Benutzerhandbuch Workshops (Auszug)

Services-Workshops

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 Dienste - DHCP

1.1 Einleitung

Im Folgenden wird die Konfiguration von Dynamic Host Configuration Protocol (DHCP) beschrieben.

Sie können Ihr Gerät entweder als DHCP-Server, DHCP-Client oder als DHCP-Relay-Agent einsetzen.

Zur Konfiguration wird hierbei das **GUI** (Graphical User Interface) verwendet.

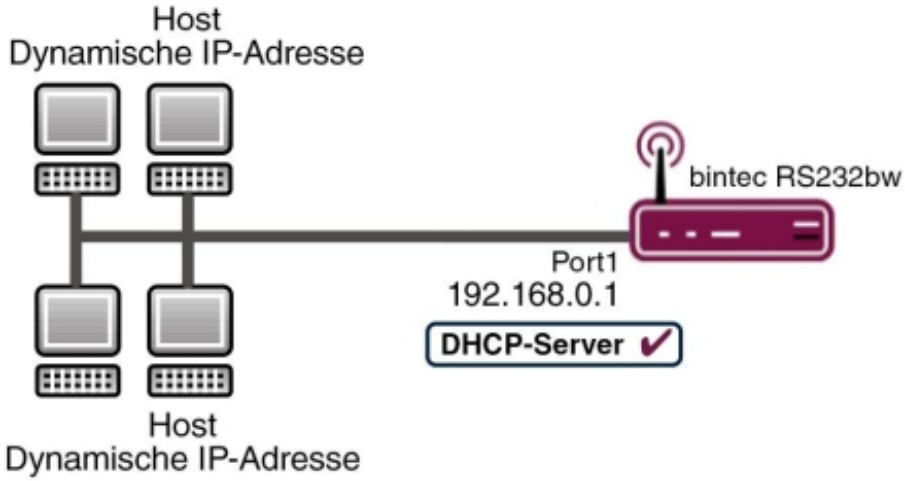


Abb. 1: Beispielszenario als DHCP-Server

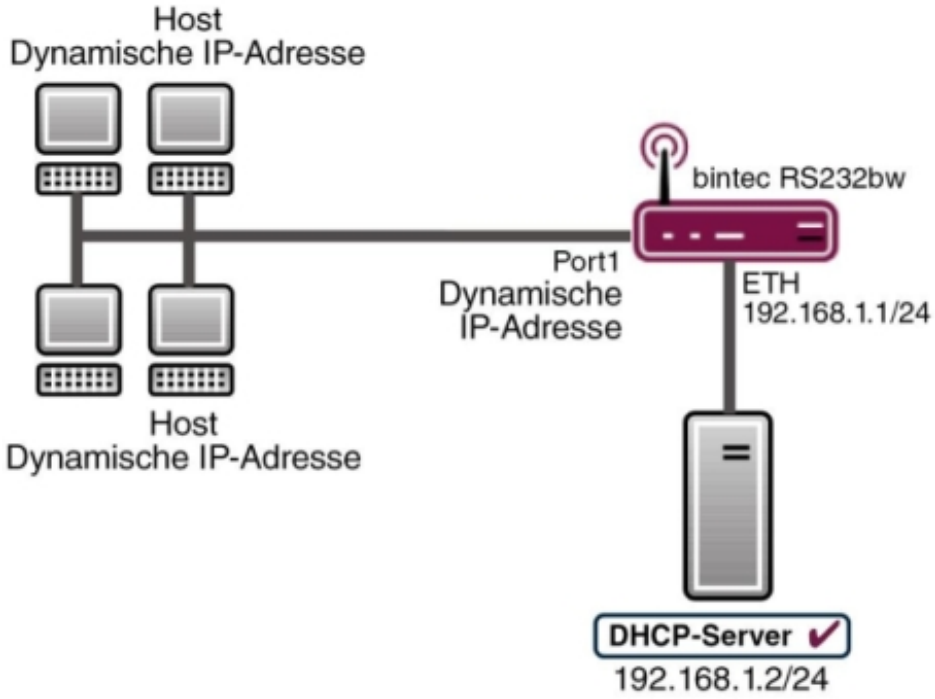


Abb. 2: Beispielszenario als DHCP-Client

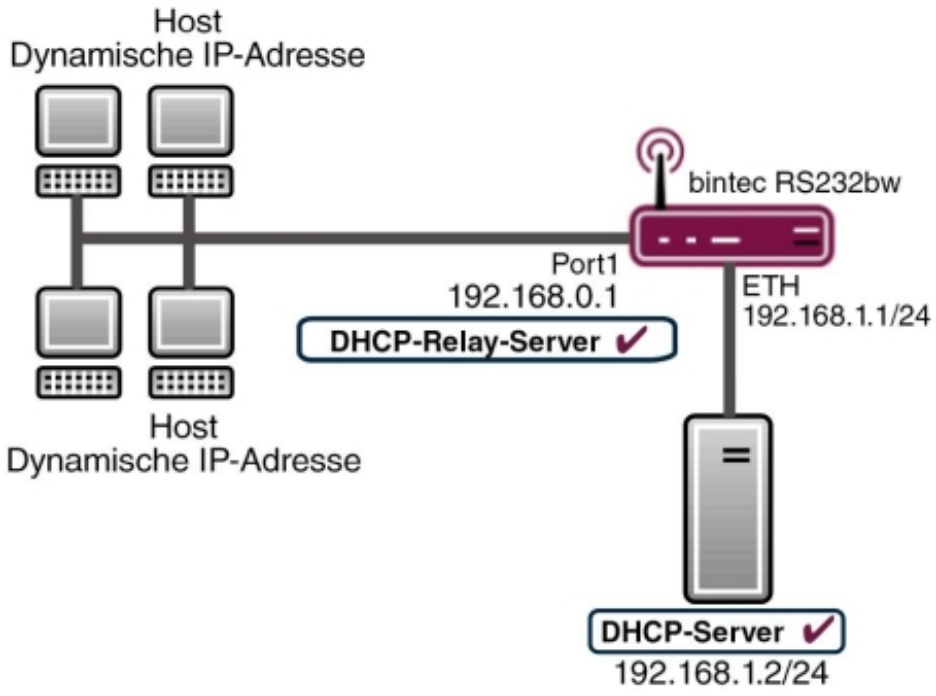


Abb. 3: Beispielszenario als DHCP-Relay-Server

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein Bootimage der Version 7.10.1
- Optional ein DHCP-Server

1.2 Konfiguration

1.2.1 Konfigurieren als DHCP-Server

Wenn Sie den Client-Computern im Netzwerk dynamisch durch Ihr Gateway eine IP-Adresse vergeben möchten, müssen Sie es als DHCP-Server konfigurieren. Um Ihr Gerät als DHCP-Server zu aktivieren, müssen Sie zunächst IP-Adress-Pools definieren, aus denen die IP-Adressen an die anfragenden Clients verteilt werden.

Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Pool** -> **Neu**.

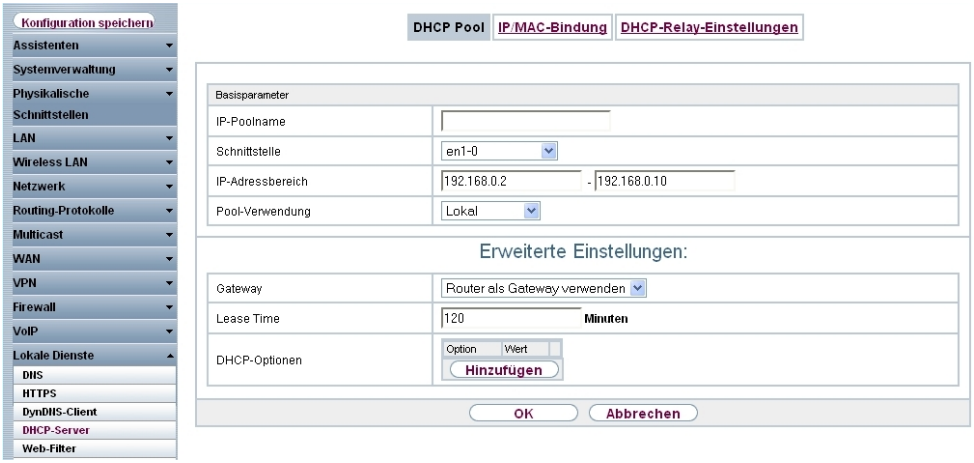


Abb. 4: **Lokale Dienste** -> **DHCP-Server** -> **DHCP Pool** -> **Neu**

Relevante Felder im Menü DHCP Pool

Feld	Bedeutung
Schnittstelle	Hier wählen Sie die Schnittstelle aus, über welche die IP-Adressen per DHCP verteilt werden sollen.
IP-Adressbereich	Geben Sie hier die erste und letzte IP-Adresse an, die per DHCP vergeben werden soll.
Pool-Verwendung	Wählen Sie aus, ob der IP-Pool für DHCP-Anfragen im gleichen Subnetz verwendet werden soll oder für DHCP-Anfragen, die aus einem anderen Subnetz zu Ihrem Gerät weitergeleitet wurden. In diesem Fall ist es möglich, IP-Adressen aus einem anderen Netz zu definieren.

Unter **Erweiterte Einstellungen** finden Sie weitere Konfigurationsparameter:

Relevante Felder im Menü Erweiterte Einstellungen

Feld	Bedeutung
Gateway	Hier legen Sie fest, ob das Gateway als Standard-Gateway verwendet werden soll, oder Sie tragen hier eine Gateway IP-Adresse ein, wenn das Gateway nicht als Standard-Gateway verwendet wird.
Lease Time	Dies ist die Zeit in Minuten, wie lange der Client die IP-Adresse behalten darf.

Gehen Sie folgendermaßen vor, um Ihr Gateway als DHCP-Server zu konfigurieren:

(1) Bei **Schnittstelle** wählen Sie Ihre LAN-Schnittstelle aus, z. B. `en1-0`.

(2) Unter **IP-Bereich** tragen Sie die erste und letzte IP-Adresse aus Ihrem LAN ein, z. B. *192.168.0.2* und *192.168.0.10*.

(3) Wählen Sie bei **Pool-Verwendung** *Lokal* aus.

(4) Bei **Gateway** wählen Sie *Router als Gateway verwenden*aus.

(5) Die **Lease Time** belassen Sie auf *120*.

(6) Bestätigen Sie mit **OK**.

Im **GUI** haben Sie die Möglichkeit zu überprüfen, ob und welche IP-Adressen an Clients aus dem DHCP-Pool vergeben sind. Um zu kontrollieren, wer eine IP-Adresse erhalten hat, gehen Sie in folgendes Menü:

(1) Gehen Sie zu **Lokale Dienste** -> **DHCP-Server** -> **IP/MAC-Bindung**.

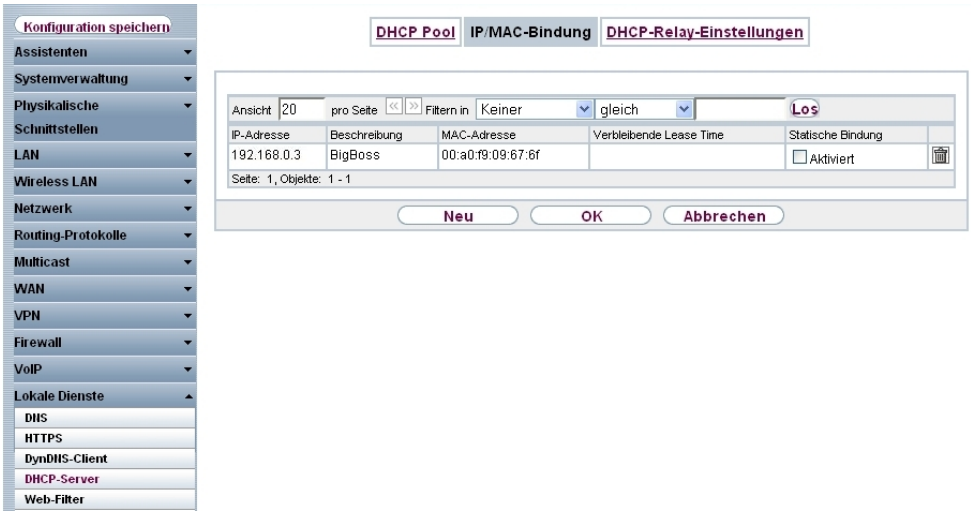


Abb. 5: **Lokale Dienste** -> **DHCP-Server** -> **IP/MAC-Bindung**

Hier erhalten Sie alle wichtigen Angaben, die die Vergabe von IP-Adressen aus dem DHCP-Pool betreffen.

Das Gateway vergibt als DHCP-Server eine IP-Adresse an den Client und übermittelt ihm ebenfalls die IP-Adresse des Gateways, aber auch die IP-Adresse des DNS-Servers.

Bestimmen Sie mit folgendem Menüpunkt, welche IP-Adresse das Gateway dem Client als DNS-Server-Adresse übermittelt:

(1) Gehen Sie zu **Lokale Dienste** -> **DNS** -> **Globale Einstellungen** -> **Erweiterte Einstellungen**.

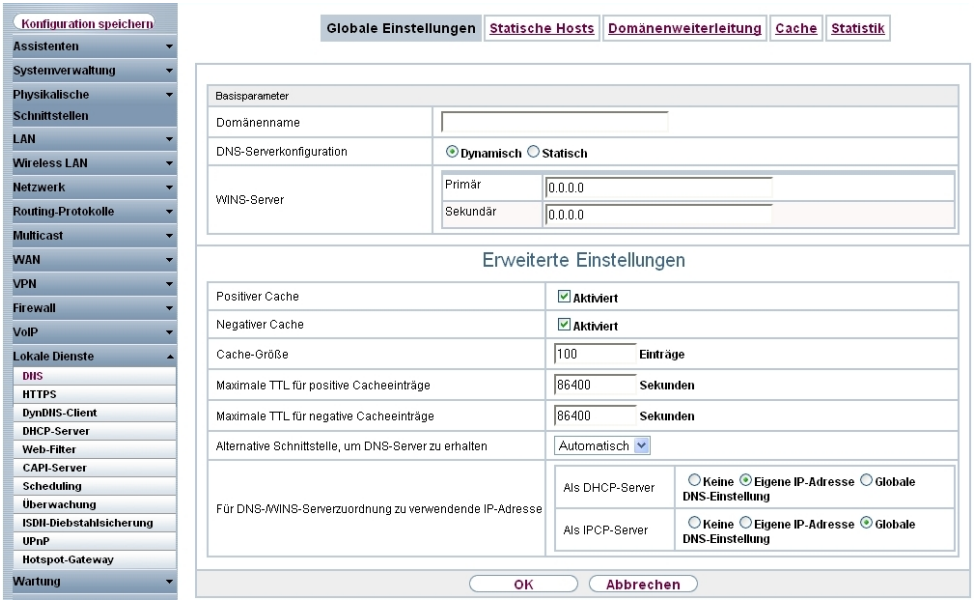


Abb. 6: **Lokale Dienste** -> **DNS** -> **Globale Einstellungen** -> **Erweiterte Einstellungen**

Relevantes Feld im Menü Erweiterte Einstellungen

Auswahl	Bedeutung
Für DNS-/WINS-Serverzuordnung zu verwendende IP-Adresse: Als DHCP-Server	Wählen Sie aus folgenden Optionen die für Ihre Netzwerkumgebung geeigneste Methode aus: • *Keiner*: Bei dieser Einstellung vergibt das Gateway keine DNS-Server-IP-Adressen. • *Eigene IP-Adresse*: Das Gateway weist seine eigene IP-Adresse als DNS zu. • *Globale DNS-Einstellung*: Das Gateway vergibt die IP-Adressen als DNS, die Sie im Menü **Lokale Dienste** -> **DNS** -> **Globale Einstellungen** konfiguriert oder dynamisch bezogen haben.

Im Standardfall können Sie für **Als DHCP-Server** die Einstellung *Eigene IP-Adresse* beibehalten.

1.2.2 Konfiguration als DHCP-Client

Das Gateway hat die Möglichkeit, selber dynamisch von einem DHCP-Server eine IP-Adresse auf einer Ethernet-Schnittstelle zu beziehen.

Gehen Sie in folgendes Menü, um an Ihrer Ethernet-Schnittstelle den DHCP-Client-Modus zu konfigurieren:

(1) Gehen Sie zu **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-4>** -> .

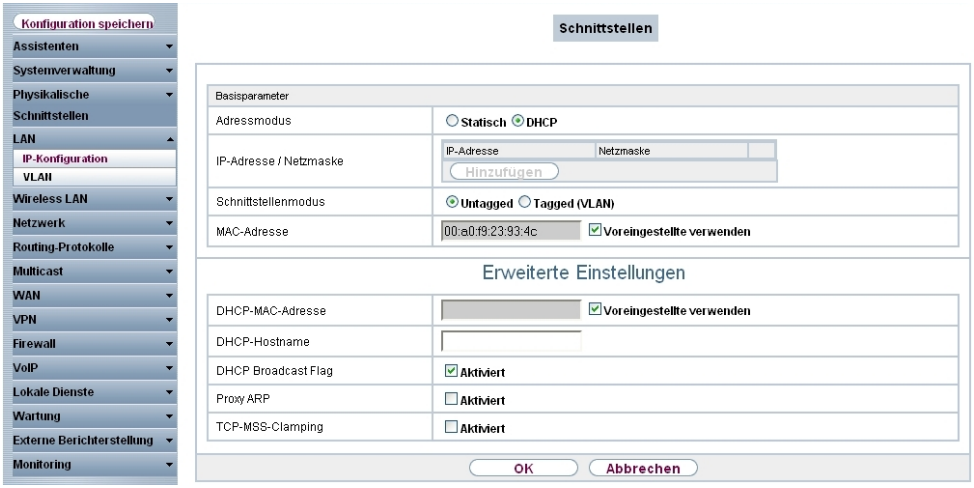


Abb. 7: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-4>** ->

Relevante Felder im Menü Schnittstellen

Feld	Bedeutung
Adressmodus	Wählen Sie DHCP aus, um als Client eine IP-Adresse über die Schnittstelle zu beziehen.

Unter **Erweiterte Einstellungen** finden Sie weitere Konfigurationsparameter.

Relevante Felder im Menü Erweiterte Einstellungen

Feld	Bedeutung
DHCP-MAC-Adresse	Wenn Sie von einem bestimmten DHCP-Server eine IP-Adresse erwarten, können Sie seine MAC-Adresse hier eintragen.

Gehen Sie folgendermaßen vor, um das Gateway als DHCP-Client zu konfigurieren:

(1) Wählen Sie bei **Adressmodus** *DHCP* aus.

(2) Bestätigen Sie mit **OK**.

Jetzt sollten Sie von Ihrem DHCP-Server alle wichtigen Konfigurationsparameter wie IP-Adresse, Gateway, und DNS übermittelt bekommen.

1.2.3 Konfiguration eines DHCP-Relay-Servers

Wenn das Gateway für das lokale Netz keine IP-Adressen per DHCP an die Clients verteilt, kann es dennoch die DHCP-Anforderungen aus dem lokalen Netzwerk stellvertretend an einen entfernten DHCP-Server weiterleiten.

Der DHCP-Server vergibt dem Gateway dann eine IP-Adresse aus seinem Pool, die dieser wiederum an den Client ins lokale Netzwerk schickt. Die Einstellungen für einen DHCP-Relay-Server können Sie in folgendem Untermenü vornehmen:

(1) Gehen Sie zu **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Relay-Einstellungen**.

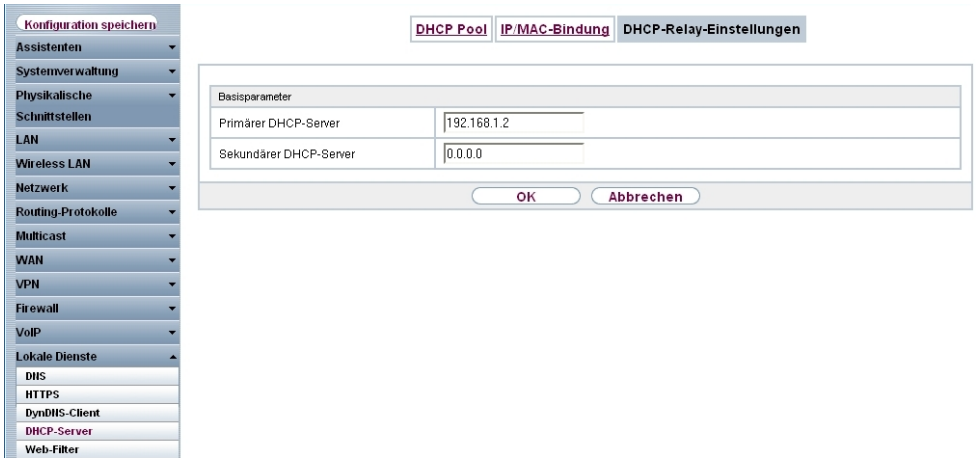


Abb. 8: **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Relay-Einstellungen**

Relevante Felder im Menü DHCP-Relay-Einstellungen

Feld	Bedeutung
Primärer DHCP-Server	Tragen Sie hier die IP-Adresse des ersten Servers ein.
Sekundärer DHCP-Server	Tragen Sie hier, falls vorhanden, die IP-Adresse des zweiten Servers ein.

Gehen Sie folgendermaßen vor, um das Gateway als DHCP-Relay-Agent zu konfigurieren:

(1) Geben Sie bei **Primärer DHCP-Server** die IP-Adresse des Servers an, z. B. `192.168.1.2`.

(2) Bestätigen Sie mit **OK**.

1.3 Konfigurationsschritte im Überblick

DHCP-Server

Feld	Menü	Wert
Schnittstelle	**Lokale Dienste** -> **DHCP-Server** -> **DHCP Pool** -> **Neu**	z. B. *en1-0*
IP-Adressbereich	**Lokale Dienste** -> **DHCP-Server** -> **DHCP Pool** -> **Neu**	z. B. *192.168.0.2* und *192.168.0.10*
Pool-Verwendung	**Lokale Dienste** -> **DHCP-Server** -> **DHCP Pool** -> **Neu**	*Lokal*
Gateway	**Lokale Dienste** -> **DHCP-Server** -> **DHCP Pool** -> **Neu** -> **Erweiterte Einstellungen**	*Router als Gateway verwenden*
Lease Time	**Lokale Dienste** -> **DHCP-Server** -> **DHCP Pool** -> **Neu** -> **Erweiterte Einstellungen**	z. B. *120*
Für DNS-/WINS-Serverzuordnung zu verwendende IP-Adresse: Als DHCP-Server	**Lokale Dienste** -> **DNS** -> **Globale Einstellungen** -> **Erweiterte Einstellungen**	z. B. *Eigene IP-Adresse*

DHCP-Client

Feld	Menü	Wert
Adressmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-4>** ->	*DHCP*
DHCP-MAC-Adresse (optional)	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-4>** -> -> **Erweiterte Einstellungen**	MAC-Adresse eines bestimmten DHCP-Servers

DHCP-Relay-Server

Feld	Menü	Wert
Primärer DHCP-Server	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Relay-Einstellungen**	z. B. *192.168.1.2*
Sekundärer DHCP-Server (optional)	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Relay-Einstellungen**	falls vorhanden

Kapitel 2 Dienste - DynDNS

2.1 Einleitung

Im Folgenden wird die Konfiguration von DynDNS beschrieben.

Sie erstellen einen Eintrag für den DynDNS-Provider `no-IP` und konfigurieren Ihren DynDNS-Namen `bintec.no-ip.com`. Anschliessend erstellen Sie NAT-Freigaben, um über das Internet per http das Gateway zu administrieren.

Zur Konfiguration wird hierbei das **GUI** (Graphical User Interface) verwendet.

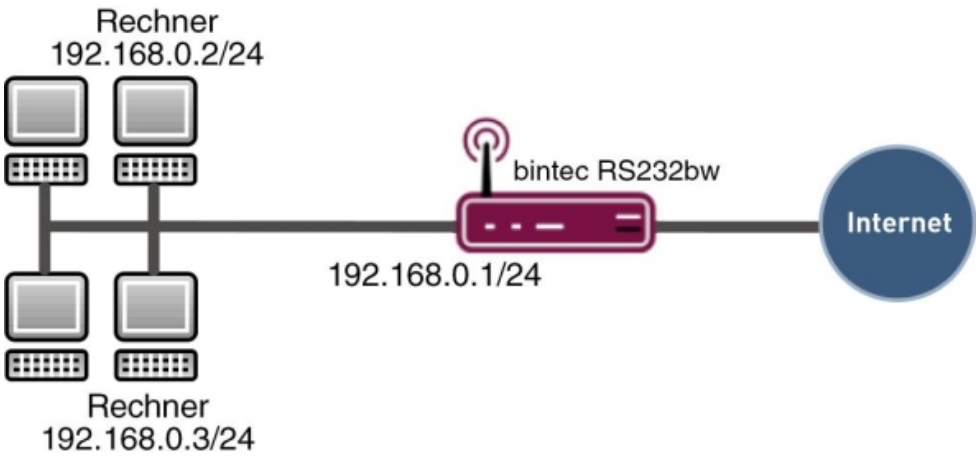


Abb. 9: Beispielszenario DynDNS

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Grundkonfiguration des Gateways
- Ein Bootimage der Version 7.10.1
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang
- Eine erfolgreiche Registrierung beim DynDNS-Provider *www.no-ip.com*

2.2 Konfiguration

Um DynDNS zu konfigurieren, muss ausschließlich folgendes Menü konfiguriert werden:

(1) Gehen Sie zu **Lokale Dienste** -> **DynDNS-Client**.

2.2.1 Neuer Provider

Wenn Sie einen DynDNS-Provider nutzen möchten, der noch nicht in der Liste im Menü **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Provider** aufgeführt ist, müssen Sie diesen über folgendes Menü hinzufügen:

(1) Gehen Sie zu **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Provider** -> **Neu**.

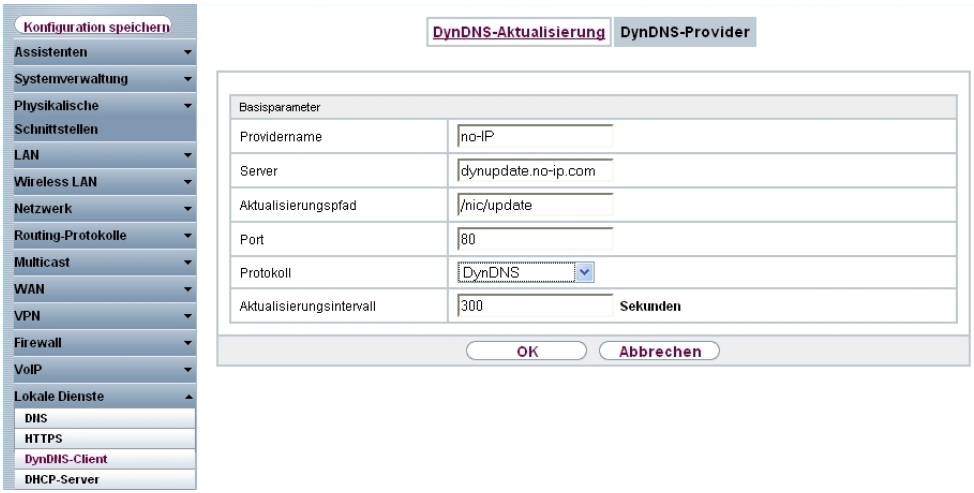


Abb. 10: **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Provider** -> **Neu**

Relevante Felder im Menü DynDNS-Provider

Feld	Bedeutung
Providername	Geben Sie dem Provider einen Namen.
Server	Tragen Sie hier die IP-Adresse oder den Domänennamen des Aktualisierungsservers ein.
Aktualisierungspfad	Hier steht der Pfad zu dem Registrierungsskript.
Port	Geben Sie den Port an, über den der Server die Aktualisierung empfängt.
Protokoll	Das Protokoll, mit dem der DynDNS Provider arbeitet.

Gehen Sie folgendermaßen vor:

(1) Tragen Sie bei **Providername** z. B. *no-IP* ein.

(2) Geben Sie bei **Server** *dynupdate.no-ip.com* an.

(3) Unter **Aktualisierungspfad** tragen Sie */nic/update* ein.

(4) Den **Port** lassen Sie auf *80*.

(5) Bei **Protokoll** wählen Sie *DynDNS* aus.

(6) Bestätigen Sie mit **OK**.

2.2.2 DynDNS konfigurieren

Erstellen Sie im Gateway einen Eintrag für Ihren registrierten DynDNS-Namen. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**.

Abb. 11: **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**

Relevante Felder im Menü DynDNS-Aktualisierung

Feld	Bedeutung
Hostname	Tragen Sie hier den kompletten Hostnamen ein, den Sie registriert haben.
Schnittstelle	Wählen Sie die Internetschnittstelle aus.
Benutzername	Geben Sie Ihren Benutzernamen an.
Passwort	Geben Sie Ihr Passwort an.

Feld	Bedeutung
Provider	Hier wählen Sie Ihren DynDNS Provider aus.
Aktualisierung aktivieren	Aktivieren oder deaktivieren Sie den Eintrag.

Gehen Sie folgendermaßen vor:

(1) Unter **Hostname** tragen Sie z. B. *bintec.no-ip.com* ein.

(2) Wählen Sie bei **Schnittstelle** z. B. *Internet* aus.

(3) Tragen Sie unter **Benutzername** z. B. *name@email.de* ein.

(4) Bei **Passwort** geben Sie z. B. *geheim* an.

(5) Der **Provider** ist *no-IP*.

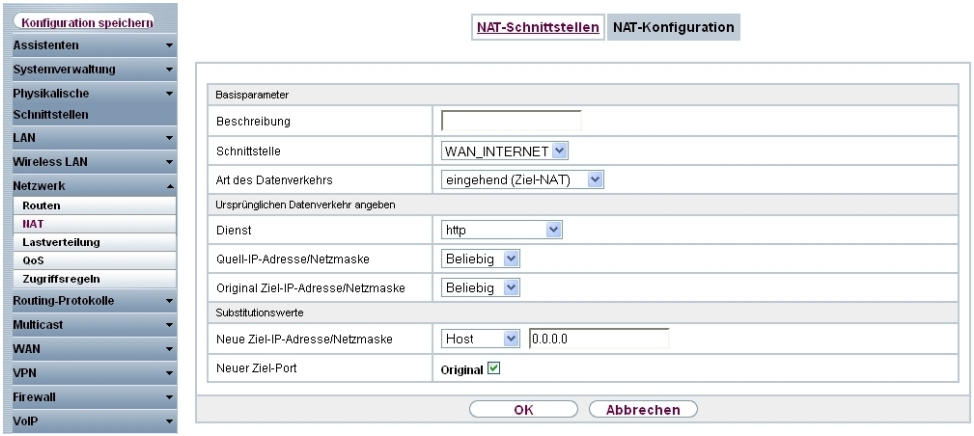
(6) Aktivieren Sie **Aktualisierung aktivieren**.

(7) Bestätigen Sie mit **OK**.

2.2.3 NAT-Einträge für die Administration mit dem GUI

Ihr Gateway soll über das Internet per HTTP administrierbar sein. Für die Konfiguration der entsprechenden NAT-Freigabe, gehen Sie bitte in folgendes Menü:

(1) Gehen Sie zu **Netzwerk** -> **NAT** -> **NAT-Konfiguration** -> **Neu**.



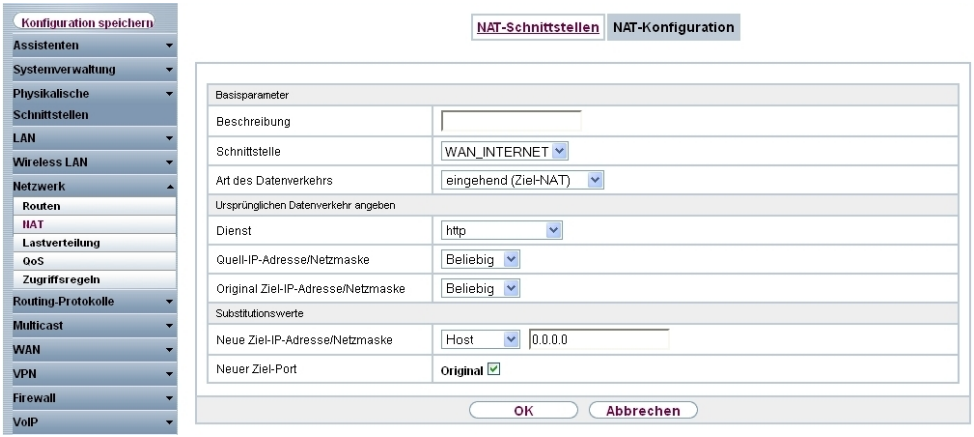


Abb. 12: **Netzwerk** -> **NAT** -> **NAT-Konfiguration** -> **Neu**

Relevante Felder im Menü NAT-Konfiguration

Feld	Bedeutung
Schnittstelle	Das ist die Verbindung, die die NAT Freigabe erhalten soll.
Dienst	Dies ist der Dienst, den Sie von extern am Gateway ansprechen.
Quell-IP-Adresse/Netzmaske	Hier tragen Sie die externe IP-Adresse des Gateways ein.
Neuer Ziel-Port	Das ist die IP-Adresse, auf die Sie umgeleitet werden möchten, wenn Sie das Gateway ansprechen.

Gehen Sie folgendermaßen vor, um die NAT-Freigabe zu konfigurieren:

(1) Die **Schnittstelle** stellen Sie auf z. B. *WAN_INTERNET*.

(2) Den **Dienst** stellen Sie auf *http*.

(3) Bei **Quell-IP-Adresse/Netzmaske** setzen Sie auf *Beliebig*.

(4) Belassen Sie die restlichen Einstellungen und bestätigen Sie Ihre Angaben mit **OK**.

2.3 Ergebnis

Sie haben den DynDNS-Provider *no-IP* und Ihren dort registrierten DynDNS-Namen in das Gateway eingetragen. Außerdem ist das bintec Gateway jetzt über das Internet administrierbar.

2.4 Kontrolle

Um zu überprüfen, ob die aktuelle IP-Adresse erfolgreich bei dem DynDNS-Provider registriert ist, gehen Sie in folgendes Menü:

(1) Gehen Sie zu **Lokale Dienste** -> **DynDNS-Client**.

Hier muss das Feld **Status** den Wert *up-to-date* haben.

Wenn Sie das bintec Gateway über das Internet administrieren möchten, geben Sie auf einem entfernten Computer im Browser Folgendes ein:

```
z. B. bintec.no-ip.com
```

Danach sollten Sie den Login des **GUI** des bintec Gateways erhalten.

2.5 Konfigurationsschritte im Überblick

Neuen Provider anlegen

Feld	Menü	Wert
Providername	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Provider** -> **Neu**	z. B. *no-IP*
Server	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Provider** -> **Neu**	*dynupdate.no-ip.com*
Aktualisierunspfad	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Provider** -> **Neu**	*/nic/update*
Port	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Provider** -> **Neu**	*80*
Protokoll	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Provider** -> **Neu**	*DynDNS*

DynDNS konfigurieren

Feld	Menü	Wert
Hostname	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	z. B. *bintec.no-ip.com*
Schnittstelle	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	z. B. *Internet*
Benutzername	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	z. B. *name@email.de*
Passwort	**Lokale Dienste** -> **DynDNS-Client** ->	z. B. *geheim*

Feld	Menü	Wert
	DynDNS-Aktualisierung -> **Neu**	
Provider	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	*no-IP*
Aktualisierung aktivieren	**Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** -> **Neu**	*Aktiviert*

NAT-Einträge

Feld	Menü	Wert
Schnittstelle	**Netzwerk** -> **NAT** -> **NAT-Konfiguration** -> **Neu**	z. B. *WAN_INTERNET*
Dienst	**Netzwerk** -> **NAT** -> **NAT-Konfiguration** -> **Neu**	*http*
Quell-IP-Adresse/Netzmaske	**Netzwerk** -> **NAT** -> **NAT-Konfiguration** -> **Neu**	*Beliebig*

Kapitel 3 Dienste - Zeitgesteuerte Aufgaben

3.1 Einleitung

Im Folgenden wird die Konfiguration von zeitgesteuerten Aufgaben beschrieben.

- Sie möchten ihr Gateway täglich in der Nacht rebooten.
- Am Wochenende soll die WLAN-Schnittstelle abgeschaltet werden.
- Zudem soll einmal im Monat die Konfiguration automatisiert auf einen TFTP-Server gesichert werden.

Zur Konfiguration wird hierbei das **GUI** (Graphical User Interface) verwendet.

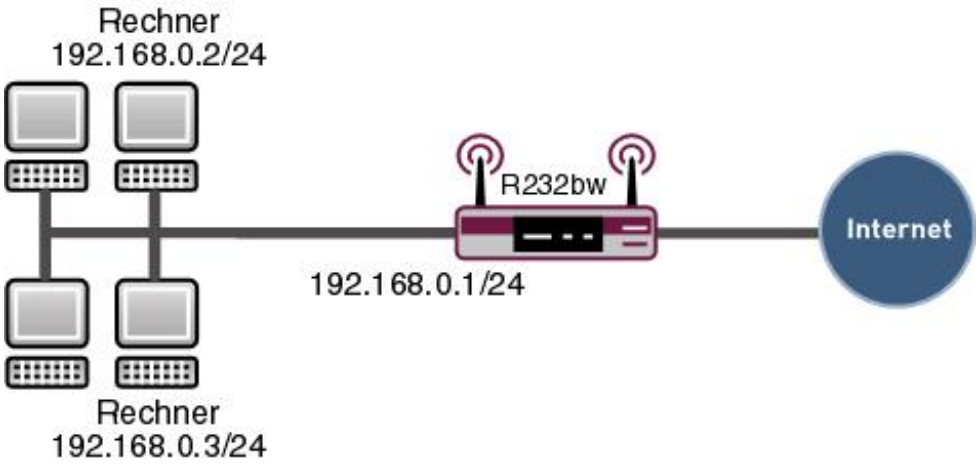


Abb. 13: Beispielszenario Zeitgesteuerte Aufgaben

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Grundkonfiguration des Gateways.
- Ein Bootimage der Version 7.8.2

3.2 Konfiguration

Um zeitgesteuerte Aufgaben zu konfigurieren, muss ausschließlich folgendes Menü konfiguriert werden:

(1) Gehen Sie zu **Lokale Dienste** -> **Scheduling** -> **Zeitplan**.

3.2.1 Täglicher Reboot

Um das Gateway so zu konfigurieren, dass es zu einer bestimmten Zeit eine bestimmte Aktion ausführt, gehen Sie bitte in folgendes Menü:

(1) Gehen Sie zu **Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**.

Abb. 14: **Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**

Relevante Felder im Menü Zeitplan

Feld	Bedeutung
Beschreibung	Geben Sie dem Eintrag einen Namen.
Aktion auswählen	Wählen Sie die Aktion aus, die das Gateway ausführen soll.
Bedingungstyp	Bestimmen Sie den zeitlichen Rhytmus, in dem die Aktion ausgeführt werden soll.
Bedingungseinstellungen	Bestimmen Sie den Tag, an dem die Aktion ausgeführt werden soll.
Startzeit	Geben Sie den Zeitpunkt an, zu dem die Aktion ausgeführt werden soll.

Gehen Sie folgendermaßen vor:

(1) Tragen Sie bei **Beschreibung** z. B. *Neustart* ein.

(2) Wählen Sie bei **Aktion auswählen** *Gerät neu starten* aus.

(3) Unter **Bedingungstyp** markieren Sie *Perioden*.

(4) Im Feld **Bedingungseinstellungen** wählen Sie *Täglich*.

(5) Bei **Startzeit** tragen Sie die Zeit ein: **Stunde** *00* **Minute** *00*.

(6) Bestätigen Sie mit **OK**.

Hinweis

Das Gateway überprüft die konfigurierten Ereignisse nur alle 300 Sekunden. Um die Zeit z. B. auf jede Sekunde zu reduzieren, gehen Sie in das Menü **Lokale Dienste** -> **Scheduling** -> **Optionen** und geben Sie für **Schedule-Intervall** z. B. *5* ein. Bedenken Sie bitte, dass eine sekundengenaue Überprüfung das Gateway auslasten kann.

Abb. 15: **Lokale Dienste** -> **Scheduling** -> **Optionen**

3.2.2 WLAN-Schnittstelle abschalten

Erzeugen Sie einen weiteren Eintrag, um die WLAN-Schnittstelle am Samstag und Sonntag zu deaktivieren.

Gehen Sie dazu bitte in folgendes Menü:

(1) Gehen Sie zu **Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**.

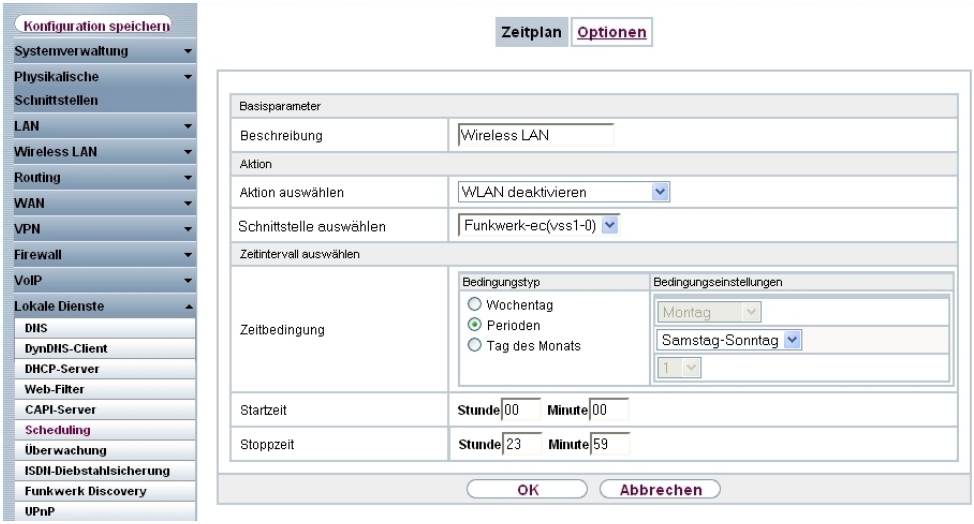


Abb. 16: **Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**

Relevante Felder im Menü Zeitplan

Feld	Bedeutung
Beschreibung	Geben Sie dem Eintrag einen Namen.
Aktion auswählen	Wählen Sie die Aktion aus, die das Gateway ausführen soll.
Schnittstelle auswählen	Markieren Sie die Schnittstelle, welche Sie ein- oder abschalten möchten.
Bedingungstyp	Bestimmen Sie den zeitlichen Rhytmus, in dem die Aktion ausgeführt werden soll.
Bedingungseinstellungen	Bestimmen Sie den Tag, an dem die Aktion ausgeführt werden soll.
Startzeit	Geben Sie den Zeitpunkt an, zu dem die Aktion ausgeführt werden soll.
Stoppzeit	Geben Sie den Zeitpunkt an, zu dem die Aktion beendet werden soll.

Gehen Sie folgendermaßen vor:

(1) Tragen Sie bei **Beschreibung** z. B. *Wireless LAN* ein.

(2) Wählen Sie bei **Aktion auswählen** *WLAN deaktivieren* aus.

(3) Markieren Sie bei **Schnittstelle auswählen** z. B. *Funkwerk-ec(vss1-0)*.

(4) Unter **Bedingungstyp** markieren Sie *Perioden*.

(5) Im Feld **Bedingungseinstellungen** wählen Sie *Samstag Sonntag*.

(6) Bei **Startzeit** tragen Sie die Zeit ein: **Stunde** *00* **Minute** *00*.

(7) Bei **Stoppzeit** tragen Sie folgendes ein: **Stunde** *23* **Minute** *59*.

(8) Bestätigen Sie mit **OK**.

3.2.3 Konfiguration monatlich sichern

Sie möchten ihre Konfiguration am ersten Tag des Monats auf einen TFTP-Server sichern.

Gehen Sie dazu bitte in folgendes Menü:

(1) Gehen Sie zu **Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**.

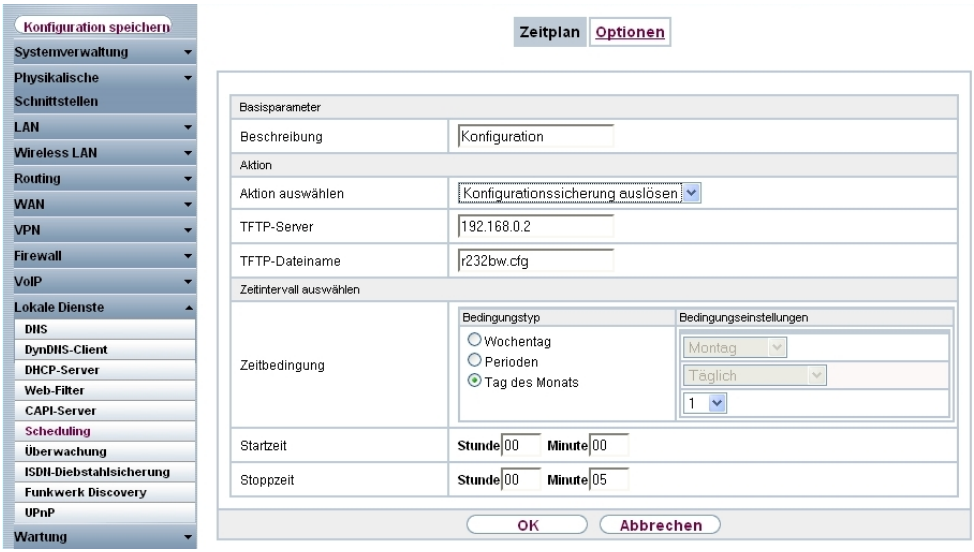


Abb. 17: **Lokale Dienste** -> **Scheduling** -> **Zeitplan**-> **Neu**

Relevante Felder im Menü Zeitplan

Feld	Bedeutung
Beschreibung	Geben Sie dem Eintrag einen Namen.
Aktion auswählen	Wählen Sie die Aktion aus, die das Gateway ausführen soll.
TFTP-Server	Tragen Sie hier die IP-Adresse des TFTP Servers ein.
TFTP-Dateiname	Geben Sie den Namen der Konfiguration auf dem Server an.
Bedingungstyp	Bestimmen Sie den zeitlichen Rhytmus, in dem die Aktion ausgeführt werden soll.
Bedingungseinstellungen	Bestimmen Sie den Tag, an dem die Aktion ausgeführt werden soll.

Feld	Bedeutung
Startzeit	Geben Sie den Zeitpunkt an, zu dem die Aktion ausgeführt werden soll.
Stoppzeit	Geben Sie den Zeitpunkt an, zu dem die Aktion beendet werden soll.

Gehen Sie folgendermaßen vor:

(1) Tragen Sie bei **Beschreibung** z. B. *Konfiguration* ein.

(2) Wählen Sie bei **Aktion auswählen** *Konfigurationssicherung auslösen* aus.

(3) Geben Sie bei **TFTP-Server** die IP-Adresse an, z. B. *192.168.0.2*.

(4) Tragen Sie bei **TFTP-Dateiname** einen Namen ein, z. B. *r232bw.cfg*.

(5) Unter **Bedingungstyp** markieren Sie *Tag des Monats*.

(6) Im Feld **Bedingungseinstellungen** wählen Sie *1*.

(7) Bei **Startzeit** tragen Sie die Zeit ein: **Stunde** *00* **Minute** *00*.

(8) Bei **Stoppzeit** tragen Sie die Zeit ein: **Stunde** *00* **Minute** *05*.

(9) Bestätigen Sie mit **OK**.

Hinweis

Für die monatliche Sicherung Ihrer Konfiguration muss ein TFTP-Server entsprechend konfiguriert vorhanden sein.

TFTP-Server überprüfen

Der TFTP- Server dient dazu, Dateien zwischen Gateway und Computer, z. B. für das Konfigurationsmanagement, zu übertragen. Vergewissern Sie sich, dass der TFTP-Server ordnungsgemäß in Betrieb ist, indem Sie die **DIME Tools** öffnen (enthalten in der **BRICKware**, die Sie von der bintec **Companion CD** installieren können). Um den TFTP-Server zu starten, drücken Sie in den **DIME Tools** die Tastenkombination **STRG + T**.

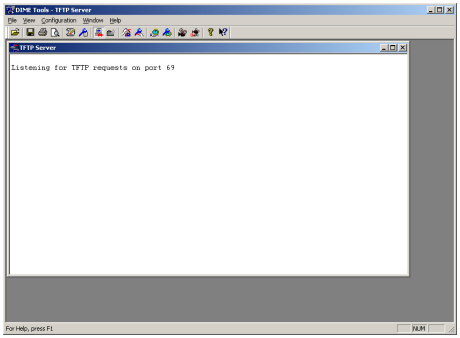


Abb. 18: DIME Tools - TFTP Server

Um dem TFTP-Server ein Verzeichnis zuzuweisen, wo z. B. Dateien gespeichert werden, können Sie unter **Configuration** -> **TFTP-Server** den gewünschten Pfad angeben.

3.3 Konfigurationsschritte im Überblick

Täglicher Reboot

Feld	Menü	Wert
Beschreibung	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	z. B. *Neustart*
Aktion auswählen	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	*Gerät neu starten*
Bedingungstyp	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	*Perioden*
Bedingungseinstellungen	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	*Täglich*
Startzeit	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	Stunde *00* Minute *00*
Schedule-Intervall	**Lokale Dienste** -> **Scheduling** -> **Optionen**	*5* sec

WLAN-Schnittstelle abschalten

Feld	Menü	Wert
Beschreibung	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	z. B. *Wireless LAN*
Aktion auswählen	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	*WLAN deaktivieren*
Schnittstelle auswählen	**Lokale Dienste** -> **Scheduling** ->	*Funkwerk-ec*

Feld	Menü	Wert
	Zeitplan -> **Neu**	*(vss1-0)*
Bedingungstyp	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	*Perioden*
Bedingungseinstellungen	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	*Samstag Sonntag*
Startzeit	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	Stunde *00* Minute *00*
Stoppzeit	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	Stunde *23* Minute *59*

Konfiguration monatlich sichern

Feld	Menü	Wert
Beschreibung	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	z. B. *Konfiguration*
Aktion auswählen	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	*Konfigurationssicherung auslösen*
TFTP-Server	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	z. B. *192.168.0.2*
TFTP-Dateiname	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	z. B. *r232bw.cfg*
Bedingungstyp	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	*Tag des Monats*
Bedingungseinstellungen	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	z. B. *1*
Startzeit	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	Stunde *00* Minute *00*
Stoppzeit	**Lokale Dienste** -> **Scheduling** -> **Zeitplan** -> **Neu**	Stunde *00* Minute *05*

Kapitel 4 Dienste - Priorisierung einer VPN IPSec-Verbindung vor weiterem Internet-Datenverkehr

4.1 Einleitung

In der Zentrale eines Unternehmens befindet sich ein **bintec R3002** Gateway. Dieses Gateway ist über einen Internetzugang mit fester WAN IP-Addresse mit dem Internet verbunden. Der Internetzugang wird für die VPN IPSec-Anbindung einer Firmenfiliale und für weitere Internetdienste genutzt. Falls die komplette Bandbreite der Internetanbindung genutzt wird, soll die Filialanbindung über höhere Priorität als der übrige Internet-Datenverkehr verfügen und somit weiterhin nutzbar sein.

In diesem Workshop wird am Beispiel eines **bintec R3002** (Gateway der Zentrale) und eines **bintec RS120** (Gateway der Filiale) die Einrichtung der Internetanbindung und die Konfiguration der VPN IPSec-Verbindung gezeigt. Anschließend wird für das Gateway der Firmenzentrale die Prorisierung der VPN IPSec-Verbindung festgelegt.

Zur Konfiguration wird hierbei das **GUI** (Graphical User Interface) verwendet.

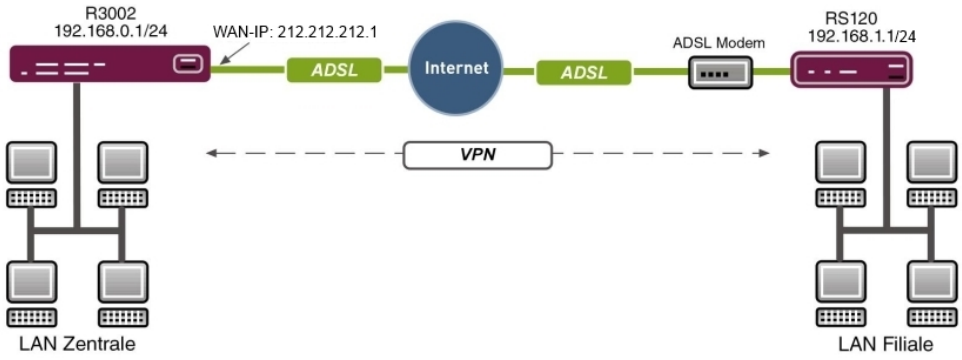


Abb. 19: Beispielszenario

Voraussetzungen

- Ein **bintec R3002** Gateway (Zentrale)
- Ein **bintec RS120** Gateway (Filiale)
- Ein Bootimage der Version 7.9.5

- Beide Gateways benötigen eine unabhängige Verbindung zum Internet
- Internetzugang der Zentrale mit der statischen WAN IP-Adresse
- **Dime Manager**-Software

4.2 Konfiguration

4.2.1 Konfiguration des Gateways in der Zentrale (bintec R3002)

Zur initialen Konfiguration kann das **bintec R3002** Gateway über den **Dime Manager** erreicht werden. Die LAN IP-Adresse des Gateways wird über das Kontextmenü geändert. Nachdem Sie die IP-Adresse geändert haben, ist die Web-Schnittstelle des **bintec R3002** erreichbar.

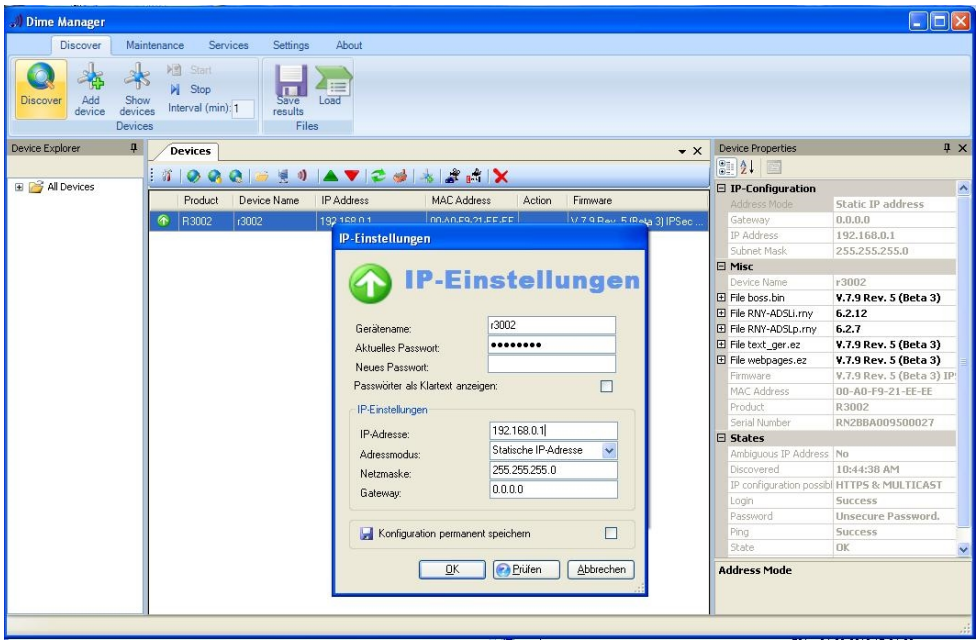


Abb. 20: Dime Manager

4.2.2 Konfiguration des Internetzugangs über den GUI Assistenten

Zur Konfiguration einer Internetverbindung verfügt das **GUI** über einen Assistenten.

Über den Assistenten kann die Internetverbindung des Gateways in wenigen Schritten eingerichtet werden. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Neu**.

(2) Wählen Sie bei **Verbindungstyp** z. B. `Internes ADSL-Modem` aus.

(3) Klicken Sie auf **Weiter** um eine neue Internetverbindung zu konfigurieren.

Geben Sie die erforderlichen Daten für die Verbindung ein.

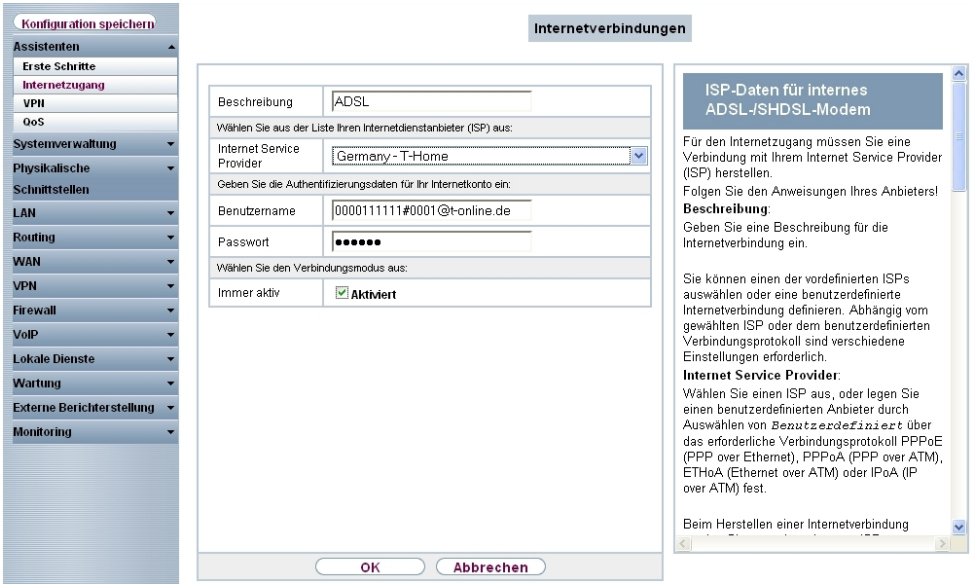


Abb. 21: **Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Weiter**

Gehen Sie folgendermaßen vor, um eine neue Internetverbindung zu konfigurieren:

(1) Bei **Beschreibung** tragen Sie z. B. `ADSL` ein.

(2) Als **Internet Service Provider** wählen Sie z. B. `Germany-T-Home` aus.

(3) Als **Benutzername** geben Sie die Zugangsdaten ein, die Sie von Ihrem Provider erhalten haben.

(4) Geben Sie das **Passwort** ein, dass Sie von Ihrem Provider erhalten haben.

(5) Damit die statische WAN IP-Adresse des VPN-Gateways der Zentrale dauerhaft für die Filial-Gateways erreichar ist muss die Option **Immer aktiv** gesetzt werden.

(6) Bestätigen Sie Ihre Angaben mit **OK**.

4.2.3 Konfiguration des VPN IPSec-Zugangs der ersten Filiale per GUI Assistenten

Wie bei der Einrichtung des Internetzugangs kann auch die VPN IPSec-Einrichtung mit dem Assistenten konfiguriert werden. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Neu**.

(2) Wählen Sie bei **VPN-Szenario** die *IPSec-LAN-zu-LAN-Verbindung* aus.

(3) Klicken Sie auf **Weiter** um eine neue VPN-Verbindung einzurichten.

Geben Sie die erforderlichen Daten für die Verbindung ein.

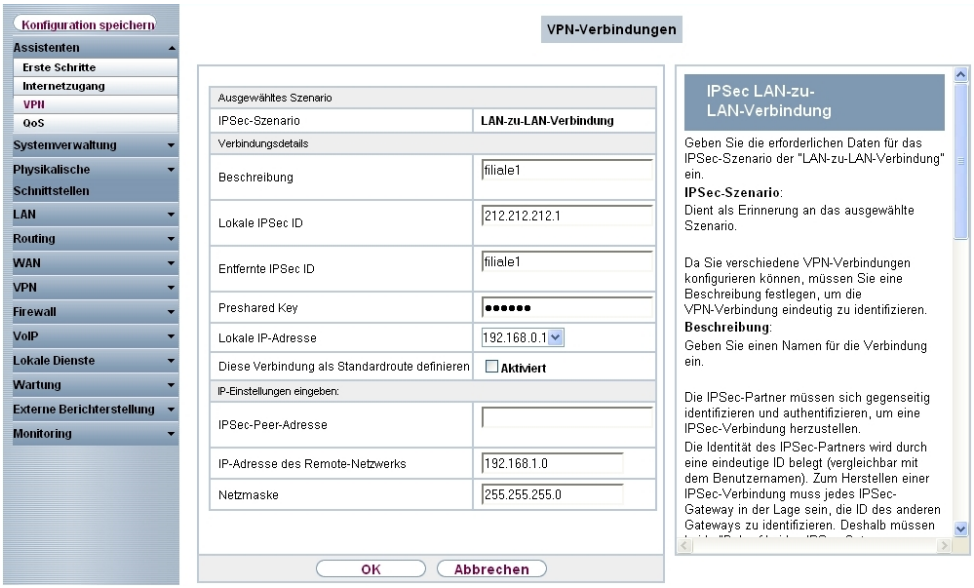


Abb. 22: **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Weiter**

Gehen Sie folgendermaßen vor, um eine neue VPN-Verbindung zu konfigurieren:

(1) Bei **Beschreibung** tragen Sie z. B. *filiale1* ein.

(2) Unter **Lokale IPSec ID** tragen Sie die statische WAN IP-Adresse des Zentral-Gateways ein, z. B. *212.212.212.1*.

(3) Unter **Entfernte IPSec ID** tragen Sie die lokale IPSec ID des Filial-Gateways ein, z. B. *filiale1* .

(4) Für die Authentifizierung geben Sie **Preshared Key** ein, z. B. *supersecretgeheimkey*.

(5) Bei **Lokale IP-Adresse** wählen Sie die IP-Adresse des **bintec R3002** aus, z. B.

192.168.0.1.

(6) Der VPN-Tunnel wird immer von der Filiale zur Zentrale aufgebaut. Deshalb wird am **bintec R3002** keine **IPSec-Peer-Adresse** gesetzt.

(7) Tragen Sie bei **IP-Adresse des Remote-Netzwerks** die Netzwerk-Adresse der Filiale ein, z. B. *192.168.1.0* und die **Netzmaske** *255.255.255.0*.

(8) Bestätigen Sie Ihre Angaben mit **OK**.

Nach dem Bestätigen der Eingaben ist die VPN-Verbindung in der Liste zu sehen.

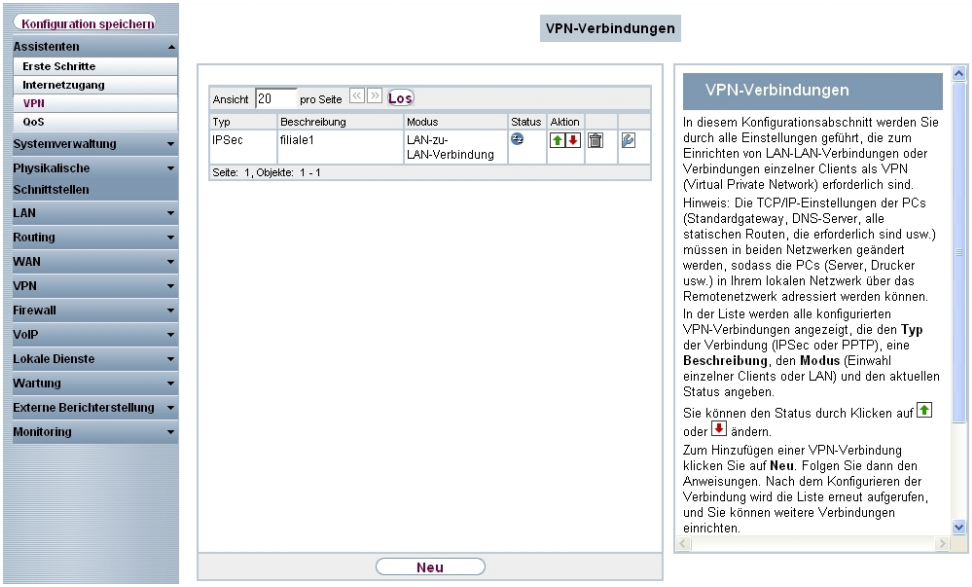


Abb. 23: **Assistenten** -> **VPN** -> **VPN-Verbindungen**

Für die Anbindung weiterer Standorte bzw. VPN-Gegenstellen kann der Assistent erneut ausgeführt werden.

4.2.4 Konfiguration des Gateways in der Filiale (bintec RS120)

Die IP-Konfiguration des Filial-Gateways (**bintec RS120**) kann wieder mit dem **Dime Manager** durchgeführt werden. Der **bintec RS120** wird dabei mit Hilfe des **Dime Managers** im Netzwerk gefunden. Anschließend kann die LAN IP-Adresse über das Kontextmenü gesetzt werden. Nach dem Ändern der IP-Adresse ist die Web-Schnittstelle, **GUI** des **bintec RS120** erreichbar.

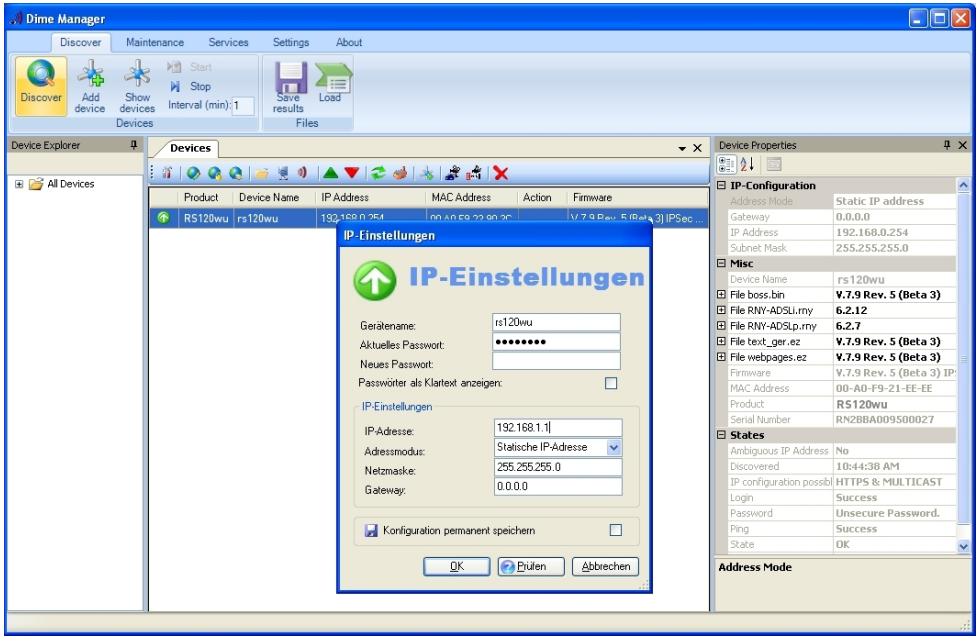


Abb. 24: Dime Manager

4.2.5 Konfiguration des Internetzugangs per GUI Assistenten

Der **GUI** Assistent erleichtert auch für den **bintec RS120** die Konfiguration des Internetzugangs. Beim **bintec RS120** wird der Internetzugang mit Hilfe eines externen ADSL-Modems hergestellt. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Neu**.

(2) Wählen Sie bei **Verbindungstyp** z. B. *Externes xDSL-Modem* aus.

(3) Klicken Sie auf **Weiter** um eine neue Internetverbindung zu konfigurieren.

Geben Sie die erforderlichen Daten für die Verbindung ein.

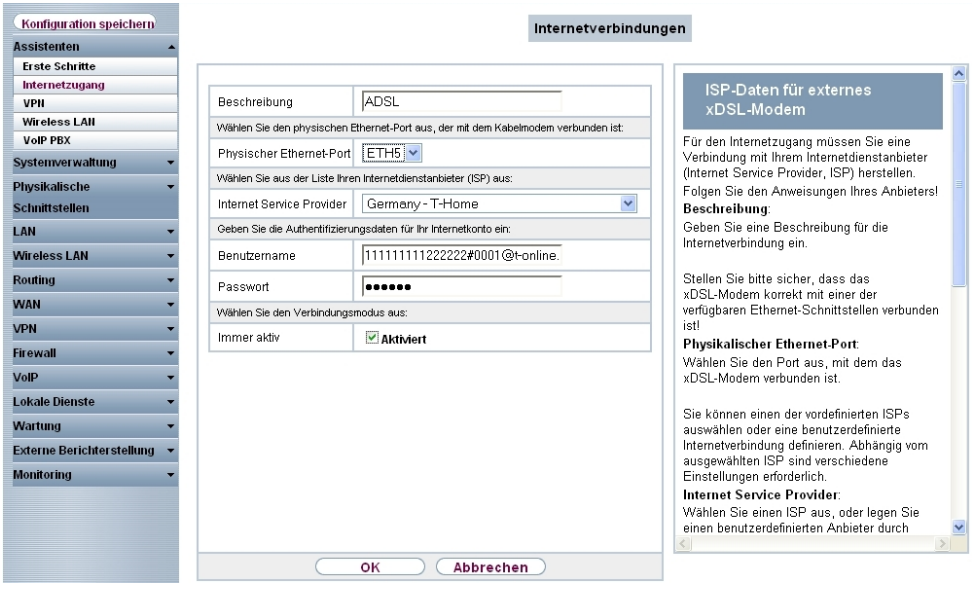


Abb. 25: **Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Weiter**

Gehen Sie folgendermaßen vor, um eine neue Internetverbindung zu konfigurieren:

(1) Bei **Beschreibung** tragen Sie z. B. `ADSL` ein.

(2) Wählen Sie bei **Physikalischer Ethernet-Port** die `ETH5` aus.

(3) Als **Internet Service Provider** wählen Sie z. B. `Germany-T-Home` aus.

(4) Als **Benutzername** geben Sie die Zugangsdaten ein, die Sie von Ihrem Provider erhalten haben.

(5) Geben Sie das **Passwort** ein, das Sie von Ihrem Provider erhalten haben.

(6) Im Feld **Immer aktiv** legen Sie fest, ob die Internetverbindung immer aktiv sein soll. Aktivieren Sie diese Option nur, wenn Sie über einen Internetzugang mit Flatrate verfügen.

(7) Bestätigen Sie Ihre Angaben mit **OK**.

4.2.6 Konfiguration des VPN IPSec-Tunnels am Filial-Gateway

Der **GUI** Assistent erleichtert auch die VPN-Konfiguration am Filial-Gateway. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Neu**.

(2) Wählen Sie bei **VPN-Szenario** die `IPSec-LAN-zu-LAN-Verbindung` aus.

(3) Klicken Sie auf **Weiter** um eine neue VPN-Verbindung einzurichten.

Geben Sie die erforderlichen Daten für die Verbindung ein.

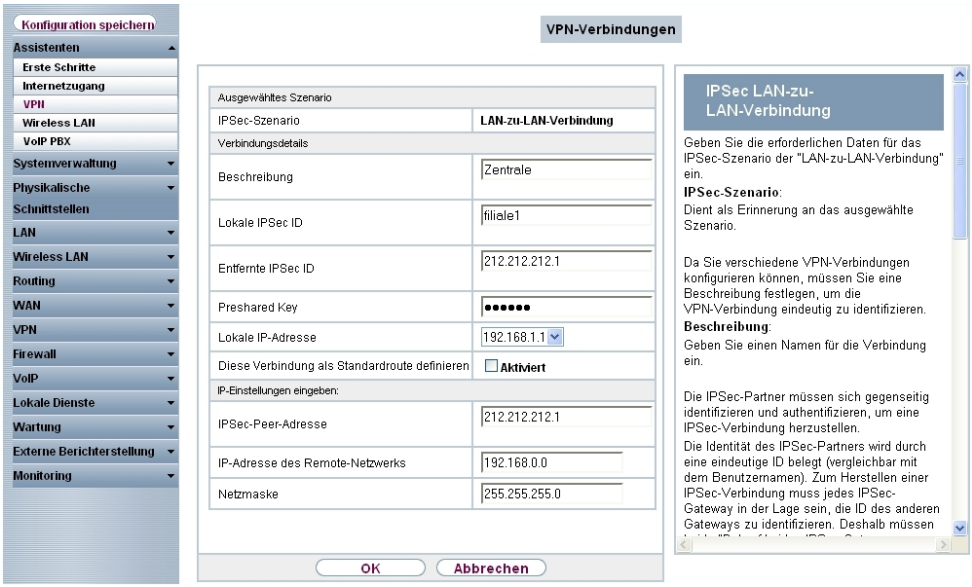


Abb. 26: **Assistenten** -> **VPN** -> **VPN-Verbindungen** -> **Weiter**

Gehen Sie folgendermaßen vor, um eine neue VPN-Verbindung zu konfigurieren:

(1) Bei **Beschreibung** tragen Sie z. B. *Zentrale* ein.

(2) Unter **Lokale IPSec ID** tragen Sie die ID des Filial-Gateways entsprechend der **Entfernten IPSec ID** des Zentral-Gateways ein, z. B. *filiale1*.

(3) Unter **Entfernte IPSec ID** tragen Sie die lokale IPSec ID des entfernten Gateways ein z. B. *212.212.212.1* .

(4) Für die Authentifizierung geben Sie **Preshared Key** ein, z. B. *supersecretgeheimkey*.

(5) Bei **Lokale IP-Adresse** wählen Sie die IP-Adresse des **bintec RS120** aus, z. B. *192.168.1.1*.

(6) Als **IPSec-Peer-Adresse** muss die WAN IP-Adresse des **bintec R3002** hinterlegt werden, z. B. *212.212.212.1*.

(7) Tragen Sie bei **IP-Adresse des Remote-Netzwerks** die Netzwerk-Adresse der Zentrale ein, z. B. *192.168.0.0* und die **Netzmaske** *255.255.255.0*.

(8) Bestätigen Sie Ihre Angaben mit **OK**.

Der VPN IPSec-Tunnel kann aufgrund der dynamischen IP-Adresse des **bintec RS120** nur in eine Richtung (Filiale -> Zentrale) aufgebaut werden. Damit die Verbindung von beiden Standorten nutzbar ist muss der Tunnel immer akiv sein. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**.

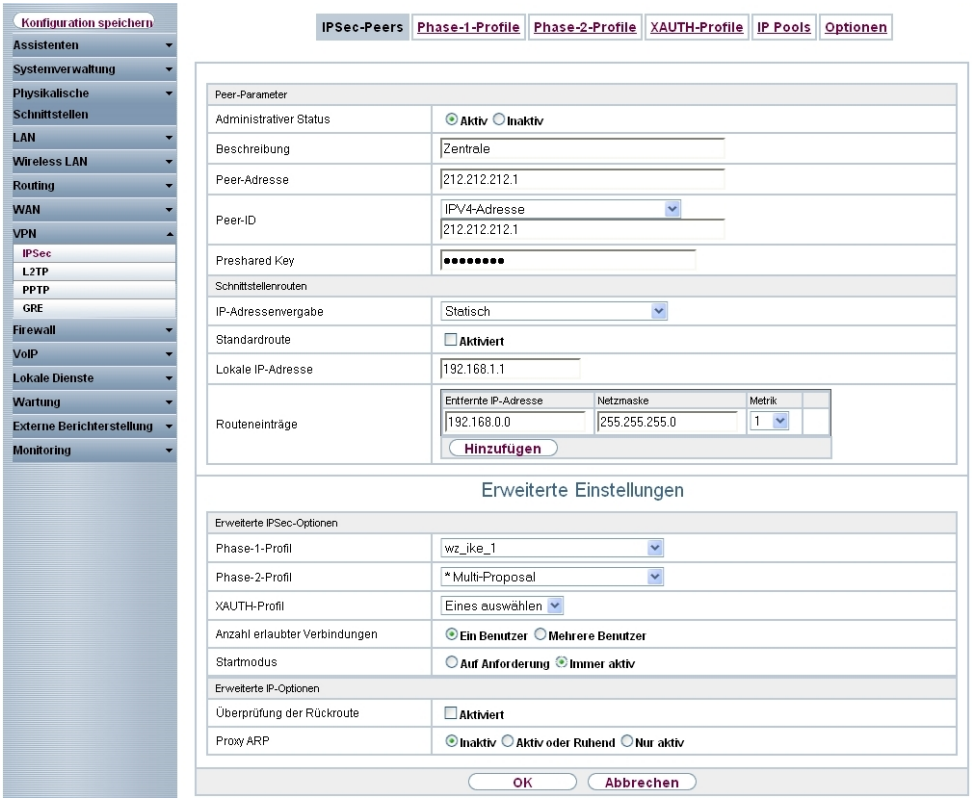


Abb. 27: **VPN** -> **IPSec** -> **IPSec-Peers** -> -> **Erweiterte Einstellungen**

Gehen Sie folgendermaßen vor, um den VPN IPSec-Tunnel zu konfigurieren:

(1) Den **Startmodus** setzen Sie auf `Immer aktiv`.

(2) Belassen Sie alle anderen Einstellungen und bestätigen Sie Ihre Angaben mit **OK**.

4.3 Test der VPN-Verbindung

Zum jetzigen Stand der Konfiguration ist der Internetzugang auf beiden Gateways eingerichtet und der VPN-Tunnel zur Standortkopplung ist auch bereits einsetzbar. Der VPN-Tunnel kann mit dem Ping-Test zwischen beiden Gateways getestet werden.

4.4 Priorisierung des VPN-Tunnels vor übrigem Internet-Datenverkehr

Der Internetzugang des **bintec R3002** (Zentrale) wird neben dem VPN-Tunnel noch für andere Internetdienste genutzt. Die Standortvernetzung soll höhere Priorität als der übrige Internet-Datenverkehr haben. Deshalb werden die für die VPN-Verbindung notwendigen Protokolle (IKE, ESP, NAT-Traversal) priorisiert. Hierzu wird QoS (Quality of Service) konfiguriert.

4.4.1 Anlegen der QoS-Filter

Zu Beginn der QoS-Konfiguration werden Filter definiert die den Datenverkehr welcher priorisiert werden soll, kennzeichnen. Zur Priorisierung von VPN IPSec-Verbindungen müssen QoS-Filter angelegt werden. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Routing** -> **QoS** -> **QoS-Filter** -> **Neu**.

Abb. 28: **Routing** -> **QoS** -> **QoS-Filter** -> **Neu**

Gehen Sie folgendermaßen vor, um QoS-Filter zu konfigurieren:

(1) Als **Beschreibung** geben Sie die Bezeichnung des Filters an, z. B. `IKE`.

(2) Wählen Sie das **Protokoll** `udp` aus.

(3) Als **Ziel-Port/Bereich** wählen Sie `Port angeben` und geben Sie die Zielport-Nummer an, z. B. `500`.

(4) Bei **Quell-Port/Bereich** wählen Sie `Port angeben` und geben Sie die Quellport-Nummer `500` an.

(5) Belassen Sie **DSCP/TOS-Filter (Layer 3)** auf `Nicht beachten`.

(6) Bestätigen Sie Ihre Angaben mit **OK**.

Legen Sie anschließend anhand folgender Tabelle weitere QoS-Filter für die Protokolle ESP und NAT-Traversal an.

Beschreibung	Protokoll	Ziel-Port/Bereich	Quell-Port/Bereich
IKE	udp	500	500
ESP	esp	-	-
NAT-T_1	udp	4500	-
NAT-T_2	udp	-	4500

Die fertige Konfiguration sieht wie folgt aus:

Abb. 29: **Routing** -> **QoS** -> **QoS-Filter**

4.4.2 Zuweisung der QoS-Filter zu QoS-Klassen bzw. der High-Priority-Klasse

Im nächsten Konfigurationsschritt werden die erstellten Filter der High-Priority-Klasse zugewiesen. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**.

Abb. 30: **Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**

Gehen Sie folgendermaßen vor, um einen neuen Klassenplan anzulegen:

(1) Als **Beschreibung** geben Sie eine Bezeichnung für den Klassenplan ein, z. B. *VPN-IPSec*.

(2) Wählen Sie **Filter** aus den Sie im Menü **Routing** -> **QoS** -> **QoS-Filter** konfiguriert haben, z. B. *IKE*.

(3) Bei **Richtung** wählen Sie *Ausgehend* aus.

(4) Aktivieren Sie die **High-Priority-Klasse**. Dadurch werden die Datenpakete der Klasse mit der höchsten Priorität zugeordnet.

(5) Wählen Sie die **Schnittstelle** aus über welche die priorisierten Daten gesendet werden z. B. *ADSL* .

(6) Bestätigen Sie mit **OK**.

Für jeden **QoS-Filter** muss die Zuteilung der QoS-Klasse (**High-Priority-Klasse**) separat durchgeführt werden. Beim Zuweisen der QoS-Filter (ESP, NAT-T_1 und NAT-T_2) wird der Klassenplan auf den neu angelegten Eintrag VPN-IPSec gesetzt. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**.

Abb. 31: **Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**

Gehen Sie folgendermaßen vor, um weitere QoS-Filter dem Klassenplan zuzuweisen:

(1) Wählen Sie den **Klassenplan** aus, (z. B. `VPN-IPSec`) welchem die QoS-Filter zugeordnet werden sollen.

(2) Wählen Sie den nächsten **Filter** aus, z. B. `ESP`.

(3) Als **Richtung** wählen Sie `Ausgehend` .

(4) Aktivieren Sie die **High-Priority-Klasse**.

(5) Bestätigen Sie Ihre Angaben mit **OK**.

Weisen Sie alle erzeugten QoS-Filter dem neuen Klassenplan `VPN-IPSec` zu.

Ergebnis:

Abb. 32: **Routing** -> **QoS** -> **QoS-Klassifizierung**

4.4.3 Aktivierung von QoS an der WAN-Schnittstelle

Im letzten Schritt der QoS-Konfiguration wird die Priorisierung an der WAN-Schnittstelle aktiviert. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Routing** -> **QoS** -> **QoS-Schnittstelle/Richtlinien** -> **Neu**.

Abb. 33: **Routing** -> **QoS** -> **QoS-Schnittstelle/Richtlinien** -> **Neu**

Gehen Sie folgendermaßen vor, um die Priorisierung an der WAN-Schnittstelle zu aktivieren:

(1) Wählen Sie die **Schnittstelle** aus, für die QoS konfiguriert werden soll, hier z. B. *ADSL*.

(2) Als **Priorisierungsalgorithmus** wählen Sie *Priority Queueing* aus.

(3) Bei der Option **Größe des Protokoll-Headers unterhalb Layer 3** wählen Sie *PPP over Ethernet* aus.

(4) Die verwendeten QoS-Queues (Hohe Priorität und Standard) werden automatisch angelegt.

(5) Bestätigen Sie Ihre Angaben mit **OK**.

4.4.4 QoS Monitoring

Mit der Konfiguration wurde, für den High Priority-Datenverkehr und für den unpriorisierten Datenverkehr, je eine Priorisierungs Queue / Warteschlange angelegt. Der Status dieser Warteschlangen wird im Menü **Monitoring** -> **QoS** angezeigt. Sobald die Bandbreite der Internetanbindung für die anstehenden VPN-Daten und die übrigen Internet-Daten nicht mehr ausreicht werden die unpriorisierten Daten zurückgestellt und die VPN-Daten bevorzugt übertragen.

(1) Gehen Sie zu **Monitoring** -> **QoS** -> **QoS**.

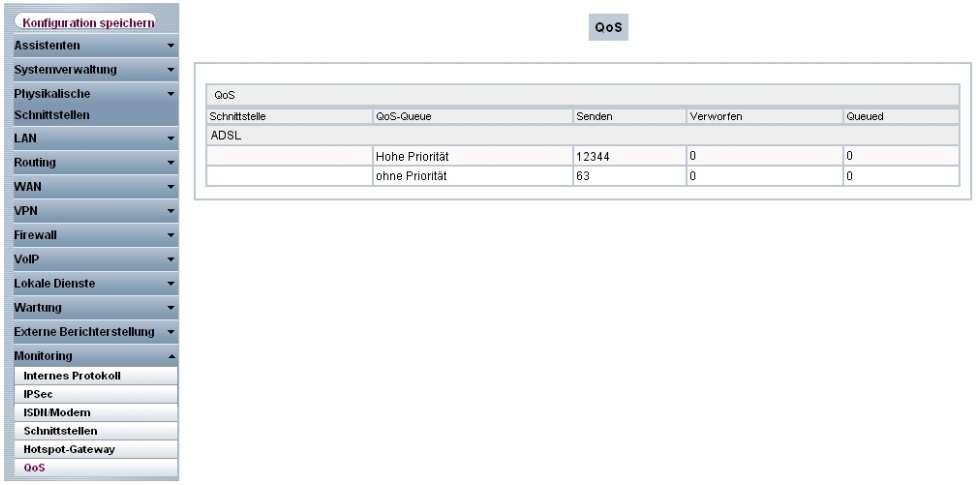


Abb. 34: **Monitoring** -> **QoS** -> **QoS**

Die Konfiguration ist hiermit abgeschlossen. Zur bootfähigen Sicherung der Konfiguration verlassen Sie das **GUI** mit **Konfiguration speichern** und bestätigen Sie die Auswahl mit **OK**.

4.5 Konfigurationsschritte im Überblick

Konfiguration des Gateways in der Zentrale (bintec R3002)

Feld	Menü	Wert
IP-Adresse	**Dime Manager** -> **IP-Einstellungen**	z. B. *192.168.0.1*

Konfiguration des Internetzugangs (Zentrale)

Feld	Menü	Wert
Verbindungstyp	**Assistenten** -> **Internetzugang** -> **Neu**	*Internes ADSL-Modem*
Beschreibung	**Assistenten** -> **Internetzugang** -> **Weiter**	*ADSL*
Internet Service Provider	**Assistenten** -> **Internetzugang** -> **Weiter**	z. B. *Germany - T-Home*
Benutzername	**Assistenten** -> **Internetzugang** -> **Weiter**	z. B. *0000111111#0001@t-online.de*
Passwort	**Assistenten** -> **Internetzugang** -> **Weiter**	z. B. *supersecretgeheimkey*
Immer aktiv	**Assistenten** -> **Internetzugang** -> **Wei-**	*Aktiviert*

Feld	Menü	Wert
	ter	

Konfiguration des VPN IPSec-Zugangs (Zentrale)

Feld	Menü	Wert
Verbindungstyp	**Assistenten** -> **VPN** -> **Neu**	*IPSec-LAN-zu-LAN-Verbindung*
Beschreibung	**Assistenten** -> **VPN** -> **Weiter**	*filiale1*
Lokale IPSec ID	**Assistenten** -> **VPN** -> **Weiter**	z. B. *212.212.212.1*
Entfernte IPSec ID	**Assistenten** -> **VPN** -> **Weiter**	z. B. *filiale1*
Preshared Key	**Assistenten** -> **VPN** -> **Weiter**	z. B. *supersecretgeheimkey*
Lokale IP-Adresse	**Assistenten** -> **VPN** -> **Weiter**	*192.168.0.1*
IP-Adresse des Remote-Netzwerks	**Assistenten** -> **VPN** -> **Weiter**	*192.168.1.0*
Netzmaske	**Assistenten** -> **VPN** -> **Weiter**	*255.255.255.0*

Konfiguration des Gateways in der Filiale (bintec RS120)

Feld	Menü	Wert
IP-Adresse	**Dime Manager** -> **IP-Einstellungen**	z. B. *192.168.1.1*

Konfiguration des Internetzugangs (Filiale)

Feld	Menü	Wert
Verbindungstyp	**Assistenten** -> **Internetzugang** -> **Neu**	*Externes xDSL-Modem*
Beschreibung	**Assistenten** -> **Internetzugang** -> **Weiter**	*ADSL*
Physischer Ethernet-Port	**Assistenten** -> **Internetzugang** -> **Weiter**	z. B. *ETH5*
Internet Service Provider	**Assistenten** -> **Internetzugang** -> **Weiter**	z. B. *Germany - T-Home*
Benutzername	**Assistenten** -> **Internetzugang** -> **Weiter**	z. B. *111111111222222#0001@t-online.de*
Passwort	**Assistenten** -> **Internetzugang** -> **Weiter**	z. B. *supersecretgeheimkey*
Immer aktiv	**Assistenten** -> **Internetzugang** -> **Wei-**	*Aktiviert*

Feld	Menü	Wert
	ter	

Konfiguration des VPN IPSec-Zugangs (Filiale)

Feld	Menü	Wert
Verbindungstyp	**Assistenten** -> **VPN** -> **Neu**	*IPSec-LAN-zu-LAN-Verbindung*
Beschreibung	**Assistenten** -> **VPN** -> **Weiter**	*Zentrale*
Lokale IPSec ID	**Assistenten** -> **VPN** -> **Weiter**	z. B. *filiale1*
Entfernte IPSec ID	**Assistenten** -> **VPN** -> **Weiter**	z. B. *212.212.212.1*
Preshared Key	**Assistenten** -> **VPN** -> **Weiter**	z. B. *supersecretgeheimkey*
Lokale IP-Adresse	**Assistenten** -> **VPN** -> **Weiter**	*192.168.1.1*
IPSec-Peer-Adresse	**Assistenten** -> **VPN** -> **Weiter**	212.212.212.1
IP-Adresse des Remote-Netzwerks	**Assistenten** -> **VPN** -> **Weiter**	*192.168.0.0*
Netzmaske	**Assistenten** -> **VPN** -> **Weiter**	*255.255.255.0*

Priorisierung des VPN-Tunnels

Feld	Menü	Wert
Startmodus	**VPN** -> **IPSec** -> **IPSec-Peers** ->  -> **Erweiterte Einstellungen**	*Immer aktiv*

Anlegen der QoS-Filter

Feld	Menü	Wert
Beschreibung	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*IKE*
Protokoll	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*udp*
Ziel-Port/Bereich	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*500*
QuellPort/Bereich	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*500*
DSCP/TOS	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*Nicht beachten*
Beschreibung	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*ESP*
Protokoll	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*esp*
Beschreibung	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*NAT-T_1*
Protokoll	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*udp*
Ziel-Port/Bereich	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*4500*

Feld	Menü	Wert
Beschreibung	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*NAT-T_2*
Protokoll	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*udp*
QuellPort/Bereich	**Routing** -> **QoS** -> **QoS-Filter** -> **Neu**	*4500*

Zuweisung der QoS-Filter zu QoS-Klassen

Feld	Menü	Wert
Beschreibung	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	*VPN-IPSec*
Filter	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	z. B. *IKE*
Richtung	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	*Ausgehend*
High-Priority-Klasse	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	*Aktiviert*
Schnittstelle	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	*ADSL*
Klassenplan	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	*VPN-IPSec*
Filter	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	z. B. *ESP*
Richtung	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	*Ausgehend*
High-Priority-Klasse	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	*Aktiviert*
Klassenplan	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	*VPN-IPSec*
Filter	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	z. B. *NAT-T_1*
Richtung	**Routing** -> **QoS** -> **QoS-Klassifizierung**-> **Neu**	*Ausgehend*
High-Priority-Klasse	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	*Aktiviert*
Klassenplan	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	*VPN-IPSec*
Filter	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	z. B. *NAT-T_2*
Richtung	**Routing** -> **QoS** ->	*Ausgehend*

Feld	Menü	Wert
	-> **Neu**	
High-Priority-Klasse	**Routing** -> **QoS** -> **QoS-Klassifizierung** -> **Neu**	*Aktiviert*

Aktivierung von QoS an der WAN-Schnittstelle

Feld	Menü	Wert
Schnittstelle	**Routing** -> **QoS** -> **QoS-Schnittstelle/Richtlinien** -> **Neu**	*ADSL*
Priorisierungsalgorithmus	**Routing** -> **QoS** -> **QoS-Schnittstelle/Richtlinien** -> **Neu**	*Priority Queueing*
Größe des Protokoll-Headers unterhalb Layer 3	**Routing** -> **QoS** -> **QoS-Schnittstelle/Richtlinien** -> **Neu**	*PPP over Ethernet*

Kapitel 5 Dienste - Automatisches Router-Backup (Redundanz) mit BRRP für ein Internet-/VPN-Gateway

5.1 Einleitung

In diesem Workshop wird die Konfiguration von BRRP (Bintec Router Redundancy Protocol) anhand von zwei **bintec RT1202** beschrieben. An beiden Gateways werden zwei Ethernet-Schnittstellen (je eine LAN- und WAN-Schnittstelle) genutzt. Fällt das Master-Gateway oder die Verbindung zum Backup-Gateway aus, z. B. Hardwaredefekt, so übernimmt das Backup-Gateway die Funktionalität des Master-Gateways. Solange das Master-Gateway aktiv ist, befindet sich das Backup-Gateway im Hot-Standby-Modus. Durch ein konfigurierbares Regelwerk kann bestimmt werden, wie die Gateways sich bei einem Ausfall verhalten.

Beim Einsatz von BRRP sind virtuelle IP- und MAC-Adressen zu konfigurieren, um bei einem Ausfall diese IP- und MAC-Adressen an das Backup-Gateway übergeben zu können. Als erstes legen Sie auf der physikalischen Ethernet-Schnittstelle, der BRRP Advertisment-schnittstelle, die IP-Adresse fest über die das Master- und Backup-Gateway miteinander kommunizieren. Über diese Schnittstelle / IP-Adresse werden die Gateways konfiguriert. Anschließend wird für die LAN- und WAN-Seite eine virtuelle Schnittstelle, ein virtueller Router, angelegt. Diese virtuelle Schnittstelle und deren IP-Adresse werden für den Datenverkehr verwendet.

Zur Konfiguration wird hierbei das **GUI** (Graphical User Interface) verwendet.

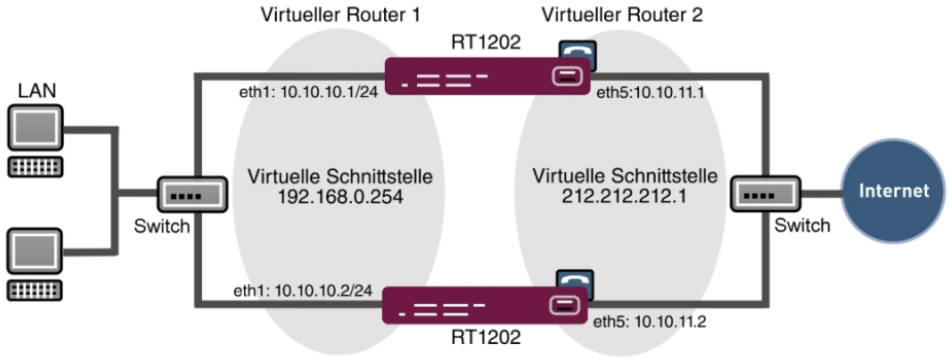


Abb. 35: Beispielszenario

Voraussetzungen

- Zwei bintec Gateways mit BRRP Funktionalität (z. B. **bintec RT1202**)
- Ein Internetzugang der per Ethernet und einem Grenzrouter/Gateway hergestellt wird
- Ein Switch zum Verbinden der Ethernet-Schnittstelle Eth1 (beider Gateways) mit dem lokalen Netzwerk
- Ein Switch zum Verbinden der Ethernet-Schnittstelle Eth5 (beider Gateways) mit dem Grenzrouter/Gateway des Internet-Providers

5.2 Konfiguration

5.2.1 Konfiguration der Advertisment- und Management IP-Adresse

Nachdem beide Gateways über einen Switch mit dem lokalen Netzwerk verbunden wurden können sie mit Hilfe des **Dime Managers** gefunden werden. In diesem Zustand verwenden beide Gateways die Standard IP-Adresse 192.168.0.254.

(1) Gehen Sie zu **Dime Manager** -> **IP-Einstellungen**.

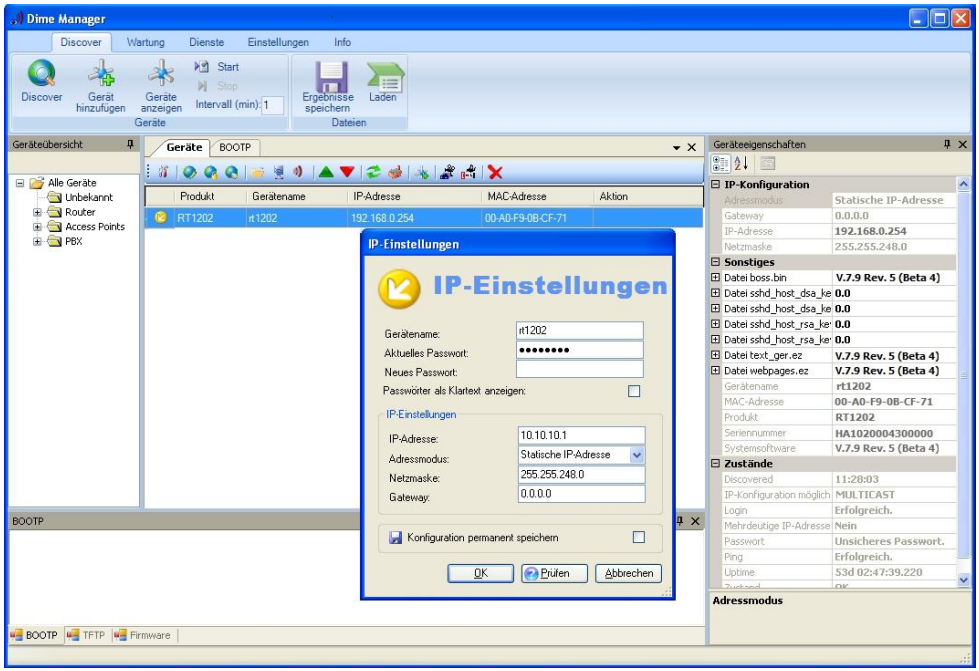


Abb. 36: **Dime Manager -> IP-Einstellungen**

Die Advertisment- und Management- IP-Adresse der beiden Gateways kann über das Kontextmenü des **Dime Managers** gesetzt werden. In diesem Workshop wird einem Gateway die Adresse 10.10.10.1/24 und dem anderen Gateway die Adresse 10.10.10.2/24 zugewiesen. Diese Schnittstellen werden nach erfolgter Konfiguration als Konfigurationszugang und zum Austausch der BRRP-Statusmeldungen verwendet.

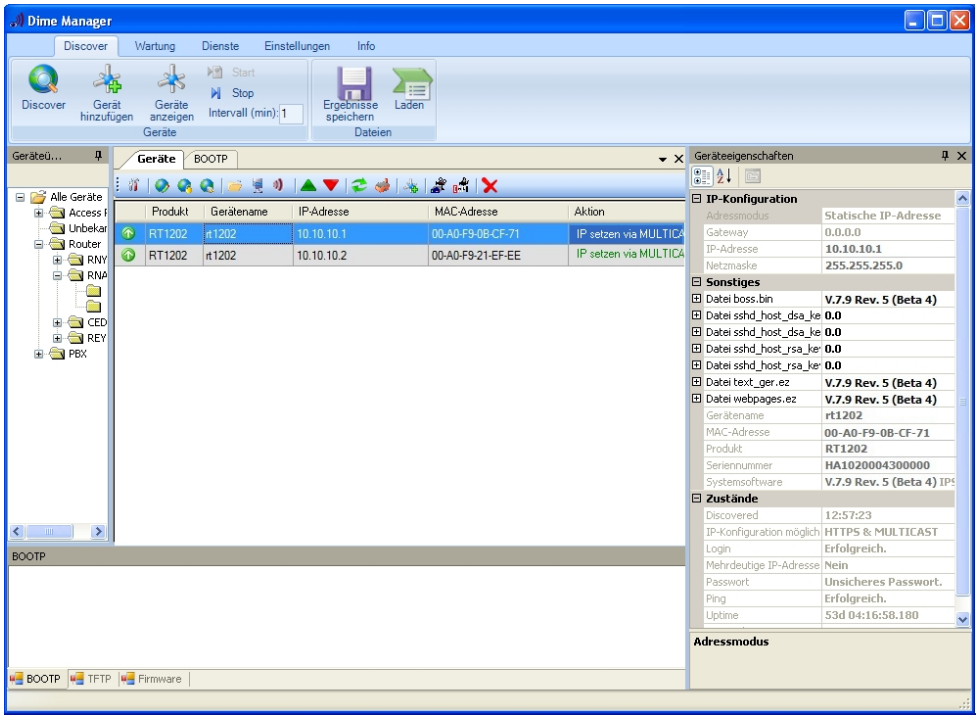


Abb. 37: Dime Manager

Anschließend sind beide Gateways über **GUI** erreichbar und die Advertisment-IP-Adressen der WAN-Schnittstelle Eth5 können gesetzt werden.

Im nächsten Schritt wird dem Gateway die WAN-Advertisment IP-Adresse mit der Netzmaske vergeben.

(1) Gehen Sie zu **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> .

Abb. 38: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** ->

Gehen Sie folgendermaßen vor, um die ETH5-Schnittstelle des ersten Gateways zu konfigurieren.

(1) Bei **IP-Adresse /Netzmaske** tragen Sie die WAN-Advertisment IP-Adresse `10.10.11.1` mit der Netzmaske `255.255.255.252` ein.

(2) Bestätigen Sie Ihre Angaben mit **OK**.

Analog dazu wird am ETH5-Port des zweiten Gateways die Adresse `10.10.11.2` mit Netzmaske `255.255.255.252` konfiguriert.

Ergebnis:

(1) Gehen Sie zu **LAN** -> **IP-Konfiguration** -> **Schnittstellen**.

Abb. 39: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** ->

Über diese Schnittstelle tauschen die beiden Gateways Statusmeldungen aus womit der BRRP-Status (Master/Slave) gesetzt wird.

5.2.2 Konfiguration der virtuellen Router

Für den Zugriff auf das lokale Netzwerk (LAN) sowie für den Zugriff in Richtung Internet (WAN) wird jeweils ein virtueller Router angelegt. Gehen Sie zum Anlegen des virtuellen Routers des Master Gateways in folgendes Menü:

(1) Gehen Sie zu **Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**.

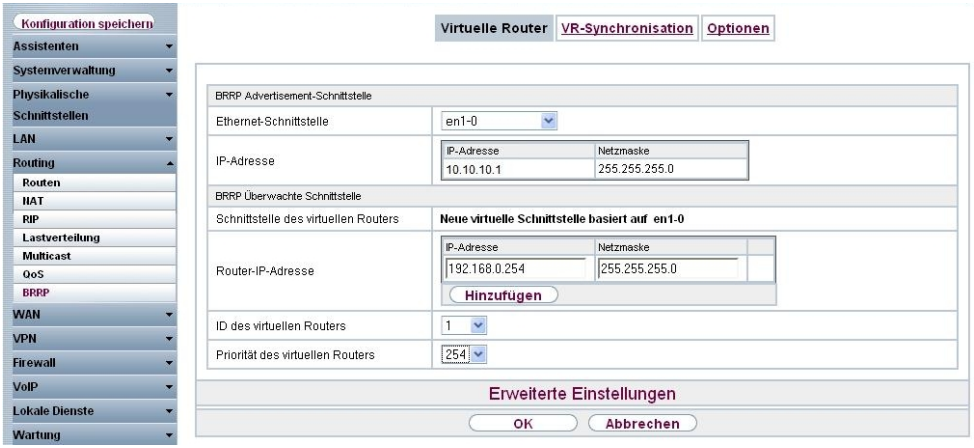


Abb. 40: **Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**

Für den Zugriff auf das lokale Netzwerk (LAN) gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Ethernet-Schnittstelle** die `en1-0` aus, wodurch dessen IP-Adresse angelegt wird.

(2) Als **Router IP-Adresse** geben Sie die IP-Adresse und die Netzmaske ein, die Sie im lokalen Netz als eigentliche Gateway-IP-Adresse verwenden wollen, z. B. `192.168.0.254` und `255.255.255.0`.

(3) Wählen Sie bei **ID des virtuellen Routers** die ID des ersten virtuellen Routers aus, z. B. `1`. Diese ID identifiziert den **virtuellen Router** innerhalb des LAN und ist Bestandteil jedes BRRP-Advertisement-Pakets, das vom aktuellen Master gesendet wird.

(4) Bei **Priorität des virtuellen Routers** setzen Sie die Priorität des Gateways welches die Master-Rolle übernimmt auf `254` .

(5) Bestätigen Sie Ihre Angaben mit **OK**.

Zur Konfiguration des virtuellen Routers in Richtung Internet (WAN) gehen Sie in folgendes Menü:

(1) Gehen Sie zu **Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**.

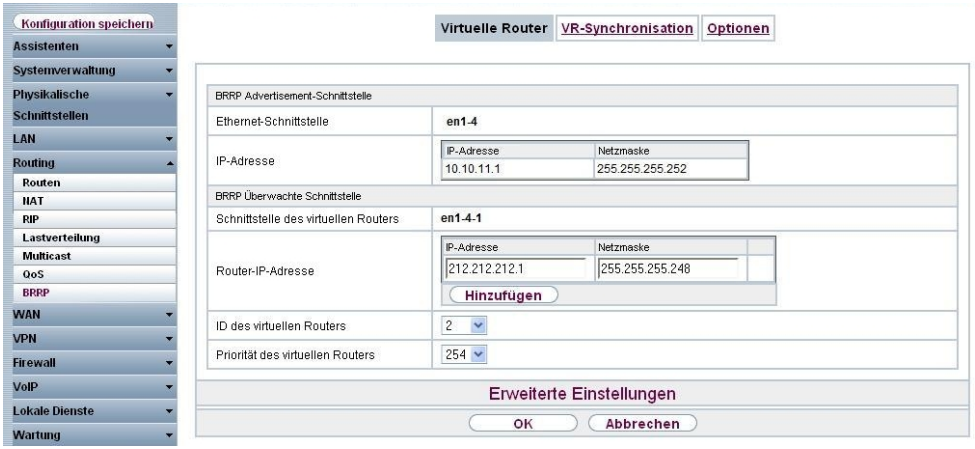


Abb. 41: **Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**

Für den Zugriff auf das Internet (WAN) gehen Sie folgendermaßen vor:

(1) Bei **Router IP-Adresse** geben Sie die IP-Adresse und die Netzmaske ein, z. B. `212.212.212.1` und `255.255.255.248`.

(2) Wählen Sie die **ID des virtuellen Routers** aus, z. B. `2`.

(3) Bei **Priorität des virtuellen Routers** wählen Sie `254` aus. Durch Priorität 254 wird dieses Gateway nach erfolgter Konfiguration die Master-Rolle übernehmen.

(4) Bestätigen Sie Ihre Angaben mit **OK**.

Die Konfigurationsschritte zum Anlegen der virtuellen Router des Backup-Gateways sind identisch mit der Konfiguration zum Master-Gateway, mit Ausnahme der **Priorität des virtuellen Routers**. Am zweiten **bintec RT1202** (Backup-Gateway), wird auf beiden virtuellen Routern der Wert `100` konfiguriert.

5.2.3 Aktivierung der BRRP-Konfiguration

Nach dem Anlegen der virtuellen Router auf beiden **bintec RT1202** Gateways wird die Funktion BRRP aktiviert. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Routing** -> **BRRP** -> **Optionen**.

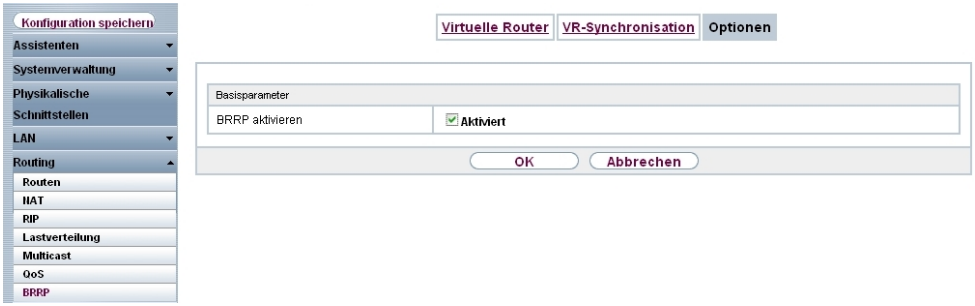


Abb. 42: **Routing** -> **BRRP** -> **Optionen**

Gehen Sie folgendermaßen vor:

(1) Aktivieren Sie die Funktion **BRRP aktivieren**.

(2) Bestätigen Sie mit **OK**.

Das Gateway mit der höheren Priorität befindet sich jetzt im Master-Status, und das Gateway mit der niedrigeren Priorität befindet sich im Backup-Status. Die Konfiguration des Master-Gateways sehen Sie im folgendem Menü:

(1) Gehen Sie zu **Routing** -> **BRRP** -> **Virtuelle Router**.

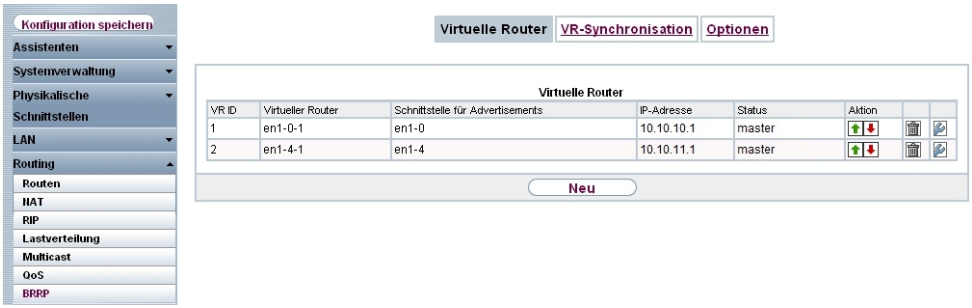


Abb. 43: **Routing** -> **BRRP** -> **Virtuelle Router**

Im Systemprotokoll sind folgende Meldungen zu sehen:

```
19:47:54 NOTICE/BRRP: started PID 67 (compiled Aug 16 2010 17:21:34) ...
19:47:54 INFO/BRRP: create_vr(vr # 1/slot 0)
19:47:54 NOTICE/BRRP: vr # 1 - now in init state
19:47:54 INFO/BRRP: create_vr(vr # 2/slot 1)
19:47:54 NOTICE/BRRP: vr # 2 - now in init state
19:47:54 INFO/BRRP: Config VR_ID 1: Prio 254 Pre-empt mode 'true'
19:47:54 INFO/BRRP: Advertisements: ifc 1000 IP 10.10.10.1 master_down 10007
19:47:54 INFO/BRRP: Virtual Router: ifc 1004 - 1 IP address(es) assigned
19:47:54 INFO/BRRP:           IP_0: 192.168.0.0
19:47:54 NOTICE/BRRP: vr # 1 - started on en1-0-1 ip 192.168.0.0 mac 00005e000101
19:47:54 NOTICE/BRRP: vr # 1 - now in backup state
19:47:54 INFO/BRRP: Config VR_ID 2: Prio 254 Pre-empt mode 'true'
19:47:54 INFO/BRRP: Advertisements: ifc 1400 IP 10.10.11.1 master_down 10007
19:47:54 INFO/BRRP: Virtual Router: ifc 1404 - 1 IP address(es) assigned
19:47:54 INFO/BRRP:           IP_0: 212.212.212.0
19:47:54 NOTICE/BRRP: vr # 2 - started on en1-4-1 ip 212.212.212.0 mac 00005e000102
19:47:54 NOTICE/BRRP: vr # 2 - now in backup state
19:47:55 INFO/BRRP: vr # 1 - pre-empt master state
19:47:55 INFO/BRRP: vr # 1 - timeout in state BACKUP
19:47:55 INFO/BRRP: vr # 1 - acquire master state
19:47:55 NOTICE/BRRP: vr # 1 - now in master state
19:47:55 INFO/BRRP: vr # 1 - router-ifc en1-0-1 up
19:47:55 INFO/BRRP: vr # 2 - pre-empt master state
19:47:55 INFO/BRRP: vr # 2 - timeout in state BACKUP
19:47:55 INFO/BRRP: vr # 2 - acquire master state
19:47:55 NOTICE/BRRP: vr # 2 - now in master state
19:47:55 INFO/BRRP: vr # 2 - router-ifc en1-4-1 up
```

5.2.4 Synchronisation der virtuellen Router

Bis zum jetzigen Stand der Konfiguration wurden auf jedem der **bintec RT1202** je zwei virtuelle Router (Zugriff auf das lokale Netzwerk und Zugriff auf das Internet) angelegt. Der Status beider virtueller Router muss pro Gateway synchronisiert werden. Mit folgendem Konfigurtionsschritt wird sichergestellt dass sich der virtuelle Router 1 immer im gleichen Status wie der virtuelle Router 2 befindet. Dieser Schritt muss auf beiden **bintec RT1202** identisch konfiguriert werden. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Routing** -> **BRRP** -> **VR-Synchronisation** -> **Neu**.

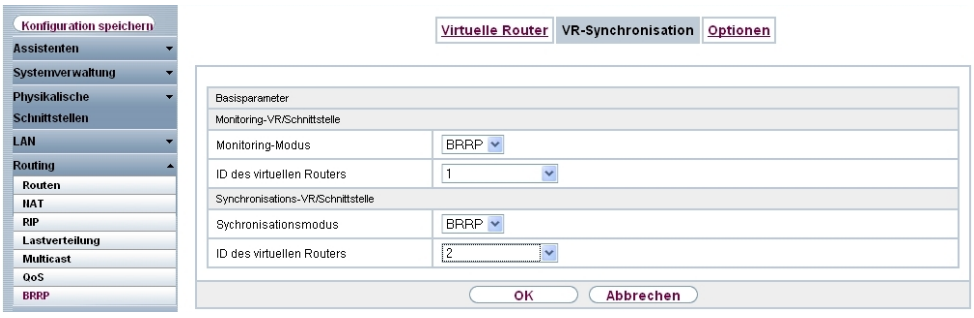


Abb. 45: **Routing** -> **BRRP** -> **VR-Synchronisation** -> **Neu**

Gehen Sie folgendermaßen vor um die Router zu synchronisieren:

(1) Wählen Sie bei **Monitoring-VR/Schnittstelle** die **ID des virtuellen Routers** aus *1*.

(2) Bei **Synchronisation-VR/Schnittstelle** wählen Sie die **ID des virtuellen Routers** *2* aus.

(3) Bestätigen Sie mit **OK**.

Synchronisieren Sie anschließend den zweiten Router, indem Sie **Routing** -> **BRRP** -> **VR-Synchronisation** -> **Neu** wählen.

(1) Wählen Sie bei **Monitoring-VR/Schnittstelle** die **ID des virtuellen Routers** aus *2*.

(2) Bei **Synchronisation-VR/Schnittstelle** wählen Sie die **ID des virtuellen Routers** *1* aus.

(3) Bestätigen Sie mit **OK**.

Ergebnis:

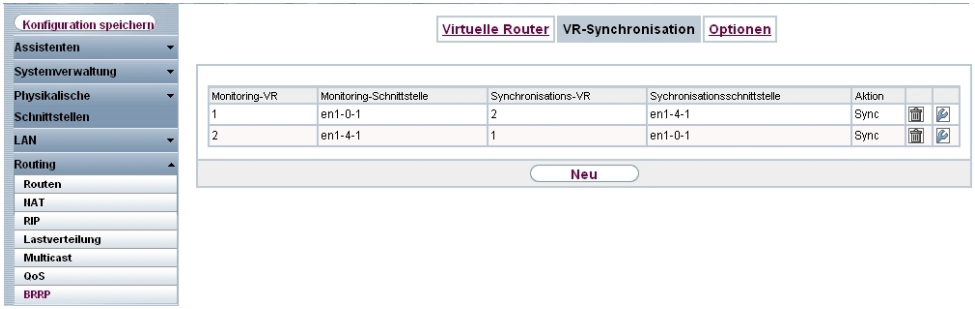


Abb. 46: **Routing** -> **BRRP** -> **VR-Synchronisation** -> **Neu**

Die Konfiguration ist hiermit abgeschlossen. Zur bootfähigen Sicherung der Konfiguration verlassen Sie das **GUI** mit **Konfiguration speichern** und bestätigen Sie die Auswahl mit **OK**.

5.3 Konfigurationsschritte im Überblick

Konfiguration der Advertisment- und Management IP-Adresse

Feld	Menü	Wert
IP-Adresse	**Dime Manager** -> **IP-Einstellungen**	z. B. *10.10.10.1*
IP-Adresse	**Dime Manager** -> **IP-Einstellungen**	z. B. *10.10.10.2*

IP-Konfiguration

Feld	Menü	Wert
IP-Adresse / Netzmaske	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** ->	z. B. *10.10.11.1* / *255.255.255.252*
IP-Adresse / Netzmask	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** ->	z. B. *10.10.11.2* / *255.255.255.252*

Konfiguration der virtuellen Router

Feld	Menü	Wert
Ethernet-Schnittstelle	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	z. B. *en1-0*
Router-IP-Adresse	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	z. B. *192.168.0.254* / *255.255.255.0*
ID des virtuellen Routers	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	z. B. *1*
Priorität des virtuellen Routers	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	*254*
Ethernet-Schnittstelle	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	z. B. *en1-4*
Router-IP-Adresse	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	z. B. *212.212.212.1*1 / *255.255.255.248*
ID des virtuellen Routers	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	z. B. *2*
Priorität des virtuellen Routers	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	*254*
Ethernet-Schnittstelle	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	z. B. *en1-0*
Router-IP-Adresse	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	z. B. *192.168.0.254* / *255.255.255.0*
ID des virtuellen Routers	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	z. B. *1*
Priorität des virtuellen Routers	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	*100*
Ethernet-Schnittstelle	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	z. B. *en1-4*
Router-IP-Adresse	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	z. B. *212.212.212.1*1 / *255.255.255.248*
ID des virtuellen Routers	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	z. B. *2*

Feld	Menü	Wert
Priorität des virtuellen Routers	**Routing** -> **BRRP** -> **Virtuelle Router** -> **Neu**	*100*

BRRP-Konfiguration aktivieren

Feld	Menü	Wert
BRRP aktivieren	**Routing** -> **BRRP** -> **Optionen**	*Aktiviert*

Synchronisation der virtuellen Router

Feld	Menü	Wert
Monitoring-Modus ID des virtuellen Routers	**Routing** -> **BRRP** -> **VR-Synchronisation** -> **Neu**	1
Synchronisationsmodus ID des virtuellen Routers	**Routing** -> **BRRP** -> **VR-Synchronisation** -> **Neu**	2
Monitoring-Modus ID des virtuellen Routers	**Routing** -> **BRRP** -> **VR-Synchronisation** -> **Neu**	2
Synchronisationsmodus ID des virtuellen Routers	**Routing** -> **BRRP** -> **VR-Synchronisation** -> **Neu**	1

Kapitel 6 Dienste - Fernwartung eines bintec RS232bu+ UMTS-Gateways mittels GSM/GPRS-Einwahl

6.1 Einleitung

In diesem Kapitel wird am Beispiel eines **bintec RS232bu+**-Gateways eine Fernwartungsmöglichkeit mittels GSM/GPRS-Einwahl gezeigt. Das **bintec RS232bu+**-Gateway stellt mit Hilfe des internen UMTS (HSPA+)-Modems eine Verbindung zum Internet her. Um die Einwahl (ohne Benutzung des Internets) zu Fernwartungszwecken zu ermöglichen ist eine Umbuchung des integrierten UMTS (HSPA+)-Modem vom UMTS-Dienst in das GSM/GPRS-Netzwerk notwendig. Diese UMTS-Fallback-Funktion wird mit einem Anruf von der Ferne initiiert. Nachdem das integrierte UMTS (HSPA+)-Modem im GSM/GPRS-Netzwerk eingebucht ist kann mit dem ISDN-Login-Dienst von einem anderen **bintec** ISDN-Gateway eine Verbindung zur Fernwartung hergestellt werden. Alternativ besteht auch die Möglicheit eine ISDN-Remote Access-Verbindung (PPP Einwahl) zu dem **bintec RS232bu+** herzustellen. Nach dem Beenden der Fernwartungsverbindung kann sich das **bintec RS232bu+**-Gateway wieder in das UMTS-Netzwerk zurück buchen und die Internetverbindung herstellen.

Zur Konfiguration wird hierbei das **GUI** (Graphical User Interface) verwendet.

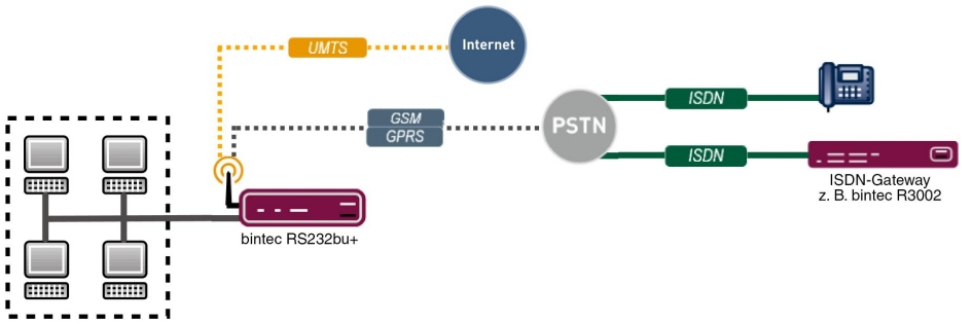


Abb. 47: Beispielszenario

Voraussetzungen

- Ein UMTS-Gateway der bintec RS-Serie (z. B. **bintec RS232bu+**)
- Für dieses Gateway muss eine Mobilfunktarif verwendet werden der Sprach- und Daten-

verbindungen ermöglicht

- Für das UMTS-Gateway der bintec RS-Serie muss ein Firmware stand ab 7.10.1 verwendet werden
- Für das integrierte Modem des UMTS-Gateway der bintec RS-Serie muss die akt. Modem Firmware verwendet werden (Link Release Notes)
- Ein Telefon/Mobiltelefon um aus der Ferne das UMTS-Fallback einzuleiten
- Ein bintec ISDN-Gateway z. B. **bintec R3002** zum Starten der Fernwartungsverbindung per ISDN-Login
- Eine ISDN-Leitung mit V.110-Unterstützung zum Starten der Fernwartungsverbindung

6.2 Konfiguration

Konfiguration der UMTS-Internetverbindung

Zur Konfiguration einer Internetverbindung verfügt das **GUI** über einen Assistenten.

Über den Assistenten kann die UMTS-Internetverbindung des **bintec RS232bu+** in wenigen Schritten eingerichtet werden. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Neu**.

(2) Wählen Sie bei **Verbindungstyp** *UMTS* aus.

(3) Klicken Sie auf **Weiter** um eine neue Internetverbindung zu konfigurieren.

(4) Geben Sie die erforderlichen Daten für die Verbindung ein.

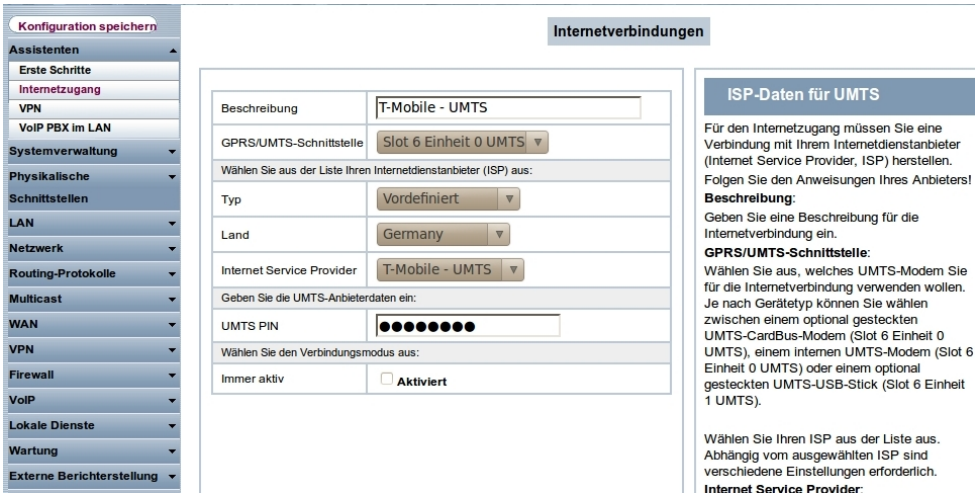


Abb. 48: **Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Weiter**

Gehen Sie folgendermaßen vor, um eine neue UMTS-Internetverbindung zu konfigurieren:

(1) Bei **Beschreibung** tragen Sie z. B. *T-Mobile - UMTS* ein.

(2) Bei **GPRS/UMTS-Schnittstelle** wählen Sie *Slot 6 Einheit 0 UMTS* aus.

(3) Als **Internet Service Provider** wählen Sie *T-Mobile - UMTS* aus.

(4) Geben Sie die **UMTS PIN** ein, welches Sie von Ihrem Provider erhalten haben, z. B. *0000*.

(5) Bestätigen Sie Ihre Angaben mit **OK**.

Konfiguration der UMTS-Fallback-Nummer und des Dienstes für eingehende Datenverbindungen (ISDN-Login)

Eingehende Verbindunden (ISDN-Login oder PPP-Einwahlverbindungen) werden vom **bintec RS232bu+**-Gateway nur im GSM/GPRS-Netzwerk angenommen. Durch die UMTS-Fallback-Funktion kann das Gateway gezwungen werden sich vom UMTS-Netzwerk in das GSM/GPRS-Netzwerk umzubuchen. Hierzu muss eine Rufnummer hinterlegt werden von der das UMTS-Fallback initiert wird. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Physikalische Schnittstellen** -> **UMTS/HSDPA** -> **UMTS/HSDPA/HSUPA** -> .

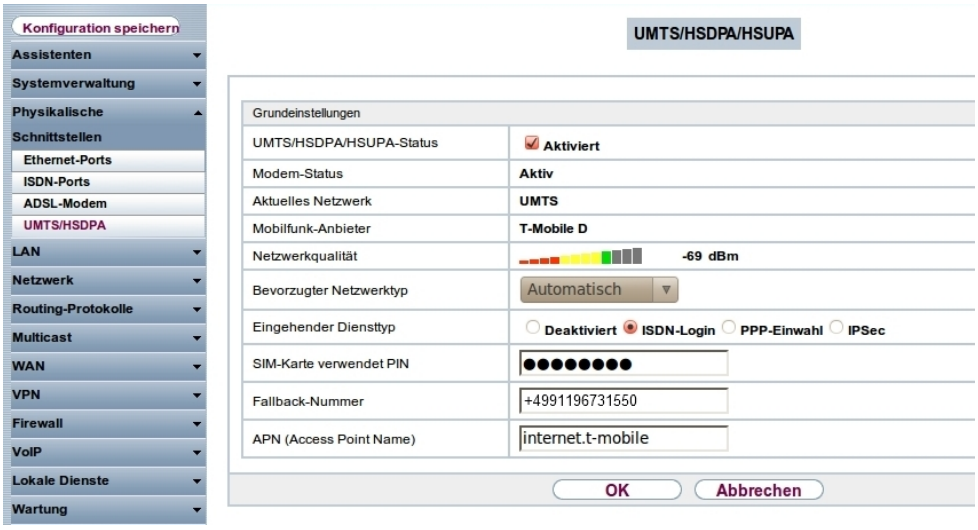


Abb. 49: **Physikalische Schnittstellen** -> **UMTS/HSDPA** -> **UMTS/HSDPA/HSUPA** ->

Gehen Sie folgendermaßen vor um die UMTS-Fallback-Nummer zu konfigurieren:

(1) Wählen Sie bei **Eingehender Diensttyp** *ISDN-Login* aus. Alternativ könnte auch die Option *PPP-Einwahl* verwendet werden um eine IP-Verbindung zu ermöglichen.

(2) Bei **Fallback-Nummer** geben Sie die Telefonnummer ein, von der der UMTS-Fallback-Anruf eingeleitet wird, z. B. *+4991196731550*.

(3) Bestätigen Sie mit **OK**.

6.3 Test des UMTS Fallbacks mittels eingehender Sprachverbindung

Im Standardverhalten stellt das **bintec RS232bu+**-Gateway eine Internetverbindung über das UMTS-Netzwerk her. Durch einen Sprachanruf (Fallback-Rufnummer) bucht sich das Gateway in das GSM/GPRS-Netzwerk ein und ermöglicht eingehende Datenverbindungen.

Debug Meldungen beim UMTS-Fallback:

```
rs232bu+:> debug all &
10:49:56 INFO/MODEM: usbTTY0: PLMN Telekom.de(Home) LAC 44B2 CID 0002AA13 AcT UMTS
10:49:59 DEBUG/MODEM: usbTTY0: switch state P1 -> R0
10:49:59 DEBUG/USB: usbTTY0: serial state notification - ring ind.
10:49:59 INFO/MODEM: usbTTY0: Voice call from '+4991196731550' - activate GSM Fallback
10:49:59 DEBUG/PPP: T-Mobile - UMTS: event: "ifAdminStatus_down event",status: "initial / dormant" (dormant) ->
"interface down" (down)
10:49:59 DEBUG/MODEM: usbTTY0: Configured Access Mode 'UMTS-Pref'
10:49:59 INFO/MODEM: usbTTY0: Select PLMN 26201 ==> 26201/UMTS ==> GSM
10:49:59 DEBUG/MODEM: usbTTY0: Actual AcM 'GPRS-Only'
10:50:00 INFO/MODEM: usbTTY0: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:00 INFO/MODEM: usbTTY0: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:00 INFO/MODEM: usbTTY0: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:00 INFO/MODEM: usbTTY0: PLMN Telekom.de(Home) LAC 44B2 CID 0002AA13 AcT UMTS
10:50:00 DEBUG/PPP: T-Mobile - UMTS: event: "ifAdminStatus_up event",status: "interface down" (down) -> "initial /
dormant" (dormant)
10:50:01 DEBUG/MODEM: usbTTY3: Temperature: 52
10:50:05 INFO/MODEM: usbTTY0: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:05 INFO/MODEM: usbTTY0: PLMN Telekom.de(Home) LAC 44B2 CID 0002AA13 AcT UMTS
10:50:05 DEBUG/MODEM: usbTTY0: Network - Registration in progress
10:50:06 INFO/MODEM: usbTTY0: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:06 INFO/MODEM: usbTTY0: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:08 DEBUG/MODEM: usbTTY0: Network - Registration in progress
10:50:08 DEBUG/MODEM: usbTTY0: Network - Receive Signal Level -79 dB
10:50:08 INFO/MODEM: usbTTY0: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:08 INFO/MODEM: usbTTY0: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:09 INFO/MODEM: usbTTY0: Registered 26201 (T-Mobile D) (AcT = GSM)
10:50:09 INFO/MODEM: usbTTY0: PLMN T-Mobile D(Home) LAC 4427 CID 00001EA7 AcT GSM
```

6.4 Einwahl per ISDN-Login von einem anderen bintec ISDN-Gateway

Nachdem der UMTS-Fallback durchgeführt wurde und das **bintec RS232bu+**-Gateway im GSM/GPRS-Netzwerk registriert ist sind eingehende Datenverbindungen möglich. Hierzu muss auf der Anruferseite eine ISDN-Datenverbindung über das V.110-Protokoll initiiert werden. In diesem Kapitel wird von einem anderen bintec ISDN-Router eine ISDN-Login-Verbindung zur Fernwartung des **bintec RS232bu+**-Gateways aufgebaut. Nach dem Login können die bekannten Konsolen-Befehle wie z. B. das SetupTool zur Fernwartung verwendet werden.

```
------------------------------------------------------------
r3002:> isdnlogin 01713315981 v110_9600
Trying...
Establishing B-channel...
Connected to 01713315981

Connected to RS232bu+, rs232bu+,
from ISDN telephonnumber +4991196730 Service modem (9600 bps)



Welcome to RS232bu+ version V.7.10 Rev. 1 IPSec from 2011/08/02 00:00:00
systemname is rs232bu+, location


Login: admin
Password:

Password not changed. Call "setup" for quick configuration.

rs232bu+:> setup
------------------------------------------------------------
```

Debug-Meldungen während der eingehenden ISDN-Login-Verbindung:

```
rs232bu+:> debug all &
10:50:41 DEBUG/USB: usbTTY0: serial state notification - ring ind.
10:50:41 DEBUG/MODEM: usbTTY0: switch state P1 -> R0
10:50:41 INFO/MODEM: usbTTY0: Data call from '+4991196730' - data mode state incoming
10:50:41 DEBUG/MODEM: usbTTY0: Modem incomming call from <+4991196730>
10:50:41 DEBUG/PPP: dialin from <+4991196730> to local number <6001> (1/2)
10:50:41 INFO/ISDN: isdnlogind: accept call from <+4991196730>
10:50:41 DEBUG/MODEM: usbTTY0: switch state R1 -> A0
10:50:41 DEBUG/MODEM: usbTTY0: attach to channel 1 - incoming
10:50:43 INFO/MODEM: usbTTY0: Accept call from '+4991196730' ==> (CONNECT 9600)
10:50:43 DEBUG/MODEM: usbTTY0: switch state D1 -> D1
10:50:43 DEBUG/USB: usbTTY0: get DCD on (ch 3)
10:50:55 INFO/ACCT: LOGIN as admin from ISDNLOGIN +4991196730 at Mon Aug  1 10:50:55 2011
```

6.5 Konfigurationsschritte im Überblick

Konfiguration der UMTS-Internetverbindung

Feld	Menü	Wert
Verbindungstyp	**Assistenten** -> **Internetzugang** -> **Neu**	*UMTS*
Beschreibung	**Assistenten** -> **Internetzugang** -> **Weiter**	*T-Mobile - UMTS*
GPRS/ UMTS-Schnittstelle	**Assistenten** -> **Internetzugang** -> **Weiter**	*Slot 6 Einheit 0 UMTS*
Internet Service Provider	**Assistenten** -> **Internetzugang** -> **Weiter**	z. B. *T-Mobile - UMTS*
UMTS PIN	**Assistenten** -> **Internetzugang** -> **Weiter**	z. B. *0000*

Konfiguration der UMTS-Fallback-Nummer

Feld	Menü	Wert
Eingehender Diensttyp	**Physikalische Schnittstellen** -> **UMTS/ HSDPA** -> **UMTS/HSDPA/HSUPA** -> 	*ISDN-Login*
Fallback-Nummer	**Physikalische Schnittstellen** -> **UMTS/ HSDPA** -> **UMTS/HSDPA/HSUPA** -> 	z. B. *+4991196731550*