Ergänzende Information zu Release 10.1.9

IPSec - IKEv2 Initiator Mode

Mit Release 10.1.9 unterstützen Geräte der RS-Serie den IKEv2 Initiator Mode. Sie können damit bei der Aushandlung der Phase 1 mit IKEv2 auch als Initiator und nicht nur als Responder eingesetzt werden. Eine besondere Konfiguration ist nicht erforderlich.

Release Notes

10.1.4

Rechtlicher Hinweis

Gewährleistung

Änderungen in dieser Veröffentlichung sind vorbehalten.

bintec elmeg GmbH gibt keinerlei Gewährleistung auf die in dieser Bedienungsanleitung enthaltenen Informationen.bintec elmeg GmbH übernimmt keine Haftung für mittelbare, unmittelbare, Neben-, Folge- oder andere Schäden, die mit der Auslieferung, Bereitstellung oder Benutzung dieser Bedienungsanleitung im Zusammenhang stehen.

Inhaltsverzeichnis

Kapitel 1 Wichtige Informationen

1.1 Vorbereitung und Update mit dem GUI

Das Update der Systemsoftware mit dem Graphical User Interface (GUI) erfolgt mit einer BLUP-Datei (Bintec Large Update), um alle notwendigen Module intelligent zu aktualisieren. Dabei werden alle diejenigen Elemente aktualisiert, die im BLUP neuer sind als auf Ihrem Gateway.

Hinweis

Die Folge eines unterbrochenen Update-Vorgangs könnte sein, dass Ihr Gateway nicht mehr bootet. Schalten Sie Ihr Gateway deshalb nicht aus, während das Update durchgeführt wird.

Gehen Sie folgendermaßen vor, um mit dem Graphical User Interface ein Update auf **Systemsoftware 10.1.4** vorzubereiten und durchzuführen:

(1) Für das Update benötigen Sie die Datei `XXXXX_bl1014.xxx`, wobei `XXXXX` für Ihr Gerät steht. Stellen Sie sicher, dass die Datei, welche Sie für das Update benötigen, auf Ihrem PC verfügbar ist. Wenn die Datei nicht auf Ihrem PC verfügbar ist, geben Sie *www.bintec-elmeg.com* in Ihren Browser ein. Die bintec-elmeg-Homepage öffnet sich. Im Download-Bereich Ihres Gateways finden Sie die benötigte Datei. Speichern Sie sie auf Ihrem PC.

(2) Sichern Sie die aktuelle Boot-Konfiguration vor dem Update. Exportieren Sie die aktuelle Boot-Konfiguration über das Menü **Wartung**->**Software &Konfiguration** des Graphical User Interface. Wählen Sie dazu: **Aktion** = *Konfiguration exportieren*, **Aktueller Dateiname im Flash** = *boot*, **Zertifikate und Schlüssel einschließen** = *aktiviert*, **Verschlüsselung der Konfiguration** = *deaktiviert*. Bestätigen Sie mit **Start**. Das Fenster **Öffnen von <Name des Gateways>.cf** öffnet sich. Belassen Sie die Auswahl bei *Datei speichern* und klicken Sie auf **OK**, um die Konfiguration auf Ihrem PC zu speichern. Die Datei `<Name des Gateways.cf>` wird gespeichert, das Fenster **Downloads** zeigt die gespeicherte Datei.

(3) Führen Sie das Update auf **Systemsoftware 10.1.4** über das Menü **Wartung**->**Software &Konfiguration** durch. Wählen Sie dazu: **Aktion** = *Systemsoftware aktualisieren*, **Quelle** = *Lokale Datei*, **Dateiname** = *XXXXX_bl1014.xxx*. Bestätigen Sie mit **Start**. Die Meldung „System Anfrage. Bitte warten. Ihre Anfrage wird bearbeitet.“ bzw. „System Maintenance. Please stand by. Operation in progress.“ zeigt, dass die gewählte Datei in das Gerät geladen wird. Wenn der Ladevorgang beendet

ist, sehen Sie die Meldung „System - Maintenance. Sucess. Operation completed successfully“. Klicken Sie auf **Reboot**. Sie sehen die Meldung „System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds“. Das Gerät startet mit der neuen Systemsoftware, das Browser-Fenster öffnet sich.

1.2 Downgrade mit dem GUI

Wenn Sie ein Downgrade durchführen wollen, gehen Sie folgendermaßen vor:

(1) Ersetzen Sie die aktuelle Boot-Konfiguration durch die zuvor gesicherte. Importieren Sie die gesicherte Boot-Konfiguration über das Menü **Wartung**->**Software &Konfiguration**. Wählen Sie dazu: **Aktion** = *Konfiguration importieren*, **Verschlüsselung der Konfiguration** = *deaktiviert*, **Dateiname** = *<Name des Geräts>.cf*. Bestätigen Sie mit **Start**. Die Meldung „System Anfrage. Bitte warten. Ihre Anfrage wird bearbeitet.“ bzw. „System Maintenance. Please stand by. Operation in progress.“ zeigt, dass die gewählte Konfiguration in das Gerät geladen wird. Wenn der Ladevorgang beendet ist, sehen Sie die Meldung „System - Maintenance. Sucess. Operation completed successfully.“ Klicken Sie auf **Reboot**. Sie sehen die Meldung „System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds.“ Das Gerät startet, das Browser-Fenster öffnet sich. Melden Sie sich an Ihrem Gerät an.

(2) Führen Sie das Downgrade auf die gewünschte Softwareversion über das Menü **Wartung**->**Software &Konfiguration** durch.
Wählen Sie dazu: **Aktion** = *Systemsoftware aktualisieren*, **Quelle** = *Lokale Datei*, **Dateiname** = *RXL_Series_bl9109.biq* (Beispiel). Bestätigen Sie mit **Start**. Die Meldung „System Anfrage. Bitte warten. Ihre Anfrage wird bearbeitet.“ bzw. „System Maintenance. Please stand by. Operation in progress.“ zeigt, dass die gewählte Datei in das Gerät geladen wird. Wenn der Ladevorgang beendet ist, sehen Sie die Meldung „System - Maintenance. Sucess. Operation completed successfully.“ Klicken Sie auf **Reboot**. Sie sehen die Meldung „System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds.“ Das Gerät startet mit der neuen Systemsoftware, das Browser-Fenster öffnet sich.

Sie können sich an Ihrem Gerät anmelden und es konfigurieren.

1.3 Unterstützte Web Browser

Das HTML-GUI unterstützt die Verwendung folgender Browser in ihrer jeweils aktuellen Version:

- Microsoft Internet Explorer
- Mozilla Firefox

.

Wichtig

Stellen Sie sicher, dass Sie Ihren Browser auf dem neuesten Stand halten, denn nur so können Sie von neuen Funktionen und Sicherheitsmerkmalen profitieren. Vom Hersteller nicht mehr unterstützte und mit Softwareaktualisierungen versorgte Versionen werden vom HTML-GUI nicht unterstützt. Informieren Sie sich ggf. auf den Web-Seiten der Softwarehersteller über die aktuell von ihnen unterstützten Versionen.

Kapitel 2 Neue Funktionen

Systemsoftware 10.1.4 enthält eine Reihe neuer Funktionen, die den Leistungsumfang gegenüber der letzten Version der Systemsoftware erheblich erweitern.

Hinweis

Bitte beachten Sie, dass nicht alle hier aufgeführten neuen Funktionen für alle Geräte zur Verfügung stehen. Informieren Sie sich ggf. im aktuellen Datenblatt Ihres Gerätes oder im entsprechenden Handbuch.

2.1 IPv4-Filterregeln

Hinweis

Ab **Systemsoftware 10.1.4** hat sich das Konzept der IPv4-Filterregeln grundlegend geändert.

In IPv4 stehen vertrauenswürdige bzw. nicht vertrauenswürdige Zonen in vergleichbarer Weise zur Verfügung wie in IPv6. In der SIF gelten initial alle LAN-Schnittstellen als vertrauenswürdig, alle WAN-Schnittstellen als nicht vertrauenswürdig.

Im Menü **Firewall**->**Richtlinien**->**IPv4-Filterregeln** können Sie mit Hilfe der Schaltfläche unter **Vertrauenswürdige Schnittstellen** eine IPv4-Schnittstellenliste anzeigen lassen und kennzeichnen, welche Schnittstellen vertrauenswürdig sind.

Bei IPv4 sind darüber hinaus folgende Menüs und Felder betroffen:

- im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**-> das Feld **Sicherheitsrichtlinie**
- die Menüs **WAN**->**Internet + Einwählen**->**PPPoE**->**Neu**, **WAN**->**Internet + Einwählen**->**PPTP**->**Neu**, **WAN**->**Internet + Einwählen**->**PPPoA**->**Neu**
- das Menü **VPN**->**IPSec**->**IPSec-Peers**->**Neu**

2.2 IPv6

Wichtig

Folgende Funktionen können mit IPv6 NICHT verwendet werden:

- Lastverteilung: Die Funktion ist auf IPv6-Schnittstellen nicht anwendbar, da IPv6-Datenverkehr nicht erfasst wird.
- Hotspot-Gateway: IPv6-Datenverkehr wird vom Hotspot Gateway nicht erfasst und kann daher auch nicht kontrolliert und ggf. beschränkt werden.
- IPv6-Tunnelmechanismen für die Übertragung von IPv6-Daten über IPv4-Netze (6in4 Relay, SixXS, Hurricane Electric, 6to4 RFC) werden nicht mehr unterstützt. Entsprechende Konfigurationen sind mit **Systemsoftware 10.1.4** nicht kompatibel.

Mit **Systemsoftware 10.1.4** steht IPv6 für ausgewählte bintec Router zur Verfügung.

IPv6-Adressen konfigurieren

Zusätzlich zu IPv4-Adressen können Sie IPv6-Adressen verwenden.

Im Folgenden sehen Sie ein Beispiel für eine IPv6-Adresse:

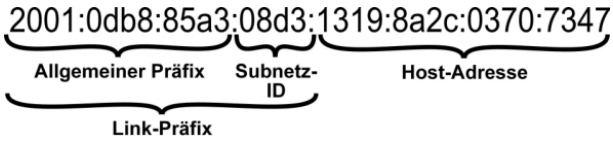

Abb. 1: IPv6-Adresse (Beispiel)

Ihr Gerät kann auf einer Schnittstelle entweder als Router oder als Host agieren. In der Regel agiert es auf den LAN-Schnittstellen als Router und auf den WAN- sowie den PPP-Verbindungen als Host.

Wenn Ihr Gerät als Router agiert, so können seine eigenen IPv6-Adressen folgendermaßen gebildet werden: ein Link-Präfix kann von einem Allgemeinen Präfix (siehe **Allgemeine IPv6-Präfixe** weiter unten) abgeleitet werden oder Sie können einen statischen Wert eingeben. Eine Host-Adresse kann über `Auto eui-64` erzeugt werden, für weitere Host-Adressen können Sie statische Werte eingeben.

Wenn Ihr Gerät als Router agiert, so verteilt es den konfigurierten Link-Präfix in der Regel per Router Advertisements an die Hosts. Über einen DHCP-Server werden Zusatzinformationen, wie z. B. die Adresse eines Zeitservers, an die Hosts übermittelt. Der Client kann

sich seine Host-Adresse entweder über Stateless Address Autoconfiguration (SLAAC) erzeugen oder diese Adresse von einem DHCP-Server zugeteilt bekommen.

Verwenden Sie für den oben beschriebenen Router-Modus im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu** die Einstellungen **IPv6-Modus** = *Router*, **Router Advertisement übertragen** *Aktiviert* **DHCP-Server** *Aktiviert* und **IPv6-Adressen Hinzufügen**.

Wenn Ihr Gerät als Host agiert, wird ihm ein Link-Präfix von einem anderen Router per Router Advertisement zugeteilt. Die Host- Adresse wird dann per SLAAC automatisch erzeugt. Zusatzinformationen, wie z. B. der Allgemeine Präfix vom Provider oder die Adresse eines Zeitservers können per DHCP bezogen werden. Verwenden Sie dazu im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu** die Einstellungen **IPv6-Modus** = *Client*, **Router Advertisement annehmen** *Aktiviert* und **DHCP-Client** = *Aktiviert*.

Allgemeine IPv6-Präfixe

Allgemeine IPv6-Präfixe werden in der Regel von IPv6-Providern vergeben. Sie können statisch zugewiesen oder über DHCP bezogen werden. Meist handelt es sich um /48- oder /56-Netze. Aus diesen Allgemeinen Präfixen können Sie /64-Subnetze erzeugen und in Ihrem Netz weiterverteilen lassen.

Das Konzept der Allgemeinen Präfixe hat zwei entscheidende Vorteile:

- Zwischen Provider und Kunde genügt eine einzige Route.
- Wenn der Provider einen neuen Allgemeinen Präfix per DHCP zuteilt oder einen statisch zugeteilten Allgemeinen Präfix ändern muss, haben Sie als Kunde keinen oder wenig Konfigurationsaufwand: Über DHCP erhalten Sie den neuen Allgemeinen Präfix automatisch. Im Falle des statisch zugeteilten Allgemeinen Präfixes müssen Sie diesen einmal in Ihr System eingeben. Alle aus diesem Allgemeinen Präfix abgeleiteten Subnetze und IPv6-Adressen ändern sich bei einem Update des Allgemeinen Präfixes automatisch.

Menüs

Folgende Menüs stehen für die Konfiguration von IPv6 zur Verfügung:

- **Assistenten**->**Erste Schritte**->**Grundeinstellungen**: Hier können Sie grundlegende IPv6-Einstellungen über den Assistenten **Erste Schritte** festlegen. Erklärungen zu den angezeigten IPv6-Parametern finden Sie direkt im GUI im rechten Fenster.
- **Assistenten**->**Internetzugang**->**Internetverbindungen**: Hier können Sie IPv6-Einstellungen für eine Internetverbindung über den Assistenten **Internetzugang** konfigurieren. Erklärungen zu den angezeigten IPv6-Parametern finden Sie direkt im GUI im rechten Fenster.

- **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu**: Hier konfigurieren Sie die gewünschten Schnittstellen für IPv6 (siehe *Schnittstellen* auf Seite 8).
- **LAN**->**IP-Konfiguration**->**Schnittstellen**-> : Hier können Sie alle IPv4- und IPv6-Adressen der entsprechenden Schnittstelle einsehen.
- **Netzwerk**->**Routen**->**IPv6-Routenkonfiguration**: In diesem Menü legen Sie neue IPv6-Routen an oder verändern bereits angelegte Routen (siehe *IPv6-Routenkonfiguration* auf Seite 17).
- **Netzwerk**->**Routen**->**IPv6-Routingtabelle**: Hier wird wird eine Liste aller im System aktiven IPv6-Routen angezeigt.
- **Netzwerk**->**Allgemeine IPv6-Präfixe**->**Konfiguration eines Allgemeinen Präfixes**: Hier legen Sie neue Allgemeine Präfixe für IPv6 an oder verändern bereits angelegte Allgemeine Präfixe (siehe *Konfiguration eines Allgemeinen Präfixes* auf Seite 20).
- **Netzwerk**->**QoS**->**IPv4/IPv6-Filter**: Hier können Sie IPv4- und IPv6-Filter konfigurieren (siehe *IPv4/IPv6-Filter* auf Seite 22).
- **WAN**->**Internet + Einwählen**->**PPPoE**->**Neu**: Hier können Sie IPv6 für PPoE konfigurieren (siehe *PPPoE* auf Seite 23).
- **WAN**->**Internet + Einwählen**->**PPPoA**->**Neu**: Hier können Sie IPv6 für PPoE konfigurieren (siehe *PPPoA* auf Seite 26).
- **VPN**->**IPSec**->**IPSec-Peers**->**Neu**: Hier können Sie IPv6 für IPSec konfigurieren (siehe *IPSec-Peers* auf Seite 28).
- **Firewall**->**Richtlinien**->**IPv6-Filterregeln**->**Neu**: Hier können Sie Filterregeln für IPv6 konfigurieren (siehe *IPv6-Filterregeln* auf Seite 32.
- **Firewall**->**Schnittstellen**->**IPv6-Gruppen**->**Neu**: Sie können die IPv6-Schnittstellen zu Gruppen zusammenfassen (siehe *IPv6-Gruppen* auf Seite 35).
- **Firewall**->**Adressen**->**Adressliste**: Hier wird eine Liste aller konfigurieren Adressen angezeigt. Sie können neue (IPv6-)Adressen anlegen (siehe *Adressliste* auf Seite 36).
- **Firewall**->**Adressen**->**Gruppen**->**Neu**: Hier können Sie Adressen zu Gruppen zusammenfassen (siehe *Gruppen* auf Seite 37).
- **Lokale Dienste**->**DNS**->**DNS-Server**->**Neu**: Hier können Sie einen DNS-Server für IPv6 anlegen (siehe *DNS-Server* auf Seite 38).
- **Lokale Dienste**->**DNS**->**Dynamische Hosts**: Hier werden die über DHCPv6 gelernten DNS-Einträge angezeigt (siehe *Dynamische Hosts* auf Seite 50). Sie sehen zm Beispiel die per DHCPv6 zugewiesenen IPv6-Adressen.
- **Lokale Dienste**->**DHCPv6-Server**: hier können Sie Ihr Gerät als DHCPv6-Server konfigurieren (siehe *DHCPv6-Server* auf Seite 39 und *DHCPv6 Global Options* auf Seite 43).
- **Wartung**->**Diagnose**->**Ping-Test** (siehe *Ping-Test* auf Seite 46).
- **Wartung**->**Diagnose**->**Traceroute-Test** (siehe *Traceroute-Test* auf Seite 47).

2.2.1 Schnittstellen

In Menü **LAN**->**IP-Konfiguration**->**Schnittstellen** werden die vorhandenen IP-Schnittstellen aufgelistet. Sie sehen, für welche Schnittstellen bereits IPv6-Adressen angelegt sind.

2.2.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um virtuelle Schnittstellen zu erstellen.

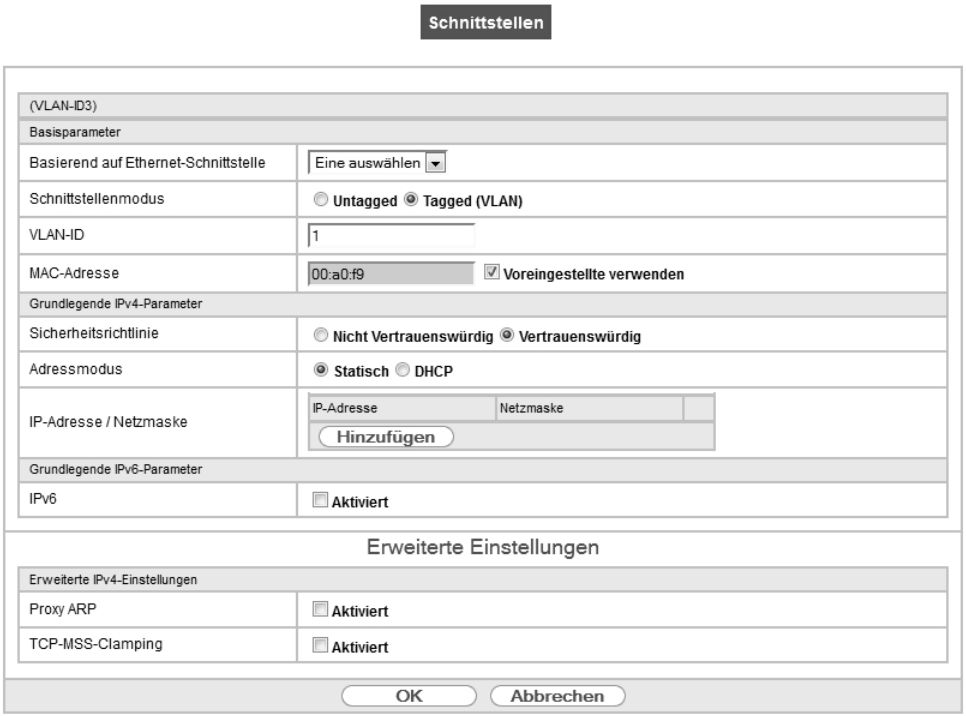

Abb. 2: **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu**

Das Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu** enthält folgende für IPv6 relevante Felder:

Felder im Menü Grundlegende IPv6-Parameter

Feld	Beschreibung
IPv6	Wählen Sie aus, ob die gewählte Schnittstelle das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll.

Feld	Beschreibung
	Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Sicherheitsrichtlinie	Hier nur für **IPv6** = *Aktiviert* Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll. Mögliche Werte: • *Vertrauenswürdig* (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen. • *Nicht Vertrauenswürdig*: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LANs verwenden wollen. Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall konfigurieren.
IPv6-Modus	Nur für **IPv6** = *Aktiviert* Wählen Sie, ob die Schnittstelle im Host- oder im Router-Modus betrieben werden soll. Abhängig von der getroffenen Auswahl werden unterschiedliche Parameter angezeigt, die Sie konfigurieren müssen. Mögliche Werte: • *Router (Transmit Router Advertisement)* (Standardwert): Die Schnittstelle wird im Router-Modus betrieben. • *Host*: Die Schnittstelle wird im Host-Modus betrieben.
Router Advertisement übertragen	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Router* Wählen Sie, ob Router Advertisements über die gewählte

Feld	Beschreibung
	Schnittstelle gesendet werden sollen. Mithilfe der Router Advertisements wird z.B. die Präfix Liste übertragen und der Router propagiert sich als Standard-Gateway. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
DHCP-Server	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Router* Legen Sie fest, ob Ihr Gerät als DHCP-Server agieren soll, d.h ob es DHCP-Options versenden soll, um z. B. Informationen zu den DNS-Servern an die Clients weiterzuleiten. Aktivieren Sie diese Option, wenn Hosts IPv6-Adressen per SLAAC erzeugen sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
IPv6-Adressen	Nur für **IPv6** = *Aktiviert* Sie können der gewählten Schnittstelle **IPv6-Adressen** zuordnen. Mit **Hinzufügen** können Sie einen oder mehrere Adresseinträge anlegen. Ein zusätzliches Fenster öffnet sich, in dem Sie eine IPv6-Adresse bestehend aus einem Link-Präfix und einem Host-Anteil festlegen können. Wenn Ihr Gerät im Host-Modus arbeitet (**IPv6-Modus** = *Host*, **Router Advertisement annehmen** *Aktiviert* und **DHCP-Client** *Aktiviert*), werden seine IPv6-Adressen per SLAAC festgelegt. Sie brauchen keine IPv6-Adressen manuell zu konfigurieren, können aber auf Wunsch zusätzliche Adressen eintippen. Wenn Ihr Gerät im Router-Modus arbeitet (**IPv6-Modus** = *Router*, **Router Advertisement übertragen** *Aktiviert* und **DHCP-Server** *Aktiviert*), so müssen Sie hier seine

Feld	Beschreibung
	IPv6-Adressen konfigurieren.
Router Advertisement annehmen	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Host* Wählen Sie, ob Router Advertisements über die gewählte Schnittstelle empfangen werden sollen. Mithilfe der Router Advertisements wird z. B. die Präfix-Liste erstellt. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
DHCP-Client	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Host* Legen Sie fest, ob Ihr Gerät als DHCP-Client agieren soll, d.h. ob es DHCP-Options empfangen soll, um z. B. Informationen zu den DNS-Servern zu erhalten. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Wenn Sie auf **Hinzufügen** klicken, öffnet sich ein zusätzliches Fenster.

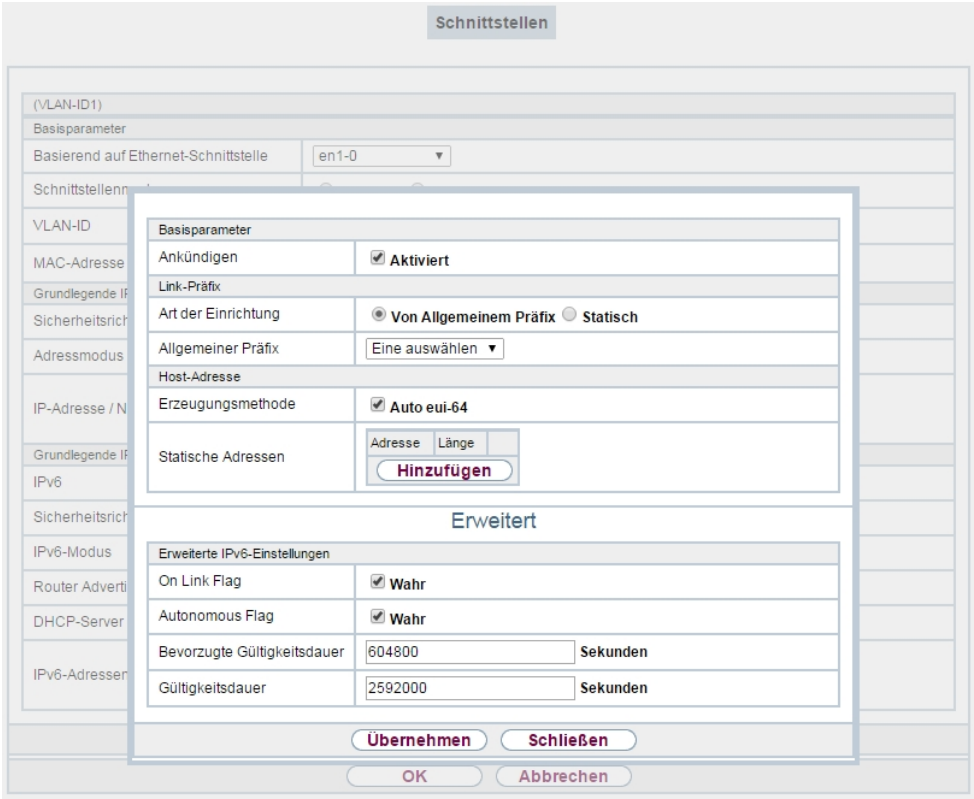

Abb. 3: **LAN->IP-Konfiguration->Schnittstellen->Neu->Hinzufügen**

Feld im Menü Basisparameter

Feld	Beschreibung
Ankündigen	Nur für **IPv6-Modus** = `Router` Hier können Sie - bezogen auf den Link-Präfix, der im aktuellen Fenster definiert wird - festlegen, ob dieser Präfix per Router Advertisement über die gewählte Schnittstelle versendet werden soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü Link-Präfix

Feld	Beschreibung
Art der Einrichtung	Wählen Sie, auf welche Weise der Link-Präfix festgelegt werden

Feld	Beschreibung
	soll. Mögliche Werte: • *Von Allgemeinem Präfix* (Standardwert): Der Link-Präfix wird von einem allgemeinen Präfix abgeleitet. • *Statisch*: Sie können den Link-Präfix eingeben.
Allgemeiner Präfix	Nur für **Art der Einrichtung** = *Von Allgemeinem Präfix* Wählen Sie den Allgemeinen Präfix, von dem der Link-Präfix abgeleitet werden soll. Sie können unter den Allgemeinen Präfixen wählen, die unter **Netzwerk**->**Allgemeine IPv6-Präfixe**->**Konfiguration eines Allgemeinen Präfixes**->**Neu** angelegt sind (siehe *Konfiguration eines Allgemeinen Präfixes* auf Seite 20).
Automatische Subnetzerstellung	Nur wenn **Art der Einrichtung** = *Von Allgemeinem Präfix* und wenn ein **Allgemeiner Präfix** gewählt ist. Wählen Sie, ob das Subnetz automatisch erstellt werden soll. Bei der automatischen Subnetzerstellung wird für das erste Subnetz die ID *0* verwendet, für das zweite Subnetz die Subnetz-ID *1*, usw. Mögliche Werte für die **Subnetz-ID** sind *0* bis *65535*. Die Subnetz-ID beschreibt das vierte der vier 16-Bit-Felder eines Link-Präfix. Bei der Subnetzerstellung wird der dezimale ID-Wert in einen hexadezimalen Wert umgerechnet. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Wenn die Funktion nicht aktiv ist, so können Sie durch Eingabe der Subnetz-ID ein Subnetz definieren.
Subnetz-ID	Nur wenn **Automatische Subnetzerstellung** nicht aktiv ist. Geben Sie eine Subnetz-ID ein, um ein Subnetz zu definieren. Die Subnetz-ID beschreibt das vierte der vier 16-Bit-Felder eines Link-Präfix. Mögliche Werte sind *0* bis *65535*.

Feld	Beschreibung
	Bei der Subnetzerstellung wird der eingegebene dezimale Wert in einen hexadezimalen Wert umgerechnet.
Link-Präfix	Nur für **Art der Einrichtung** = *Statisch* Sie können den Link-Präfix einer IPv6-Adresse eingeben. Dieser Präfix muss mit *::* enden. Seine Länge ist mit *64* vorgegeben.

Felder im Menü Host-Adresse

Feld	Beschreibung
Erzeugungsmethode	Legen Sie fest, ob der Host-Anteil der IPv6-Adresse mittels EUI-64 automatisch aus der MAC-Adresse erzeugt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. EUI-64 setzt folgenden Prozess in Gang: • Die hexadezimale 48-Bit MAC Adresse wird in 2 x 24 Bit geteilt. • In die entstandene Lücke wird *FFFE* eingefügt, um 64 Bit zu erhalten. • Die hexadezimale Schreibweise der 64 Bit wird in die duale Schreibweise umgewandelt. • Im ersten 8-Bit-Feld wird Bit 7 auf *1* gesetzt.
Statische Adressen	Sie können, unabhängig von der automatischen Erzeugung, die unter **Erzeugungsmethode** festgelegt ist, mit **Hinzufügen** den Host-Anteil einer IPv6-Adresse oder mehrerer IPv6-Adressen manuell eingeben. Seine Länge ist mit *64* vorgegeben. Beginnen Sie die Eingabe mit *::* .

Die Felder im Menü **Erweitert** sind Bestandteil der Präfix-Informationen, die im Router Advertisement gesendet werden, wenn **Ankündigen** aktiv ist. Das Menü **Erweitert** besteht aus folgenden Feldern:

Felder im Menü Erweiterte IPv6-Einstellungen

Feld	Beschreibung
On Link Flag	Wählen Sie, ob das On-Link Flag (L-Flag) gesetzt werden soll.

Feld	Beschreibung
	Dadurch fügt der Host das Präfix der Präfixliste hinzu. Mit Auswahl von *Wahr* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Autonomous Flag	Wählen Sie, ob das Autonomous Address Configuration Flag (A-Flag) gesetzt werden soll. Dadurch nutzt ein Host das Präfix und eine Schnittstellen-ID, um daraus seine Adresse abzuleiten. Mit Auswahl von *Wahr* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Bevorzugte Gültigkeitsdauer	Geben Sie eine Zeitspanne in Sekunden ein. Während dieser Zeit werden die Adressen, die mit Hilfe des Präfix per SLAAC erzeugt wurden, bevorzugt verwendet. Der Standardwert ist *604800* Sekunden.
Gültigkeitsdauer	Geben Sie eine Zeitspanne in Sekunden an, für die das Präfix gültig ist. Der Standardwert ist *2592000* Sekunden. **Hinweis** Der Wert für die Gültigkeitsdauer sollte niedriger sein als derjenige, der unter **Erweiterte IPv6-Einstellungen** für die Option **Router-Gültigkeitsdauer** konfiguriert ist.

Das Menü **Erweiterte Einstellungen** enthält folgende für IPv6 relevante Felder:

Felder im Menü Erweiterte IPv6-Einstellungen

Feld	Beschreibung
Router-Gültigkeitsdauer	Nur für **IPv6** = *Aktiviert*, **IPv6-Modus** = *ger(Router (Transmit Router Advertisement))* und **Router Advertisement übertragen** = *Aktiviert* Geben Sie eine Zeitspanne in Sekunden an. Für dieses Intervall

Feld	Beschreibung
	verbleibt der Router in der Default Router List. Der Standardwert ist *600* Sekunden. Der Maximalwert ist *65520* Sekunden. Ein Wert von *0* besagt, dass der Router kein Standardrouter ist und nicht in die Default Router List eingetragen werden soll.  **Hinweis** Der Wert für die **Router-Gültigkeitsdauer** sollte höher sein als die kürzeste Link-Präfix-Gültigkeitsdauer, die im unter **Grundlegende IPv6-Parameter** für die Schnittstelle konfiguriert ist.
Router-Präferenz	Nur für **IPv6** = *Aktiviert*, **IPv6-Modus** = *Router* und **Router Advertisement übertragen** = *Aktiviert* Wählen Sie die Präferenz Ihres Routers für die Wahl des Standardrouters. Dies ist in Fällen nützlich, in denen ein Knoten Advertisements von mehreren Routern erhält oder in Back-Up-Szenarien. Mögliche Werte: • *Hoch* • *Mittel* (Standardwert) • *Niedrig*
DHCP-Modus	Nur für **IPv6** = *Aktiviert*, **IPv6-Modus** = *Router* und **Router Advertisement übertragen** = *Aktiviert* Wählen Sie die an den DHCP-Client weitergeleiteten Informationen aus.  **Hinweis** Der Router muss nicht als DHCP-Server eingerichtet sein. Mit Auswahl von *Andere - DNS-Server, SIP-Server* (Standardwert) werden nicht-adressbezogene Informationen,

Feld	Beschreibung
	wie z. B. DNS, VoIP, usw. durchgeleitet. Aktivieren Sie diese Option, wenn die Hosts im Netzwerk ihre IP-Adresse über SLAAC automatisch bilden sollen. Der Router sendet in diesem Fall ausschließlich nicht-adressbezogene Daten über DHCP. Mit Auswahl von *Verwaltet - IPv6-Adressverwaltung* werden sowohl die IPv6-Adressen als auch alle nicht adressbezogenen Daten vom Host per DHCP bezogen.

DNS-Propagation	Nur für **IPv6-Modus** = *Router* und **Router Advertisement übertragen** *Aktiviert*
	
	Wählen Sie aus, ob DNS-Server-Adressen über Router Advertisements propagiert werden sollen und wenn ja, auf welche Weise. Es werden maximal zwei DNS-Server-Adressen propagiert.
	
	Mögliche Werte:
	
	• *Aus*: Es wird keine DNS-Server-Adresse propagiert.
	• *Selbst*: Die eigene IP-Adresse wird als DNS-Server-Adresse propagiert. Bei mehreren Adressen, werden die Adressen in folgender Reihenfolge propagiert:
	  • Globale Adressen
	  • ULA (Unique Local Addresses)
	  • Link-Lokale-Adressen
	• *Sonstige*: Die statisch konfigurierten und die dynamisch gelernten DNS-Server-Einträge werden gemäß ihrer Priorität propagiert. Sind keine Einträge vorhanden, werden keine Adressen propagiert.

2.2.2 IPv6-Routenkonfiguration

Im Menü **Netzwerk**->**Routen**->**IPv6-Routenkonfiguration** wird eine Liste aller konfigurierten IPv6-Routen angezeigt.

2.2.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Routen anzulegen.

Routen, die über kein -Symbol verfügen, wurden vom Router automatisch erstellt und können nicht bearbeitet werden.

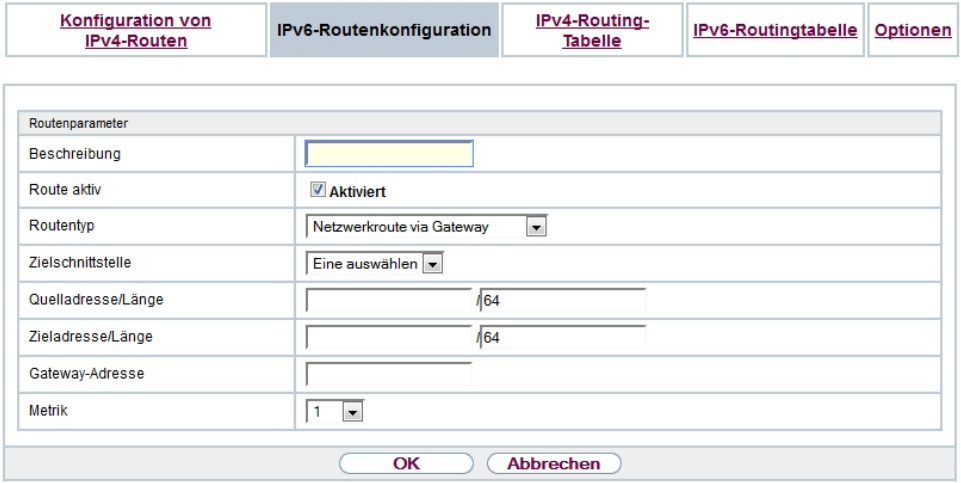

Abb. 4: **Netzwerk->Routen->IPv6-Routenkonfiguration->Neu**

Das Menü **Netzwerk->Routen->IPv6-Routenkonfiguration->Neu** besteht aus folgenden Feldern:

Felder im Menü Routenparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die IPv6-Route an.
Route aktiv	Wählen Sie, ob die Route aktiv oder inaktiv sein soll. Mit *Aktiviert* wird die Route auf den Status aktiv gesetzt. Standardmäßig ist die Funktion aktiv.
Routentyp	Wählen Sie die Art der Route aus. Mögliche Werte: • *Standardroute über Schnittstelle* : Route über eine spezifische Schnittstelle, die verwendet wird, wenn keine andere passende Route verfügbar ist. • *Standardroute über Gateway*: Route über ein spezifisches Gateway, die verwendet wird, wenn keine andere passende Route verfügbar ist.

Feld	Beschreibung
	• *Host-Route über Schnittstelle*: Route zu einem einzelnen Host über eine spezifische Schnittstelle. • *Host-Route via Gateway*: Route zu einem einzelnen Host über ein spezifisches Gateway. • *Netzwerkroute via Schnittstelle*: Route zu einem Netzwerk über eine spezifische Schnittstelle. • *Netzwerkroute via Gateway* (Standardwert): Route zu einem Netzwerk über ein spezifisches Gateway.
Zielschnittstelle	Wählen Sie die IPv6-Schnittstelle aus, welche für diese Route verwendet werden soll. Sie können unter den Schnittstellen wählen, die unter **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu** angelegt sind und für welche die Nutzung von IPv6 aktiviert ist.
Quelladresse/Länge	Geben Sie die IPv6-Quelladresse mit der entsprechenden Präfixlänge ein. Die Eingabe *::* beschreibt eine unspezifische Adresse. Standardmäßig ist eine Präfixlänge von *64* vorgegeben.
Zieladresse/Länge	Geben Sie die IPv6-Zieladresse mit der entsprechenden Präfixlänge ein. Die Eingabe *::* beschreibt eine unspezifische Adresse. Standardmäßig ist eine Präfixlänge von *64* vorgegeben.
Gateway-Adresse	Geben Sie die IPv6-Adresse für den nächsten Hop ein.
Metrik	Wählen Sie die Priorität der Route aus. Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route. Wertebereich von *0* bis *255*, der Standardwert ist *1*.

2.2.3 IPv6-Routingtabelle

Im Menü **Netzwerk**->**Routen**->**IPv6-Routingtabelle** wird eine Liste aller im System aktiven IPv6-Routen angezeigt.

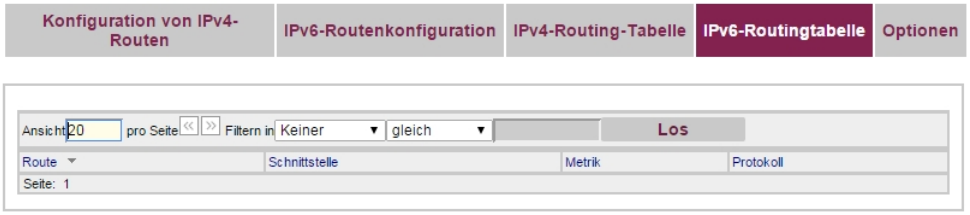

Abb. 5: **Netzwerk->Routen->IPv6-Routingtabelle**

Felder im Menü IPv6-Routingtabelle

Feld	Beschreibung
Route	Zeigt die Quell- und die Zieladresse, die für diese Route verwendet wird an, sowie die Gateway IP-Adresse. Im Falle von per DHCP erhaltenen Routen wird hier nichts angezeigt.
Schnittstelle	Zeigt die Schnittstelle an, welche für diese Route verwendet wird.
Metrik	Zeigt die Priorität der Route an. Je niedriger der Wert, desto höhere Priorität besitzt die Route.
Protokoll	Zeigt an, wie der Eintrag erzeugt wurde, z. B. manuell (*Lokal*) oder über eins der verfügbaren Protokolle.

2.2.4 Konfiguration eines Allgemeinen Präfixes

Im Menü **Netzwerk->Allgemeine IPv6-Präfixe->Konfiguration eines Allgemeinen Präfixes** wird eine Liste aller konfigurierten IPv6-Präfixe angezeigt.

2.2.4.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Präfixe zu konfigurieren.

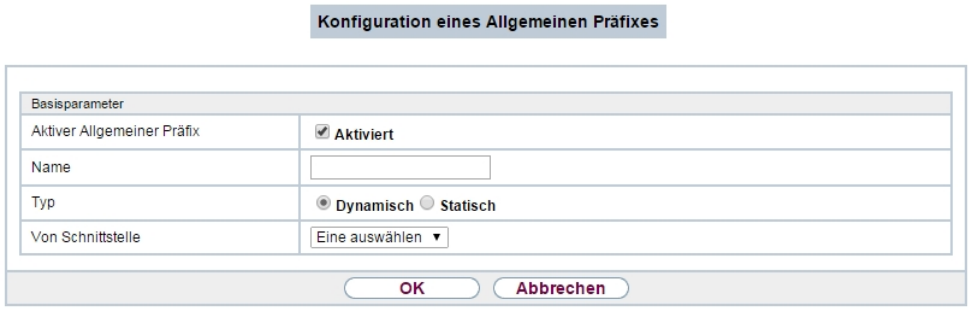

Abb. 6: **Netzwerk->Allgemeine IPv6-Präfixe->Konfiguration eines Allgemeinen Präfixes->Neu**

Felder im Menü Basisparameter

Feld	Beschreibung
Aktiver Allgemeiner Präfix	Wählen Sie, ob das Präfix aktiv oder inaktiv sein soll. Mit `Aktiviert` wird das Präfix auf den Status aktiv gesetzt. Standardmäßig ist das Präfix aktiv.
Name	Geben Sie einen Namen für das Allgemeine Präfix ein. Ein sprechender Name dient dazu, das Allgemeine Präfix aus einer Präfixliste leichter auswählen zu können.
Typ	Wählen Sie, wie der Adressraum zugewiesen werden soll. Mögliche Werte: • `Dynamisch` (Standardwert): Der Allgemeine Präfix wird dynamisch mittels einer DHCP-Übertragung festgesetzt, z. B. von einem Provider. • `Statisch`: Das Präfix wird fest vorgegeben, z. B. durch einen Provider.
Von Schnittstelle	Nur bei **Typ** = `Dynamisch` Wählen Sie die IPv6-Schnittstelle aus, von welcher ein **Allgemeiner Präfix** bezogen werden soll. Sie können unter den Schnittstellen wählen, die unter **LAN->IP-Konfiguration->Schnittstellen->Neu** angelegt sind und die folgende Bedingungen erfüllen: • **IPv6** ist `Aktiviert`.

Feld	Beschreibung
	• **IPv6-Modus** = *Host* • **DHCP-Client** ist *Aktiviert*.
Benutzter Präfix/Länge	Nur bei **Typ** = *Statisch* Geben Sie das Präfix ein, das verwendet werden soll. Geben Sie die zugehörige Länge ein. Dieser Präfix muss mit :: enden. Standardmäßig ist eine Länge von *48* vorgegeben.

2.2.5 IPv4/IPv6-Filter

Im Menü **Netzwerk**->**QoS**->**IPv4/IPv6-Filter** werden IP-Filter konfiguriert.

Die Liste zeigt ebenfalls alle ggf. konfigurierten Einträge aus **Netzwerk**->**Zugriffsregeln**->**Regelketten**.

2.2.5.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Filter zu definieren.

Abb. 7: **Netzwerk**->**QoS**->**IPv4/IPv6-Filter**->**Neu**

Das Menü **Netzwerk**->**QoS**->**IPv4/IPv6-Filter**->**Neu** besteht aus folgenden Feldern:

Relevante Felder im Menü Basisparameter

Feld	Beschreibung
IPv6-Zieladresse/-länge	Geben Sie die IPv6 Ziel-Adresse der Datenpakete und die Präfixlänge ein.

Feld	Beschreibung
	Mögliche Werte: • *Beliebig* (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert. • *Host*: Geben Sie die Ziel-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Ziel-Netzwerk-Adresse und die Präfixlänge ein.
IPv6-Quelladresse/-länge	Geben Sie die IPv6 Quell-Adresse der Datenpakete und die Präfixlänge ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Quell-IP-Adresse/Länge ist nicht näher spezifiziert. • *Host*: Geben Sie die Quell-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.

2.2.6 PPPoE

Im Menü **WAN**->**Internet + Einwählen**->**PPPoE** wird eine Liste aller PPPoE-Schnittstellen angezeigt.

PPP over Ethernet (PPPoE) ist die Verwendung des Netzwerkprotokolls Point-to-Point Protocol (PPP) über eine Ethernet-Verbindung.

2.2.6.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere PPPoE Schnittstellen einzurichten.

Abb. 8: **WAN->Internet + Einwählen->PPPoE->Neu**

Das Menü **WAN->Internet + Einwählen->PPPoE->Neu** besteht aus folgenden Feldern:

Felder im Menü IPv6-Einstellungen

Feld	Beschreibung
IPv6	Wählen Sie aus, ob die gewählte PPPoE- Schnittstelle das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Sicherheitsrichtlinie	Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle

Feld	Beschreibung
	betrieben werden soll. Mögliche Werte: • *Nicht Vertrauenswürdig* (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen. • *Vertrauenswürdig*: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen. Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall konfigurieren.
IPv6-Modus	Nur für **IPv6** = *Aktiviert* Die gewählte PPPoE-Schnittstelle wird im Host-Modus betrieben.
Router Advertisement annehmen	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Host* Wählen Sie, ob Router Advertisements über die Schnittstelle empfangen werden sollen. Mithilfe der Router Advertisements wird die Default Router List sowie die Präfix-Liste erstellt. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
DHCP-Client	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Host* Legen Sie fest, ob Ihr Gerät als DHCP-Client agieren soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

2.2.7 PPPoA

Im Menü **WAN**->**Internet + Einwählen**->**PPPoA** wird eine Liste aller PPPoA-Schnittstellen angezeigt.

In diesem Menü konfigurieren Sie eine xDSL-Verbindung, die zum Verbindungsaufbau PPPoA verwendet. Bei PPPoA wird die Verbindung so konfiguriert, dass ein PPP-Datenstrom direkt über ein ATM-Netzwerk transportiert wird (RFC 2364).

Bei Verwendung des internen DSL-Modems, muss in **WAN**->**ATM**->**Profile**->**Neu** für diese Verbindung eine PPPoA-Schnittstelle mit **Client-Typ** = *Auf Anforderung* konfiguriert werden.

2.2.7.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere PPPoA-Schnittstellen einzurichten.

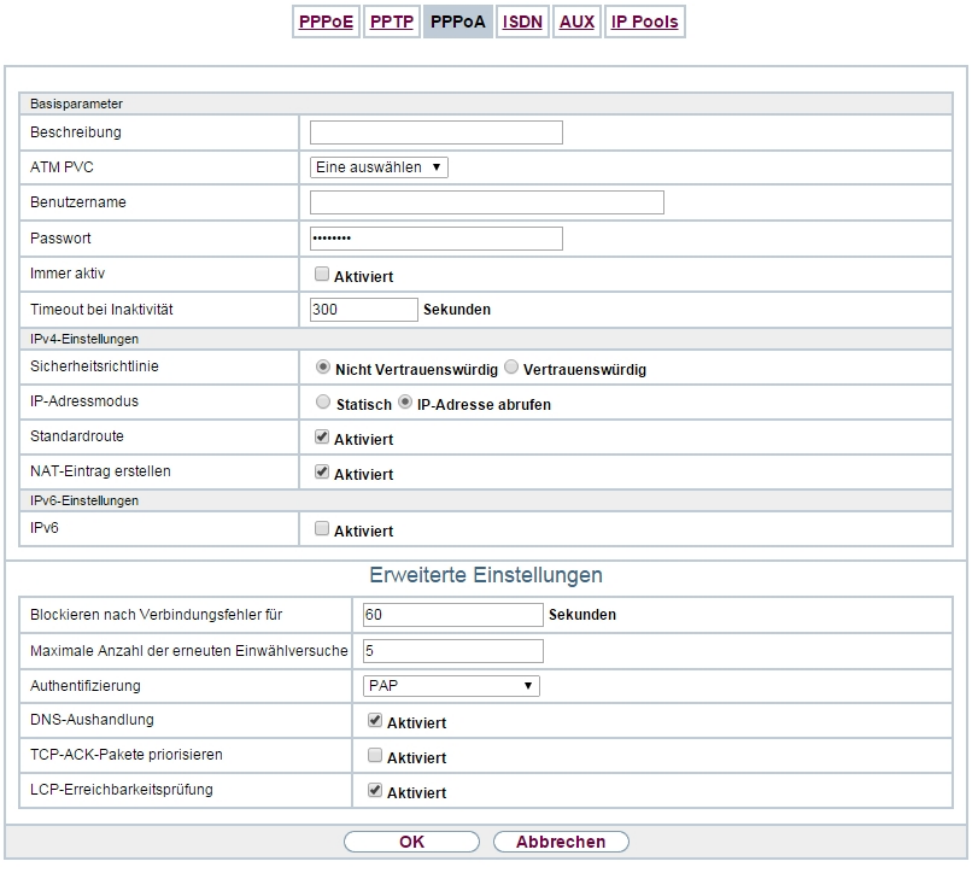

Abb. 9: **WAN->Internet + Einwählen->PPPoA->Neu**

Das Menü **WAN->Internet + Einwählen->PPPoA->Neu** besteht aus folgenden Feldern:

Felder im Menü IPv6-Einstellungen

Feld	Beschreibung
IPv6	Wählen Sie aus, ob das gewählte ATM-Profil das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Sicherheitsrichtlinie	Wählen Sie, mit welcher Sicherheitseinstellung das gewählte ATM-Profil betrieben werden soll. Mögliche Werte:

Feld	Beschreibung
	• *Nicht Vertrauenswürdig* (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen. • *Vertrauenswürdig*: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen. Ausnahmen für die gewählte Einstellung können Sie im Menü **Firewall** konfigurieren.
IPv6-Modus	Nur für **IPv6** = *Aktiviert* Das gewählte ATM-Profil wird im Host-Modus betrieben.
Router Advertisement annehmen	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Host* Wählen Sie, ob Router Advertisements über das ATM-Profil empfangen werden sollen. Mithilfe der Router Advertisements wird die Default Router List sowie die Präfix-Liste erstellt. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
DHCP-Client	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Host* Legen Sie fest, ob Ihr Gerät als DHCP-Client agieren soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

2.2.8 IPSec-Peers

Als Peer wird ein Endpunkt einer Kommunikation in einem Computernetzwerk bezeichnet. Jeder Peer bietet dabei seine Dienste an und nutzt die Dienste der anderen Peers.

Im Menü **VPN**->**IPSec**->**IPSec-Peers** wird eine Liste aller konfigurierter IPSec-Peers nach

Priorität sortiert angezeigt.

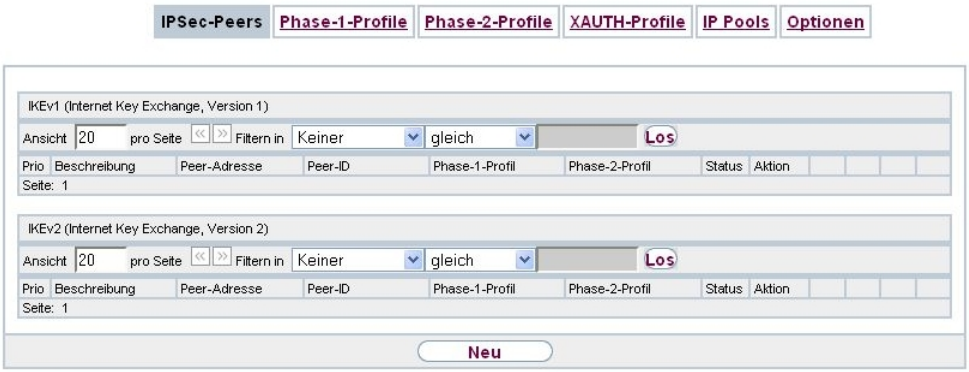

Abb. 10: **VPN->IPSec->IPSec-Peers**

2.2.8.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IPSec-Peers einzurichten.

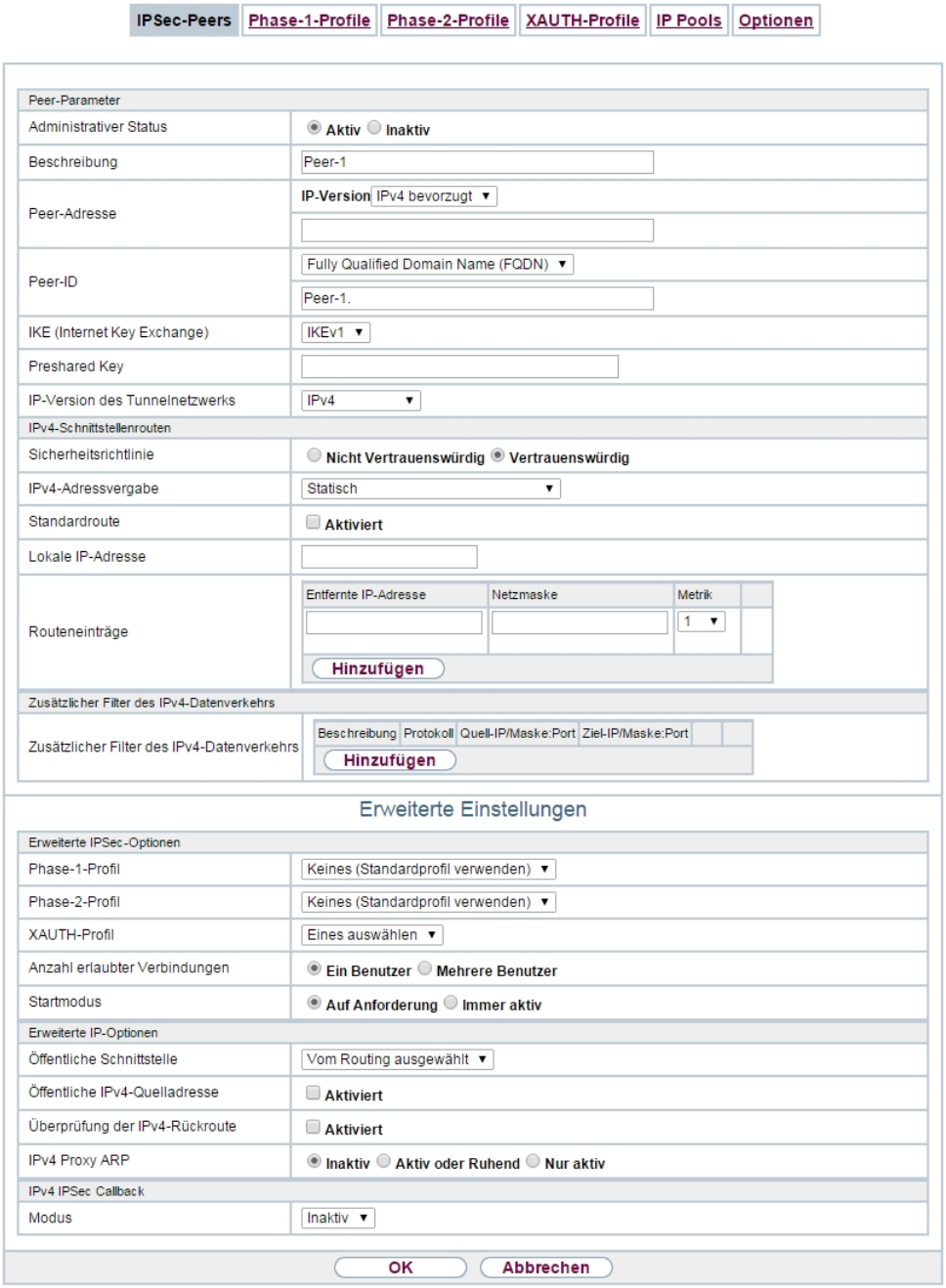

Abb. 11: **VPN->IPSec->IPSec-Peers->Neu**

Das Menü **VPN->IPSec->IPSec-Peers->Neu** besteht aus folgenden Feldern:

Relevante Felder im Menü Peer-Parameter

Feld	Beschreibung
Peer-Adresse	Wählen Sie die **IP-Version** aus. Sie können wählen, ob IPv4 oder IPv6 bevorzugt verwendet werden soll oder ob nur eine der beiden IP-Versionen erlaubt sein soll. **Hinweis** Diese Auswahl ist nur relevant, wenn ein Host-Name als Peer-Adresse eingegeben wird. Mögliche Werte: • *IPv4 bevorzugt* • *IPv6 bevorzugt* • *Nur IPv4* • *Nur IPv6* Geben Sie die offizielle IP-Adresse des Peers bzw. seinen auflösbaren Host-Namen ein. Die Eingabe kann in bestimmten Konfigurationen entfallen, wobei Ihr Gerät dann keine IPSec-Verbindung initiieren kann.
IP-Version des Tunnelnetzwerks	Wählen Sie aus, ob IPv4 oder IPv6 oder beide Versionen für den VPN-Tunnel verwendbar sein sollen. Mögliche Werte: • *IPv4* • *IPv6* • *IPv4 und IPv6*

Felder im Menü IPv6-Schnittstellenrouten

Feld	Beschreibung
Sicherheitsrichtlinie	Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll. Mögliche Werte:

Feld	Beschreibung
	• *Nicht Vertrauenswürdig*: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen. • *Vertrauenswürdig* (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen. Ausnahmen für die gewählte Einstellung können Sie im Menü **Firewall** konfigurieren.
Lokales IPv6-Netzwerk	Wählen Sie ein Netzwerk aus. Sie können unter den Link-Präfixen wählen, die unter **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu** angelegt sind. Geben Sie die Lokale IPv6-Adresse mit der entsprechenden Präfixlänge ein. Dieser Präfix muss mit :: enden. Standardmäßig ist eine Präfixlänge von /64 vorgegeben.
Entferntes IPv6-Netzwerk	Fügen Sie mit **Hinzufügen** einen neuen **Präfix** hinzu. Geben Sie die Adresse der Tunnelgegenstelle ein. Standardmäßig ist eine **Länge** von *64* und eine **Priorität** von *1* vorgegeben. Je niedriger der Wert der Priorität ist, desto höhere Priorität besitzt die Route.

2.2.9 IPv6-Filterregeln

Im Menü **Firewall**->**Richtlinien**->**IPv6-Filterregeln** wird eine Liste aller konfigurierten IPv6-Filterregeln angezeigt.

Hinweis

Beachten Sie, dass - im Gegensatz zur IPv4-Firewall - die IPv6-Firewall immer eingeschaltet ist und nicht ausgeschaltet werden kann.

Abb. 12: **Firewall->Richtlinien->IPv6-Filterregeln**

Mit der Schaltfläche in der Zeile **Vertrauenswürdige Schnittstelle** können Sie festlegen, welche Schnittstellen **Vertrauenswürdig** sind. Es öffnet sich ein neues Fenster mit einer Schnittstellenliste. Sie können die einzelnen Schnittstellen als vertrauenswürdig markieren.

Hinweis

Beachten Sie, dass die Schnittstellenliste für IPv6 leer ist, solange IPv6 für keine Schnittstelle aktiviert ist.

Mit der Schaltfläche können Sie vor dem Listeneintrag eine weitere Richtlinie einfügen. Es öffnet sich das Konfigurationsmenü zum Erstellen einer neuen Richtlinie.

Mit der Schaltfläche können Sie den Listeneintrag verschieben. Es öffnet sich ein Dialog, in dem Sie auswählen können, an welche Position die Richtlinie verschoben werden soll.

2.2.9.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IPv6-Filterregeln einzurichten.

Abb. 13: **Firewall->Richtlinien->IPv6-Filterregeln->Neu**

Das Menü **Firewall->Richtlinien->IPv6-Filterregeln->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Quelle	Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets aus. In der Liste stehen alle WAN-/ LAN-Schnittstellen, Schnittstellengruppen (siehe **Firewall->Schnittstellen->IPv6-Gruppen**), Adressen (siehe **Firewall->Adressen->Adressliste**) und Adressgruppen (siehe **Firewall->Adressen->Gruppen**) zur Auswahl, für die IPv6 aktiviert ist.
Ziel	Wählen Sie einen der vorkonfigurierten Aliase für das Ziel des Pakets aus. In der Liste stehen alle WAN-/ LAN-Schnittstellen, Schnittstellengruppen (siehe **Firewall->Schnittstellen->IPv6-Gruppen**), Adressen (siehe **Firewall->Adressen->Adressliste**) und Adressgruppen (siehe **Firewall->Adressen->Gruppen**) zur Auswahl, für die IPv6 aktiviert ist.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus, dem das zu filternde Paket zugeordnet sein muss. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: • *ftp* • *telnet* • *smtp* • *dns*

Feld	Beschreibung
	• *http* • *nntp* Weitere Dienste werden in **Firewall**->**Dienste**->**Diensteliste** angelegt. Außerdem stehen die in **Firewall**->**Dienste**->**Gruppen** konfigurierten Dienstegruppen zur Auswahl.
Aktion	Wählen Sie die Aktion aus, die auf ein gefiltertes Paket angewendet werden soll. Mögliche Werte: • *Zugriff* (Standardwert): Die Pakete werden entsprechend den Angaben weitergeleitet. • *Verweigern* : Die Pakete werden abgewiesen. • *Zurückweisen* : Die Pakete werden abgewiesen. Eine Fehlermeldung wird an den Sender des Pakets ausgegeben.

2.2.10 IPv6-Gruppen

Im Menü **Firewall**->**Schnittstellen**->**IPv6-Gruppen** wird eine Liste aller konfigurierter IPv6-Schnittstellen-Gruppen angezeigt.

Sie können die Schnittstellen Ihres Geräts zu Gruppen zusammenfassen. Dies vereinfacht die Konfiguration von Firewall-Regeln.

2.2.10.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IPv6-Schnittstellen-Gruppen einzurichten.

Abb. 14: **Firewall**->**Schnittstellen**->**IPv6-Gruppen**->**Neu**

Das Menü **Firewall**->**Schnittstellen**->**IPv6-Gruppen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der IPv6-Schnittstellen-Gruppe ein.
Mitglieder	Wählen Sie aus den zur Verfügung stehenden Schnittstellen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte **Auswahl**.

2.2.11 Adressliste

Im Menü **Firewall**->**Adressen**->**Adressliste** wird eine Liste aller konfigurierter Adressen angezeigt.

2.2.11.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Adressen einzurichten.

Abb. 15: **Firewall**->**Adressen**->**Adressliste**->**Neu**

Das Menü **Firewall**->**Adressen**->**Adressliste**->**Neu** besteht aus folgenden Feldern:

Relevante Felder im Menü Basisparameter

Feld	Beschreibung
IPv6	Erlaubt die Konfiguration von IPv6-Adresslisten. Mit *Aktiviert* wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Adresse/Präfix	Nur für **IPv6** = *Aktiviert* Geben Sie die IPv6-Adresse und das zugehörige Präfix ein.

2.2.12 Gruppen

Im Menü **Firewall**->**Adressen**->**Gruppen** wird eine Liste aller konfigurierter Adressgruppen angezeigt.

Sie können Adressen zu Gruppen zusammenfassen. Dieses vereinfacht die Konfiguration von Firewall-Regeln.

2.2.12.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Adressgruppen einzurichten.

Abb. 16: **Firewall**->**Adressen**->**Gruppen**->**Neu**

Das Menü **Firewall**->**Adressen**->**Gruppen**->**Neu** besteht aus folgenden Feldern:

Relevantes Feld im Menü Basisparameter

Feld	Beschreibung
IP-Version	Wählen Sie die verwendete IP-Version aus. Mögliche Werte: • *IPv4* • *IPv6* Standardmäßig ist *IPv4* ausgewählt.

2.2.13 DNS-Server

Im Menü **Lokale Dienste**->**DNS**->**DNS-Server** wird eine Liste aller konfigurierten DNS-Server angezeigt.

2.2.13.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere DNS-Server einzurichten.

Sie können hier sowohl globale DNS-Server konfigurieren als auch DNS-Server, die einer bestimmten Schnittstelle zugewiesen werden sollen.

Einen DNS-Server für eine bestimmte Schnittstelle zu konfigurieren ist zum Beispiel nützlich, wenn Accounts zu verschiedenen Providern über unterschiedliche Schnittstellen eingerichtet sind und Lastverteilung verwendet wird.

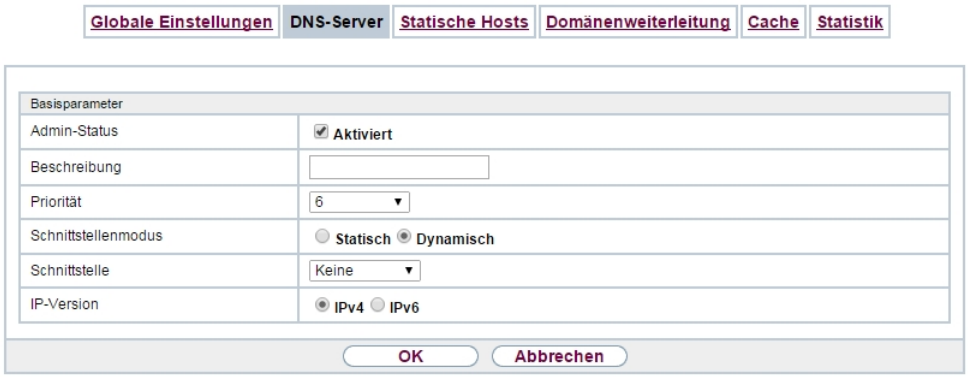

Abb. 17: **Lokale Dienste**->**DNS**->**DNS-Server**->**Neu**

Das Menü **Lokale Dienste**->**DNS**->**DNS-Server**->**Neu** besteht aus folgenden Feldern:

Relevante Felder im Menü Basisparameter

Feld	Beschreibung
IP-Version	Wählen Sie die verwendete IP-Version aus. Mögliche Werte: • *IPv4* • *IPv6* Standardmäßig ist *IPv4* ausgewählt.

Feld	Beschreibung
Primärer IPv6-DNS-Server	Nur bei **Schnittstellenmodus** = *Statisch* Geben Sie die IPv6-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.
Sekundärer IPv6-DNS-Server	Nur bei **Schnittstellenmodus** = *Statisch* Geben Sie optional die IPv6-Adresse eines alternativen Name-Servers ein.

2.2.14 DHCPv6-Server

Sie können Ihr Gerät als DHCPv6-Server verwenden. Dieser DHCPv6-Server kann IP-Adressen und DHCP-Optionen an Clients verteilen oder auch nur DHCP-Optionen ohne Adressen. Diese Parameter werden in einem sogenannten "Option Set" zusammengefasst. Ein Option Set kann an eine Schnittstelle gebunden werden (siehe unter **Lokale Dienste**->**DHCPv6-Server**->**DHCPv6-Server**->**Neu**) oder es kann global konfiguriert werden (siehe unter **Lokale Dienste**->**DHCPv6-Server**->**DHCPv6 Global Options**->**Neu**). DHCP-Optionen können zum Beispiel Informationen über DNS-Server oder Zeitserver enthalten.

Hinweis

Ein IPv6-Adress-Pool entsteht durch die Zuweisung eines IPv6-Link-Präfixes (Subnetz mit der Länge /64) zu einem DHCPv6 Option Set. Die Definition eines eigenen Abschnitts von IPv6-Aderssen, wie z. B. fc00:1:2:3::1..fc00:1:2:3::100 ist anders als im DHCPv4 nicht vorgesehen.

Für die Konfiguration eines IPv6-Adress-Pools müssen folgende Voraussetzungen erfüllt sein:

(a) IPv6 muss auf der betreffenden Schnittstelle aktiviert sein.

(b) Ein IPv6-Link-Präfix (Subnetz) mit der Länge /64 muss auf der gewünschten Schnittstelle konfiguriert sein. Ein IPv6-Link-Präfix kann auf zwei Arten definiert sein:

- Der IPv6-Link-Präfix ist von einem Allgemeinen IPv6-Präfix (Präfix mit einer Länge von zum Beispiel /56 oder /48) abgeleitet. In diesem Fall muss der Allgemeine IPv6-Präfix im Menü **Netzwerk**->**Allgemeine IPv6-Präfixe**->**Konfiguration eines Allgemeinen Präfixes** konfiguriert sein.
- Der IPv6-Link-Präfix mit Länge /64 wird manuell auf der entsprechenden Schnittstelle konfiguriert und nicht von einem Allgemeinen IPv6-Präfix abgeleitet.

(c) Die Option **DHCP-Server** muss für die Schnittstelle aktiviert sein.

Darüber hinaus sind folgende Einstellungen empfehlenswert:

- Die Werte für die Optionen **Bevorzugte Gültigkeitsdauer** und **Gültigkeitsdauer** sollten auf Werte gesetzt werden, die größer sind als der Wert für **Router-Gültigkeitsdauer**.

  Bei einer **Router-Gültigkeitsdauer** von 600 Sekunden, empfehlen sich z. B. eine **Bevorzugte Gültigkeitsdauer** von 900 Sekunden und eine **Gültigkeitsdauer** von 1800 Sekunden.
- Die Option **DHCP-Modus** sollte aktiviert sein.

Zur Einstellung der o.g. Optionen wählen Sie das Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**. Mit dem Symbol wählen Sie die gewünschte Schnittstelle. Aktivieren Sie IPv6 und setzen den **IPv6-Modus** auf `Router`. Klicken Sie im Feld **IPv6-Adressen** auf **Hinzufügen** und konfigurieren Sie den Link-Präfix. Bestätigen Sie Ihre Konfiguration mit **Übernehmen**. Die Konfiguration der empfohlenen Einstellungen erfolgt dann in folgenden Menüs:

- **Router-Gültigkeitsdauer**: **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu / Bearbeiten**->**Erweiterte Einstellungen**->**Erweiterte IPv6-Einstellungen**
- **Bevorzugte Gültigkeitsdauer** und **Gültigkeitsdauer**: **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu / Bearbeiten**->**Grundlegende IPv6-Parameter**->**Hinzufügen**->**Erweitert**

Hier können Sie - bezogen auf eine Schnittstelle - in einem Option Set Adresspools anlegen und DHCP-Options definieren.

2.2.14.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um ein Option Set anzulegen. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Abb. 18: **Lokale Dienste->DHCPv6-Server->DHCPv6-Server->Neu**

Das Menü **Lokale Dienste->DHCPv6-Server->DHCPv6-Server->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Name	Geben Sie einen Namen für das Option Set ein.
Schnittstelle	Wählen Sie die IPv6-Schnittstelle, an die das Option Set gebunden sein soll. Zur Auswahl stehen Schnittstellen mit folgender Konfigurator: • IPv6 ist aktiviert. • Die Option **DHCP-Server** ist aktiviert. Im Auslieferungszustand ist IPv6 für alle Schnittstellen deaktiviert. Erscheint die gewünschte Schnittstelle nicht in der Auswahl, konfigurieren Sie sie im Menü **LAN->IP-Konfiguration->Schnittstellen** gemäß den in der Einleitung genannten Vorgaben.
Address assignment	Die Definition eines IPv6-Adresspools erfolgt durch Zuweisung eines IPv6-Link-Präfixes (Subnetz mit Länge /64) zu einem DHCPv6 Option Set. Der IPv6-Adress-Pool umfasst immer den

Feld	Beschreibung
	kompletten 64-Bit-Adressraum des gewählten IPv6-Link-Präfixes. Die Adressvergabe erfolgt zufällig. Mit **Hinzufügen** können Sie dem IPv6 Option Set einen oder mehrere IPv6-Link-Präfixe zuordnen. **Hinweis** Bitte beachten Sie, dass hier ausschließlich die IPv6-Link-Präfixe zur Auswahl stehen, die der gewählten Schnittstelle zugewiesen sind.

Felder im Menü Server Options

Feld	Beschreibung
DNS-Domänen-Suchliste	Mit **Hinzufügen** können Sie eine Liste von Domain-Namen erstellen, die auf Client-Seite als Domain-Suchliste bei der Namensauflösung verwendet werden soll (DHCPv6 Option 24 "Domain Search List"). Die Domain-Namen werden gemäß der durch die Liste vorgegebenen Reihenfolge an die Clients übermittelt.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Advanced Server Options

Feld	Beschreibung
DNS-Server	Hier können Sie die DNS-Server konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 23 "DNS Recursive Name Server"). In der Standardeinstellung werden die globalen DNS-Server des Systems propagiert. (Die globalen DNS-Server werden im Feld **DNS-Propagation** im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**-> ->**Erweiterte Einstellungen** mit **IPv6** = `Aktiviert` konfiguriert.) Sie können aber auch DNS-Server manuell angeben und an die Clients übertragen. Deaktivieren Sie hierzu die Option **RA oder globalen Fallback-DNS-Server verwenden** und erstellen Sie mit **Hinzufügen** die gewünschten DNS-Server-Einträge.

Feld	Beschreibung
SNTP-Server	Hier können Sie die Zeitserver konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Mit **Hinzufügen** können Sie die gewünschten Zeitserver-Einträge anlegen.

2.2.15 DHCPv6 Global Options

In diesem Menü können Sie die für den DHCPv6-Server global gültigen DHCPv6-Optionen konfigurieren. Eine hier konfigurierte Option wird immer dann propagiert, wenn für diese Option keine exaktere Definition (z.B. keine schnittstellenspezifische oder Vendor-ID-spezifische Definition) existiert.

Abb. 19: **Lokale Dienste->DHCPv6 Global Options->Neu**

Das Menü **Lokale Dienste->DHCPv6 Global Options->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
DNS-Domänen-Suchliste	Mit **Hinzufügen** können Sie eine Liste von Domain-Namen erstellen, die auf Client-Seite als Domain-Suchliste bei der Namensauflösung verwendet werden soll (DHCPv6 Option 24 "Domain Search List"). Die Domain-Namen werden gemäß der durch die Liste vorgegebenen Reihenfolge an die Clients übermittelt. Der Domain-Name (z. B. dev.bintec.de.) muss mit Punkt (.) enden.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Server-Priorität

Feld	Beschreibung
Server-Priorität	In den vom DHCPv6 Server an die Clients gesendeten DHCPv6 Advertisements kann die DHCPv6-Option 7 Preference enthalten sein. Mögliche Werte sind *0...255*. In einem Netzwerk mit mehreren DHCPv6 Servern wird über diese Option gesteuert, welcher DHCPv6-Server im Netzwerk die höchste Priorität besitzt. Empfängt ein Client DHCPv6 Advertisements mit unterschiedlicher Priorität von verschiedenen Servern, so wird der Client in der Regel die Werte des Servers mit der höchsten Priorität übernehmen. Der Client kann jedoch auch DHCPv6 Advertisements mit niedrigerer Priorität akzeptieren, wenn der im DHCPv6 Advertisement enthaltene Parametersatz mehr den vom Client angeforderten Optionen entspricht. Der Wert *0* bedeutet "nicht spezifiziert" (niedrigste Priorität), *255* bedeutet höchste Priorität.

Felder im Menü Erweiterte Server-Optionen

Feld	Beschreibung
DNS-Server	Hier können Sie die DNS-Server konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 23 "DNS Recursive Name Server"). In der Standardeinstellung werden die globalen DNS-Server des Systems propagiert. (Die globalen DNS-Server werden im Feld **DNS-Propagation** im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**->  ->**Erweiterte Einstellungen** mit **IPv6** = *Aktiviert* konfiguriert.) Sie können aber auch DNS-Server manuell angeben und an die Clients übertragen. Deaktivieren Sie hierzu die Option **RA oder globalen Fallback-DNS-Server verwenden** und erstellen Sie mit **Hinzufügen** die gewünschten DNS-Server-Einträge.
SNTP-Server	Hier können Sie die Zeitserver konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Mit **Hinzufügen** können Sie die gewünschten Zeitserver-Einträge anlegen.

2.2.16 Zustandsbehaftete Clients

Hier sehen Sie Informationen zu zustandsbehafteten Clients, sobald diese eine IPv6-Adresse bezogen haben.

Abb. 20: **Lokale Dienste->DHCPv6-Server->Zustandsbehaftete Clients**

2.2.17 Konfiguration von zustandsbehafteten Clients

Bei einer zustandsbezogenen Konfiguration von IPv6 Clients, wird dem Client neben den DHCP-Optionen auch der IPv6-Präfix übermittelt.

2.2.17.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um Einträge für Stateful Clients anzulegen. Normalerweise müssen Sie keine Einträge anlegen. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Sie sollten jeden automatisch angelegten Eintrag einmal aufrufen, um den Inhalt zu prüfen und gegebenenfalls anzupassen.

Abb. 21: **Lokale Dienste->DHCPv6-Server->Konfiguration von zustandsbehafteten Clients+Neu**

Das Menü besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
DUID	Ein Client verwendet das Feld **DUID** (DHCP Unique Identifier), um sich zu identifizieren und eine IP-Adresse vom DHCPv6-Server zu beziehen. Wenn Sie mit der Schaltfläche **Neu** einen Eintrag anlegen, können Sie die **DUID** als 16- bis 20-stellige HEX-Zahl eingeben. Sie können sie mit den Trennzeichen Minus eingeben wie unter Windows oder als Block ohne Trennzeichen wie unter Linux.
Client FQDN akzeptieren	Wenn **Client FQDN akzeptieren** aktiviert ist, wird der Client mit dem Parameter FQDN (Fully Qualified Domain Name) im Cache des Domain Name Servers eingetragen.
Administrative FQDNs	Mit **Hinzufügen** können Sie - auch bei automatisch angelegten Einträgen - den Parameter FQDN (Fully Qualified Domain Name) eingeben.
Kennung der statischen Schnittstelle	Das Feld **Kennung der statischen Schnittstelle** ist der Host-Anteil der IPv6-Adresse, d.h. die letzten 64 Bit der IPv6-Adresse. Dieser Präfix muss mit :: anfangen.

2.2.18 Ping-Test

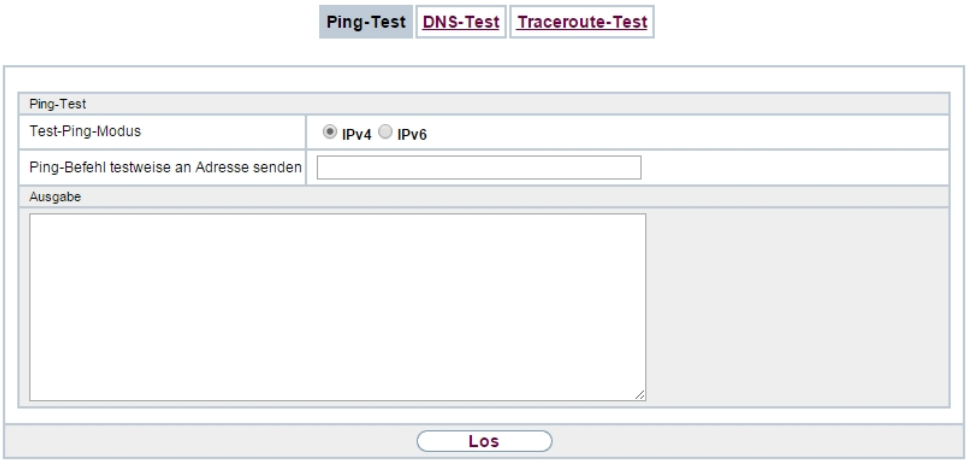

Abb. 22: **Wartung**->**Diagnose**->**Ping-Test**

Mit dem Ping-Test können Sie überprüfen, ob ein bestimmter Host im LAN oder eine Internetadresse erreichbar sind.

Relevante Felder im Menü Ping-Test

Feld	Beschreibung
Test-Ping-Modus	Wählen Sie die für den Ping-Test verwendete IP-Version. Mögliche Werte: • *IPv4* • *IPv6*
Zu verwendende Schnittstelle	Nur für **Test-Ping-Modus** = *IPv6* Wählen Sie für Link-Lokale-Adressen die Schnittstelle, die für den Ping-Test verwendet werden soll. Für globale Adressen kann *Standard* verwendet werden.

Durch Anklicken der **Los**-Schaltfläche wird der Ping-Test gestartet. Das **Ausgabe**-Feld zeigt die Meldungen des Ping-Tests an.

2.2.19 Traceroute-Test

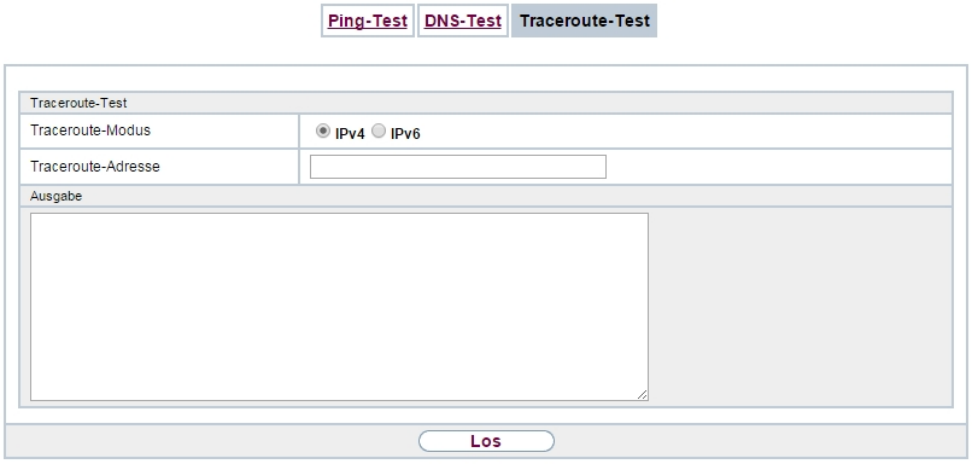

Abb. 23: **Wartung->Diagnose->Traceroute-Test**

Mit dem Traceroute-Test können Sie die Route zu einer bestimmten Adresse (IP-Adresse oder Domänenname) anzeigen lassen, sofern diese erreichbar ist.

Relevantes Feld im Menü Traceroute-Test

Feld	Beschreibung
Traceroute-Modus	Wählen Sie die für den Traceroute-Test verwendete IP-Version. Mögliche Werte: • *IPv4* • *IPv6*

Durch Anklicken der **Los**-Schaltfläche wird der Traceroute-Test gestartet. Das **Ausgabe**-Feld zeigt die Meldungen des Traceroute-Tests an.

2.3 IPSec - Neue Algorithmen

Ab **Systemsoftware 10.1.4** stehen für IPSec neue Algorithmen zur Verfügung. Im Menü **VPN**->**IPSec**->**Phase-1-Profile**->**Neues IKEv1-Profil erstellen bzw. Neues IKEv2-Profil erstellen**->**Neu** bzw. **VPN**->**IPSec**->**Phase-2-Profile**->**Neu** sind unter **Proposals** die neuen Hash-Algorithmen *SHA2-256*, *SHA2-384* und *SHA2-512* verfügbar. Sie sind im GUI unter der Bezeichnung **Authentifizierung** wählbar.

SHA2 ist der Nachfolger von SHA1. Die Zahl, die auf "SHA2" folgt, gibt die jeweilige Länge des Hash-Wertes in Bit an. Im Gegensatz zu SHA1 gilt der Hash-Algorithmus SHA2 aktuell als sicher.

Im Menü **VPN**->**IPSec**->**Phase-1-Profile**->**Neues IKEv2-Profil erstellen**->**Neu** stehen unter **Proposals** die neuen Diffie-Hellman-Gruppen *14 (2048 Bit)*, *15 (3072 Bit)* und *16 (4096 Bit)* zur Verfügung.

Die Diffie-Hellman-Gruppen legen die Stärke des Schlüssels fest. Größere Gruppennummern bedeuten mehr Sicherheit, erfordern aber auch höheren Rechenaufwand bei der Berechnung des Schlüssels.

Hinweis

Beachten Sie bitte folgende Hinweise zu dieser Erweiterung:

Die neuen Algorithmen - insbesondere die zur Erzeugung langer Schlüssel für den Diffie-Hellman-Austausch - erfordern eine erhebliche Rechenleistung. Folgende Geräte werden diese neuen Algorithmen unterstützen:

- bintec RS3xx- und RS123x-Serie
- be.IP-Serie

- bintec RXL-Serie.

Bei allen Geräten ist in Abhängigkeit von der Anzahl der aktiven IPSec-Tunnel ein teilweise erheblicher Einfluss auf die Leistung des Geräts zu erwarten. Die bintec RXL-Serie wird in einem späteren Release über eine Hardwareunterstützung der Algorithmen verfügen, was zu einer deutlichen Leistungssteigerung gegenüber den nur softwarebasierten Lösungen führen wird.

Die Geräte der Rxx02- und RTxx02-Serien unterstützen aufgrund ihrer älteren Hardwareausstattung die neuen Algorithmen NICHT.

2.4 IKEv2 Routing

Ab **Systemsoftware 10.1.4** steht für den Aufbau eines Tunnels mit einem Cisco FlexVPN Server als Gegenstelle das sogenannte "IKEv2 Routing" zur Verfügung. Ihr bintec Router teilt als Client seine Netzwerke dem FlexVPN-Server mit, der sie in seine Routing-Tabelle einträgt.

2.5 WLAN - Mehrere Bridge Links verfügbar

Ab **Systemsoftware 10.1.4** können Sie im Menü **Wireless LAN**->**WLAN**->**Bridge Links** mehrere Einträge für Bridge Links im Slave Modus anlegen.

2.6 Wartung - Neue Optionen (hybird)

Ab **Systemsoftware 10.1.4** stehen bei allen Geräten der hybird-Serien, bei denen eine SD-Karte gesteckt ist, im Menü **Wartung**->**Software & Konfiguration**->**Optionen** im Feld **Aktion** die neuen Optionen *Zusätzliche Dateien laden (in den USB-Speicher)* und *MMC/SD-Karte formatieren* zur Verfügung.

2.7 SIA

Ab **Systemsoftware 10.1.4** können Sie im Menü **Externe Berichterstellung**->**SIA**->**SIA** eine Datei erstellen lassen, die dem Support umfassende Informationen zum Zustand des Geräts liefert, wie z. B. die aktuelle Konfiguration, den verfügbaren Speicher, die Betriebszeit des Geräts usw.

2.8 Factory Reset

Ab **Systemsoftware 10.1.4** können Sie Ihr Gerät über das GUI im Menü **Wartung**->**Factory Reset** in den Auslieferungszustand versetzen.

2.9 Hersteller über MAC-Adresse anzeigen

Ab **Systemsoftware 10.1.4** können Sie im Menü **Systemverwaltung**->**Globale Einstellungen**->**System** die Anzeige des Herstellers in der MAC-Adresse ein- oder ausschalten. Für den Herstellernamen (meist eine Abkürzung desselben) werden bis zu acht Zeichen am Anfang der MAC-Adresse verwendet. Statt `00:a0:f9:37:12:c9` wird mit Herstelleranzeige zum Beispiel `BintecCo_37:12:c9` angezeigt.

2.10 Neues DNS-Menü

2.10.1 Dynamische Hosts

Im Menü **Lokale Dienste**->**DNS**->**Dynamische Hosts** sehen Sie die relevanten Angaben zu den Dynamischen DNS-Einträgen.

Abb. 24: **Lokale Dienste**->**DNS**->**Dynamische Hosts**

2.11 Benutzer ausloggen

Es kann vorkommen, dass durch eine nicht vollständig abgebaute Konfigurationssitzung Funktionen der Konfigurationsoberfläche beeinträchtigt werden. In diesem Fall können in diesem Menü alle noch bestehenden Verbindungen zum GUI eingesehen und ggf. beendet werden.

2.11.1 Benutzer ausloggen

In diesem Menü sehen Sie zunächst eine Auflistung aller aktiven Konfigurationsverbindungen.

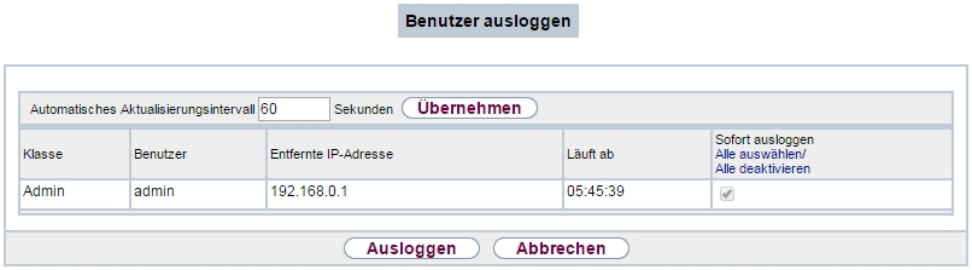

Abb. 25: **Wartung->Benutzer ausloggen->Benutzer ausloggen**

Felder im Menü Benutzer ausloggen

Feld	Beschreibung
Klasse	Zeigt die Benutzerklasse an, der der angemeldete Benutzer angehört.
Benutzer	Zeigt den Benutzernamen an.
Entfernte IP-Adresse	Zeigt die IP-Adresse an, von der die Verbindung aufgebaut wurde. Die kann die Adresse eines PCs sein, aber auch die Adresse eines zwischengelagerten Routers.
Läuft ab	Zeigt an, wann die Verbindung automatisch getrennt wird.
Sofort ausloggen	Wenn sie das Kontrollkästchen aktivieren, wird dieser Benutzer mit einem klick auf **Ausloggen** vom System abgemeldet.

2.11.1.1 Logout-Optionen

Nachdem Sie die Auswahl der zu beendenden Verbindungen mit Ausloggen bestätigt haben, können Sie wählen ob und welche Konfigurationen, die mit den entsprechenden Sitzungen zusammenhängen, vor dem Abmelden der Benutzer gespeichert werden.

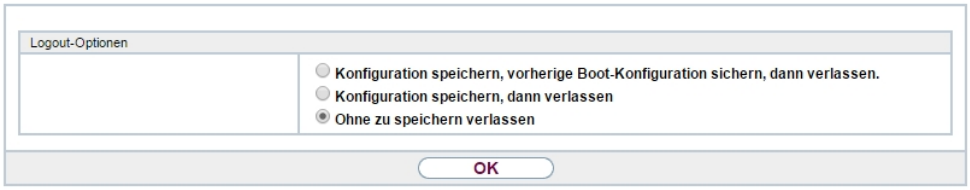

Abb. 26: **Wartung->Benutzer ausloggen->Ausloggen**

2.12 Automatischer VDSL-/ADSL-Modus

Im Menü **WAN->Internet + Einwählen->PPPoE->Neu** steht im Feld **PPPoE-Ethernet-Schnittstelle** der Wert `Automatisch` zur Verfügung, um den automatischen VDSL-/ADSL-Modus zu unterstützen, der im Assistenten bereits verfügbar war. In diesem Modus wird die Schnittstelle für der Internetzugang automatisch gewählt. Achten Sie darauf, dass für einen ADSL-Zugang im Menü ATM eine Schnittstelle angelegt sein muss, für einen VDSL-Zugang ist dies nicht notwendig.

2.13 Firewall - Zurücksetzen

Ab **Systemsoftware 10.1.4** können Sie im Menü **Firewall->Richtlinien->Optionen** die Firewall auf ihre Werkseinstellungen zurücksetzen.

2.14 Notrufe

Ab **Systemsoftware 10.1.4** werden Notrufe priorisiert. Sind alle vorhandenen Kanäle (auch SIP-Kanäle werden berücksichtigt) belegt, wird ein bestehender Ruf beendet, um den Notruf absetzen zu können.

2.15 elmeg IP680 verfügbar

Ab **Systemsoftware 10.1.4** ist das IP-Telefon **elmeg IP680** verfügbar. Es wird von elmeg hybird Systemen automatisch erkannt und als Endgerät unter **Endgeräte->elmeg Systemtelefone->elmeg IP** angezeigt.

2.16 Telefone in Teams

Bei Verwendung von Teams können ab **Systemsoftware 10.1.4** die Funktionen `Bei Nichtmelden` und `Bei Besetzt` verwendet werden, da nicht aktive Telefone automatisch aus den Teams ausgelogged werden.

Kapitel 3 Änderungen

Folgende Änderungen sind in **Systemsoftware 10.1.4** vorgenommen worden.

Hinweis

Bitte beachten Sie, dass möglicherweise eine Änderung für unterschiedliche Geräte zu unterschiedlichen Zeitpunkten zur Verfügung gestellt wurde.

3.1 Passwortänderung beim ersten Einloggen

Ab **Systemsoftware 10.1.4** wird die Seite zum Ändern des Passworts aufgerufen, solange das Admin Passwort nicht geändert ist, und nicht wie bisher die Seite zum Einloggen angezeigt. Der Administrator muss sich daher jetzt nicht mehr erst einloggen, bevor er sein Passwort ändern kann.

3.2 PBX-Assistent erweitert

Im Menü **Assistenten**->**PBX** wurde der PBX-Assistent um die Reiter **Erste Schritte**, **Endgeräte** und **Rufverteilung** erweitert.

3.3 Bezeichnungen angepasst

Wegen der Einführung von IPv6 wurden einige Bezeichnungen unter IPv4 zur besseren Unterscheidbarkeit angepasst, z. B. wurde im Menü **Firewall**->**Richtlinien**->**Optionen** das Feld **Firewall Status** in **Status der IPv4-Firewall** umbenannt.

3.4 Menü-Bezeichnung geändert

Die Menü-Bezeichnung **Endgeräte**->**elmeg Systemtelefone**->**elmeg IP1x** wurde in **Endgeräte**->**elmeg Systemtelefone**->**elmeg IP** geändert.

3.5 Domänenweiterleitung geändert

Im Menü **Lokale Dienste**->**DNS**->**Domänenweiterleitung**->**Neu** wurden mit **Weiterleiten** = *Domäne* die Eingabemöglichkeiten im Feld **Domäne** erweitert.

Bisher konnten Sie als **Domäne** zum Beispiel **.qa.bintec.de* eingeben, um **.qa.bintec.de* zu verwenden.

Ab **Systemsoftware 10.1.4** wird bei Eingabe ohne führende Wildcard *** und nach Bestätigen mit **OK** automatisch eine führende Wildcard eingefügt. Sie können zum Beispiel *.qa.bintec.de* oder *qa.bintec.de* eingeben und verwenden nach Bestätigen mit **OK** automatisch **.qa.bintec.de*.

3.6 VDSL - TCP Upstream Performance verbessert

Bei VDSL-Verbindungen wurde die TCP Upstream Performance durch Reduzierung des Paketverlusts signifikant verbessert und bewegt sich jetzt im selben Bereich wie bei vergleichbaren Geräten anderer Hersteller.

3.7 LEDs für bintec RS353jv-4G geändert

Ab **Systemsoftware 10.1.4** zeigen die LEDs *LTE* und *USB* im Gerät **bintec RS353jv-4G** folgendes Verhalten:

LED Statusanzeige

LED	Farbe	Status	Information
LTE	grün	im 1-Sekunden-Intervall blinkend	Mobilfunkverbindung wird initialisiert
	grün	an	WAN-Verbindung hergestellt.
	grün	im Übertragungsintervall blinkend	Datenverkehr über 3G/4G
	grün	im 3-Sekunden-Intervall blinkend	Ein Fehler ist aufgetreten
		aus	Keine SIM-Karte im Gerät
USB	grün	an	USB-LTE-Stick installiert
	grün	blinkend	Datenverkehr über USB
		aus	Keine USB-Verbindung.

Mobilfunkstandard

Über die MIB-Variable **biboadmledmeter** können Sie einen zusätzlichen LED-Modus aktivieren, der es Ihnen erlaubt, den Zustand der Mobilfunkverbindung genauer zu bestimmen. Mit **biboadmledmeter**= *1* aktivieren Sie den Modus, mit **biboadmledmeter**= *2* deaktivieren Sie ihn wieder. Wenn Sie den Zustand des LED-Modus nicht speichern wollen, können Sie ihn auch aktivieren, indem Sie drei Mal hintereinander für ca. 1 Sekunde die Reset-Taste drücken. Ein erneuter kurzer Druck deaktiviert dem Modus dann wieder.

Es besteht folgender Zusammenhang zwischen dem Leuchten einer LED und dem verwendeten Mobilfunkstandard:

LED	Mobilfunkstandard
BRI	GSM
USB	UMTS
LTE	LTE

Darüber hinaus können Sie die Signalqualität an den acht Ethernet LEDs ablesen. Wenn alle acht LEDs leuchten, liegt eine beinah perfekte Verbindung vor. Bei geringerer Signalqualität leuchten entsprechend weniger LEDs.

3.8 WLAN - Konfigurationsmöglichkeiten

Je nach Konfiguration stehen im WLAN eine unterschiedliche Anzahl von Masters und Slaves zur Verfügung:

Betriebsmodus	Kanal	Unterstützt
Aus		
Access Client	Auto/fester Wert	1 Client
Bridge Link Client	Auto	1 Slave (bei mehreren der erste in der Liste)
Bridge Link Client	Fester Wert	x Slaves
Access Point / Bridge Link Master	Auto	x Access Points + x Masters
Access Point / Bridge Link Master	Fester Wert	x Access Points + x Masters + x Slaves

3.9 SIP-Verbindungen verbessert

SIP- Unterbrechungen werden schneller erkannt und behoben.

Kapitel 4 Fehlerbehebungen

Folgende Fehler sind in **Systemsoftware 10.1.4** behoben worden:

Hinweis

Bitte beachten Sie, dass möglicherweise eine Fehlerbehebung für unterschiedliche Geräte zu unterschiedlichen Zeitpunkten zur Verfügung gestellt wurde.

4.1 Stacktrace

ID 19229

Wenn eine Ethernet-Schnittstelle, z. B. *en1-0*, und eine WLAN-Schnittstelle, z. B. *vss7-10*, derselben Bridge-Gruppe *br0* zugeordnet wurden, trat ein sporadischer Stacktrace auf.

4.2 Panic (hybird 600)

ID 19574

Es konnte vorkommen, dass eine **hybird 600** täglich neu startete. Bei einigen der angeschlossenen Telefone traten Probleme bei der Gesprächsannahme auf.

4.3 Assistenten - Internet-Assistent fehlerhaft

ID 19394

Wenn der Internet-Assistent verwendet wurde, der **Verbindungstyp** = *UMTS/LTE* eingestellt war und **Immer aktiv** *Aktiviert* war, so legte der Assistent zwei Standard-Routen an.

4.4 Internet Assistent - Falscher Parameter

ID n/a

Unter bestimmten Bedingungen wurde im Internet Assistenten bei einem korrekt eingegebenen Benutzernamen vom System fälschlicherweise `t-online-com/` hinzugefügt.

4.5 Probleme mit Telekom Speedstick LTE V

ID 19147

Der Telekom Speedstick LTE V (Huawei E3372) funktionierte nicht korrekt.

4.6 Internetverbindung down

ID n/a

Wenn auf eine Schaltfläche geklickt wurde, konnte es vorkommen, dass eine Internetverbindung gekappt wurde, die bereits aufgebaut war.

4.7 Schlechte Perfomance

n/a

In einem Bridging Szenario, in dem der Datenverkehr vom Ethernet in ein WLAN weitergeleitet wurde, konnte es vorkommen, dass die CPU zu fast 100 % ausgelastet war.

4.8 Dasselbe Symbol für unterschiedliche Aktionen

ID n/a

Für das Anstoßen und für das Zurücksetzen von Aktionen wurde fälschlicherweise dasselbe Symbol  verwendet. Ab **Systemsoftware 10.1.4** steht für das Zurücksetzen von Aktionen das Symbol  zur Verfügung. Sie können zum Beispiel unter

Konfigurationszugriff->**Zugriffsprofile** die Profile in den Auslieferungszustand zurücksetzen.

4.9 Fehlermeldung nicht korrekt

ID 19420

Bei Eingabe der **Länderkennzahl** konnte es vorkommen, dass eine falsche Fehlermeldung angezeigt wurde.

4.10 Einträge konnten nicht gelöscht werden

ID 19638

Es war nicht möglich, Einträge im Menü **Physikalische Schnittstellen**->**ISDN-Ports**->**MSN-Konfiguration** mit Hilfe des Symbols  zu löschen.

4.11 Unbeabsichtigte Trennung einer Verbindung (hybird)

ID 19334

Es konnte vorkommen, dass eine von einer elmeg hybird gewählte Verbindung nach externer Übergabe getrennt wurde.

4.12 Firmware Update misslungen

ID 19327

Ohne IPv6-Verbindung war kein Firmware Update möglich.

4.13 LTE - Echo-Request-Pakete erreichten ihr Ziel nicht

ID 19333

Echo-Request-Pakete, die auf einem Router mit integriertem LTE(4G)-Modem mittels Keepalive Monitoring erzeugt wurden, erreichten den Target Host nicht.

4.14 Roaming-Probleme

ID n/a

Bei M2M-Karten konnten Probleme beim Daten-Roaming auftreten.

4.15 SSH - Verbindung schlug fehl

ID 19213

Nach einem ordnungsgemäßen Routerbetrieb von ungefähr zwei Tagen schlug plötzlich die SSH-Verbindung fehl.

4.16 Falsche Seite

ID 19506

Es konnte vorkommen, dass nach dem Einloggen eine falsche Seite geladen wurde.

4.17 Konfigurationssitzung unvollständig

ID 19493

Es konnte vorkommen, dass eine Konfigurationssitzung nicht beendet werden konnte und TR069 nicht konfiguriert werden konnte, wenn der Benutzer - statt sich auszuloggen - nur den Browser schloss.

4.18 Windows 10 Edge Browser - Ungewollte Zeilenumbrüche

ID n/a

Die ungewollten Zeilenumbrüche im Output des Browsers Windows Edge (Spartan) wurden durch einen Fix von Microsoft beseitigt. Der interne Fix wurde entfernt, da er nicht mehr benötigt wird.

4.19 Verbindungsabbrüche (hybird)

ID 19334

Unter bestimmten Umständen konnte es zu Verbindungsabbrüchen kommen.

4.20 System - LED-Modus fälschlicherweise angezeigt (RS-Serie)

19074

Bei Geräten der RS-Serie wurde im Menü **Systemverwaltung**->**Globale Einstellungen**->**System** fälschlicherweise das Feld **LED-Modus** angezeigt. Dieses Feld ist ausschließlich für WLAN-Geräte vorgesehen.

4.21 SSL - Keine Übertragung von Konfigurationsdateien

ID 19219

Über eine SSL-Verbindung konnten keine Konfigurationsdateien übertragen werden.

4.22 FAX funktionierte nicht korrekt

ID 19098

Beim Versuch ein FAX zu senden, konnte es vorkommen, dass eine Systemblockade auftrat und der Router die Verbindung nicht mehr beendete.

4.23 VoIP - Keine Sprachübertragung

ID 19184

Wenn in einem Team ein analoges oder ein ISDN-Telefon verwendet wurde, wurde ein kommender Ruf zwar korrekt signalisiert, bei Annahme des Rufs fand aber keine Sprachübertragung statt.

4.24 VoIP - Account nicht verwendbar

ID 19551

Bei Verwendung von VoIP Clients (z. B. einem Smart Phone mit VoIP Client oder einem VoIP-Telefon) war der VoIP Account wegen eines NAT-Konflikts nicht verwendbar.

4.25 VoIP - Providerprobleme

ID n/a

Es konnte vorkommen, dass Provider mit bestimmten Profilen nicht angezeigt wurden und/oder nicht editiert oder gelöscht werden konnten.

4.26 WLAN - Stacktrace

ID 19496

Wenn mehrere SSIDs pro Funkmodul angelegt waren und eine VSS-Schnittstelle über das GUI aktiviert wurde, trat beim Access Point eine Panic auf.

4.27 WLAN - Panic

ID 19678

Bei Access Points im Slave-Modus konnte es vorkommen, dass mehrmals am Tag eine Panic auftrat.

4.28 WLAN - Access Points

ID 19530

Wenn Access Points von unterschiedlichem Typ zusammen eingesetzt wurden, konnte es vorkommen, dass die GUI während der Konfiguration eines Slave Access Points merkwürdige Fehler anzeigte oder dass die Slave Access Points nicht funktionierten.

4.29 WLAN - LED-Modus fehlte

ID n/a

Bei WLAN-Geräten fehlte im Menü **Systemverwaltung**->**Globale Einstellungen**->**System** der Parameter **LED-Modus**.

4.30 WLAN - Automatische Kanalwahl fehlerhaft

ID 18836

Bei Verwendung eines Wireless LAN Controllers mit benutzerdefiniertem Kanalplan konnte es mit Access Points von Qualcomm Atheros vorkommen, dass die Kanalwahl nicht korrekt funktionierte.

4.31 WLAN - Aktives Funkmodulprofil nicht wählbar

ID 19198

Wenn mindestens ein Access Point vom Wireless LAN Controller verwaltet wurde, so

konnte im Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Slave Access Points**-> unter **Aktives Funkmodulprofil** kein Funkmodulprofil ausgewählt werden.

4.32 Funkmodul - Profil falsch angezeigt

ID 19320

Im Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Slave Access Points**-> konnte man im Feld **Aktives Funkmodulprofil** fälschlicherweise den Wert *1* wählen.

4.33 WLAN Controller - WTP funktionierte nicht korrekt

ID 19553

Wenn mehrere WTPs von einem WLAN Controller verwaltet wurden, konnte es vorkommen, dass nach dem Aus- und wieder Einschalten eines WTP sich ein anderer WTP in einem falschen Zustand befand.

4.34 WLAN Controller - Stacktrace

19698

Wenn Slave Access Points von einem Wireless LAN Controller verwaltet wurden, konnte es vorkommen, dass be einigen Access Points mehrmals ein Stacktrace auftrat.

4.35 Netzwerk - Reboots

ID 19484

Bei Verwendung einer Drop-In-Gruppe kam es zu zwei oder drei Reboots pro Tag.

4.36 QoS - Keine Klassifizierung der High-Priority-Pakete

ID 19527

Die interne Klassifizierung der High-Priority-Pakete wurde durch eine aktive Firewall gestört.

4.37 QoS - Konfiguration nicht korrekt

19366

Bei Verwendung des Assistenten **Erste Schritte** war die QoS-Konfiguration nicht korrekt.

4.38 QoS - 1TR112-Anforderungen nicht erfüllt

ID 19296

Die QoS-Signalisierung entsprach nicht den Anforderungen von 1TR112.

4.39 Codec-Problem

ID 19471

Wenn der Codec, der laut RFC4040 als "Clearmode" bezeichnet wird, zusammen mit anderen Codecs zur Wahl stand, konnten keine Daten übertragen werden.

4.40 Codec-Probleme (hybird 600)

Id 19606

Bei Verhandlung des Codec zwischen einer Polycom Soundstation IP 6000 und einer **hybird 600** kam es zu Problemen.

4.41 SIP - Verbindung abgebrochen

19587

Es konnte vorkommen, dass eine Verbindung nach einer Anrufweiterleitung abgebrochen wurde.

4.42 SIP - Rufe abgewiesen

ID 19486

Es konnte vorkommen, dass eingehende Rufe mit der Statusmeldung 480 (Temporarily not available) abgewiesen wurden. Die Anlage gab dabei die Debug-Meldung "No matching codecs, call rejected" aus.

4.43 SIP - Eingehende Rufe ignoriert

ID 19432

Es konnte vorkommen, dass eingehende SIP-Rufe ignoriert wurden.

4.44 SIP - Falsches Format

ID 19447

Unter speziellen Bedingungen konnte es vorkommen, dass ein falsches Rufnummernformat verwendet wurde.

4.45 Telefonie - Rufe nicht möglich

ID 19373

Es konnte vorkommen, dass keine Rufe von der Haupt-MSN aus möglich waren.

4.46 Telefonie - Falsche Verbindungsdaten

ID 19422

Bei längeren Telefongesprächen wurden falsche Verbindungsdaten angezeigt.

4.47 Telefonie - Provisionierungsprobleme

19449

Bei Provisionierung einzelner Telefone konnte es vorkommen, dass der Provisionierungsprozess nur ein einziges Mal funktionierte und kein Update möglich war.

4.48 Telefonie - Sprachverbindungen fehlerhaft (hybird)

ID 19002

Es konnte vorkommen, dass Sprachverbindungen nur einseitig nutzbar waren.

4.49 PBX - Registrierungsprozess verzögert

ID 19417

Unter speziellen Bedingungen konnte es bei einer Telefonanlage vorkommen, dass sich Rufnummern nur sehr verzögert registrierten.

4.50 DISA-Problem (hybird)

17964

Die Wahl über DISA funktionierte nicht mit SIP-Anschlüssen und DTMF Inband.

4.51 Netzwerk - Full Cone NAT

ID n/a

Wenn im Menü **Netzwerk**->**NAT**->**NAT-Konfiguration** ->**Neu** die Einstellung **NAT-Methode** = *full-cone* verwendet wurde, traten unter bestimmten Umständen Probleme auf und die NAT Session wurde abgebrochen.

4.52 PPP - Keine Einwahl

ID 19156

Die PPP-Einwahl über GPRS/GSM funktionierte nicht.

4.53 ISDN - Ruf abgebrochen

ID 19080

Eine kurze Deaktivierung von ISDN führte zu einem Abbruch des Rufs.

4.54 IPSec - Kein Datenverkehr

ID 19538

Es konnte vorkommen, dass über IPSec keine Daten übermittel wurden, sobald die darunterliegende PPPoE-Verbindung kurz unterbrochen war.

4.55 SIF - Alias-Probleme

19502

Unter speziellen Umständen existierte der Schnittstellen-Alias für die Schnittstelle *ANY* weder für IPv4 noch für IPv6. Der Schnittstellen-Alias für die Schnittstelle *LAN_Local* existierte für IPv4 nicht.

4.56 DNS funktionierte nicht

ID 19363

Da bei der Konfiguration des SIP-Providers der Port mit einem falschen Wert vorbelegt war, funktionierte der Dienst DNS nicht.

4.57 HTTPS - Zertifikatsauswahl fälschlicherweise möglich

ID 19511

Obwohl die Gerätefamilie **hybird 300/600** Zertifikate nicht unterstützt, konnten im Menü **Systemverwaltung**->**Zertifikate** Zertifikate konfiguriert werden und im Menü **Lokale Dienste**->**HTTPS** konnten diese Zertifikate ausgewählt werden.

4.58 DynDNS-Client - Eingabemöglichkeit fehlerhaft

ID 19464

Im Menü **Lokale Dienste**->**DynDNS-Client**->**DynDNS-Provider**->**Neu** durfte das Feld **Aktualisierungspfad** nicht leer gelassen werden, obwohl das nicht bei jeder Konfiguration sinnvoll ist.

4.59 Lokale Dienste - Scheduling fehlerhaft

ID 18745

Wenn das **Schedule-Intervall** auf *0* gesetzt wurde, wurden fälschlicherweise konfigurierte Scheduling-Aktionen ausgeführt.

4.60 Falsche Alert-Meldung

ID 18979

Eine Syslog-Meldung, die bei jeder Hotspot-Benutzer-Authentifizierung auftritt ("HACC: Got IPC-reply: ..."), wurde als Alert-Meldung angezeigt, obwohl es sich um keinen Fehlerzustand handelt.

4.61 Hotspot-Gateway - Speicherproblem

ID 19274

Bei Verwendung des Hotspot-Gateways zusammen mit RADIUS konnte es vorkommen, dass ein Speicherüberlauf auftrat.

4.62 Hotspot-Gateway - Timeout nicht abschaltbar

ID 19290

Im Menü **Lokale Dienste**->**Hotspot-Gateway**->**Hotspot-Gateway**->**Neu**->**Erweiterte Einstellungen** konnte im Feld **Standard-Timeout bei Inaktivität** der Wert *0* nicht eingegeben werden, obwohl dieser Wert zulässig ist, um die Funktion abzuschalten.

4.63 BRRP - Probleme mit Virtuellem Router

ID 19252

Bei BRRP löschten Änderungen eines Virtuellen Routers die VLAN ID der entsprechenden Advertisement-Schnittstelle.

4.64 BRRP - Panics (RXL)

ID 19399

Bei Verwendung von BRRP traten ca. 6 - 8 Reboots pro Monat auf.

4.65 Externe Berichterstellung - Benachrichtigungsdienst funktionierte nicht korrekt

ID 19291

Der **Benachrichtungsdienst** im Menü **Externe Berichterstellung** funktionierte mit dem Provider *mail.selfhost.de* nicht korrekt.

4.66 Monitoring - Keepalive Monitoring fehlerhaft

ID 19313

Keepalive Monitoring funktionierte nicht, wenn im Menü **Lokale Dienste**->**Überwachung**->**Hosts**->**Neu** die Zahl der **Erfolgreichen Versuche** größer war als die Zahl der **Fehlgeschlagenen Versuche**.

4.67 Setup Tool - Falsche Anzeige

ID 18789

Bei Verwendung eines Modems des Typs **MC7710** wurde im Setup Tool der Parameter **LTE Signal Level** = *n/a* angezeigt.

4.68 MIB-Tabelle ipsecPeerTable nicht änderbar

ID 19222

Im GUI in der Ansicht **SNMP-Browser** konnten die Einträge in der MIB-Tabelle **ipsecPeerTable** nicht geändert werden.