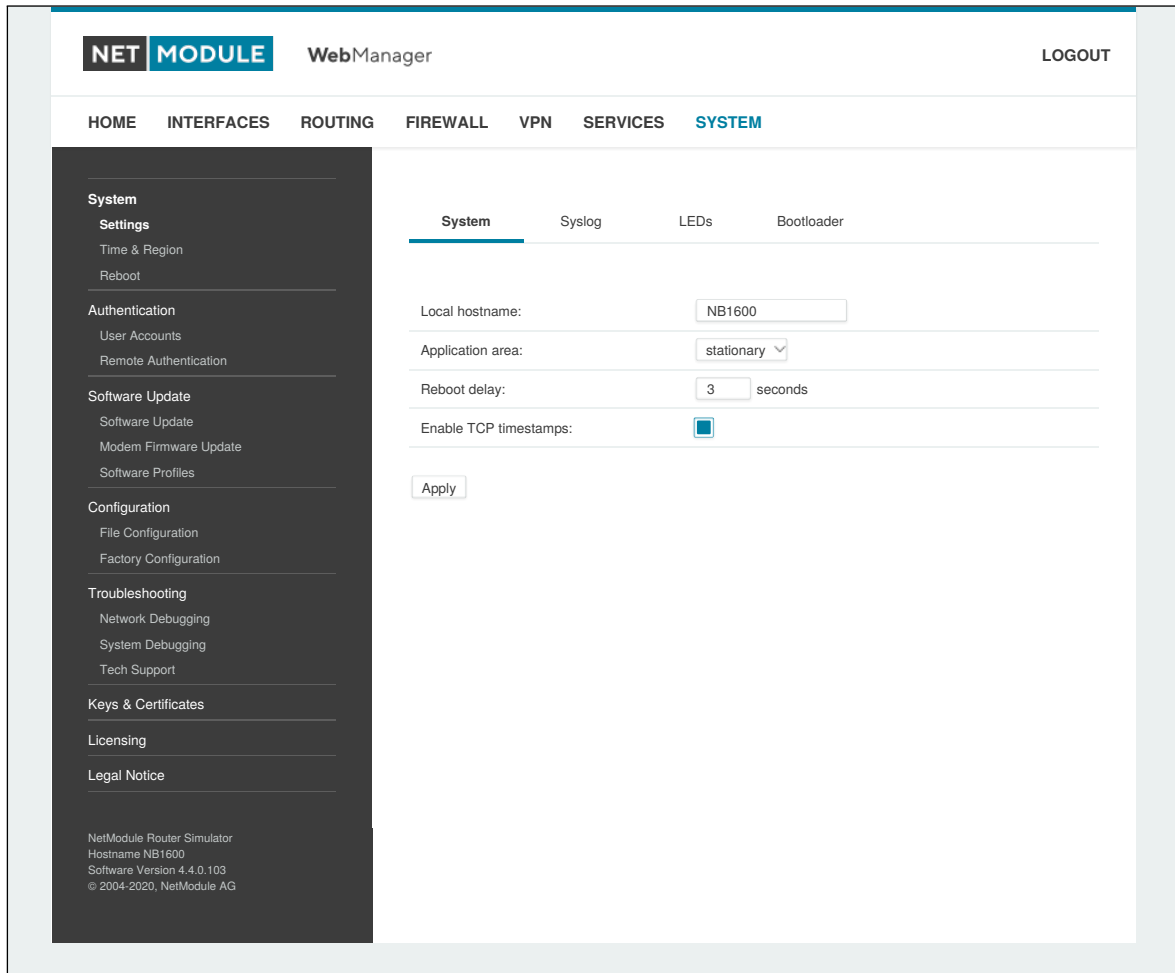


Abbildung 5.58.: System

System

Es stehen die folgenden Systemeinstellungen zur Verfügung:

| Parameter | Systemeinstellungen |
|------------------|---|
| Local hostname | Der Hostname des Systems |
| Application area | Der Anwendungsbereich, der das Systemverhalten beeinflusst, wie z. B. Anmelde-Timeouts oder andere Anpassungen beim Betrieb in mobilen Umgebungen. |
| Reboot delay | Die Anzahl der Sekunden, die gewartet wird, bevor das System regelmäßig neu gebootet wird (kann für das Ereignis <code>system-rebooting</code> benötigt werden) |

| Parameter | Systemeinstellungen |
|--|---|
| Enable TCP timestamps | Aktiviert TCP-Zeitstempel für die systemweite TCP-Kommunikation. Dies wird für den Schutz vor abgefangenen Sequenznummern (Protection Against Wrapped Sequence, PAWS) benötigt. Allerdings kann mit diesen aktivierten Zeitstempeln ein Angreifer von außen die Betriebszeit des Systems erraten. Die Betriebszeit ist eine Untergrenze für das Alter der Hauptsystemkomponenten wie des Kernels. Wenn das System eine Betriebszeit von 3 Jahren anzeigt, ist es unwahrscheinlich, dass aktuelle Sicherheitspatches eingespielt wurden. |
| Show messages and infos on log-in screen | Fehlermeldungen und Benachrichtigungen auf dem Anmeldebildschirm anzeigen. Wenn diese Option aktiviert ist, werden diese Meldungen auch vor der Anmeldung mit Anmeldedaten angezeigt. |
| Enable ignition sense | Wenn aktiviert, schaltet der Router nach der angegebenen Haltezeit (in Sekunden, max. 3600) aus, wenn die Zündspannung (PWR-Anschluss, Pin 3) abgefallen ist. Für das Wiedereinschalten muss erneut die Zündspannung (PWR-Anschluss, Pin 3) anliegend sein. Falls zusätzlich Graceful Shutdown aktiviert ist, wird nach ablaufen der Haltezeit das Gerät korrekt heruntergefahren. Ohne Graceful Shutdown wird das Gerät direkt ausgeschaltet. |

Syslog (Systemprotokoll)

Es stehen die folgenden Einstellungen zur Verfügung:

| Parameter | Syslog-Einstellungen |
|------------------|---|
| Storage | Das Speichergerät, auf dem die Protokolldateien gespeichert werden sollen. |
| Max. filesize | Die maximale Größe, die eine Protokolldatei (in kB) erreichen darf, bis eine neue angefangen wird. |
| Redirect address | Legt eine IP-Adresse fest, an die Protokollmeldungen umgeleitet werden sollen. Ein einfacher Systemprotokoll-Server für Windows ist in TFTP32 enthalten, das von unserer Website heruntergeladen werden kann. |

In der Regel verfügt das Gerät über einen internen Flash-Speicher. Je nach Modell kann dies durch zusätzliche Flash- oder USB-Disks erweitert werden. Die folgenden Speichergeräte können angegeben werden:

| Parameter | Speichergeräte |
|---------------|---|
| flash root | Die Root-Partition des internen Flash-Speichers |
| flash data | Die Datenpartition des internen Flash-Speichers |
| extended disk | Eine erweitertes Speichergerät |
| USB disk | Ein an den externen USB-Anschluss angeschlossenes Speichergerät |

LEDs

Es stehen die folgenden LED-Einstellungen zur Verfügung:

| Parameter | LED-Einstellungen |
|-----------|--|
| LED | Sie können das Verhalten aller Status-LEDs auf der Frontplatte des Geräts anpassen. Sie sind in der Regel in zwei Reihen unterteilt (oben/unten). Sie können auch einen Umschaltmodus konfigurieren, sodass die LEDs regelmäßig zwischen zwei getrennt konfigurierten LED-Schemata wechseln. |

Bootloader

Es stehen die folgenden Bootloader-Einstellungen zur Verfügung:

| Parameter | Bootloader-Einstellungen |
|-----------|---|
| Password | Das Passwort zum Entsperren des Bootloaders. Wenn hier nichts angegeben ist, wird das Admin-Passwort verwendet. |

Autorun (Automatische Ausführung)

Diese Funktion kann automatisch ein Shell-Skript starten oder ein Software-/Konfigurations-Update durchführen, sobald ein externes Speichergerät eingesteckt wurde. Zur Authentifizierung muss eine Datei namens `autorun.key` im Stammverzeichnis eines FAT16/32-formatierten Geräts vorhanden sein. Es kann von dieser Seite heruntergeladen werden und enthält den SHA256-Hash-Schlüssel des Autorun-Passworts. Die Datei kann mehrere Hashes enthalten, die bei der Authentifizierung zeilenweise abgearbeitet werden, wodurch Sie mehrere Systeme mit unterschiedlichen Admin-Passwörtern einrichten können.

Bei neuen Geräten mit einem leeren Passwort wird der Hash-Schlüssel

```
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

verwendet.

Hash-Schlüssel können durch Ausführen des folgenden Befehls `echo -n «password» sha256sum` auf einem Linux-System erzeugt werden oder mit einem Hash-Schlüsselgenerator im Internet (suchen Sie nach `Bha-256 hash calculator`).

Nach erfolgreicher Authentifizierung sucht das System im Stammverzeichnis nach anderen Dateien, die die folgenden Aktionen ausführen können:

1. Zum Ausführen eines Skripts: `autorun.sh`
2. Für ein Konfigurations-Update: `cfg-<SERIALNO>.zip` (z. B. `cfg-00112B000815.zip`), oder, falls nicht vorhanden, `cfg.zip`
3. Für ein Software-Update: `sw-update.img`

Zeit und Region

Auf dieser Seite können Sie die Systemzeit einstellen und die Zeitzone festlegen. Sie können außerdem die Sommerzeitumstellung für die gewählte Zeitzone aktivieren. NetModule-Router können ihre Systemzeit über einen oder mehrere Server mit dem Network Time Protocol (NTP) synchronisieren oder auch über GNSS. Wenn aktiviert, wird die Zeitsynchronisation normalerweise nach dem Aufbau

einer WAN-Verbindung, aber vor dem Start von VPN-Verbindungen ausgelöst. Weitere Zeitsynchronisationszyklen werden im Hintergrund eingeplant.

Die meisten Router verfügen nicht über eine batteriegepufferte Echtzeituhr. Bei ihnen wird die Systemzeit beim Booten auf die letzte gültige Zeit, z. B. vor dem Ausschalten, gesetzt.

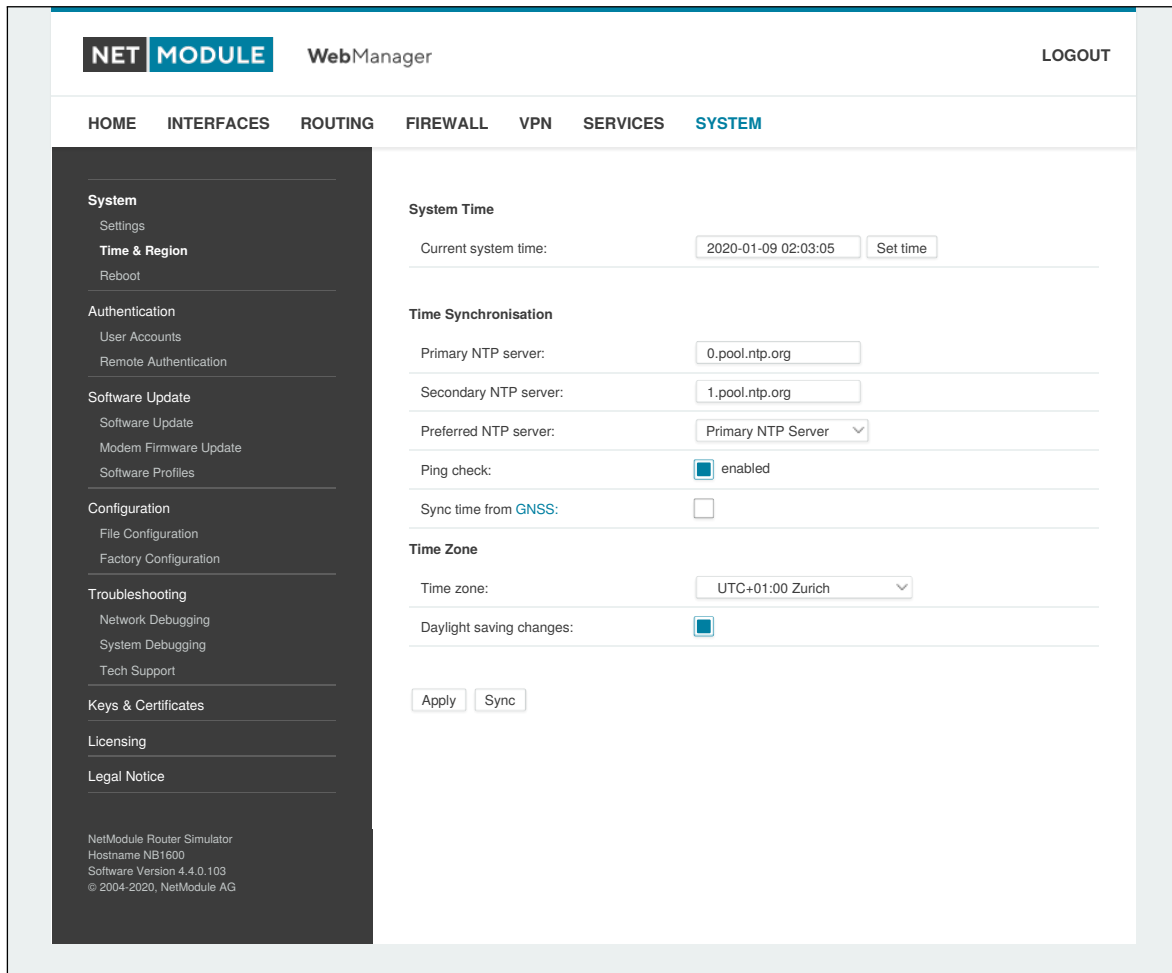


Abbildung 5.59.: Regionseinstellungen

| Parameter | Zeitsynchronisation |
|---------------------|--|
| NTP server | Adresse des primären NTP-Servers |
| NTP server 2 | Optional die Adresse eines zweiten NTP-Servers |
| Ping check | Prüft mit einem ICMP-Ping, ob NTP-Server verfügbar sind, wenn die erste Zeitaktualisierung ausgeführt wird |
| Sync time from GNSS | Zeit vom ersten GNSS-Gerät beziehen (falls aktiviert) |

| Parameter | Zeitzone |
|-------------------------|---|
| Time Zone | Legt die geltende lokale Zeitzone fest. |
| Daylight saving changes | Aktiviert/deaktiviert die Sommerzeitumstellung. |

Virtualisierung

Mit Virtualisierungstechniken können mehrere voneinander isolierte Gastsysteme auf dem Host ausgeführt werden. Die NetModule-Router bewirken eine Virtualisierung auf Betriebssystemebene: Ein System wird auf Betriebssystemebene virtualisiert und ermöglicht so mehrere isolierte Benutzerbereiche bzw. Benutzerinstanzen.

Diese werden als Container bezeichnet. Für die Implementierung aller Gastumgebungen wird der gleiche Betriebssystemkern verwendet. Anwendungen, die in einer Gastumgebung laufen, sehen diese als eigenständiges System.

Allgemeine Einstellungen:

| Parameter | Virtualisierungseinstellungen |
|-----------------------|--|
| Administrative status | Legt fest, ob die Virtualisierung aktiviert ist oder nicht |

Die folgenden Parameter stehen zur Konfiguration eines virtuellen Gastsystems zur Verfügung:

| Parameter | Gasteinstellungen |
|-------------|--|
| Type | Legt fest, welche Virtualisierungstechnik verwendet wird |
| Description | Eine Beschreibung des Gastsystems |
| Storage | Legt das Speichergerät fest, auf dem das Root-Dateisystem des Gastsystems angelegt werden soll |

Zur Installation eines Root-Dateisystems können Sie eine URL einrichten, von der das Image geladen und die Installation ausgelöst wird:

| Parameter | Installation |
|-----------|--|
| URL | Die URL, von der das Image geladen werden soll. Das Image muss als XZ-komprimiertes TAR-Archiv bereitgestellt werden, das die Dateien eines Root-Dateisystems enthält, die zu unserer CPU-Architektur (ppc) kompatibel ist. Für die Transaktion können verschiedene Protokolle verwendet werden, z. B. HTTP, HTTPS, FTP oder TFTP. Wenn Sie das Image im Voraus auf den Router hochgeladen hatten, können Sie auch "file://", gefolgt vom lokalen Pfadnamen der Datei, verwenden. Auf Anfrage können wir verschiedene maßgeschneiderte Linux-Distributionen (z. B. Debian) als Images bereitstellen. |
| Install | Legt fest, ob das Herunterladen des Image direkt nach abgeschlossener Definition beginnt. Ein eventuell vorhandenes Root-Dateisystem wird überschrieben. Dieser Parameter wird nicht in der Konfiguration gespeichert. Nach erfolgter Installation wird der Wert zurückgesetzt und muss neu gesetzt werden, wenn ein neues Image installiert werden soll. |

Die Kommunikation zum und vom Gastsystem wird ermöglicht über definierte Netzwerkschnittstellen, die entweder zum Gastsystem geroutet oder mit einer LAN-Schnittstelle gebrückt werden können:

| Parameter | Netzwerke für Gastsysteme |
|------------------|--|
| Guest interface | Der Name der Schnittstelle innerhalb des Gastsystems |
| Mode | Der Netzwerkmodus für diese Schnittstelle (geroutet oder gebrückt) |
| Address | Die IP-Adresse der Schnittstelle innerhalb des Gastsystems |
| Netmask | Die Netzmaske der Schnittstelle innerhalb des Gastsystems |
| Gateway | Das innerhalb des Gastsystems verwendete Gateway, das auch an der Host-Schnittstelle eingestellt ist |
| Bridge interface | Die Schnittstelle, zu der die Gastsystem-Schnittstelle gebrückt werden soll |

Der Gastgeräte-Parameter zeigt eine Liste von Geräten (z. B. Bluetooth, CAN), die dem Gastsystem zur Verfügung gestellt werden können.

| Parameter | Gastsystem-Geräte |
|----------------|--|
| Enable devices | Legt fest, ob Geräte für das Gastsystem aktiviert werden |

Um die Ressourcen für einen Gast zu begrenzen, können die folgenden Einstellungen vorgenommen werden:

| Parameter | Begrenzungen für Gastsysteme |
|-----------|--|
| CPU | Die Anzahl der für das Gastsystem verwendeten CPUs |
| Memory | Die für das Gastsystem verfügbare Speichermenge |

Neustart

Auf dieser Seite können Sie einen regelmäßigen automatischen Neustart einrichten, aber auch einen sofortigen manuellen Neustart auslösen.

5.8.2. Authentifizierung

Benutzerkonten

Auf dieser Seite können Sie die Benutzerkonten im System verwalten.

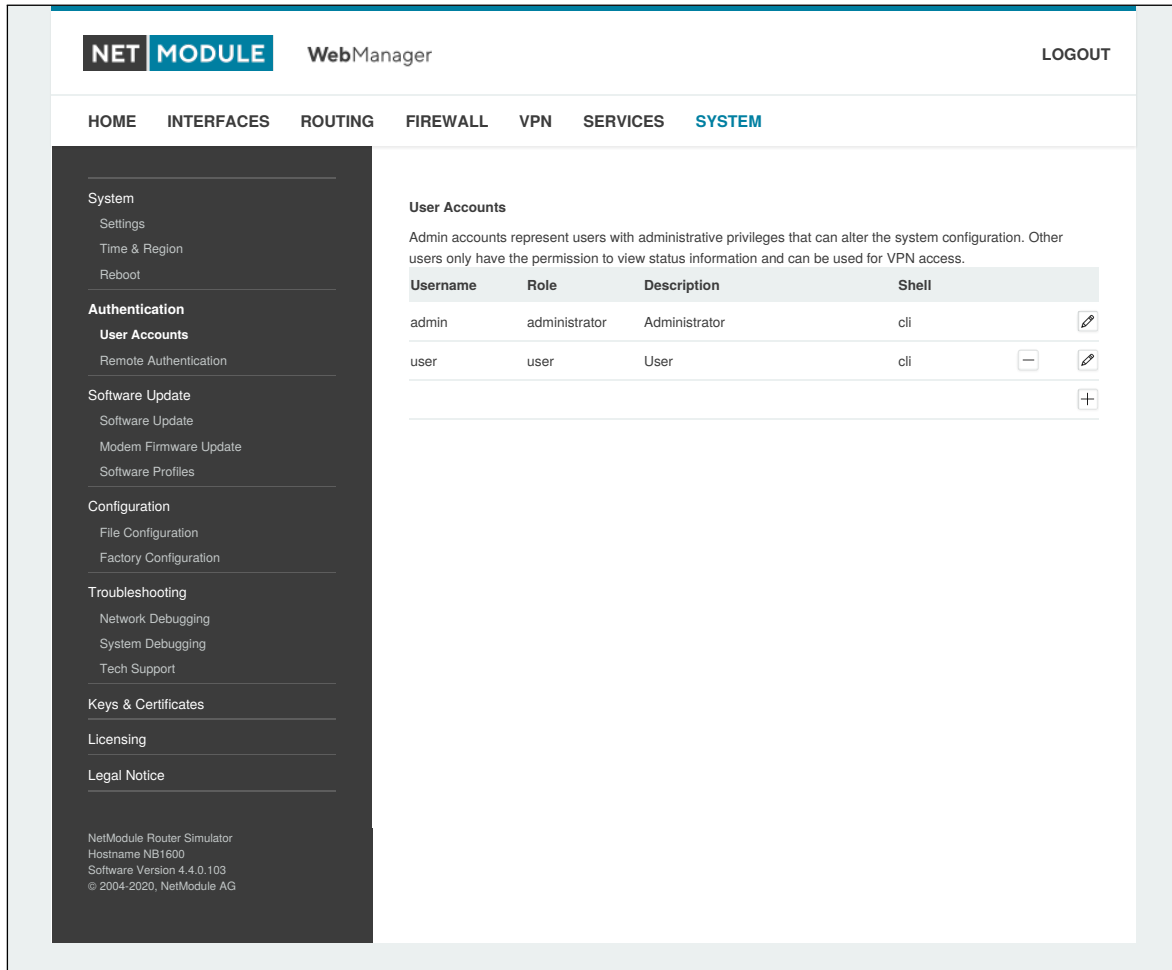


Abbildung 5.60.: Benutzerkonten

Der Benutzer `admin` ist ein vordefinierter Hauptbenutzer, der Standardadministrator des Systems. Hinweis: Das für den Benutzer `admin` gültige Passwort gilt auch für den Benutzer `root` - dieser kann eine System-Shell aufrufen. Es können weitere Admin-Konten mit administrativen Rechten hinzugefügt werden, die auch die Systemkonfiguration ändern oder administrative Systemaufgaben durchführen können. Andere Benutzer haben nur die Berechtigung, Statusinformationen anzuzeigen. Sie können auch für den VPN-Zugang verwendet werden.

Der Web Manager unterstützt bis zu 5 gleichzeitige Benutzer. Benutzer werden nach 30 Minuten ohne Aktivität abgemeldet. Wenn die Anmeldung erfolgreich war, werden alle Duplikate des Benutzers von anderen Remote-Hosts abgemeldet. Remote-Hosts werden nach 10 fehlgeschlagenen Anmeldeversuchen für 5 Minuten blockiert.

| Parameter | Benutzerkontenverwaltung |
|-----------|--------------------------|
| Username | Der Name des Benutzers |

| Parameter | Benutzerkontenverwaltung |
|----------------------------|---|
| Description | Eine kurze Anmerkung zum Benutzer |
| Role | Entweder Admin(istrator) oder User (normaler Benutzer) |
| Shell | Legt fest, ob dem Benutzer die CLI oder eine SHELL als Schnittstelle angeboten wird |
| Store password unencrypted | Das Passwort wird unverschlüsselt auf dem Gerät gespeichert (nicht empfohlen) |
| Old password | Das alte Passwort des Benutzers |
| New password | Das neue Passwort des Benutzers |
| Confirm new password | Das bestätigte neue Passwort des Benutzers |

Bitte beachten Sie, dass Sie beim Hinzufügen weiterer Admin-Benutzer das Passwort des Standard-Administrators angeben müssen.



Speicherung von Passwörtern

Normalerweise werden Passwörter als kryptographischer Hash auf dem Gerät gespeichert. Dies entspricht den empfohlenen Verfahren. Leider benötigt die Implementierung des SNMP-Dienstes das Passwort in unverschlüsselter Form.

Stellen Sie sicher, den angelegten Benutzern nur die Rechte einzuräumen, die wirklich benötigt werden.

Remote-Authentifizierung

Für die Authentifizierung von Remote-Benutzern kann ein RADIUS-Server verwendet werden. Dies gilt für den Web Manager, das WLAN-Netzwerk und andere Dienste, die die Remote-Authentifizierung unterstützen und integrieren.

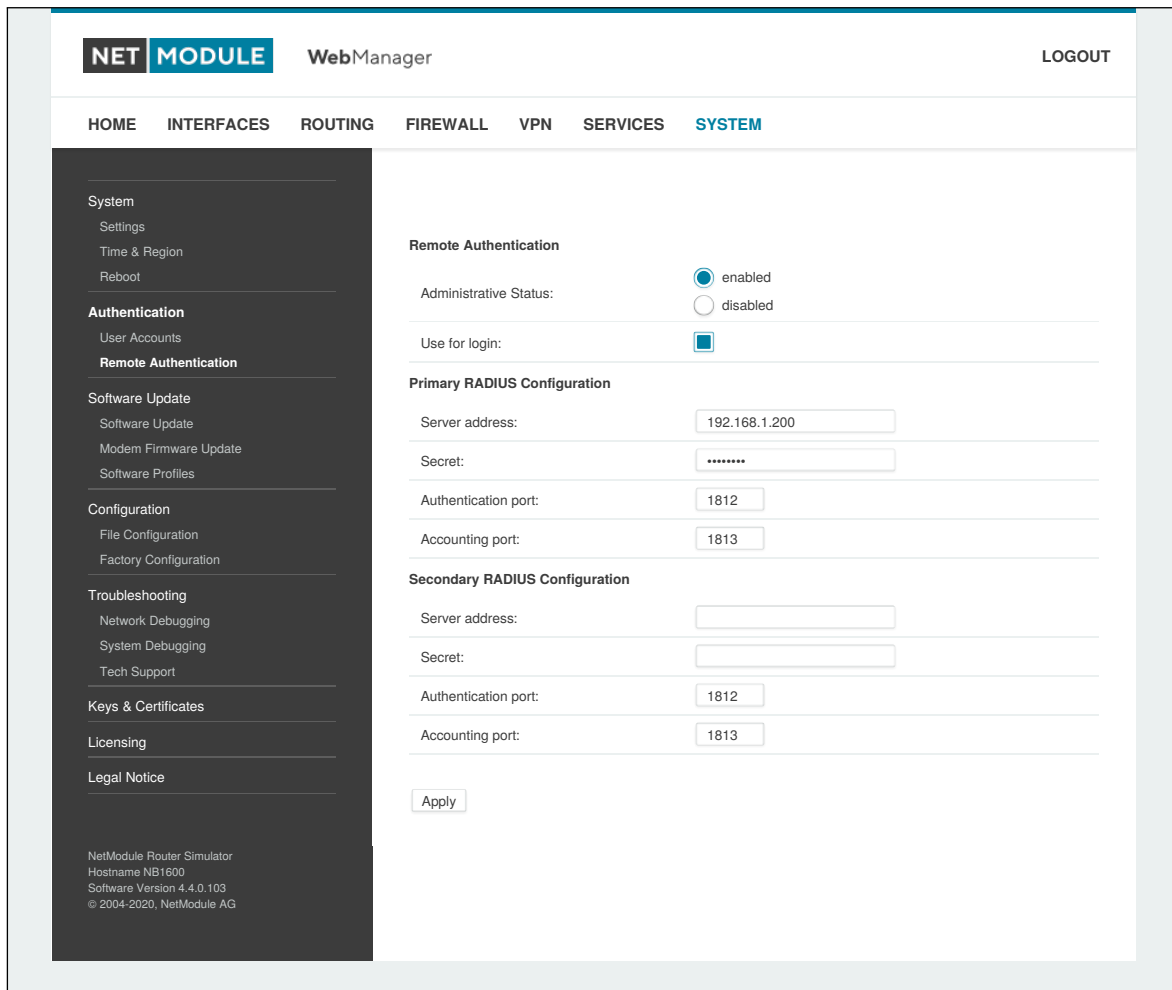


Abbildung 5.61.: Remote-Authentifizierung

Es bestehen die folgenden Konfigurationsmöglichkeiten:

| Parameter | Einstellungen für die Remote-Authentifizierung |
|-----------------------|---|
| Administrative status | Legt fest, ob ein Remote-Server für die Authentifizierung verwendet werden soll |
| RADIUS server | Die Adresse des RADIUS-Servers |
| RADIUS secret | Die zur Authentifizierung gegenüber dem RADIUS-Server verwendete Passphrase |
| Authentication port | Der für die Authentifizierung verwendete Port |
| Accounting port | Der für Abrechnungsmeldungen verwendete Port |
| Use for login | Legt fest, dass der Remote-Benutzer Zugriff auf den Web-Manager hat (ansonsten wird dieser nur von Diensten verwendet, die ihn explizit konfiguriert haben, z. B. WLAN) |

5.8.3. Software-Updates

Manuelle Software-Updates

In diesem Menü können Sie ein manuelles Software-Update des Systems durchführen.

| Parameter | Manuelle Software-Updates |
|------------------------|--|
| Update operation | Die verwendete Update-Methode. Sie können das Update als Image hochladen, es von einer URL herunterladen oder die neueste Version von unserem Server verwenden |
| URL | Die Server-URL, von der das Update-Image heruntergeladen werden soll |
| Administrator password | Administrator-Passwort für Downgrade auf Softwareversionen vor 4.2.x |



Vorsicht

Ab der Softwareversion 4.2 ist standardmäßig voreingestellt, dass Passwörter nicht gespeichert und stattdessen Passwort-Hashes verwendet werden. Das Speichern von Passwörtern für Benutzer kann aktiviert werden, wird aber für neue Anwendungen nicht empfohlen.

Bei älteren Softwareversionen müssen die Passwörter verschlüsselt auf dem Gerät gespeichert werden. Da diese Möglichkeit in Version 4.2 und später nicht mehr besteht, müssen Sie das Administrator-Passwort angeben, wenn Sie ein Downgrade auf eine Version 4.1.x und niedriger durchführen möchten. Die gleiche Passphrase wird auch für die Anmeldung beim Bootloader verwendet.

Benutzer, die kein Passwort auf dem Gerät gespeichert haben, können sich nach dem Downgrade nicht mehr anmelden und müssen neue Passwörter erhalten.

Ein Uniform Resource Locator (URL) kann eines der folgenden Formate haben:

```
http://<Benutzername>:<Passwort>@<Host>:<Port>/<Pfad>  
https://<Benutzername>:<Passwort>@<Host>:<Port>/<Pfad>  
ftp://<Benutzername>:<Passwort>@<Host>:<Port>/<Pfad>  
sftp://<Benutzername>:<Passwort>@<Host>:<Port>/<Pfad>  
tftp://<Host>/<Pfad>  
file:///<Pfad>
```

Bei einem Software-Update wird die aktuelle Konfiguration (einschließlich Dateien wie Schlüssel/Zertifikate) gesichert. Alle anderen Änderungen am Dateisystem werden gelöscht.

Die Konfiguration ist im Allgemeinen abwärtskompatibel. Wir sorgen auch für Vorwärtskompatibilität bei einem Downgrade auf eine frühere Softwareversion innerhalb der gleichen Release-Linie durchgeführt wird. Dies wird durch Aussortieren von unbekanntem Konfigurationsanweisungen erreicht, was zum Verlust von Einstellungen und Funktionen führen könnte. Daher ist es immer eine gute Idee, eine Sicherungskopie der Arbeitskonfiguration vorzuhalten.

**Vorsicht**

Falls Sie ein Major-Downgrade auf einen früheren Versionszweig durchführen (z. B. 3.7.0 auf 3.6.0), stellen Sie bitte sicher, dass Sie immer die neueste Version dieses Zweigs (d. h. 3.6.0.X) verwenden, da nur diese in der Regel vollständig vorwärtskompatibel sind. Denken Sie auch daran, dass einige Hardware-Funktionen möglicherweise nicht funktionieren (z. B. weil sie in dieser Vorversion nicht implementiert sind). Im Zweifelsfall wenden Sie sich bitte an unser Support-Team.

Ein Software-Image kann entweder über den Web Manager hochgeladen oder von einer bestimmten URL abgerufen werden. Es wird entpackt und auf einer Ersatzpartition bereitgestellt, die aktiviert wird, wenn das Update erfolgreich abgeschlossen wurde. Während des Update-Vorgangs blinken alle grünen LEDs. Der anschließende Neustart des Systems wird durch eine langsam blinkende Status-LED angezeigt. Die gesicherte Konfiguration wird beim Hochfahren übernommen, und die Status-LED blinkt während dieses Vorgangs schneller. Abhängig von der vorhandenen Konfiguration kann dies eine Weile dauern.

Automatische Software-Updates

In diesem Menü können Sie ein automatisches Software-Update des Systems durchführen.

| Parameter | Automatische Software-Updates |
|-------------|--|
| Status | Legt fest, ob automatische Software-Updates aktiviert sind |
| Time of day | Jeden Tag um diese Uhrzeit führt der Router eine Prüfung auf Updates durch |
| Aktion | Das neueste Image vom Server herunterladen oder unter einer bestimmten URL das Software-Updatepaket beziehen. Unterstützt werden die Protokolle TFTP, HTTP, HTTPS und FTP. Geben Sie eine URL an, wie <code><Protokoll>://<Server>/<Pfad>/<Datei></code> |

Hinweis: SSL-Zertifikate von HTTPS-URLs werden nur überprüft, wenn eine Liste von CA-Root-Zertifikaten bereitgestellt wird, wie beschrieben in Kapitel 5.8.8.

Nach der Installation der neuen Software wird beim Booten die zuletzt geltende Konfiguration angewendet. Dies wird durch ein schnelleres Blinken der grünen Status-LED angezeigt.

5.8.4. Updates für Modul-Firmware

In diesem Menü können Sie ein Firmware-Update eines bestimmten Moduls durchführen.

| Parameter | Updates für Modul-Firmware |
|------------------|--|
| Update operation | Die verwendete Update-Methode. Sie können entweder ein Firmware-Paket hochladen oder es von einer bestimmten URL beziehen. |
| Module | Das Modul, das aktualisiert werden soll. |

| Parameter | Updates für Modul-Firmware |
|-----------|--|
| Storage | Der temporäre Speicher, der für das Update verwendet werden soll. Für Geräte mit begrenztem Flash-Speicher ist es möglich, einen USB-Stick zu verwenden, der aber im USA-Abschnitt richtig eingerichtet sein muss und ein geeignetes Dateisystem enthält, z. B. ext4. |
| URL | Die Server-URL, von der das Firmware-Paket heruntergeladen werden soll (z.B. <code><Protokoll>://<Server>/<Pfad>/<Datei></code>). Unterstützt werden die Protokolle TFTP, HTTP, HTTPS und FTP. Für Geräte mit begrenztem Flash-Speicher können Sie auch Folgendes verwenden: <code>usb0://<Pfad_zum_Firmwarepaket></code> . |

Ein Firmware-Paket (im ZIP-Format) besteht in der Regel aus einem Flash-Dienstprogramm, einer Infodatei und den entsprechenden Firmware-Dateien. Unter <https://www.netmodule.com/en/support> erhalten Sie die jeweils neueste Version.

5.8.5. Software-Profile

Das System besteht aus zwei Root-Partitionen, die unterschiedliche Softwareversionen enthalten können. In diesem Menü können Sie zwischen ihnen umschalten. So können Sie eine neuere Softwareversion testen und bei auftretenden Problemen einfach wieder zur bisherigen Version zurückkehren.

5.8.6. Konfiguration

Die Konfiguration über den Web Manager wird bei einer größeren Anzahl von Geräten mühsam. Der Router bietet daher eine automatische und eine manuelle dateibasierte Konfigurationsmöglichkeit. Wenn Sie das System einmal erfolgreich eingerichtet haben, können Sie die Konfiguration sichern und anschließend damit wiederherstellen. Sie können entweder eine einzelne Konfigurationsdatei (.cfg) oder ein komplettes Paket (.zip) hochladen, das die Konfigurationsdatei und eine gepackte Version anderer wichtiger Dateien (z. B. Zertifikate) im Root-Verzeichnis enthält.

Manuelle Konfiguration per Datei

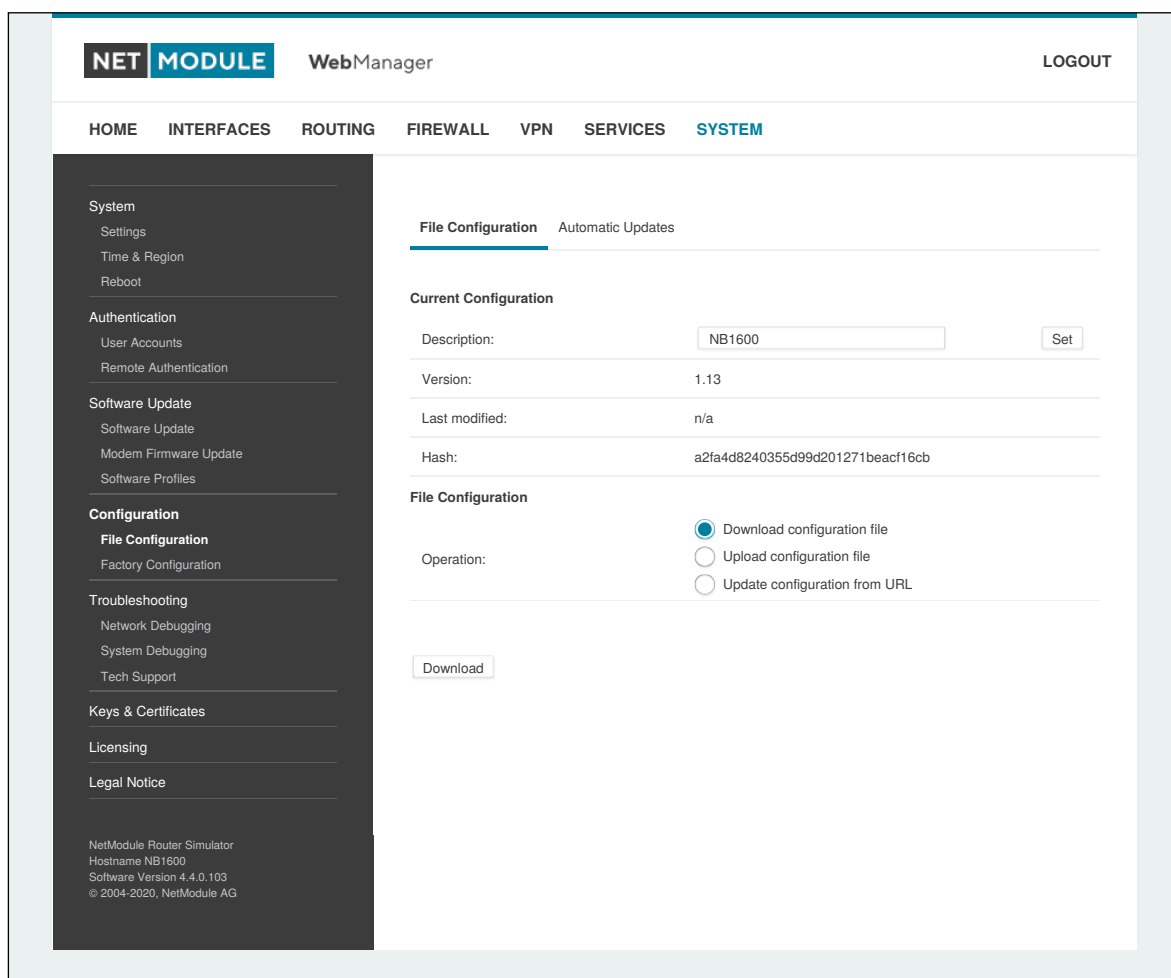


Abbildung 5.62.: Manuelle Konfiguration per Datei

In diesem Abschnitt können Sie die aktuell laufende Systemkonfiguration (einschließlich wichtiger Dateien wie z. B. Zertifikate) herunterladen. Um eine bestimmte Konfiguration wiederherzustellen, können Sie eine zuvor heruntergeladene Konfiguration hochladen. Sie können wählen, ob fehlende Konfigurationsanweisungen auf die Werkseinstellungen gesetzt oder ignoriert werden sollen, d. h. eventuell vorhandene Konfigurationsanweisungen bleiben im System erhalten.

Automatische Konfiguration per Datei

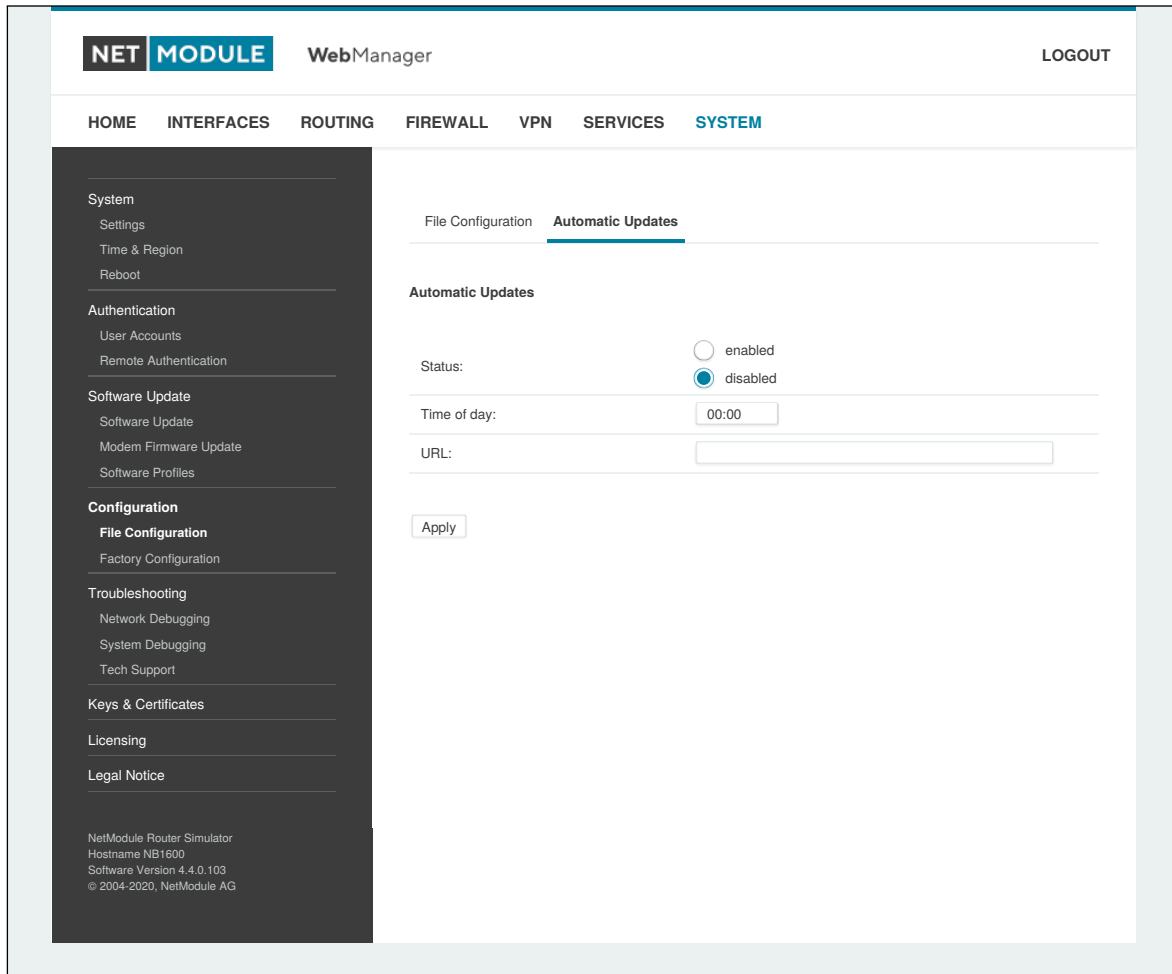


Abbildung 5.63.: Automatische Konfiguration per Datei

In diesem Menü können Sie ein automatisches Konfigurations-Update des Systems durchführen. Es bestehen die folgenden Einstellungsmöglichkeiten:

| Parameter | Automatische Konfiguration per Datei |
|-------------|--|
| Status | Legt fest, ob automatische Konfigurations-Updates aktiviert sind |
| Time of day | Uhrzeit, zu der das System nach Updates suchen soll |
| URL | Die URL, von der die Konfigurationsdatei abgerufen werden soll (unterstützte Protokolle sind HTTP, HTTPS, TFTP, FTP) |

Werkseinstellungen

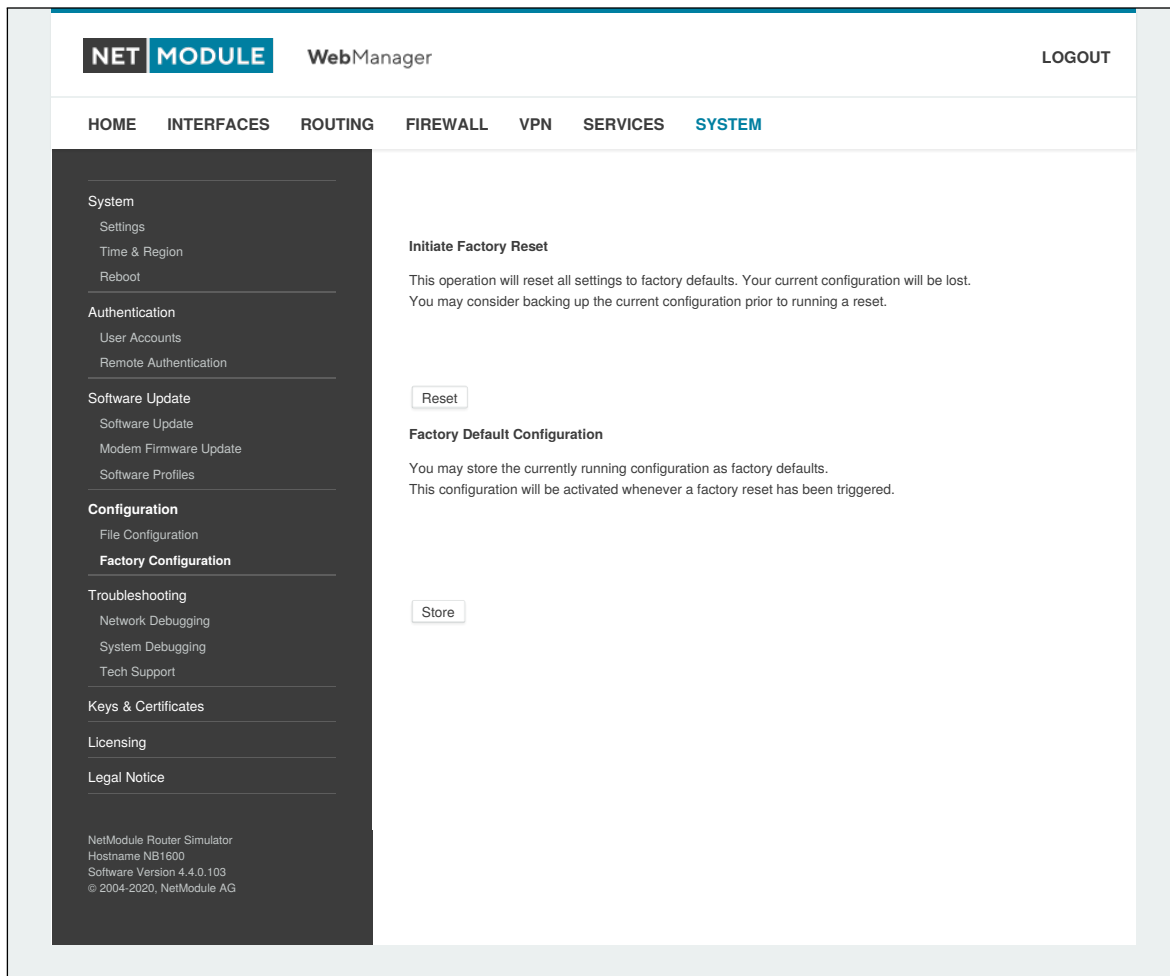


Abbildung 5.64.: Werkseinstellungen

In diesem Menü können Sie das Gerät auf die Werkseinstellungen zurücksetzen. Die aktuelle Konfiguration geht dabei verloren. Ein erfolgreich eingeleiteter Rücksetzvorgang ist daran zu erkennen, dass alle LEDs leuchten.

Beim Zurücksetzen auf die Werkseinstellungen wird die IP-Adresse der ersten Ethernet-Schnittstelle auf 192.168.1.1 zurückgesetzt. Sie können mit dem Gerät kommunizieren, indem Sie die Standard-Netzwerkparameter verwenden. Sie können die aktuell laufende Konfiguration als Werkseinstellung speichern, die auch dann aktiv bleibt, wenn ein Zurücksetzen (z. B. durch Ihre Servicetechniker) ausgelöst wurde.

Bitte stellen Sie sicher, dass diese Konfiguration funktionsfähig ist. Ein echtes Zurücksetzen auf die Werkseinstellungen können Sie erreichen, indem Sie die ursprüngliche Werkskonfiguration wiederherstellen und den Rücksetzvorgang erneut auslösen.

5.8.7. Fehlersuche und Fehlerbehebung

Fehlersuche im Netzwerk

Es gibt mehrere Tools zur Fehlersuche im Netzwerk, z. B. ping, traceroute, tcpdump und darkstat.

| Parameter | Aktion |
|-------------|--|
| Ping | Das Dienstprogramm "ping" kann prüfen, ob ein Remote-Host über IP erreichbar ist. |
| Time of day | Das Dienstprogramm "traceroute" kann die Route der Pakete zu einem Remote-Host ausdrucken. |
| tcpdump | Das Dienstprogramm "tcpdump" erzeugt einen Netzwerk-Dump (PCAP) einer Schnittstelle, die später mit Wireshark analysiert werden kann. |
| Darkstat | Das Dienstprogramm "darkstat" visualisiert die aktuellen Netzwerkverbindungen und den Datenverkehr auf einer bestimmten Schnittstelle. |

Fehlersuche im System

Sie können das Systemprotokoll hier anzeigen, indem Sie die Option *Debug log* wählen, oder wenn Sie das Boot-Protokoll sehen wollen, wählen Sie *Boot log*.

Eine andere Möglichkeit, zu prüfen, was im Gerät vor sich geht, ist das Eröffnen einer SSH- oder Telnet-Sitzung als *root* - geben Sie dann ein: `tail -log`. Außerdem kann das Systemprotokoll an einen Syslog-Server umgeleitet werden. Siehe Kapitel 5.8.1.

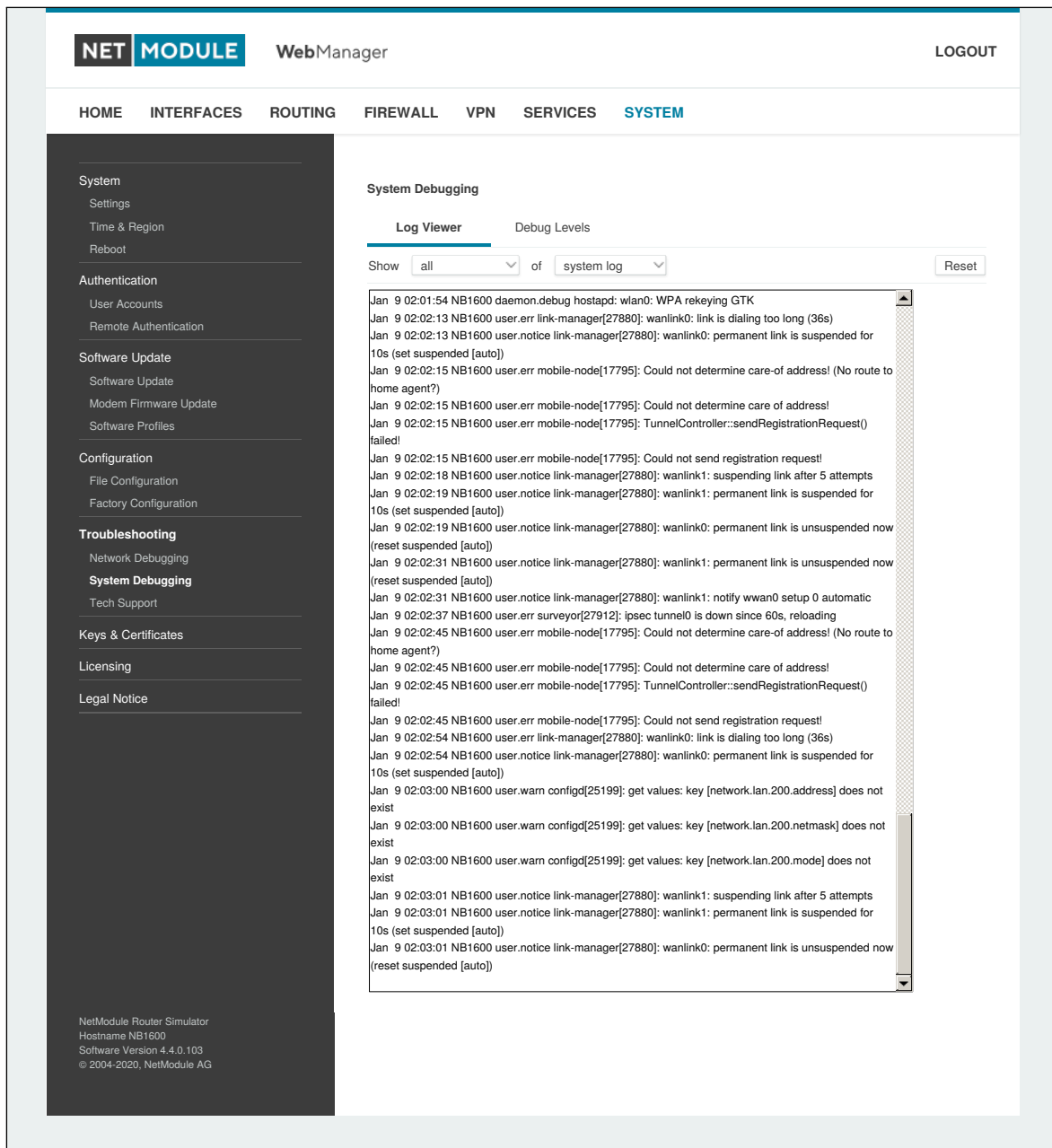


Abbildung 5.65.: Log-Viewer

Technischer Support

Hier können Sie eine Datei für den technischen Support erzeugen und herunterladen. Wir empfehlen dringend, diese Datei bereitzustellen, wenn Sie sich mit unserem Support-Team in Verbindung setzen, entweder per E-Mail oder über unser Online-Supportformular, da dies den Prozess der Analyse und Lösung des Problems erheblich beschleunigen kann. Protokolldateien können hier heruntergeladen und zurückgesetzt werden. Bitte studieren Sie sie bei Problemen sorgfältig. Auf dieser Seite befinden sich verschiedene Tools zur weiteren Analyse potenzieller Konfigurationsprobleme.

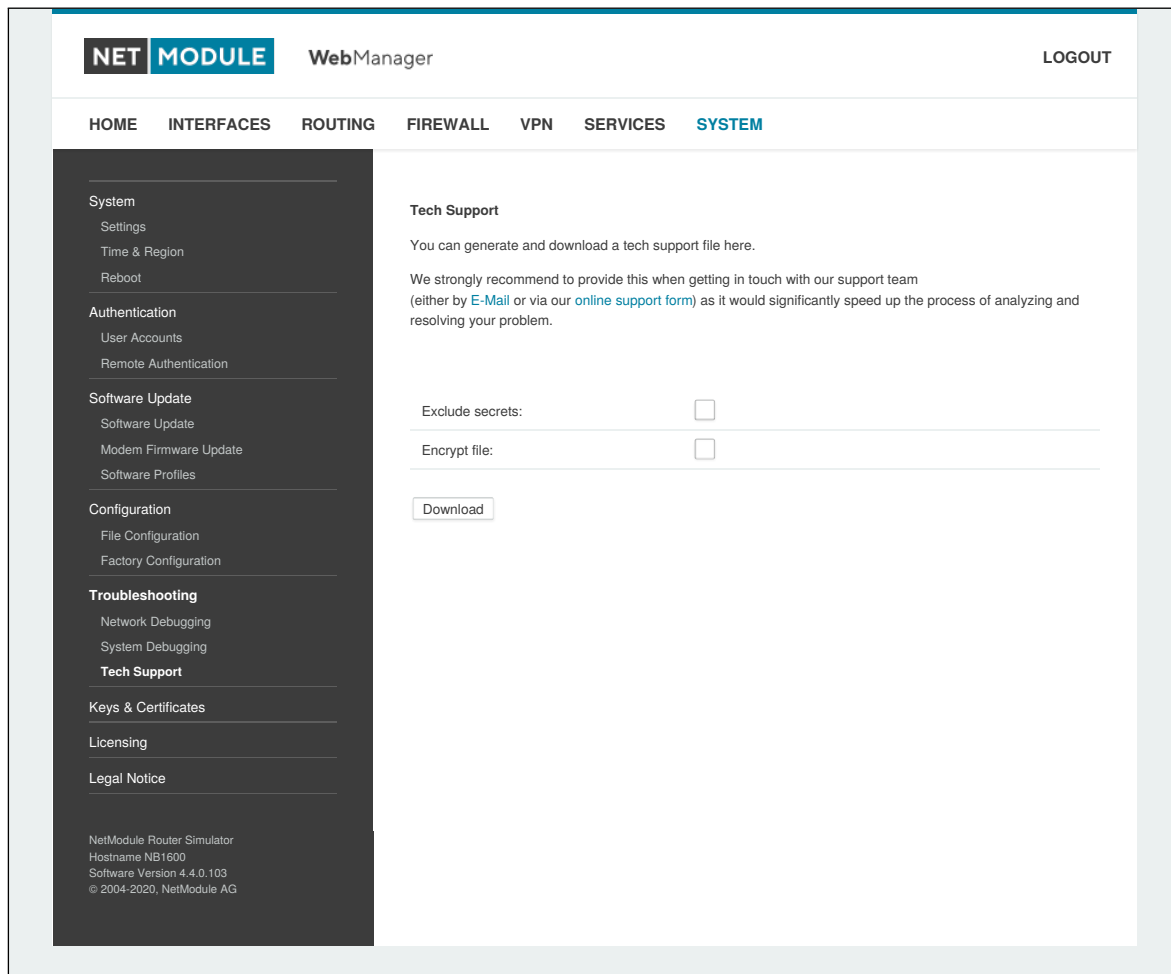


Abbildung 5.66.: Datei für den technischen Support

Es ist möglich, beliebige IP-Schnittstellen zu verfolgen und die Übertragung einzelne Pakete zwischen Hosts zu untersuchen. Hierzu melden Sie sich am Gerät an und starten eine Netzwerkpaketerfassung mit dem Tool *tcdump*. Wir empfehlen die Angabe des Schalters *-n*, um die Namensauflösung zu umgehen (z. B. *tcpdump -n -i lan0*). Sie können auch einen Dump im PCAP-Format mit dem Web Manager erzeugen, ihn auf Ihren Computer herunterladen und weitere Untersuchungen mit Wireshark durchführen (verfügbar unter www.wireshark.org).

5.8.8. Schlüssel und Zertifikate

Auf dieser Seite können Sie die erforderlichen Dateien für die Sicherung Ihrer Dienste (z. B. HTTP- und SSH-Server), aber auch zur Implementierung von Authentifizierung und Verschlüsselung für zertifikatsbasierte VPN-Tunnel und WLAN-Clients erzeugen.

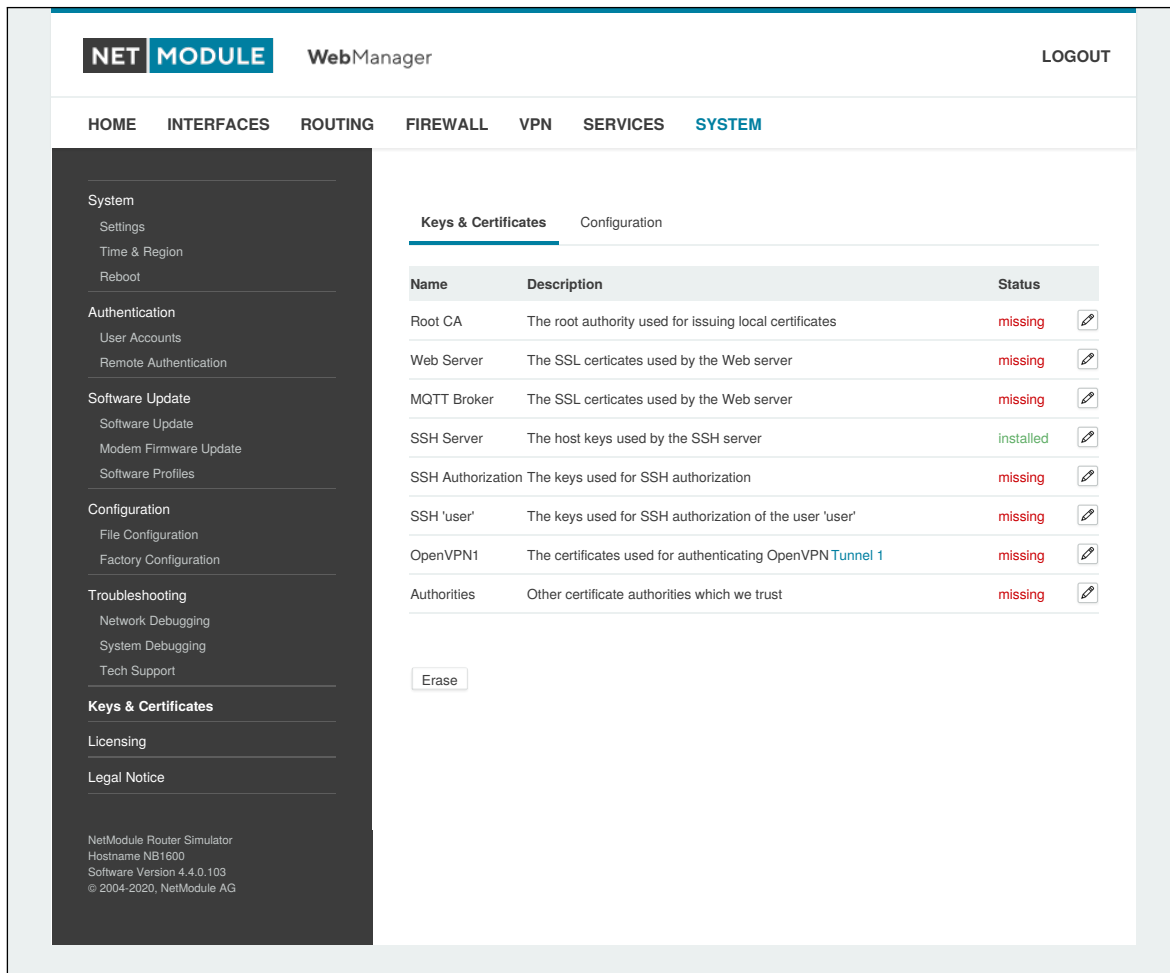


Abbildung 5.67.: Schlüssel und Zertifikate

Die Eingangsseiten zeigen eine Übersicht über installierte Schlüssel und Zertifikate. Es können dabei die folgenden Abschnitte auftreten:

| Type | Description |
|-------------|--|
| Root CA | Die Stammzertifizierungsstelle (Root Certificate Authority, CA), die Zertifikate ausstellt, deren Schlüssel zur Zertifizierung als vertrauenswürdige Dritte auf anderen Systemen verwendet werden kann |
| Web Server | Die Zertifikate für den Webserver, die zum Ausführen von HTTP über SSL (HTTPS) erforderlich sind. |
| MQTT Broker | Die Zertifikate für den MQTT Broker, die für den Betrieb von MQTT über eine TLS-verschlüsselte Verbindung erforderlich sind. |

| Type | Description |
|------------------------|---|
| SSH Server | Die DSS/DSA-Schlüssel für den SSH-Server. |
| SSH Authorization | Die für die SSH-Autorisierung verwendeten Schlüssel. |
| OpenVPN | Server- oder Client-Schlüssel und Zertifikate für den Betrieb von OpenVPN-Tunneln. |
| IPsec | Server- oder Client-Schlüssel und -Zertifikate für den Betrieb von IPsec-Tunneln. |
| WLAN | Schlüssel und Zertifikate zur Implementierung einer zertifikatsbasier-ten WLAN-Authentifizierung (z. B. WPA-EAP-TLS). |
| ETH | Schlüssel und Zertifikate zur Authentifizierung via IEEE 802.1X an Ethernet-Anschlüssen. |
| Zertifizierungsstellen | Andere Zertifizierungsstellen, denen wir beim Aufbau von SSL-Client-Verbindungen vertrauen. |

Tabelle 5.165.: Zertifikatsabschnitte

Für jeden Zertifikatsabschnitt können Sie die folgenden Aktionen durchführen:

| Aktion | Beschreibung |
|------------------------|---|
| generate locally | Schlüssel und Zertifikat lokal auf dem Gerät erzeugen; weitere Optionen siehe Kapitel 5.8.8 |
| upload files | Schlüssel und Zertifikat werden hochgeladen. Unterstützt werden Dateien im PKCS12-, PKCS7- und PEM/DER-Format sowie RSA/DSS-Schlüssel im OpenSSH- oder Dropbear-Format. |
| enroll via SCEP | Schlüssel und Zertifikat über SCEP einbuchen; weitere Optionen siehe Kapitel 5.8.8 |
| download certificate | Schlüssel und Zertifikat im ZIP-Format herunterladen (die Dateien werden im PEM-Format kodiert) |
| create signing request | Schlüssel lokal erzeugen und eine Signieranforderung erstellen, um ein von einer anderen Stelle signiertes Zertifikat abzurufen |
| erase certificate | Alle Schlüssel und Zertifikate löschen, die mit diesem Abschnitt verbunden sind |

Tabelle 5.166.: Zertifikatsaktionen

Konfiguration

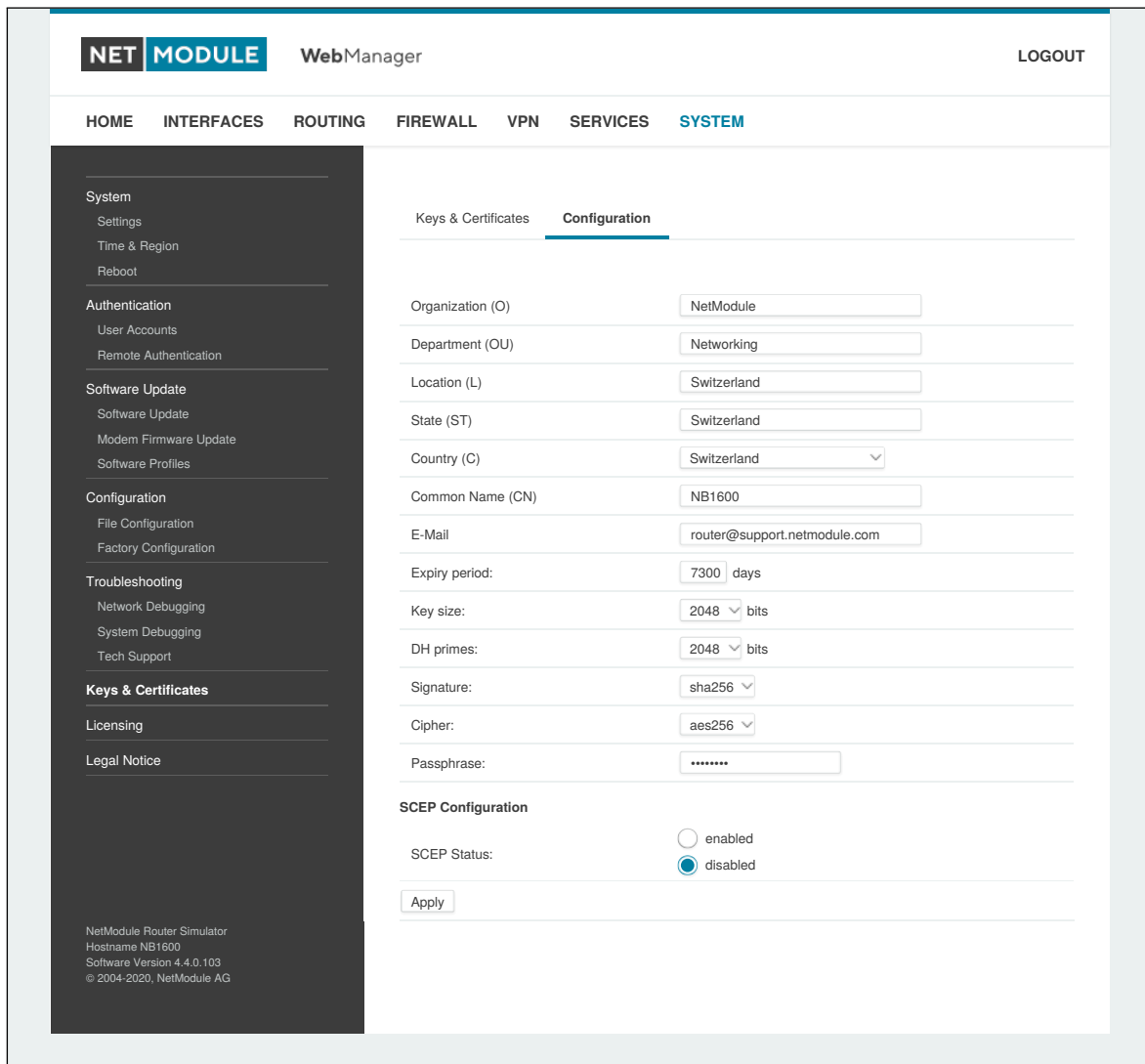


Abbildung 5.68.: Konfiguration von Zertifikaten

Auf dieser Seite können Sie einige allgemeine Konfigurationsoptionen festlegen, die bei der Arbeit mit Schlüsseln und Zertifikaten angewendet werden.

Wenn Schlüssel, Zertifikate und Signieranforderungen lokal erzeugt werden, werden die folgenden Einstellungen berücksichtigt:

| Parameter | Konfiguration von Zertifikaten |
|------------------|--|
| Organization (O) | Firma/Organisation des Zertifikatsinhabers |
| Department (OU) | Name der Organisationseinheit, zu der der Zertifikatsaussteller gehört |
| Location (L) | Standort des Zertifikatsinhabers |
| State (ST) | Bundesland/Kanton des Zertifikatsinhabers |

| Parameter | Konfiguration von Zertifikaten |
|------------------|--|
| Country (C) | Land des Zertifikatsinhabers (normalerweise als TLD-Abkürzung) |
| Common Name (CN) | Name des Zertifikatsinhabers, hauptsächlich zur Identifizierung eines Hosts verwendet |
| E-Mail | E-Mail-Adresse des Zertifikatsinhabers |
| Expiry period | Anzahl der Tage, die das Zertifikat noch gültig ist |
| Key size | Länge des privaten Schlüssels in Bit |
| DH primes | Die Anzahl der Bits für benutzerdefinierte Diffie-Hellman-Primzahlen |
| Signature | Der Signaturalgorithmus beim Signieren von Zertifikaten |
| Passphrase | Die Passphrase für den Zugriff auf einen privaten Schlüssel. Diese wird beim ersten Login (siehe Kapitel 5.1.1) mit einer zufälligen Zeichenfolge vorbelegt. |

Bitte beachten Sie, dass der lokale Zufallszahlengenerator (RNG) für die meisten Anwendungen eine recht gute Zufälligkeit bietet. Wenn eine stärkere Verschlüsselung erforderlich ist, empfehlen wir, die Schlüssel auf einem externen RNG-Gerät zu erzeugen oder alle Zertifikate komplett auf einem entfernten Zertifizierungsserver zu verwalten. Nichtsdestoweniger kann eine lokale Zertifizierungsstelle alle benötigten Zertifikate ausstellen und verwalten und auch eine Zertifikatsperrliste (CRL) führen.

Beim Importieren von Schlüsseln können die Zertifikats- und Schlüsseldatei einzeln kodiert im PEM/DER- oder PKCS7-Format hochgeladen werden. Alle Dateien (CA-Zertifikat, Zertifikat und privater Schlüssel) können auch mit dem Containerformat PKCS12 auf einen Schlag hochgeladen werden. RSA/DSS-Schlüssel können aus OpenSSH- oder Dropbear-Formaten konvertiert werden. Es ist möglich, die Passphrase zum Öffnen des privaten Schlüssels anzugeben. Hinweis: Das System wendet bei der Installation des Zertifikats generell die systemweite Zertifikatspassphrase auf einen Schlüssel an. Wenn Sie also die allgemeine Passphrase ändern, werden alle lokalen Schlüssel mit dem neuen Schlüssel ausgestattet.

SCEP-Konfiguration

Wenn Zertifikate mit Hilfe des Simple Certificate Enrollment Protocol (SCEP) registriert werden, können die folgenden Einstellungen konfiguriert werden:

| Parameter | SCEP-Konfiguration |
|-----------------------|--|
| SCEP status | Legt fest, ob SCEP aktiviert ist |
| URL | SCEP-URL, meist im Format <code>http://<Host>/<Pfad>/pkiclient.exe</code> |
| CA fingerprint | Der Fingerabdruck des Zertifikats, der zur Identifizierung der Gegenstelle verwendet wird. Wenn Sie dies leer lassen, wird jeder Zertifizierungsstelle vertraut. |
| Fingerprint algorithm | Der Fingerprint-Algorithmus zur Identifizierung der CA (MD5 oder SHA1) |
| Poll interval | Das Abfrageintervall in Sekunden für eine Zertifikatsanforderung |

| Parameter | SCEP-Konfiguration |
|-----------------|---|
| Request timeout | Die maximale Abfragedauer in Sekunden für eine Zertifikatsanforderung |
| ID type | Kann IP, E-Mail oder DNS sein |
| Password | Das Passwort für den SCEP-Server. |

Bei der Registrierung von Zertifikaten wird das CA-Zertifikat zunächst über die angegebene SCEP-URL abgerufen, und zwar über die Aktion `get.ca` - diese wird auf der Konfigurationsseite angezeigt, und es muss überprüft werden, ob sie zur richtigen Zertifizierungsstelle gehört. Andernfalls muss die CA abgelehnt werden. Dieser Teil ist bei der Verwendung von SCEP wesentlich, da er die Vertrauenskette aufbaut.

Wenn bei der Anforderung einer Zertifikatsregistrierung eine Zeitüberschreitung auftritt, kann die unterbrochene Registrierungsanforderung erneut ausgelöst und mit dem zuvor erzeugten Schlüssel fortgesetzt werden. Falls eine Anfrage abgelehnt wurde, müssen Sie das Zertifikat zunächst löschen und dann den Registriervorgang von vorn beginnen.

Zertifizierungsstellen

Gür Clientverbindungen (wie sie von SDK-Funktionen oder beim Herunterladen von Konfigurations-/Software-Images verwendet werden) können Sie eine Liste von CA-Zertifikaten hochladen, die als vertrauenswürdig gelten.

Um das CA-Zertifikat von einer bestimmten Website mit Mozilla Firefox zu erhalten, sind folgende Schritte erforderlich:

- Rufen Sie mit dem Browser die entsprechende HTTPS-Website auf.
- Klicken Sie auf das Vorhängeschloss in der Adressleiste.
- Klicken Sie auf **Mehr Informationen** und dann auf **Zertifikat ansehen**
- Wählen Sie **Details** und klicken Sie auf **Export**
- Wählen Sie einen Pfadnamen für die Datei (z. B. `website.pem`)

Zertifikate von selbstsignierten Zertifizierungsstellen können auch abgerufen werden, indem Sie Folgendes ausführen:

```
echo quit | \  
openssl s_client -showcerts -connect <host>:443 | \  
sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > other.crt
```

PEM-kodierte X.509-Zertifikatsdateien können mit einem einfachen Editor bearbeitet und verkettet (falls erforderlich) und dann auf das Gerät hochgeladen werden. Nach der Installation wird eine SSL-Client-Verbindung abgebrochen, wenn die Überprüfung mit einem dieser CA-Zertifikate fehlschlägt.

5.8.9. Lizenzierung

Bestimmte Funktionen der NetModule-Router erfordern eine gültige Lizenz im System, teilweise in Abhängigkeit von den installierten Modulen. Bitte setzen Sie sich mit uns in Verbindung, um eine gültige Lizenz für die verfügbaren Komponenten zu erhalten. Wir stellen Ihnen dann eine Lizenzdatei basierend auf Ihrer Seriennummer zur Verfügung, die Sie anschließend auf dem Router installieren können.

The screenshot shows the 'NET MODULE WebManager' interface. The top navigation bar includes 'HOME', 'INTERFACES', 'ROUTING', 'FIREWALL', 'VPN', 'SERVICES', and 'SYSTEM'. The left sidebar contains a menu with categories like System, Authentication, Software Update, Configuration, Troubleshooting, Keys & Certificates, Licensing, and Legal Notice. The main content area is titled 'License Installation' and includes options for 'Upload license file' (selected) and 'Download license from URL'. Below this is a 'License file:' field with a 'Choose File' button and the text 'No file selected'. An 'Install' button is also present. The 'Licensing Status' section shows a 'Serial number: 00112B025026' and a message 'A valid license is installed.' Below this is a table with columns 'Feature', 'Availability', and 'Licensing Status'.

| Feature | Availability | Licensing Status |
|---------|--------------|------------------|
| FMS2IP | no | unlicensed |
| GPS | yes | licensed |
| GSM | yes | licensed |
| ITXPT | no | unlicensed |
| LTE | yes | licensed |
| SERVER | yes | licensed |
| TX_ADV | yes | licensed |
| UMTS | yes | licensed |
| VIRT | no | licensed |
| VOICE | yes | licensed |
| WLAN | yes | licensed |

NetModule Router Simulator
Hostname NB1600
Software Version 4.4.0.103
© 2004-2020, NetModule AG

Abbildung 5.69.: Lizenzierung

5.8.10. Rechtlicher Hinweis

Open-Source-Software

Hiermit informieren wir Sie, dass NetModule-Produkte Open-Source-Software enthalten können. Wir stellen Ihnen diese Open-Source-Software zur Verfügung unter den Bedingungen der GNU General Public License (GPL), GNU Lesser General Public License (LGPL) oder anderen Open-Source-Lizenzen.

Diese Lizenzen erlauben das Ausführen, Kopieren, Verteilen, Untersuchen, Ändern und Verbessern von Software, die unter die GPL, Lesser GPL oder andere Open-Source-Lizenzen fällt, ohne dass wir oder unser Endbenutzer-Lizenzvertrag Einschränkungen in Bezug auf die Nutzung dieser Software vorsehen. Sofern nicht durch geltendes Recht vorgeschrieben oder schriftlich vereinbart, wird Software, die unter Open-Source-Lizenzen vertrieben wird, wie besehen, ohne ausdrückliche oder stillschweigende Gewährleistung und ohne Bedingungen gleich welcher Art, bereitgestellt.

Um den entsprechenden Open-Source-Code zu erhalten, der unter diese Lizenzen fällt, wenden Sie sich bitte an unseren technischen Support unter support@netmodule.com.

Danksagungen

Dieses Produkt enthält PHP, frei verfügbar unter <http://www.php.net>.

Dieses Produkt enthält Software des OpenSSL-Projekts zur Verwendung im OpenSSL-Toolkit (<http://www.openssl.org>).

Dieses Produkt enthält Kryptografiesoftware von Eric Young (eay@cryptsoft.com).

Dieses Produkt enthält Software von Tim Hudson (tjh@cryptsoft.com).

Dieses Produkt enthält Software von Jean-Loup Gailly und Mark Adler.

Dieses Produkt enthält die Software MD5 Message-Digest-Algorithmus von RSA Data Security, Inc.

Dieses Produkt enthält eine Implementierung des AES-Verschlüsselungsalgorithmus, basierend auf dem von Dr. Brian Gladman veröffentlichten Code.

Arithmetischer Code für Operationen mit mehrfacher Genauigkeit, ursprünglich von David Ireland geschrieben

Software aus dem FreeBSD-Projekt (www.freebsd.org)

Copyright (c) 2023, NetModule. Alle Rechte vorbehalten.



5.9. ABMELDEN

In diesem Menü melden Sie sich beim Web Manager ab.

6. Kommandozeile (CLI)

Die Befehlszeile (Command Line Interface, CLI) ist eine allgemeingültige Steuerungsschnittstelle für den Router: Hier können Sie Konfigurationsparameter abrufen oder setzen, Updates anwenden, Dienste neu starten oder andere Systemaufgaben durchführen.

Sie wird automatisch im interaktiven Modus gestartet, wenn Sie sich als *admin* anmelden oder den Befehl `cli -i` eingeben. Es gilt jedoch die gleiche Syntax, wie wenn Sie sie von der System-Shell aus aufrufen. Eine Liste der verfügbaren Befehle erhalten Sie mit `cli -l`.

Die CLI unterstützt die TAB-Vervollständigung, d. h. das Erweitern eingegebener Wörter oder Wortfragmente durch Drücken der TAB-Taste zu einem beliebigen Zeitpunkt. Dies gilt für Befehle, aber auch für einige Argumente, und ist eine bequemere Möglichkeit, mit der Shell zu arbeiten.

Hinweis: Jede CLI-Sitzung führt nach einer bestimmten Zeit der Inaktivität (standardmäßig 10 Minuten) eine automatische Abmeldung aus. Dieses Verhalten kann ausgeschaltet werden mit dem Befehl `no-autologout`.

6.1. Arbeiten mit der Befehlszeile

Wenn Sie mit der Befehlszeile im interaktiven Modus betreiben, wird jeder eingegebene Befehl mit der EINGABETASTE abgeschlossen. Mit den Tasten PFEIL-NACH-LINKS und PFEIL-NACH-RECHTS können Sie die Schreibmarke zwischen den eingegebenen Zeichen bewegen. Mit den Tasten PFEIL-NACH-OBEN und PFEIL-NACH-UNTEN können Sie die Liste der bisher eingegebenen Befehle durchblättern. Wenn Sie `exit` gefolgt von der EINGABETASTE eingeben oder auf einer leeren Befehlszeile `STRG-c` oder `STRG-d` zweimal drücken, wird der Befehlszeilenmodus beendet. (Hinweis: Auf Schweizer Tastaturen ist die `STRG`-Taste mit `CTRL` beschriftet.)

Liste der unterstützten Tastenkombinationen:

| Tastenkombination | Action |
|-----------------------|---|
| <code>STRG-a</code> | An den Anfang der Zeile bewegen |
| <code>STRG-e</code> | An das Ende der Zeile bewegen |
| <code>STRG-f</code> | Ein Zeichen nach rechts bewegen |
| <code>STRG-b</code> | Ein Zeichen nach links gehen |
| <code>ALT-f</code> | Nach rechts zum Ende des nächsten Wortes gehen |
| <code>ALT-b</code> | Nach links zum Anfang des aktuellen oder vorherigen Wortes gehen |
| <code>STRG-l</code> | Bildschirm löschen und nur die aktuelle Zeile am oberen Bildschirmrand anzeigen bei Angabe eines Arguments die aktuelle Zeile aktualisieren, ohne den Bildschirm zu löschen |
| <code>STRG-p</code> | Vorigen Befehl aus der Verlaufsliste anzeigen |
| <code>STRG-n</code> | Nächsten Befehl aus der Verlaufsliste anzeigen |
| <code>ALT-<</code> | Ersten Befehl der Verlaufsliste zeigen |
| <code>ALT-></code> | Letzten Befehl der Verlaufsliste zeigen |
| <code>STRG-r</code> | Rückwärts suchen, beginnend bei der aktuellen Zeile und aufwärts durch die Verlaufsliste |

| Tastenkombination | Action |
|-------------------|---|
| STRG-s | Sitzung einfrieren |
| STRG-q | Eingefrorene Sitzung reaktivieren |
| STRG-d | Zeichen an der Schreibmarke löschen (oder CLI beenden, wenn die Schreibmarke am Anfang einer leeren Zeile steht) |
| STRG-t | Zeichen vor der Schreibmarke mitsamt der Schreibmarke eine Position nach links ziehen; wenn sich die Schreibmarke am Ende der Zeile befindet, werden die beiden Zeichen davor vertauscht |
| ALT-t | Zeichen vor der Schreibmarke mitsamt der Schreibmarke eine Position nach rechts ziehen; wenn sich die Schreibmarke am Ende der Zeile befindet, werden die beiden Wörter davor vertauscht. |
| STRG-k | Text von der Schreibmarke bis zum Ende der Zeile löschen |
| STRG-y | Anfang des gelöschten Textes an der Schreibmarke in den Puffer ziehen |

Hinweis: Bei Argumenten, die Leerzeichen enthalten, müssen gegebenenfalls Anführungszeichen (") gesetzt werden.

6.2. Hilfe ausgeben

Der Befehl `help` zeigt die Liste der verfügbaren Befehle an, wenn er ohne Argumente aufgerufen wird; anderenfalls die Syntax des angegebenen Befehls.

```
> help
Syntax:
    help [<Befehl>]
```

Verfügbare Befehle

| | |
|----------------------------|---|
| <code>get</code> | Konfigurationsparameter abrufen |
| <code>set</code> | Konfigurationsparameter setzen |
| <code>done</code> | Abschluss der Konfigurationsarbeiten prüfen |
| <code>update</code> | Systemressourcen aktualisieren |
| <code>cert</code> | Schlüssel und Zertifikate verwalten |
| <code>status</code> | Statusinformationen abrufen |
| <code>scan</code> | Netzwerke scannen |
| <code>send</code> | E-Mail oder SMS an mail, sms, techsupport, ussd |
| <code>restart</code> | Dienste neu starten |
| <code>debug</code> | System debuggen |
| <code>reset</code> | System auf Werkseinstellungen zurücksetzen |
| <code>reboot</code> | System neu starten |
| <code>shell</code> | Shell-Befehl ausführen |
| <code>help</code> | Hilfe für Befehl ausgeben |
| <code>no-autologout</code> | Auto-Logout deaktivieren |
| <code>history</code> | Befehlsverlauf anzeigen |
| <code>exit</code> | Beenden |

6.3. Konfigurationsparameter abrufen

Der Befehl `get` ruft Konfigurationswerte ab.

```
> get -h
Syntax:
    get [-hsvfc] <Parameter> [<Parameter>..]
```

Argumente:

- s quelldatenfähige Ausgaben erzeugen
- v Konfigurationsparameter validieren
- f Werksvoreinstellung statt aktuellem Wert laden
- c Konfigurationsabschnitte anzeigen

6.4. Konfigurationsparameter setzen

Der Befehl `set` stellt Konfigurationswerte ein.

```
> set -h
Syntax:
    set [-hv] <Parameter>=<Wert> [<Parameter>=<Wert>..]
```

Argumente:

- v Konfigurationsparameter validieren

6.5. Abschluss der Konfigurationsarbeiten prüfen

Der Befehl `done` überprüft, ob nach einer Konfigurationsänderung alle Änderungsskripte abgeschlossen wurden.

```
> done -h
Syntax:
    done [-h]
```

6.6. Statusinformationen abrufen

Der Befehl `status` zeigt verschiedene Statusinformationen des Systems an.

```
> status -h
Syntax:
    status [-hs] <Abschnitt>
```

Argumente:

- s quelldatenfähige Ausgaben erzeugen

Verfügbare Abschnitte:

summary Kurze Statuszusammenfassung

| | |
|---------------|---|
| info | System- und Konfigurationsinformationen |
| config | Aktuelle Konfiguration |
| system | Systeminformation |
| configuration | Konfigurationsinformationen |
| license | Lizenzinformationen |
| wwan | Status des WWAN-Moduls |
| wlan | Status des WLAN-Moduls |
| gnss | Status des GNSS- (GPS-) Moduls |
| eth | Status der Ethernet-Schnittstelle |
| lan | Status der LAN-Schnittstelle |
| wan | Status der WAN-Schnittstelle |
| openvpn | OpenVPN-Verbindungsstatus |
| ipsec | IPsec-Verbindungsstatus |
| pptp | PPTP-Verbindungsstatus |
| gre | GRE-Verbindungsstatus |
| dialin | Dial-In-Verbindungsstatus |
| mobileip | Status von MobileIP |
| dio | Status des digitalen Ein-/Ausgangs |
| audio | Status des Audiomoduls |
| can | Status des CAN-Moduls |
| uart | Status des UART-Moduls |
| ibis | Status des IBIS-Moduls |
| redundancy | Redundanzstatus |
| sms | SMS-Status |
| firewall | Firewall-Status |
| qos | QoS-Status |
| neigh | Nachbarschaftsstatus |
| location | Aktueller Standort |

6.7. Netzwerke scannen

Der Befehl `scan` sucht nach verfügbaren WWAN- und WLAN-Netzwerken.

```
> scan -h
Syntax:
    scan [-hs] <Schnittstelle>
```

Argumente:

- `-s` quelldatenfähige Ausgaben erzeugen

6.8. E-Mail oder SMS senden

Der Befehl `send` sendet eine Nachricht per E-Mail/SMS an die angegebene Adresse/Telefonnummer.

```
> send -h
Syntax:
    send [-h] <Typ> <Ziel> <Text>
```

Argumente:

- `<Typ>` Art der zu sendenden Nachricht (mail, sms, techsupport, ussd)
- `<Ziel>` Ziel der Nachricht (Mail-Adresse, Rufnummer oder Index)
- `<Text>` Zu sendende Nachricht

6.9. Systemressourcen aktualisieren

Der Befehl `update` aktualisiert verschiedenen Systemressourcen.

```
> update -h
```

Syntax:

```
update [-hfrsn] <software|config|license|sshkeys> <URL>
```

Argumente:

```
-r      Neustart nach Update
-f      Update erzwingen
-n      Fehlende Konfigurationswerte nicht auf Standard zurücksetzen
-s      Update-Status anzeigen
```

Verfügbare Update-Ziele:

```
software      Software-Update durchführen
firmware      Modul-Firmware-Update durchführen
config        Konfiguration aktualisieren
license       Lizenzen aktualisieren
sshkeys       Autorisierte SSH-Schlüssel installieren
```

Sie können auch `update software latest` ausführen, um die neueste Version von unserem Server zu installieren.

6.10. Schlüssel und Zertifikate verwalten

Der Befehl `cert` verwaltet Schlüssel und Zertifikate.

```
> cert -h
```

Syntax:

```
cert [-h] [-p Passphrase] <Aktion> <Zertifikat> [<url>]
```

Mögliche Aktionen:

```
install       Zertifikat von der angegebenen URL installieren
create        Zertifikat lokal erzeugen
enroll        Zertifikat über SCEP registrieren
erase         Installiertes Zertifikat löschen
view          Installiertes Zertifikat anzeigen
```

6.11. Dienste neu starten

Der Befehl `restart` startet Systemdienste neu.

```
> restart -h
```

Syntax:

```
restart [-h] <Dienst>
```

Verfügbare Dienste:



| | |
|--------------|-----------------------|
| configd | Konfigurations-Daemon |
| dnsmasq | DNS-/DHCP-Server |
| dropbear | SSH-server |
| firewall | Firewall und NAT |
| gpsd | GPS-Daemon |
| gre | GRE-Verbindungen |
| ipsec | IPsec-Verbindungen |
| lighttpd | HTTP-Server |
| link-manager | WAN-Verbindungen |
| network | Netzwerk allgemein |
| openvpn | OpenVPN-Verbindungen |
| pptp | PPTP-Verbindungen |
| qos | QoS-Daemon |
| smsd | SMS-Daemon |
| snmpd | SNMP-Daemon |
| surveyor | Supervisions-Daemon |
| syslog | Syslog-Daemon |
| telnet | Telnet-Server |
| usbipd | USB-/IP-Daemon |
| voiced | Voice-Daemon |
| vrrpd | VRRP-Daemon |
| wlan | WLAN-Schnittstellen |
| wwan-manager | WWAN-Manager |

6.12. System debuggen

Der Befehl debug zeigt Debug-/Protokollmeldungen an.

```
> debug -h
Syntax:
    debug [-h] <Ziel>
```

Verfügbare Debug-Ziele:

```
configd
event-manager
home-agent
+led-manager
link-manager
mobile-node
qmid
qosd
scripts
sdkhost
ser2net
smsd
surveyor
swupdate
system
voiced
watchdog
wwan-manager
wwanmd
```

6.13. System auf Werkseinstellungen zurücksetzen

Der Befehl `reset` setzt den Router auf die Werkseinstellungen zurück.

```
> reset -h
Syntax:
    reset [-h]
```

6.14. System neu starten

Der Befehl `reboot` startet den Router neu.

```
> reboot -h
Syntax:
    reboot [-h]
```

6.15. Shell-Befehl ausführen

Der Befehl `shell` ruft eine System-Shell auf und kann eine beliebige Anwendung starten oder ein Skript anstoßen

```
> shell -h
Syntax:
    shell [-h] [<Befehl>]
```

6.16. Arbeiten mit der Verlaufsliste

Der Befehl `history` gibt die Liste der eingegebenen Befehle (pro Benutzer) aus.

```
> history -h
Syntax:
    history [-c]
```

Die Verlaufsliste kann gelöscht werden mit `history -c`.

6.17. CLI-PHP

Es ist in der Werkskonfiguration aktiviert, kann also für Einrichtungszwecke verwendet werden, wird aber deaktiviert, sobald das Administratorkonto eingerichtet ist.

Der Dienst kann später ein-/ausgeschaltet werden, indem Sie den Konfigurationsparameter `cliphp.status` angeben:

| | |
|------------------------------|------------------------|
| <code>cliphp.status=0</code> | Dienst ist deaktiviert |
| <code>cliphp.status=1</code> | Dienst ist aktiviert |

Dieser Abschnitt beschreibt die CLI-PHP-Schnittstelle für Version 2. Sie akzeptiert POST- und GET-Anforderungen.



Achtung

Die folgenden Beispiele verwenden der besseren Verständlichkeit und Nachvollziehbarkeit halber GET und HTTP. Für den Produktiveinsatz sollten POST und HTTPS verwendet werden. Bitte beachten Sie, dass die Browser-Historie GET-Anfragen inklusive der versendeten Passwörter und anderer ggf. sensitiven Daten speichert, wenn Sie einen Web-Browser verwenden, um die Beispiele nachzuvollziehen oder das Interface zu testen.

Bei GET-Anfragen ist die allgemeine Verwendung wie folgt definiert:

Syntax:

```
http(s)://cli.php?<Param1>=<Wert1>&<Param2>=<Wert2>..<ParamN>=<WertN>
```

Verfügbare Parameter:

| | |
|-------------|--|
| output | Ausgabeformat (HTML, Text) |
| usr | Benutzername für die Authentifizierung |
| pwd | Passwort für die Authentifizierung |
| command | Auszuführender Befehl |
| arg0..arg31 | An Befehle übergebene Argumente |

Hinweise:

Die Befehle entsprechen den CLI-Befehlen, wie sie von "`cli -l`" angezeigt werden ; die Argumente (`arg0..arg31`) werden direkt an die Befehlszeile übergeben.

Eine URL, die die folgende Sequenz enthält:

```
command=get&arg0=admin.password&arg1=admin.debug
```

bewirkt, dass die CLI so aufgerufen wird:

```
cli get "admin.password" "admin.debug"
```

Leerzeichen werden unterstützt, doch sind alle Sonderzeichen der URL laut RFC1738 anzugeben (das übernehmen gängige Clients wie

wget, lynx, curl).

Rückgabewerte:

Die zurückgegebene Antwort enthält immer eine Statuszeile im Format:

```
<Rückgabewert>: <Text>
```

mit den Rückgabewerten OK bei Erfolg und ERROR bei Misserfolg. Anschließend folgen alle Ausgaben der aufgerufenen Befehle.

Beispiele:

```
OK: status command successful
ERROR: authentication failed
```

status - Statusinformationen abrufen

Syntax:

```
command=status[&arg0=<Abschnitt>]
```

Hinweise:

Die Liste der verfügbaren Abschnitte wird abgerufen mit
"command=status&arg0=-h".

Bitte beachten Sie, dass die Statuszusammenfassung auch ohne Authentifizierung angezeigt werden kann.

Beispiele:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
status&arg0=-h
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
status&arg0=summary
```

```
http://192.168.1.1/cli.php?version=2&output=html&command=status
```

get - Konfigurationsparameter abrufen

Syntax:

```
command=get&arg0=<Konfig.-Schlüssel>[&arg1=<Konfig.-Schlüssel>..]
```

Beispiele:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
get&arg0=config.version
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
get&arg0=openvpn.status&arg1=snmp.status&arg2=ipsec.status
```

set - Konfigurationsparameter setzen

Syntax:

```
command=set&arg0=<Konfig.-Param.>&arg1=<Konfig.-Wert>[&arg2=<Konfig.-Param.>&
arg3=<Konfig.-Wert>..]
```

Hinweise:

Im Gegensatz zu den anderen Befehlen benötigt dieser Befehl wegen des reservierten "="-Zeichens eine Menge von Tupeln als Argumente, d. h.
[arg0=key0, arg1=val0], [arg2=key1, arg3=val1], [arg4=key2, arg5=val2], usw.

Beispiele:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
set&arg0=snmp.status&arg1=1
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
set&arg0=snmp.status&arg1=0&arg2=openvpn.status&arg3=1
```

restart - Dienste neu starten

Syntax:

```
command=restart&arg0=<Dienst>
```

Hinweise:

Die Liste der verfügbaren Dienste wird abgerufen mit `"command=restart&arg0=-h"`

Beispiele:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
restart&arg0=-h
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
restart&arg0=link-manager
```

reboot - Systemneustart auslösen

Syntax:

```
command=reboot
```

Beispiele:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
reboot
```

reset - Zurücksetzen auf Werkseinstellungen

Syntax:

```
command=reset
```

Beispiele:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
reset
```

update - Systemressourcen aktualisieren

Syntax:

```
command=update&arg0=<Ressource>&arg1=<URL>
```

Hinweise:

Die Liste der verfügbaren Ressourcen wird abgerufen mit `"command=update&arg0=-h"`

Beispiele:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=update&arg0=software&arg1=tftp://192.168.1.254/latest
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=update&arg0=config&arg1=tftp://192.168.1.254/user-config.zip
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=update&arg0=license&arg1=http://192.168.1.254/xxx.lic
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=update&arg0=firmware&arg1=wwan0&arg2=tftp://192.168.1.254/firmware
```

send - SMS senden

Syntax:

```
command=send&arg0=sms&arg1=<Zahl>&arg2=<Text>
```

Hinweise:

Die Rufnummer muss im internationalen Format angegeben werden, z. B. +123456789 einschließlich eines führenden Pluszeichens (das als %2B verschlüsselt werden kann). Der SMS-Daemon muss ordnungsgemäß konfiguriert sein, bevor Sie diese Funktion verwenden können.

Beispiele:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=send&arg0=sms&arg1=%2B123456789&arg2=test
```

send - E-Mail senden

Syntax:

```
command=send&arg0=mail&arg1=<Adresse>&arg2=<Text>
```

Hinweise:

Die Adresse muss eine gültige E-Mail-Adresse sein, z. B. abc@abc.com (das at-Zeichen kann als %40 kodiert werden). Der E-Mail-Client muss ordnungsgemäß konfiguriert sein, bevor Sie diese Funktion verwenden können.

Beispiele:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=send&arg0=mail&arg1=abc%40abc.com&arg2=test
```

send - An Technischen Support senden

Syntax:

```
command=send&arg0=techsupport&arg1=stdout  
command=send&arg0=techsupport&arg1=<Adresse>&arg2=<Betreff>
```


Hinweise:

Die Adresse muss eine gültige E-Mail-Adresse sein, z. B. abc@abc.com (das at-Zeichen kann als %40 kodiert werden). Der E-Mail-Client muss ordnungsgemäß konfiguriert sein, bevor Sie diese Funktion verwenden können.

Im Falle von "stdout" als Ausgabe erhält die heruntergeladene Support-Datei den Namen "download".

Beispiele:

```
http://192.168.1.1/cli.php?version=2&output=mime&usr=admin&pwd=admin01&command=send&arg0=techsupport&arg1=stdout
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=send&arg0=techsupport&arg1=abc%40abc.com&arg2=subject
```

send - USSD-Code senden**Syntax:**

```
command=send&arg0=ussd&arg1=<Karte>&arg2=<Code>
```

Hinweise:

Das Argument <Karte> gibt den Kartenmodulindex an (z. B. 0 für wwan0). Der USSD-Code kann aus Ziffern, Pluszeichen, Sternchen (kann als %2A codiert werden) und Bindestrichen (kann als %23 codiert werden) bestehen.

Beispiele:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=send&arg0=ussd&arg1=0&arg2=%2A100%23
```

A. Anhang

A.1. Abkürzungen

| Abkürzung | Beschreibung |
|-----------|--|
| ANY | Bezieht sich auf alle Optionen, die der aktuelle Abschnitt bietet |
| APN | Access Point Name (Name des Zugangspunkts) |
| ASU | Arbitrary Strength Unit (Maßeinheit für Empfangsfeldstärke) |
| CID | Cell ID (eine allgemeine eindeutige Nummer zur Identifizierung einer Base Transceiver Station, BTS) |
| CID | Zell-ID |
| CLI | Command Line Interface (Befehlszeilenschnittstelle zum Abfragen des Routers oder zum Ausführen von Systemaufgaben) |
| DHCP | Dynamic Host Configuration Protocol (dynamisches Host-Konfigurationsprotokoll) |
| DNS | Domain Name System (Domainnamensystem) |
| ETHx | Ethernet-Schnittstellen (einzelne oder geschwichte) |
| FQDN | Fully qualified domain name (vollständig qualifizierter Domainname) |
| GNSSx | Ein Modul des Global Navigation Satellite System |
| ICCID | Integrated Circuit Card Identifier (einmalige Identifikationsnummer der SIM-Karte) |
| IMEI | International Mobile Station Equipment Identity (Seriennummer, das jedes GSM- oder UMTS-Endgerät weltweit eindeutig identifiziert) |
| IMSI | International Mobile Subscriber Identity (interne Mobilfunk-Teilnehmerkennung) |
| INx | Ein digitaler E/A-Eingang (DIx) |
| LAC | Location Area Code (Aufenthaltsbereichskennzahl, Teil der LAI) |
| LAC | Location Area Code (Kennung einer Gruppe von Basisstationen, die zum Optimieren der Signalisierung gruppiert sind) |
| LAI | Location Area Identification (Kennzeichnung des Aufenthaltsbereich innerhalb eines Mobilfunknetzes) |
| LAI | Location Area Identity (weltweit eindeutige Nummer, die das Land, den Netzbetreiber und den Standortbereich identifiziert) |
| LANx | LAN-Schnittstellen, die in der Regel auf Ethernet-Schnittstellen basieren (einschließlich Bridges) |
| MCC | Mobile Country Code (Teil der LAI) |
| MEID | Mobile Equipment Identifier (eindeutige Seriennummer von UMTS-Endgeräten) |
| MNC | Mobile Network Code (Teil der LAI) |



| Abkürzung | Beschreibung |
|-----------------------|---|
| Mobile _x | Ein WWAN-Modem |
| MOBILEIP _x | Bezieht sich auf eine Mobile-IP-Tunnel-Schnittstelle |
| MSISDN | Mobile Subscriber Integrated Services Digital Network Number (weltweit eindeutige Rufnummer eines Mobilfunkteilnehmers) |
| MSS | Maximum Segment Size (maximale Segmentgröße) |
| MTU | Maximum Transmission Unit (maximale Größe der Übertragungseinheit) |
| NAPT | Network Address and Port Translation (Netzwerkadresse und Portübersetzung) |
| OUT _x | Ein digitaler I/O-Ausgang (DO _x) |
| PPTP _x | Eine PPTP-Tunnel-Schnittstelle an |
| RSRP | Reference Signal Received Power (Referenzsignal Empfangsleistung) |
| RSRQ | Reference Signal Received Quality (Referenzsignal Empfangsqualität) |
| SDK | Script Development Kit (für die Anwendungsprogrammierung) |
| SERIAL _x | Eine serielle Schnittstelle |
| SIM _x | Ein SIM-Steckplatz, wie auf der Frontplatte zu sehen |
| SIM | Subscriber Identity Module (Identitätsmodul, insbesondere für den Mobilfunk) |
| SMS | Short Message System (Kurzmitteilungsdienst) |
| SSID | Service Set Identifier (wird verwendet, um mehrere WLAN-Netzwerke auf einem Modul zu implementieren) |
| STP | Spanning Tree Protocol (Teil einer Switch-Infrastruktur) |
| TAP _x | Eine OpenVPN-Tunnel-Schnittstelle (basierend auf TAP) |
| TUN _x | Eine OpenVPN-Tunnel-Schnittstelle (basierend auf TUN) |
| USSD | Unstructured Supplementary Service Data (Steuerbefehle im GSM-Mobilfunknetz) |
| VPN | Virtual Private Network (virtuelles privates Netzwerk) |
| VRRP | Virtual Router Redundancy Protocol (Verfahren zur Steigerung der Verfügbarkeit wichtiger Gateways im LAN) |
| WAN | WAN-Verbindungen umfassen alle WAN-Schnittstellen, die derzeit im System aktiviert sind |
| WLAN _x | Eine Wireless-LAN-Schnittstelle, die als zusätzliche LAN-Schnittstelle dargestellt wird, wenn sie als Access Point konfiguriert ist |
| WWAN _x | Eine Wireless-Wide-Area-Network- (2G/3G/4G-) Verbindung |

| Abkürzung | Beschreibung |
|-----------|--------------|
|-----------|--------------|

Tabelle A.1.: Abkürzungen

Interne Schnittstellen werden in der Regel klein geschrieben und können auch einer anderen Namensgebung folgen. Ihr Index beginnt bei 0. Die vom Benutzer gesehenen Schnittstellen werden in Großbuchstaben geschrieben, ihr Index beginnend bei 1.

A.2. System-Ereignisse

| ID | Ereignis | Beschreibung |
|-----|---------------------|-----------------------------------|
| 101 | wan-up | WAN-Verbindung aufgebaut |
| 102 | wan-down | WAN-Verbindung unterbrochen |
| 201 | dio-in1-on | DIO IN1 eingeschaltet |
| 202 | dio-in1-off | DIO IN1 ausgeschaltet |
| 203 | dio-in2-on | DIO IN2 eingeschaltet |
| 204 | dio-in2-off | DIO IN2 ausgeschaltet |
| 205 | dio-out1-on | DIO OUT1 eingeschaltet |
| 206 | dio-out1-off | DIO OUT1 ausgeschaltet |
| 207 | dio-out2-on | DIO OUT2 eingeschaltet |
| 208 | dio-out2-off | DIO OUT2 ausgeschaltet |
| 301 | gps-up | GPS-Signal verfügbar |
| 302 | gps-down | GPS-Signal nicht verfügbar |
| 401 | openvpn-up | OpenVPN-Verbindung aufgebaut |
| 402 | openvpn-down | OpenVPN-Verbindung unterbrochen |
| 403 | ipsec-up | IPsec-Verbindung aufgebaut |
| 404 | ipsec-down | IPsec-Verbindung unterbrochen |
| 406 | pptp-up | PPTP-Verbindung aufgebaut |
| 407 | pptp-down | PPTP-Verbindung unterbrochen |
| 408 | dialin-up | Dial-In-Verbindung aufgebaut |
| 409 | dialin-down | Dial-In-Verbindung unterbrochen |
| 410 | mobileip-up | Mobile IP-Verbindung aufgebaut |
| 411 | mobileip-down | Mobile IP-Verbindung unterbrochen |
| 412 | gre-up | GRE-Verbindung aufgebaut |
| 413 | gre-down | GRE-Verbindung unterbrochen |
| 501 | system-login-failed | Anmeldung fehlgeschlagen |

| ID | Ereignis | Beschreibung |
|------|------------------------|---|
| 502 | system-login-succeeded | Anmeldung erfolgreich |
| 503 | system-logout | Benutzer abgemeldet |
| 504 | system-rebooting | Systemneustart eingeleitet |
| 505 | system-startup | System gestartet |
| 506 | test | Testereignis |
| 507 | sdk-startup | SDK gestartet |
| 508 | system-time-updated | Systemzeit aktualisiert |
| 509 | system-poweroff | Systemabschaltung ausgelöst |
| 510 | system-error | System befindet sich im Fehlerzustand |
| 511 | system-no-error | System hat Fehlerzustand verlassen |
| 601 | sms-sent | SMS gesendet |
| 602 | sms-notsent | SMS nicht gesendet |
| 603 | sms-received | SMS empfangen |
| 604 | sms-report-received | SMS-Bericht empfangen |
| 701 | call-incoming | Eingehender Sprachanruf |
| 702 | call-outgoing | Abgehender Sprachanruf wird aufgebaut |
| 801 | ddns-update-succeeded | Aktualisierung des Dynamic DNS erfolgreich |
| 802 | ddns-update-failed | Aktualisierung des Dynamic DNS fehlgeschlagen |
| 901 | usb-storage-added | USB-Speichergerät hinzugefügt |
| 902 | usb-storage-removed | USB-Speichergerät entfernt |
| 903 | usb-eth-added | USB-Ethernet-Gerät hinzugefügt |
| 904 | usb-eth-removed | USB-Ethernet-Gerät entfernt |
| 905 | usb-serial-added | Seriell USB-Gerät hinzugefügt |
| 906 | usb-serial-removed | Seriell USB-Gerät entfernt |
| 1001 | redundancy-master | Router ist jetzt der Master-Router |
| 1002 | redundancy-backup | Router ist jetzt der Backup-Router |

Tabelle A.2.: Systemereignisse



A.3. Werkseinstellungen

Die Werkskonfiguration einschließlich der Standardwerte für jeden Konfigurationsparameter kann aus der Datei `/etc/config/factory-config.cfg` auf dem Router ausgelesen werden. Sie können auch `cli get -f <Parameter>` aufrufen, wenn Sie einen bestimmten Standardwert ermitteln möchten.



A.4. SNMP VENDOR MIB

Die NetModule SNMP VENDOR MIB kann hier bezogen werden,
<https://share.netmodule.com/public/system-software/latest/NETMODULE-VENDOR-MIB.mib>.

A.5. SDK-Beispiele

| Ereignis | Beschreibung des Skripts |
|----------------------------|---|
| best-operator.are | Sucht beim Start nach Betreibernetzen und wählt dasjenige mit dem besten Signal aus |
| candump.are | Kann zum Empfang von CAN-Nachrichten verwendet werden |
| config-summary.are | Zeigt eine Zusammenfassung der aktuell laufenden Konfiguration an |
| dio.are | Legt einen digitalen Ausgangsport fest |
| dio-monitor.are | Überwacht die DIO-Ports und sendet eine SMS an die angegebene Rufnummer |
| dio-server.are | Implementiert einen TCP-Server zur Steuerung der DIO-Ports |
| dynamic-operator.are | Scannt Mobile2 und wählt die entsprechende SIM auf Mobile1 an |
| email-to-sms.are | Implementiert einen kompakten SMTP-Server, der E-Mails empfangen und als SMS an eine Telefonnummer weiterleiten kann. |
| etherwake.are | Kann einen schlafenden Host aufwecken (WakeOnLan) |
| gps-broadcast.are | Sendet den lokalen GPS-NMEA-Stream an einen entfernten UDP-Server (inkl. Geräteidentität) |
| gps-monitor.are | Aktiviert WLAN, sobald die GPS-Position (lat,lon) innerhalb eines bestimmten Bereichs liegt |
| gps-udp-client.are | Sendet den lokalen GPS-NMEA-Stream an einen entfernten UDP-Server |
| gps-udp-client-compat.are | Sendet den lokalen GPS-NMEA-Stream an einen entfernten UDP-Server (inkl. seriell/Prüfsumme) |
| led.are | Schaltet eine LED ein |
| modbus-rtu-master.are | Kann Nachrichten von der seriellen Schnittstelle lesen |
| modbus-rtu-slave.are | Implementiert einen Modbus-Slave-Server |
| modbus-tcp-rtu-gateway.are | Implementiert ein Modbus-TCP-RTU-Gateway |
| mount-media.are | Meldet einen USB-Speicherstick an |
| opcua-browse.are | Sucht nach Knoten an einem entfernten OPC-UA-Server |
| opcua-json.are | Fragt beliebige Temperaturknoten eines OPC-UA-Servers ab und sendet sie JSON-kodiert an einen Remote-Server |
| opcua-read.are | Liest den Knotenwert an einem OPC-UA-Server aus |
| opcua-write.are | Schreibt einen neuen Wert in einen Knoten an einem OPC-UA Server |
| ping-supervision.are | Überwacht einen bestimmten Host. |
| read-config.are | Liest einen Konfigurationsparameter aus |
| remote-mail.are | Liest und sendet E-Mails von einem Remote-IMAP-/POP3-/SMTP-Server |

| Ereignis | Beschreibung des Skripts |
|--------------------------|--|
| scan-mobile.are | Wechselt die Mobile LAI entsprechend den verfügbaren Netzwerken |
| scan-wlan.are | Wechselt das WLAN-Client-Netzwerk je nach Verfügbarkeit |
| send-mail.are | Sendet eine E-Mail an die angegebene Adresse |
| send-sms.are | Sendet eine SMS an die angegebene Rufnummer |
| send-techsupport.are | Erzeugt eine Datei für den technischen Support und sendet sie an die angegebene E-Mail-Adresse |
| serial-read.are | Kann Nachrichten von der seriellen Schnittstelle lesen |
| serial-readwrite.are | Schreibt auf die serielle Schnittstelle und liest von ihr |
| serial-tcp-broadcast.are | Liest Mitteilungen, die von der seriellen Schnittstelle kommen, und leitet sie über TCP an Remote-Hosts weiter (und umgekehrt) |
| serial-tcsetattr.are | Legt Attribute der seriellen Schnittstelle fest oder liest sie aus |
| serial-udp-server.are | Liest Mitteilungen von der seriellen Schnittstelle und leitet sie per UDP an einen Remote-Host weiter (und umgekehrt) |
| serial-write.are | Schreibt eine Mitteilung auf die serielle Schnittstelle |
| set-ipsec-route.are | Legt die Route zum IPSEC-Server abhängig vom aktiven WWAN-/WLAN-Netzwerk fest |
| sms-confirm.are | Sendet eine Mitteilung und bestätigt deren Zustellung |
| sms-control.are | Führt per SMS empfangene Befehle aus |
| sms-delete-inbox.are | Leert den SMS-Posteingang |
| sms-read-inbox.are | Liest den SMS-Posteingang aus |
| sms-to-email.are | Leitet eingehende SMS an eine E-Mail-Adresse weiter |
| sms-to-serial.are | Schreibt eine eingegangene SMS auf die serielle Schnittstelle |
| snmp-agent.are | Erweitert die MIB-Einträge des SNMP-Agenten |
| snmp-cmd.are | Gibt SNMP set/get-Befehle aus |
| snmp-trap.are | Sendet SNMP-Traps |
| status.are | Zeigt den Inhalt aller Statusvariablen an |
| syslog.are | Trägt eine einfache Meldung in das Systemprotokoll ein |
| tcpclient.are | Sendet eine Mitteilung an einen TCP-Server. |
| tcpserver.are | Implementiert einen TCP-Server, der Mitteilungen empfangen kann. |
| techsupport.are | Überträgt eine Datei für den technischen Support an einen Remote-FTP-Server |
| transfer.are | Speichert die letzten GNSS-Positionen in einer Datei auf einem Remote-FTP-Server |
| transfer-file.are | Archiviert eine entfernte Datei |
| udpclient.are | Sendet eine Nachricht an einen Remote-UDP-Server |



| Ereignis | Beschreibung des Skripts |
|----------------------------|---|
| udp-msg-server.are | Setzt einen UDP-Server auf, der Mitteilungen empfängt und als SMS/E-Mail weiterleitet |
| udpserver.are | Implementiert einen UDP-Server der Mitteilungen empfängt |
| update-config.are | Nimmt ein Konfigurations-Update vor |
| voice-dispatcher-audio.are | Implementiert einen Audio-Voice-Dispatcher |
| webpage.are | Erzeugt eine Seite, die im Web Manager angezeigt werden kann |
| write-config.are | Setzt einen Konfigurationsparameter |

Tabelle A.3.: SDK-Beispiele