Carpobox I Anleitung

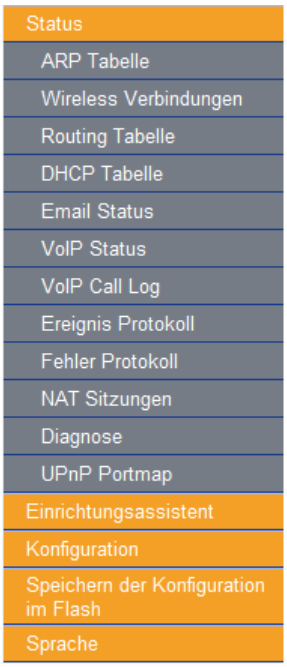
zum Konfigurationsmenü

Inhaltsverzeichnis:

carpo

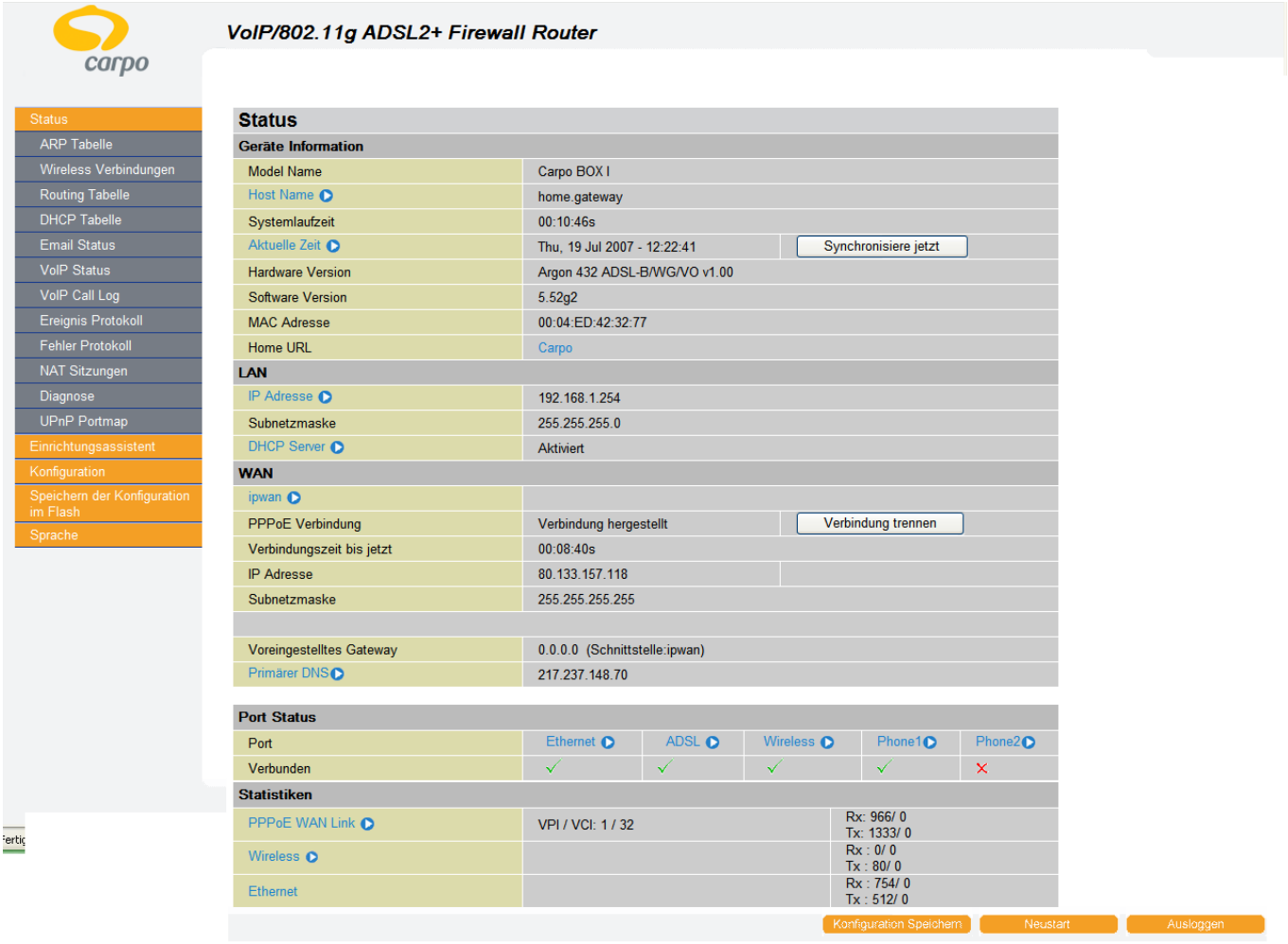
1. STATUS

Hier wird der allgemeine Status des Routers sowie der wichtigsten Dienste des Gerätes dargestellt. Um eine allgemeine Funktionalität zu prüfen, empfiehlt es sich immer erst die Stati zu prüfen.



Dieses Menü bietet folgende Untermenüs:

- **1.1 ARP Tabelle**
- **1.2 Wireless Verbindungen**
- **1.3 Routing**
- **1.4 DHCP Tabelle**
- **1.5 Email Status**
- **1.6 VoIP Status**
- **1.7 VoIP Call Log**
- **1.8 Ereignis Protokoll**
- **1.9 Fehler Protokoll**
- **1.10 NAT Sitzungen**
- **1.11 Diagnose**
- **1.12 UPnP Portmap**



Geräteinformationen

Model Name: Produktname des Gerätes
Host Name: Aliasname des Gerätes, alternativ kann dieser Name statt der IP-Adresse des Routers verwendet werden
Systemlaufzeit: Zeitraum seitdem der Router eingeschaltet und gestartet wurde
Aktuelle Zeit: Aktuelle Uhrzeit, wird automatisch mit einem NTP-Server (Network Time Protocol) im Internet synchronisiert
Hardware Version: Bezeichnung der verbauten Hardware im Router (nicht aktualisierbar!)
Software Version: Bezeichnung der aktuell installierten Firmware (kann aktualisiert werden)
MAC Adresse: Hardwareadresse des Routers (Media Access Control)
Homeurl: Verknüpfung zur Internetseite www.carpo.com

LAN (Local Area Network)

IP Adresse: Lokale IP-Adresse des Routers, zeitgleich ist dies der Gateway für alle angeschlossenen Computer/Geräte im lokalen Netzwerk
Subnetzmaske: Dazugehörige Subnetzmaske des lokalen Netzwerk
DHCP Server: Gibt an, ob der DHCP-Dienst im Router aktiviert werden soll. Ist der DHCP-Server aktiv, so können sich alle angeschlossenen Computer automatisch eine IP-Adresse vom Router beziehen

WAN (Wide Area Network)

ipwan: Verknüpfung zu den generellen Einstellungen der WAN Verbindung (siehe S. xx)
PPPoE Verbindung: Zeigt den derzeitigen Status der Onlineverbindung zum Internet Provider an
Verbindungszeit bis jetzt: Momentane Zeitdauer der Onlineverbindung
IP Adresse: Externe Internet Adresse des Routers (WAN IP-Adresse)
Subnetzmaske: Dazugehörige externe Subnetzmaske des Routers
Voreingestelltes Gateway: IP-Adresse des externen Gateway des Internet Providers, zu dem man sich eingewählt hat (0.0.0.0 bedeutet immer, dass die Adresse automatisch bezogen werden soll)
Primärer DNS: IP-Adresse des externen DSN-Servers (Domain Name System) des Internetproviders

Port Status

Port: Jeweilige Bezeichnung des Anschlusses am Router
Verbunden: Gibt an, ob am jeweiligen Anschluss ein Gerät verbunden wurde

Statistiken

PPPoE WAN Link: Gibt diverse Statistiken zur genutzten bzw. aktiven Leitung an, wie übertragene und empfangene Pakete

1.1. ARP Tabelle

Dieser Abschnitt behandelt die Routers ARP (Address Resolution Protocol) Tabelle, welche zu den entsprechenden Internet (IP) Adressen die zugehörige Ethernet (MAC) Adresse anzeigt. Diese ist sehr nützlich um die MAC Adressen der angeschlossenen PCs für die Funktionen Firewall – MAC Adressen Filter zu nutzen. Lesen Sie weitere Informationen darüber im Abschnitt Firewall in dieser Anleitung. Bitte beachten Sie, dass die aufgeführte Tabelle nur zur Erläuterung aufgeführt ist und von Ihrer abweicht.

ARP Tabelle

IP <> MAC Liste

IP Adresse	MAC Adresse	Schnittstelle	Statisch
192.168.1.100	00:0b:6a:ae:c7:a1	iplan	no

IP Adresse: Eine Liste von IP Adressen Ihrer Geräte im LAN (Local Area Network).

MAC Adresse: Die MAC (Media Access Control) Adresse für jedes Gerät in Ihrem LAN.
Schnittstelle: Der Name der Schnittstelle (am Router) wo diese IP verbunden ist.
Statisch: Status des ARP Tabelleneintrages:

- "**no**" für dynamisch-generierte ARP Tabelleneinträge
- "**yes**" für statische ARP Tabelleneinträge die vom Benutzerhinzugefügt worden sind

1.2. Wireless Verbindungen

Hier werden die derzeit über WLAN verbundenen Endgeräte im lokalen Netzwerk angezeigt.

Wireless Verbindungstabelle

MAC Adresse des Wireless Client und die dazugehörige IP Adresse

IP Adresse	MAC

IP Adresse: Die IP Adresse des Wireless Clients der diesem Netzwerk angeschlossen ist
MAC: Die MAC-Adresse (Media Access Control) des Wireless Client

1.3. Routing Tabelle

Es werden alle generellen Routings von kompletten IP Bereichen der Carpobox aufgelistet.

Routing Tabelle

Routing Tabelle

Gültig	Ziel	Netzmaske	Gateway/Schnittstelle	Kosten
✓	0.0.0.0	0.0.0.0	0.0.0.0/ ipwan	1

RIP Routing Tabelle

Ziel	Netzmaske	Gateway	Kosten
0.0.0.0	0.0.0.0	0.0.0.0	1

Routing Tabelle

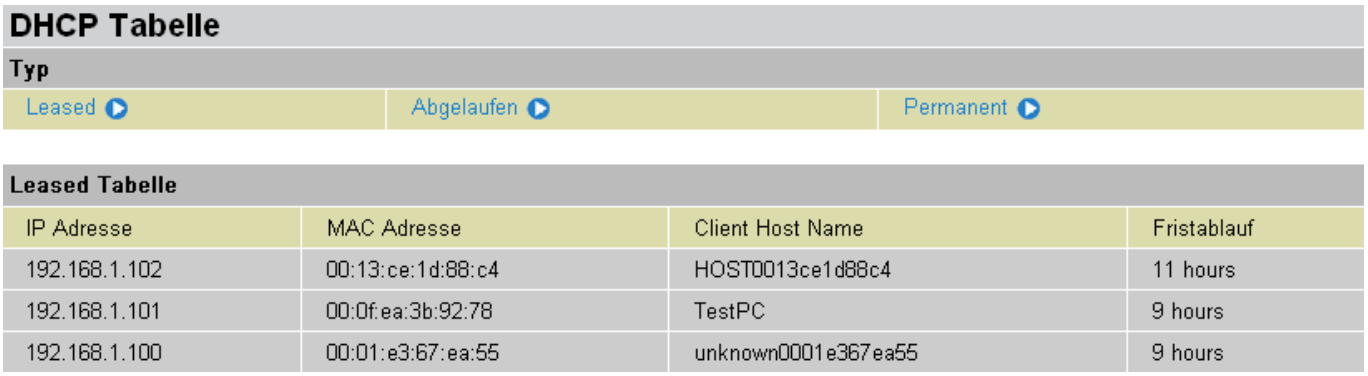
Gültig: Zeigt einen erfolgreichen Routing Status an.
Ziel: Die IP Adresse des Ziel Netzwerk.
Netzmaske: Die Ziel Netzmaske Adresse.
Gateway/Schnittstelle: Die IP Adresse des Gateway oder Schnittstelle die diese Route benutzt
Kosten: Die Anzahl der Hops zählt als Kosten der Route

RIP Routing Tabelle

Ziel: Die IP Adresse des Ziel Netzwerk
Netzmaske: Die Ziel Netzmaske Adresse
Gateway: Die IP Adresse des Gateway welches diese Route benutzt
Kosten: Die Anzahl der Hops zählt als Kosten der Route

1.4. DHCP Tabelle

Hier werden alle verbundenen Geräte (LAN + WLAN) im lokalen Netzwerk aufgelistet, die sich automatisch vom Router eine IP-Adresse bezogen haben.



Mit einem Klick auf die jeweiligen Kategorien, kann die DHCP Tabelle nach folgenden Kriterien gefiltert werden:

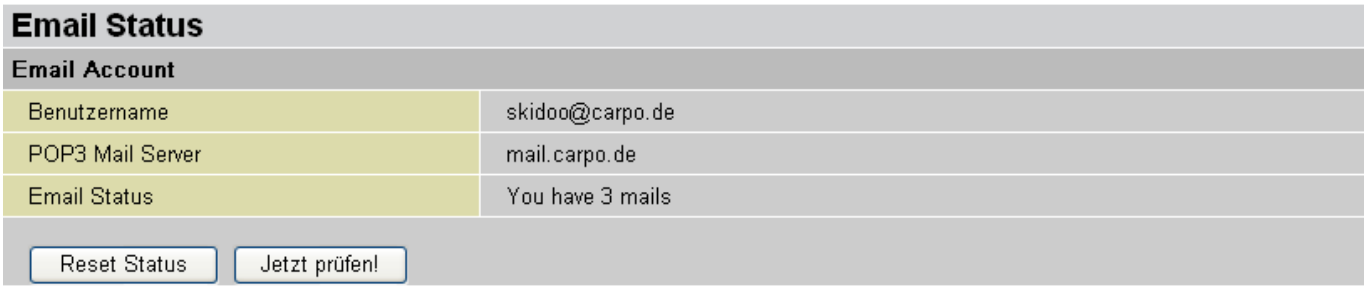
Leased: Informationen zu den derzeitigen IP Adressen, die durch den DHCP Server zugewiesen wurden
Abgelaufen: Informationen zu den abgelaufenen IP Adressen
Permanent: Informationen zu durch die MAC-Adressen fest zugewiesenen IP-Adressen

Diese zeigen Aufschluss über die folgenden Geräteeigenschaften:

IP Adresse: Zugehörige IP-Adresse des Gerätes im LAN
MAC Adresse: Zugehörige MAC-Adresse des Gerätes im LAN
Client Host Name: Zugehöriger Gerätename im LAN, der alternativ zur IP-Adresse verwendet werden kann
Fristablauf: Nach Ablauf dieser Frist, weist der DHCP Server dem Gerät eine neue (ggf. jedoch gleiche) IP-Adresse zu

1.5. Email Status

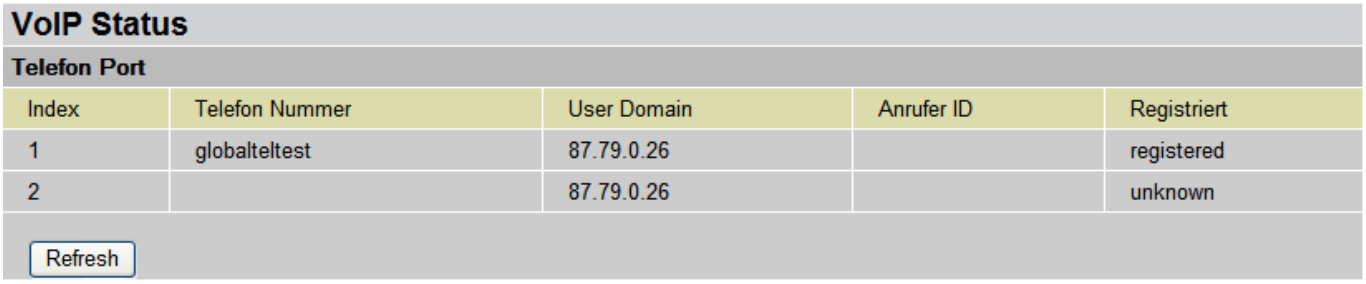
Wurde eine Email Adresse unter **[KONFIGURATION] → [ERWEITERT] → [PRÜFE EMAIL]** konfiguriert, so werden hier die neuen Mails auf dem eingestellten Mailserver angegeben.



ACHTUNG: Die Mails werden nur angezeigt, jedoch nicht vom Router abgerufen. Um die Mails lesen zu können, ist es notwendig, diese mit einem Email Client herunterzuladen!

1.6. VoIP Status

Hier wird der aktuelle Registrierungsstatus der konfigurierten VoIP-Ports 1 und 2 angezeigt.



VoIP Status

Telefon Port

Index	Telefon Nummer	User Domain	Anrufer ID	Registriert
1	globalteltest	87.79.0.26		registered
2		87.79.0.26		unknown

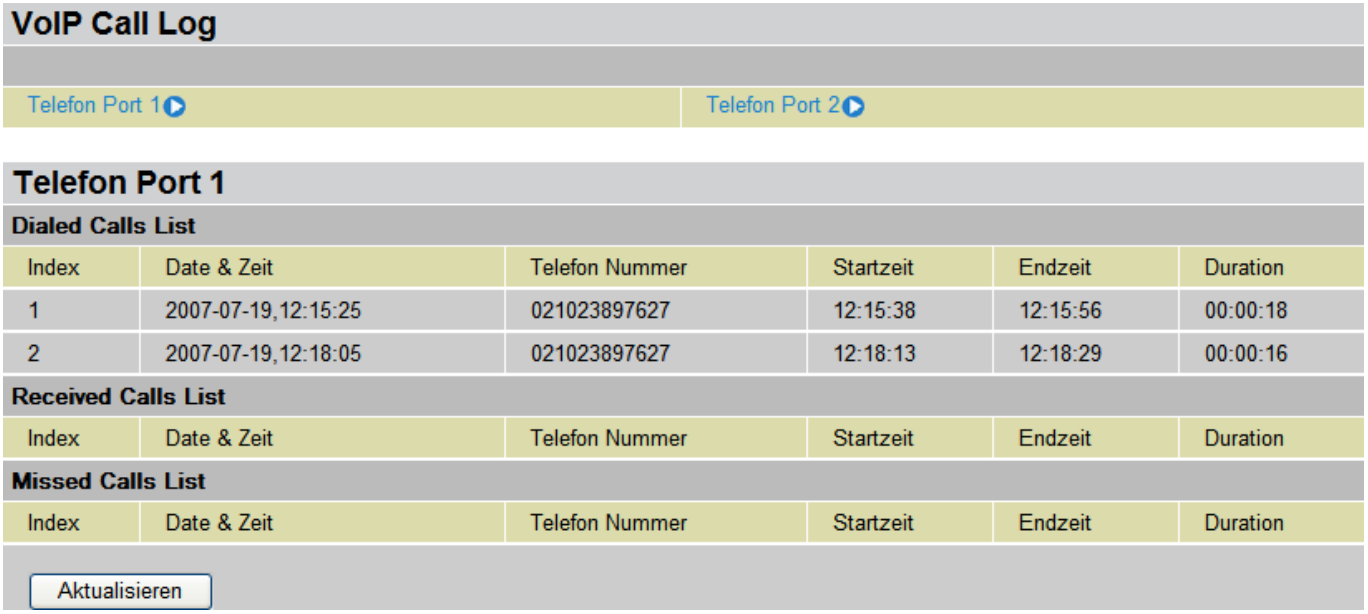
Refresh

Folgende Stati sind möglich und haben meist die genannten Angaben zur Ursache:

Registered: erfolgreich angemeldet
Authfailure: falscher Benutzername/Passwort
Unknown: keine oder falsche Benutzerdaten eingegeben

1.7. VoIP Call Log

Hier werden sämtliche Telefonate aufgelistet, die über das Internet (VoIP) geführt worden. Diese Liste lässt sich nach den jeweilig genutzten Telefonports 1 oder 2 filtern, so dass nur dementsprechend betroffene Verbindungen dargestellt werden.



VoIP Call Log

Telefon Port 1 | Telefon Port 2

Telefon Port 1

Dialed Calls List

Index	Date & Zeit	Telefon Nummer	Startzeit	Endzeit	Duration
1	2007-07-19,12:15:25	021023897627	12:15:38	12:15:56	00:00:18
2	2007-07-19,12:18:05	021023897627	12:18:13	12:18:29	00:00:16

Received Calls List

Index	Date & Zeit	Telefon Nummer	Startzeit	Endzeit	Duration

Missed Calls List

Index	Date & Zeit	Telefon Nummer	Startzeit	Endzeit	Duration

Aktualisieren

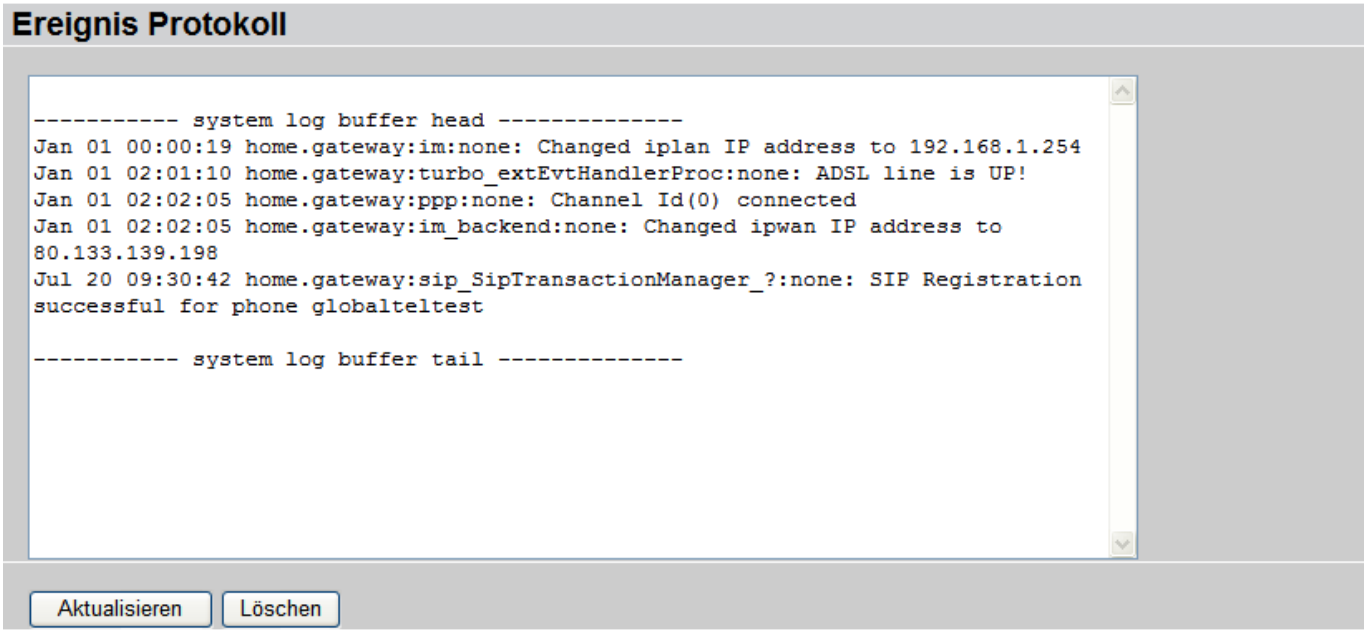
Dialed Calls List: Liste der gewählten Nummern, ausgehendende Verbindungen
Received Calls List: Liste der empfangenen Nummern, eingehende Verbindungen
Missed Calls List: Liste der empfangenen Anrufe in Abwesenheit, eingehende Verbindungen

Diese Listen zeigen Aufschluss über folgende Informationen:

Index: Fortlaufende Zahl, Indizierung der geführten Gespräche
Date & Zeit: Datum und Uhrzeit der jeweiligen Verbindung
Telefon Nummer: Rufnummer der jeweiligen Gegenstelle
Startzeit: Uhrzeit zu dem die Verbindung aufgebaut wurde
Endzeit: Uhrzeit zu dem die Verbindung beendet wurde
Duration: Dauer der Verbindung

1.8. Ereignis Protokoll

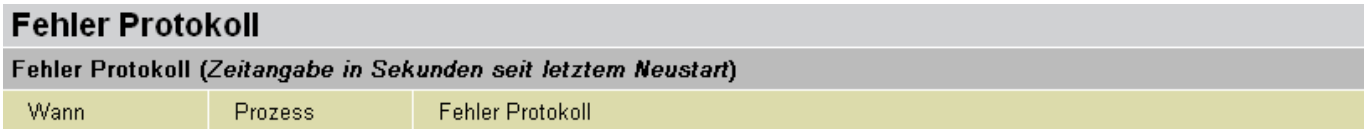
Diese Seite zeigt die Router Ereignisanzeige an. Wichtige System-Protokollierungs-Informationen sind dort vorhanden, wie ADSL Verbindung abgebrochen, Firewall Events wenn Sie dies in der Firewall Konfiguration für diesen Router aktiviert haben. Für weitere Hinweise schauen Sie im Abschnitt [FIREWALL] nach um Firewall Logging zu aktivieren.



Die Liste lässt sich auf Wunsch manuell aktualisieren sowie komplett löschen. Bei jedem Neustart des Routers wird die Liste ebenfalls komplett gelöscht.

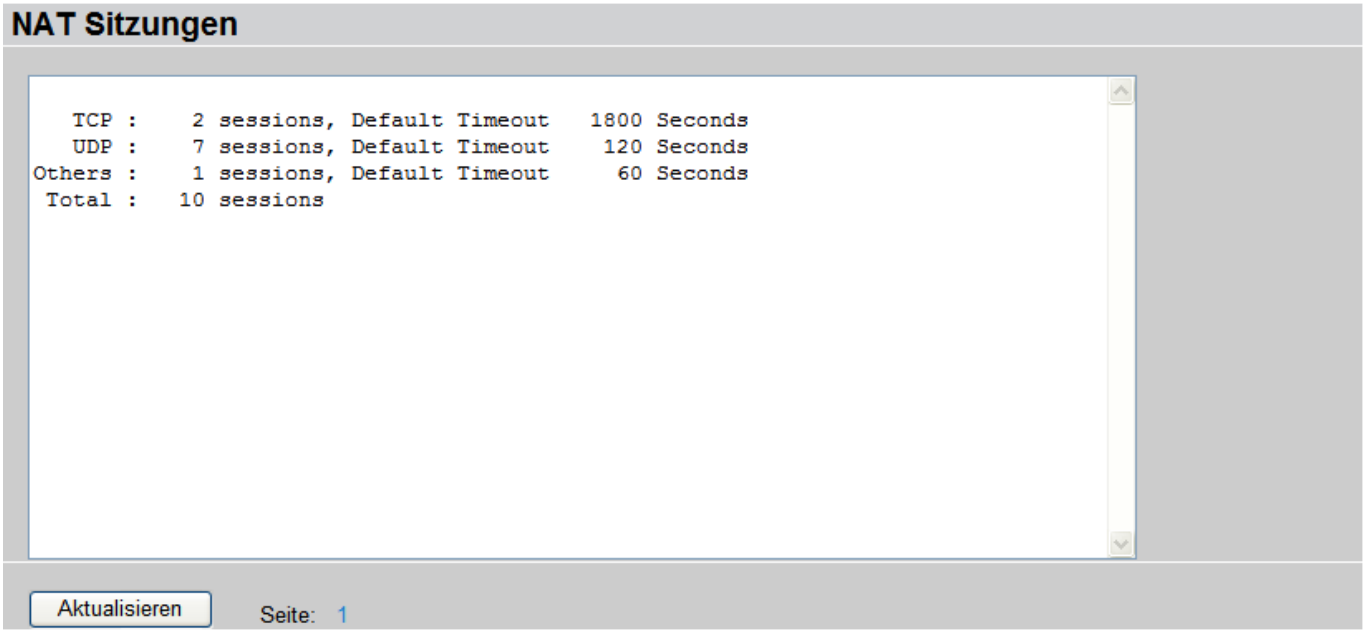
1.9. Fehler Protokoll

Jegliche Fehler die der Router feststellt werden in diesem Fenster gespeichert. (z.B.: ungültige Namenseinträge).

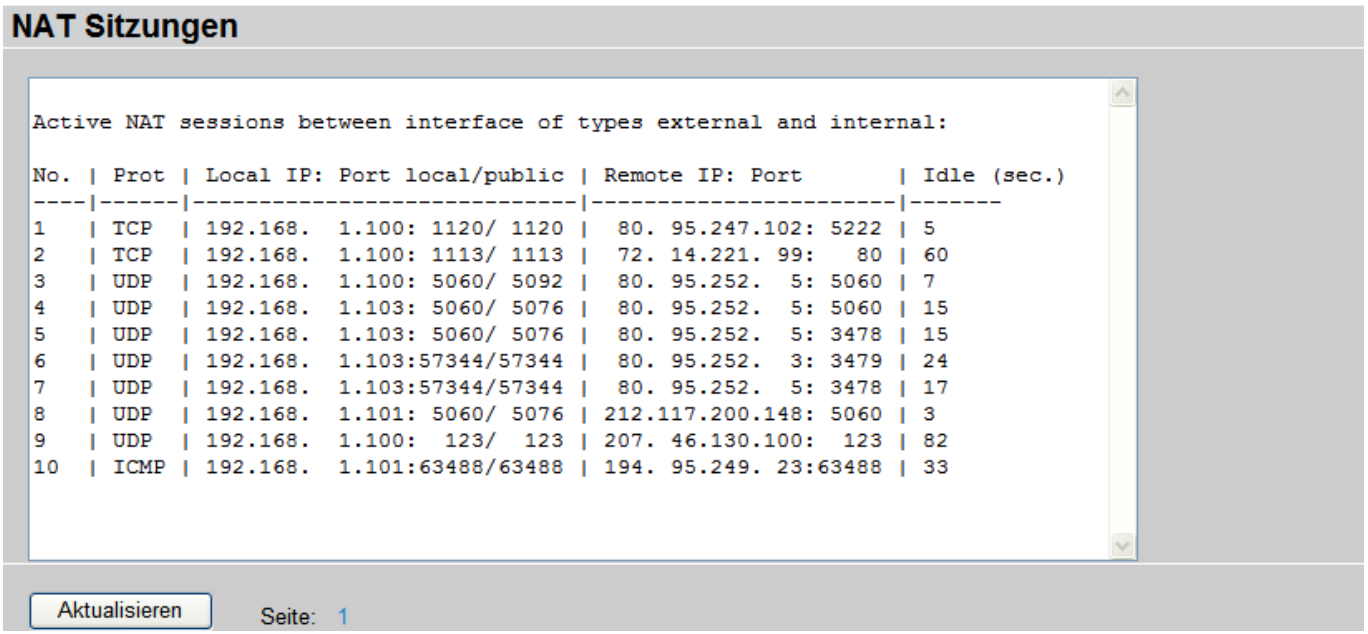


1.10. NAT Sitzungen

Hier werden alle derzeitigen Sitzungen/Verbindungen zwischen internen Geräten (LAN) und dem Internet (WAN) aufgelistet. Diese werden noch nach verwendetem Protokoll (TCP/UDP/Andere) unterteilt.



Mit einem Klick auf **[SEITE 1]** erhält man eine detaillierte Übersicht der Verbindungen:



Die Informationen werden wie folgt aufgeschlüsselt:

No.: Fortlaufende Index-Nummer der Verbindung
Prot.: Verwendetes Netzwerkprotokoll
Local IP: IP-Adresse des lokalen Gerätes, welches eine Verbindung aufgebaut hat
Port local/public: Verwendeter interner (local) Port sowie der nach außen (public) ins Internet verwendete Port
Remote IP: WAN IP-Adresse der Gegenstelle zu dem ein lokales Gerät eine Verbindung hergestellt hat
(Remote) Port: Dazugehörige externe WAN Port der Gegenstelle zu dem eine Verbindung hergestellt wurde
Idle: Leerlaufzeit seit dem das letzte Datenpaket übertragen wurde

1.11. Diagnose

Es werden verschiedene Verfahren zur allgemeinen Leitungs- bzw. Zugangsdiagnose des Routers durchgeführt:

Diagnose

LAN Verbindung	
Test Ethernet LAN Verbindung	BESTANDEN
Test Wireless LAN Verbindung	BESTANDEN
WAN Verbindung	
Test ADSL Synchronisation	BESTANDEN
Test WAN Verbindung	BESTANDEN
Ping Primären Domain Name Server	BESTANDEN
PING www.google.com	BESTANDEN

Aktualisieren

Folgende Details verbergen sich hinter den jeweiligen Tests:

LAN Verbindung

Test Ethernet LAN Verbindung: Prüft die interne Funktionalität der LAN-Anschlüsse

Test Wireless LAN Verbindung: Prüft die interne Funktionalität der WLAN-Verbindung

WAN Verbindung

Test ADSL Synchronisation: Prüft, ob eine Synchronisation mit der Vermittlungsstelle (DSLAM) erfolgreich durchgeführt wurde

Test WAN Verbindung: Prüft, ob eine erfolgreiche Verbindung anhand von Benutzername und Passwort zum Internet Provider aufgebaut wurde

Ping Primären Domain Name Server: Prüft anhand einiger Testdatenpakete ob eine Verbindung zum derzeitig zugewiesenen DNS-Server besteht

PING www.google.com: Prüft anhand einiger Testpakete, ob der DNS-Server korrekt arbeitet und der Hostname (www.google.com) in eine gültige IP-Adresse umgewandelt werden kann (z.B. 209.85.135.147)

1.12. UPnP Portmap

Bestimmte Programme und Dienste benötigten eigene Ports für die Kommunikation ins Internet. Wird dabei die Funktion Universal Plug'n'Play (UPnP) unterstützt, so handelt die Software bzw. der Client mit dem Router direkt ungenutzte Ports aus und weist diese entsprechend dem lokalen Gerät zu. Wird die Software bzw. der Dienst beendet, schließen sich die genutzten Ports wieder selbständig.

Die Liste gibt Aufschluss über die bisher durch UPnP automatisch zugewiesenen Ports Auskunft.

UPnP Portmap

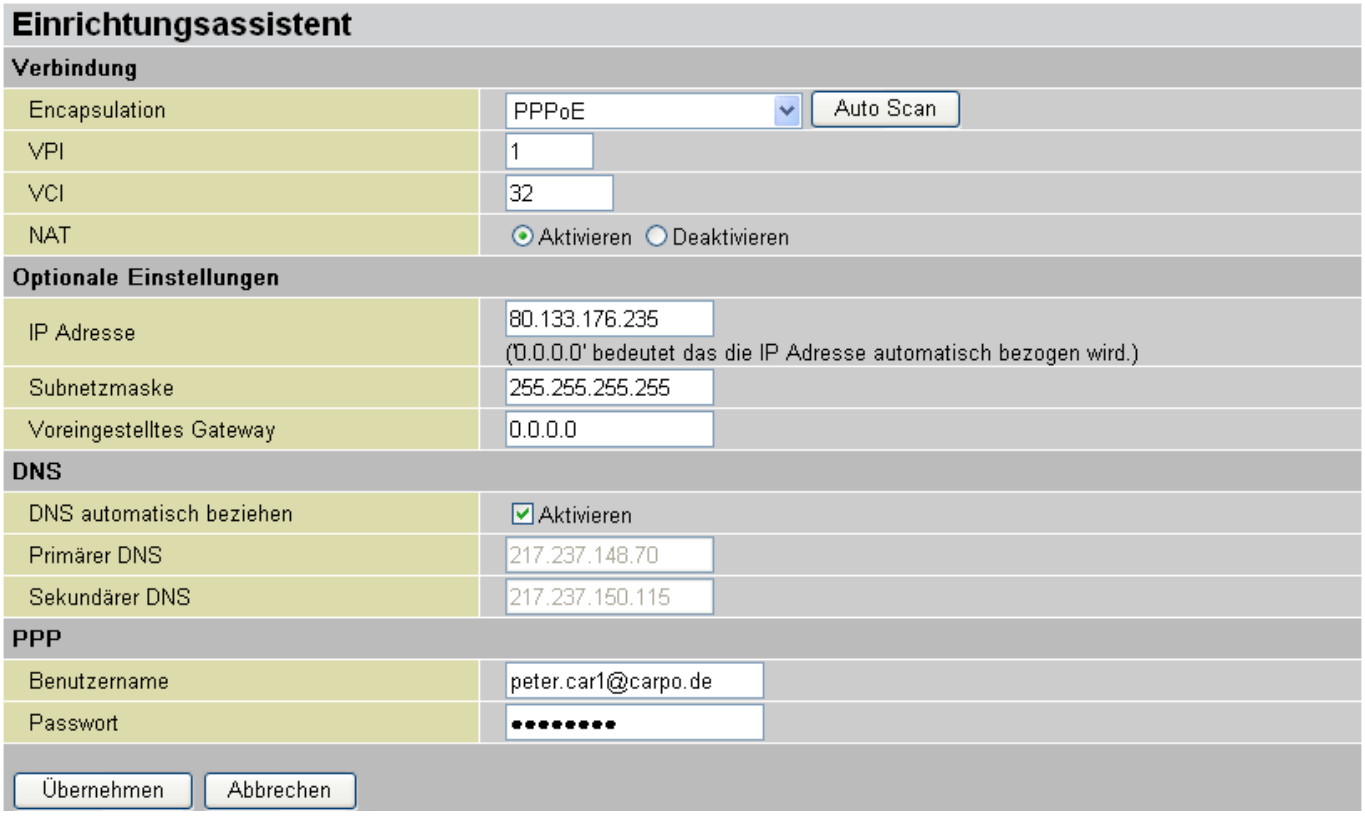
UPnP Portmap Tabelle

Name	Protokoll	Externer Port	Umgeleiteter Port	IP Adresse
item0	17	5062	5062	192.168.1.101
item1	17	5064	5064	192.168.1.101
item2	17	30000	30000	192.168.1.101
item3	17	30001	30001	192.168.1.101
item4	17	30002	30002	192.168.1.101
item5	17	30003	30003	192.168.1.101
item6	17	30004	30004	192.168.1.101

2. Einrichtungsassistent

Der Einrichtungsassistent bietet die wichtigsten Einstellungsmöglichkeiten für den DSL-Zugang zum Internet Service Provider (ISP).

- Hierbei werden im Regelfall lediglich Benutzername und Passwort benötigt
- Wurde vom Provider eine feste Internet IP-Adresse vergeben, so muss diese ebenfalls angegeben werden



Folgende Funktionen können über den Einrichtungsassistent eingestellt werden:

Verbindung

Encapsulation: Art der Verkapslung der Internetleitung, abhängig vom ISP

Auto Scan: Bietet die Möglichkeit die Kapslung der Leitung automatisch zu erkennen, wenn diese nicht bekannt ist. Genaue Informationen zu dieser Funktion sind im Abschnitt **[2.1 Auto Scan]** dokumentiert

VPI: Virtual Path Identifier, wird vom ISP vorgegeben

VCI: Virtual Channel Identifier, wird vom ISP vorgegeben

NAT: Network Address Translation, Netzwerkadressübersetzung zwischen dem Internet (WAN) und den internen Netzwerk (LAN). Wird die Funktion deaktiviert, so kann kein lokales Gerät mehr auf das Internet zugreifen und muss dazu seine eigene Verbindung aufbauen

Optionale Einstellungen

IP Adresse: Externe WAN IP-Adresse des ISP, ein leeres bzw. mit **0.0.0.0** ausgefülltes Feld bedeutet, dass die IP-Adresse automatisch nach der Einwahl bezogen wird

Subnetzmaske: Dazugehörige Subnetzmaske der externen IP-Adresse, im Regelfall ist dies immer **255.255.255.255**

Voreingestelltes Gateway: Externe IP-Adresse vom Gateway des ISP, wird in der Regel automatisch vergeben. Ein leeres bzw. mit **0.0.0.0** ausgefülltes Feld bedeutet, dass die IP-Adresse automatisch nach der Einwahl bezogen wird

DNS (Domain Name Service)

DNS Automatisch beziehen: Gibt an, ob die externe IP-Adresse des genutzten DNS-Servers automatisch nach der Einwahl vom ISP bezogen werden soll

Primärer DNS: Gibt die externe IP-Adresse des primären DNS-Servers an

Sekundärer DNS: Gibt die externe IP-Adresse des sekundären DNS-Servers an, dieser wird genutzt, wenn der primäre DNS-Server ausfällt bzw. nicht antwortet

HINWEIS: Ist das Feld **[DNS Automatisch beziehen]** aktiviert, so werden die Felder **[Primärer DNS]** und **[Sekundärer DNS]** automatisch deaktiviert!

2.1. Auto Scan

Ist die Protokollart des verwendeten Internet Service Providers nicht bekannt, so kann diese automatisch erkannt werden. Hierzu bietet der Einrichtigungsassistent die Funktion [Auto Scan].

Nach einem Klick auf **[Auto Scan]** müssen bei Verwendung einer festen externen WAN IP-Adresse sowie eines festen WAN-Gateways diese Adressen angegeben werden. Wird die WAN IP-Adresse sowie der Gateway automatisch vom ISP zugewiesen, so können die Felder leer bleiben. Der Auto Scan beginnt anschließend mit einem Klick auf **[Start]**.

Anschließend wird die erkannte Kapslungsart der Verbindung ins Internet aufgelistet, welche mit einem Klick auf **[Übernehmen]**:

3. Konfiguration

(Diese Funktionen können teilweise nicht beim Standarduser aufgerufen werden)
Wenn Sie dieses Feld anklicken, erhalten Sie folgendes Untermenü, um den Router zu konfigurieren.

- **3.1 LAN**
- **3.2 WAN**
- **3.3 System**
- **3.4 Firewall**
- **3.5 VoIP**
- **3.6 QoS**
- **3.7 Virtual Server**
- **3.8 Zeitplan**
- **3.9 Erweitert**

Untermenüs:

3. Konfiguration

3.1.LAN
- 3.1.1. Bridge Schnittstelle
- 3.1.2. Ethernet
- 3.1.3. IP Alias
- 3.1.4. Ethernet Client Filter
- 3.1.5. Wireless
- 3.1.6. Wireless Sicherheit
- 3.1.7. Wireless Client Filter
- 3.1.8. Port Einstellungen
- 3.1.9. DHCP Server

3.2. WAN
- 3.2.1. ISP
- 3.2.2. DNS
- 3.2.3. ADSL

3.3. System
- 3.3.1. Zeitzone
- 3.3.2. Remote Zugriff
- 3.3.3. Firmware Upgrade
- 3.3.4. Sichern/Wiederherstellen
- 3.3.5. Neustart
- 3.3.6. Benutzer Verwaltung

3.4. Firewall
- 3.4.1. Generelle Einstellungen
- 3.4.2. Paket Filter
- 3.4.3. Angriffserkennung
- 3.4.4. URL Filter
- 3.4.5. IM/P2P Blocking
- 3.4.6. Firewall Protokoll

3.5. VoIP
- 3.5.1. Assistent
- 3.5.2. Generelle Einstellungen
- 3.5.3. Telefon Port
- 3.5.4. PSTN Dial Plan
- 3.5.5. VoIP Wählplan
- 3.5.6. Anruffunktionen
- 3.5.7. Klingeln & Rufton

3.6. QoS
- 3.6.1. Priorisation
- 3.6.2. IP Throttling ausgehend
- 3.6.3. IP Throttling eingehend

3.7. Virtual Server

3.8. Zeitplan

3.9. Erweitert
- 3.9.1. Statische Route
- 3.9.2. Dynamischer DNS
- 3.9.3. Prüfe Email
- 3.9.4. Geräte Management
- 3.9.5. IGMP
- 3.9.6. VLAN Bridge

3.1 LAN (Local Area Network)

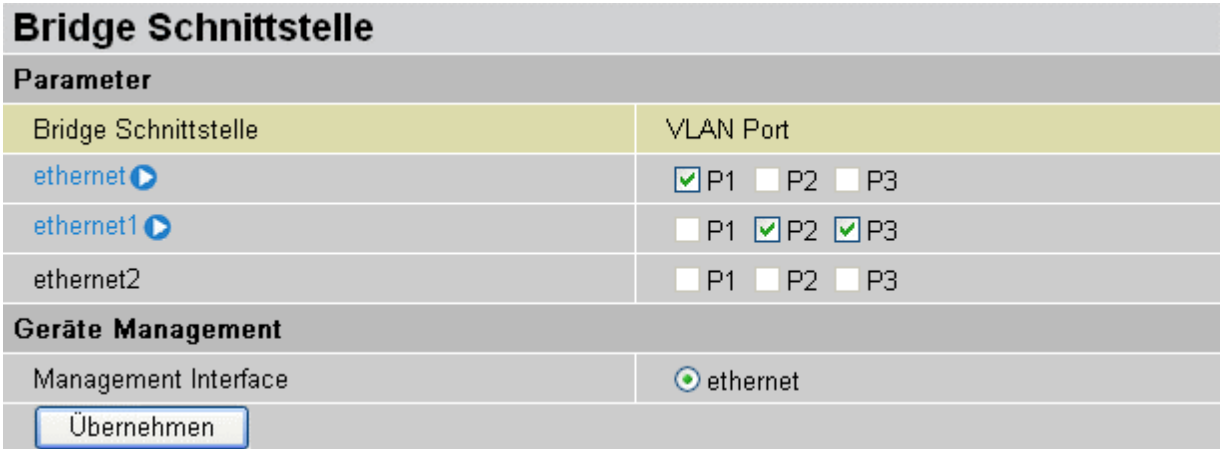
Alle am Router, auch per WLAN, angeschlossenen Geräte befinden sich zunächst in einem gemeinsamen lokalen Netzwerk. Somit können diese Geräte untereinander kommunizieren. Der Router stellt mit seiner Funktion die Brücke in andere Netze (Internet) dar. Sämtliche Einstellungen in dieser Kategorie beziehen sich auf das lokale Netzwerk.

3.1.1. Bridged Schnittstelle

Diese Konfiguration ermöglicht es, die jeweiligen physikalischen LAN-Anschlüsse des Routers zu einer sog. VLAN-Gruppe (Virtual LAN) zusammenzufassen. Im folgenden Beispiel werden 2 VLAN-Gruppen erstellt:

- Ethernet: P1 (Port1 am Router)
- Ethernet1: P2, P3 (Port2 und Port3 am Router)

HINWEIS: Hierbei müssen P2 und P3, welche ursprünglich in der Gruppe „Ethernet" waren, zuvor deaktiviert werden, bevor sie einer neuen Gruppe zugewiesen werden können!



Es können immer nur VLAN-Gruppen nach folgenden Kriterien erstellt werden:

Bridge Schnittstelle	VLAN Port (Startet immer mit)
Ethernet	P1 / P2 / P3
Ethernet1	P2 / P3
Ethernet2	P3

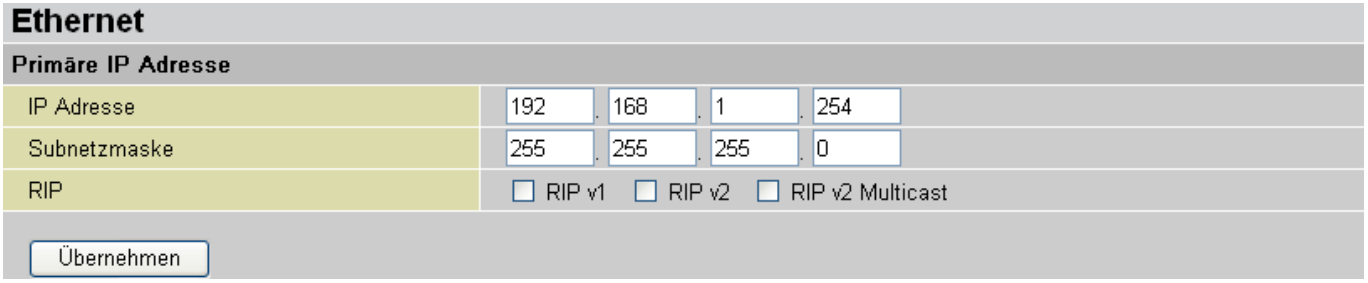
Management Schnittstelle: Hier wird angegeben, welche VLAN Gruppe den Router verwalten darf

Weitere Informationen zur Erstellung von VLANs sind im Abschnitt **[ERWEITERT → VLAN BRIDGE]** erläutert.

3.1.2 Ethernet

Hier kann die lokale IP-Adresse des Routers eingestellt werden. Diese Adresse stellt dann für alle im LAN befindlichen Clients den Gateway sowie den DNS-Server dar. Der Router erhält die Anfragen von den Lokalen Geräten und leitet diese stellvertrentend ins Internet weiter, zeitgleich teilt er jede Antwort aus dem Internet, dem Gerät zu, welches die Anfrage hierfür gestellt hat.

Werksseitig verwendet der Router die lokale IP-Adresse 192.168.1.254

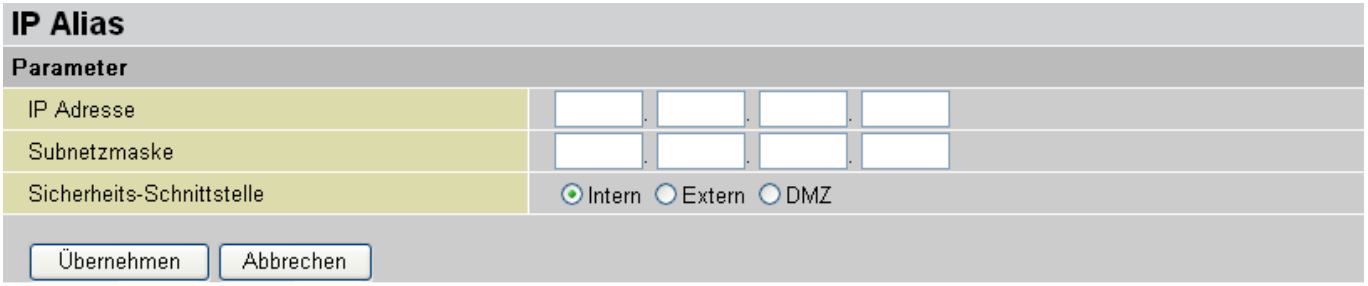


Der Router unterstützt das Routing Information Protocol (RIP), welches bei Bedarf aktiviert werden kann. Beim Starten eines Routers kennt dieser nur seine direkt angeschlossenen Netzwerke und sendet diese Routingtabelle an die benachbarten Router. Mit diesen Informationen ergänzt dieser Router seine Routingtabelle und lernt somit, welche Netzwerke jeweils über welchen Router aus erreicht werden können (bei Einsatz mehrerer Router und mehrerer LANs).

3.1.3. IP Alias

Der Router bietet die Möglichkeit bis zu acht zusätzliche LAN IP-Adresse zu generieren, über die auf das Gerät zugegriffen werden kann. Dies ist nützlich, wenn die mit dem Router verbundenen Geräte in unterschiedliche lokale IP-Netze aufgeteilt sind (z.B. 192.168.0.x und 192.168.1.x).

Über den Button [HINZUFÜGEN] kann ein neuer IP-Alias hinzugefügt werden:



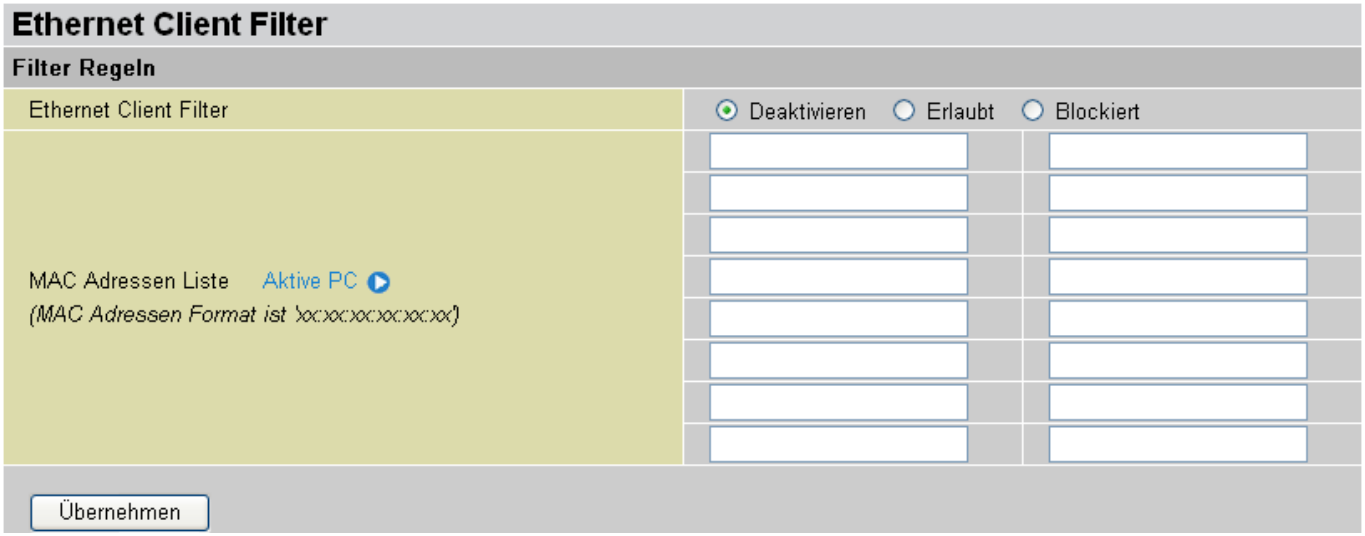
Folgende Einstellungen können hierbei getätigt werden:

IP Adresse: Zusätzliche LAN-IP unter welcher der Router erreicht werden kann
Subnetzmaske: Zusätzliche dazugehörige Subnetzmaske
Sicherheits-Schnittstelle:

3.1.4 Ethernet Client Filter

Der Ethernet Client Filter unterstützt bis zu 16 Ethernet Geräte, welche anhand der MAC-Adresse identifiziert werden. Dies hilft das Netzwerk zu administrieren bzw. zu kontrollieren, damit nur bestimmte Geräte Ihr LAN nutzen bzw. nicht nutzen dürfen.

Ethernet Client Filter: In der Werkseinstellung sind die Filter deaktiviert



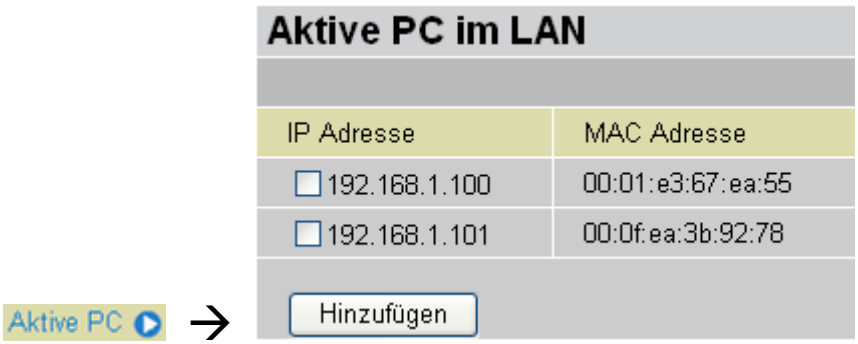
- **Erlaubt:** Autorisierte Geräte erhalten Zugriff auf das LAN-Netzwerk, indem die MAC Adresse eintragen oder das Gerät über [AKTIVE PC] ausgewählt wird. Vergewissern Sie sich das Ihr PC mit der MAC Adresse gelistet ist.

- **Blockiert:** Nicht autorisierte Geräte erhalten keinen Zugriff auf das LAN-Netzwerk, indem die MAC Adresse eintragen oder das Gerät über [AKTIVE PC] ausgewählt wird. Vergewissern Sie sich das Ihr PC mit der MAC Adresse nicht gelistet ist.

Hinweis: Folgen Sie diesem MAC Adressen Format xx:xx:xx:xx:xx:xx. Doppelpunkt (:) muss angegeben werden

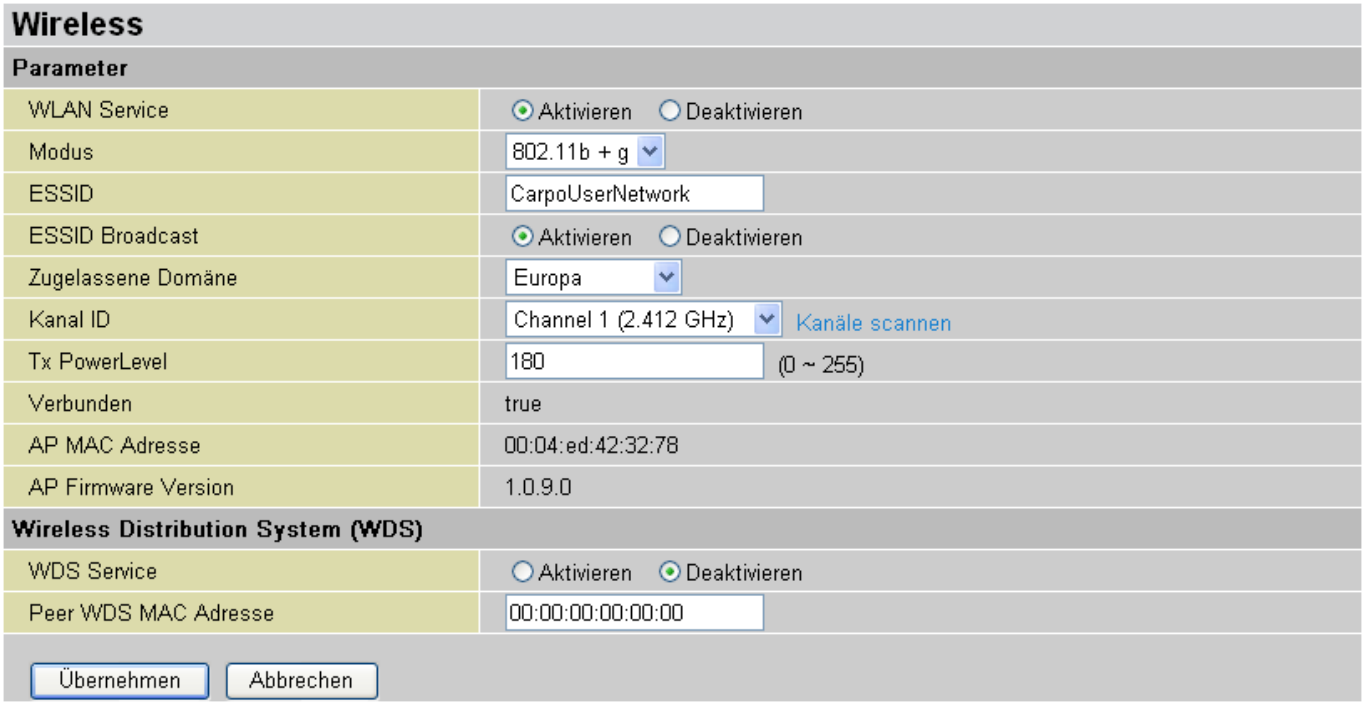
- Die maximale Anzahl beträgt 16 Clients
- Die MAC Adressen sind 6 Bytes lang und nur im Hexadezimalen Format angegeben
- Die Zahlen 0 – 9 werden akzeptiert
- Buchstaben a - f werden akzeptiert

Aktive PC: Alle Geräte, welche über Ethernet mit dem Router verbunden sind, werden hier automatisch mit IP- sowie MAC-Adresse angezeigt. Mit einem Klick auf die jeweilige Adresse wird diese ausgewählt



3.1.5 Wireless

Hier können die grundlegenden Einstellungen für das Wireless LAN (WLAN) getätigt werden.



Parameter:

WLAN Service: Die WLAN-Funktion kann hier grundlegend de-/aktiviert werden

Modus: Der jeweilige WLAN-Standard lässt sich hier auswählen
- 802.11b
- 802.11g
- 802.11b+g

ESSID: Name des WLAN-Netzes

HINWEIS: Die Groß- und Kleinschreibung wird beim WLAN beachtet. Die ESSID darf nicht mehr als 32 Zeichen haben. Es ist sicherzustellen, dass die Wireless Clients die identische ESSID verwenden, damit diese sich mit dem Netzwerk verbinden können.

ESSID Broadcast:
- aktiviert: Name des WLAN wird öffentlich angezeigt
- deaktiviert: Name des WLAN wird nicht öffentlich angezeigt

Zugelassene Domäne: Je nach Land gibt es andere Funkfrequenz, die genutzt werden dürfen. Hier lässt sich das entsprechende Land einstellen, nach dem anschließend die zur Verfügung stehenden Frequenz-Kanäle unter **[Kanal ID]** aufgelistet werden

Kanal ID: Nutzbare Frequenzen in der Funkübertragung werden in Kanäle unterteilt, hier lässt sich der jeweilig zu nutzende Frequenzkanal einstellen. Über die Funktion [Kanäle scannen] können bereits genutzte Frequenzkanäle, z.B. durch die Nachbarschaft, herausgefiltert werden.

HINWEIS: Werden manche Kanäle bereits genutzt, z.B. durch einen anderen WLAN-Router in der Nachbarschaft, so empfiehlt es sich immer einen Kanal zwischen diesem und dem eigens genutzten Kanal freizulassen.

Tx PowerLevel: Die Stärke des Übertragungssignals lässt sich in 256 Abstufungen justieren und kann bei Bedarf herunter geregelt werden

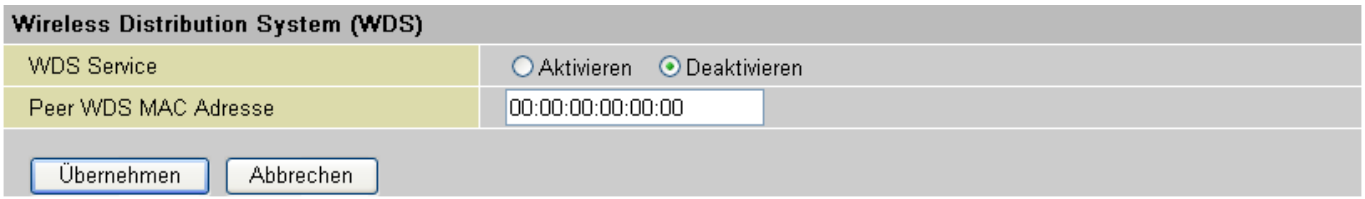
AP MAC Adresse: Hardware MAC-Adresse des Accesspoints (WLAN Router)

AP Firmware Version: Aktuelle Firmware-Version des Accesspoints (WLAN Router)

Wireless Distribution System (WDS)

Dies ist ein Modus des Wireless Access Points, welcher einen Wireless Link und die Kommunikation zu einem anderen Access Point herstellt. Diese Funktion ist einfach zu verwenden, indem Sie die MAC Adresse des anderen Access Points eintragen. WDS erspart Ihnen die Verwendung einer separaten Wireless Bridge. Sie können ohne weitere Verkabelung das Netzwerk ausbauen.

HINWEIS: Zusätzlich kann die Sicherheit mittels WEP-Verschlüsselung gewährleistet werden. Der eingesetzte WEP-Schlüssel muss auf beiden Access Points identisch sein. Bei Verwendung einer WPA-Verschlüsselung ist es nicht möglich das Wireless Distribution System einzusetzen!



WDS Service: Werksseitig ist die Funktion deaktiviert und kann hier aktiviert werden

Peer WDS MAC Adresse: Die MAC Adresse des zu verbindenden Access Points. Es ist wichtig, dass der andere Access Point die MAC Adresse dieses Routers eingetragen hat, damit eine Authentifizierung und somit eine Verbindung hergestellt werden kann.

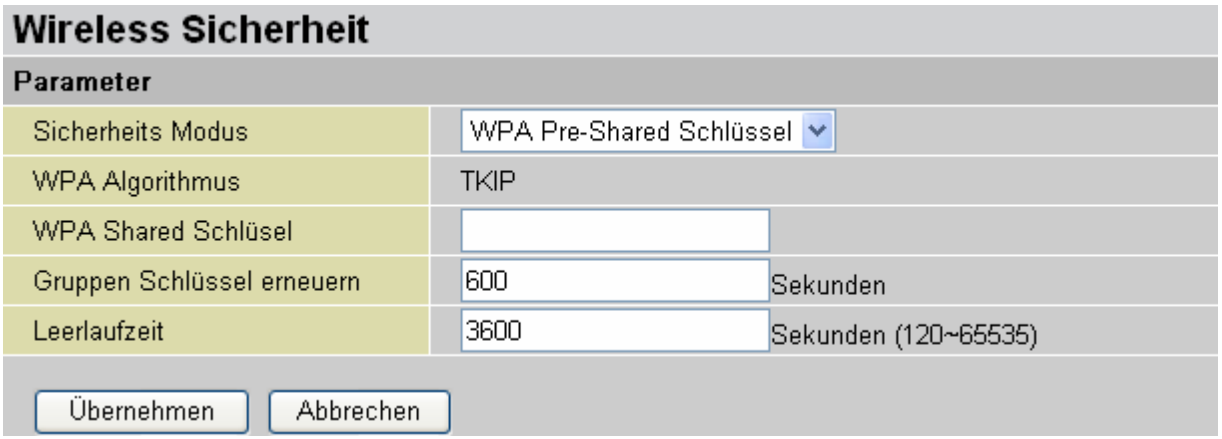
3.1.6 Wireless Sicherheit

Der Router bietet die Möglichkeit sein WLAN-Netz zu verschlüsseln, um so unberechtigten Zugriff Dritter vorzubeugen. Unterstützt werden folgende Sicherheitsmodi:

- WEP (64 und 128 Bit)
- WPA (TKIP)
- WPA2 (AES)

Die Standardeinstellung für die Wireless Sicherheit ist deaktiviert.

Folgendes Beispiel zeigt die Einstellungen für eine **WPA Verschlüsselung**:



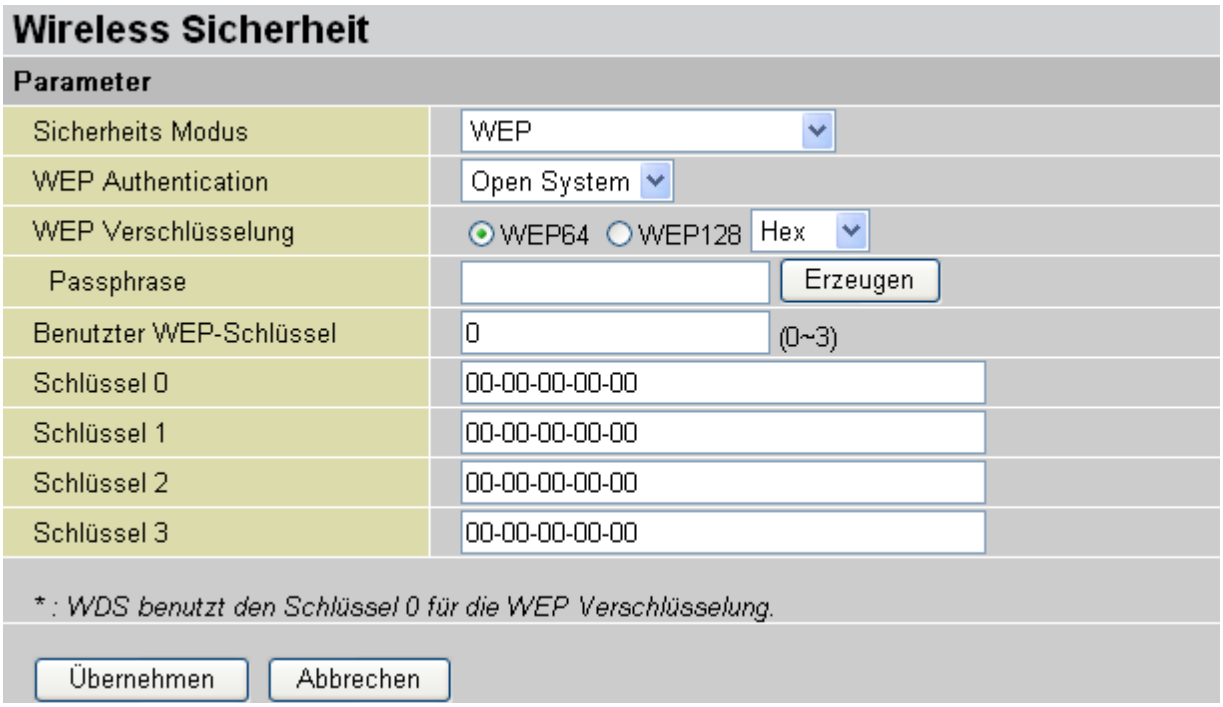
WPA Algorithmus: TKIP (Temporal Key Integrity Protocol) verwendet einen stärkere Verschlüsslungsmethode und berücksichtigt Message Integrity Code (MIC) um einen Schutz gegen Hacker zu erreichen.

WPA Shared Schlüssel: Der Schlüssel für die Netzwerkauthentifizierung. Das Eingabeformat ist beliebig und die Schlüssellänge reicht von 8 bis 63 Zeichen.

Gruppen Schlüssel erneuern: Der Intervall wonach der Sicherheitsschlüssel automatisch zwischen Wireless Client und Access Point (AP) erneuert wird.

Leerlaufzeit: Werksseitig auf 3600 Sekunden eingestellt. Die Leerlaufzeit basiert auf den Fall dass keine Daten gesendet bzw. empfangen werden. Sobald der Router erkennt dass keine Daten übermittelt werden fängt die Zeit an zu laufen und beendet die Verbindung zum Wireless Client wenn die angegebene Leerlaufzeit erreicht wurde. Danach wird eine neue Verbindung hergestellt.

Folgendes Beispiel zeigt die Einstellungen für die **WEP-Verschlüsselung**:



WEP Verschlüsselung: Um unautorisierten Wireless Stationen den Zugriff auf Daten des Netzwerkes zu verweigern, bietet der Wireless Router sichere Datenverschlüsselung, bekannt als WEP, an. Wenn Sie eine hohe Sicherheitsstufe in der Datenübermittlung verlangen, gibt es zwei Arten, aus denen Sie wählen können: WEP 64 und WEP 128. WEP 128 bietet eine höhere Sicherheit als WEP 64 an.

Passphrase: Dient zur automatischen Generierung von WEP Schlüsseln, wenn Sie Zeichen oder vordefinierte Algorithmen eingeben. Sie können dieselben Zeichen sowohl im AP als auch im Client eingeben, um denselben WEP Schlüssel zu generieren. Bitte beachten Sie, dass Sie keine Eingaben bei Schlüssel (0-3) vornehmen, wenn Sie Passphrase verwenden.

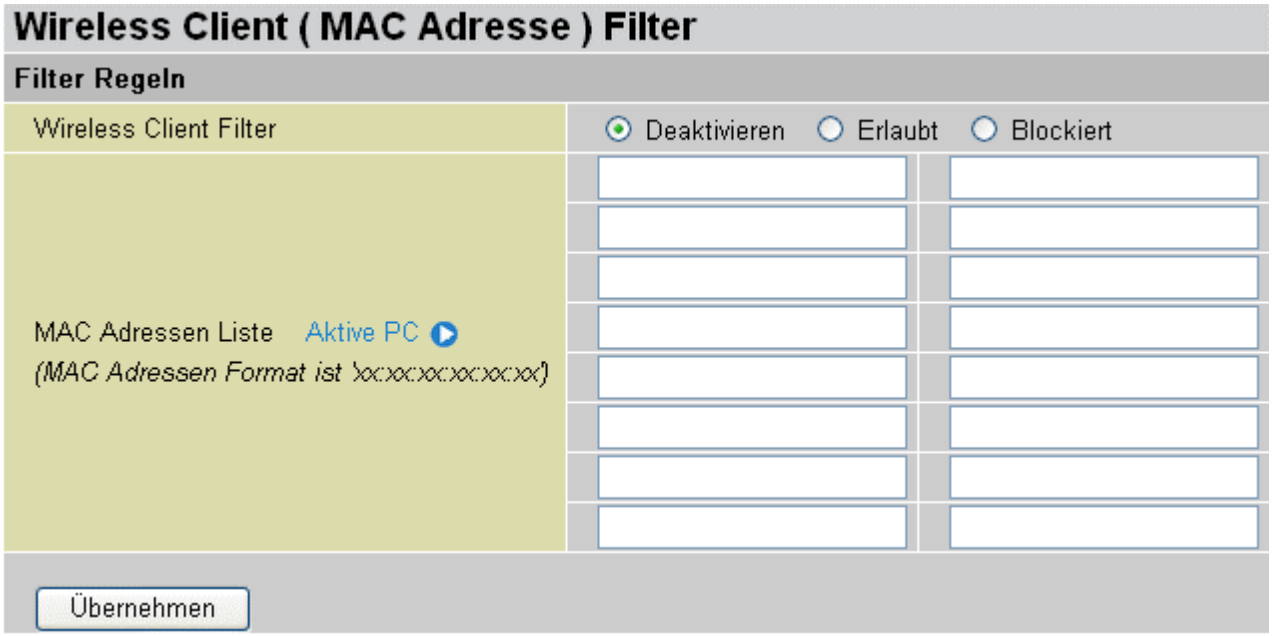
Benutzter WEP Schlüssel: Wählen Sie die Schlüssel ID; weiter Informationen unten (0-3).

Schlüssel (0-3): Geben Sie den Schlüssel ein um die Wireless Daten zu verschlüsseln. Um verschlüsselte Datenübertragung zu erlauben, muss auf allen Wireless Stationen der gleiche Schlüssel wie beim Router verwendet werden. Es gibt vier Schlüssel zu Ihrer Auswahl.

- Die Eingabe erfolgt im HEX Format (0-9 und a-f)
- Für WEP64 müssen Sie 5 Zeichen eingeben
- Für WEP128 müssen Sie 13 Zeichen eingeben, wobei das Trennungszeichen "-" ist z.B.: für WEP64 ist 11-22-33-44-55 ein gültiger Schlüssel, während 1122334455 ungültig ist

3.1.7 Wireless Client Filter

Der Wireless Client Filter unterstützt bis zu 16 WLAN Geräte, welche anhand der MAC-Adresse identifiziert werden. Dies hilft das WLAN Netzwerk zu administrieren bzw. zu kontrollieren, damit nur bestimmte Geräte Ihr LAN nutzen bzw. nicht nutzen dürfen.



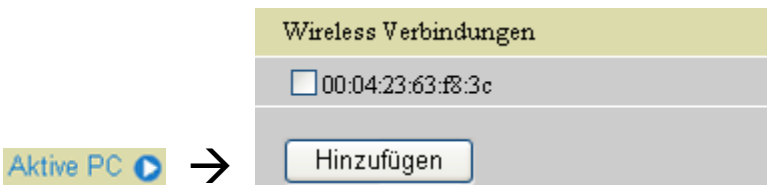
- **Erlaubt:** Autorisierte Geräte erhalten Zugriff auf das LAN-Netzwerk, indem die MAC Adresse eintragen oder das Gerät über [AKTIVE PC] ausgewählt wird. Vergewissern Sie sich das Ihr PC mit der MAC Adresse gelistet ist.

- **Blockiert:** Nicht autorisierte Geräte erhalten keinen Zugriff auf das LAN-Netzwerk, indem die MAC Adresse eintragen oder das Gerät über [AKTIVE PC] ausgewählt wird. Vergewissern Sie sich das Ihr PC mit der MAC Adresse nicht gelistet ist.

Hinweis: Folgen Sie diesem MAC Adressen Format xx:xx:xx:xx:xx:xx. Doppelpunkt (:) muss angegeben werden

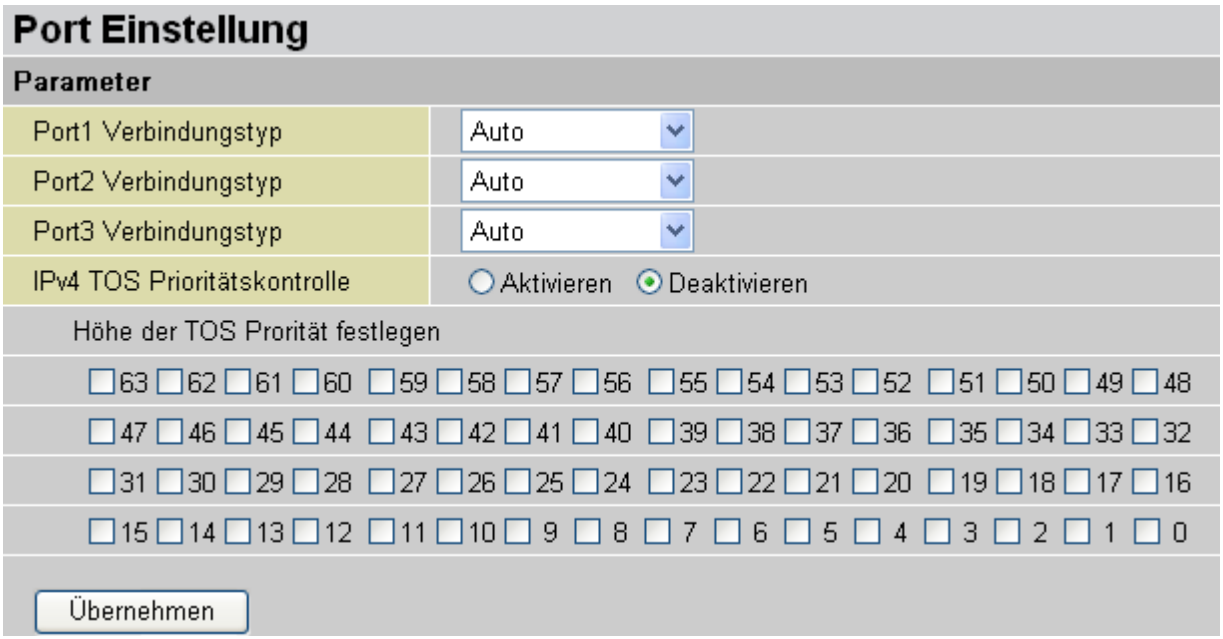
- Die maximale Anzahl beträgt 16 Clients
- Die MAC Adressen sind 6 Bytes lang und nur im Hexadezimalen Format angegeben
- Die Zahlen 0 – 9 werden akzeptiert
- Buchstaben a - f werden akzeptiert

Aktive PC: Alle Geräte, welche über Ethernet mit dem Router verbunden sind, werden hier automatisch mit IP- sowie MAC-Adresse angezeigt. Mit einem Klick auf die jeweilige Adresse wird diese ausgewählt



3.1.9 Port Einstellungen

Dieser Abschnitt erlaubt es die Einstellungen der Ethernet Ports des Routers zu konfigurieren um eventuell vorhandene Kompatibilitätsprobleme die unter umständen bei der Verbindung mit dem Internet auftreten zu beheben. Benutzer können zusätzlich die Performance Ihres Netzwerkes optimieren.



Es gibt 5 verschiedene Port Verbindungstypen:

- Auto
- 10M half-duplex
- 10M full-duplex
- 100M half-duplex
- 100M full-duplex

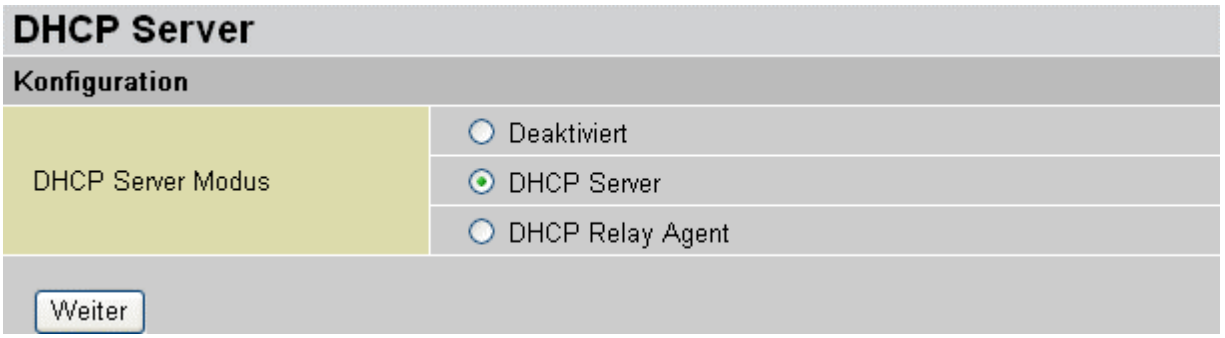
Manchmal gibt es Ethernet Kompatibilitätsprobleme mit alten Ethernet Geräten und Sie können verschiedene Geschwindigkeiten konfigurieren um diese Probleme zu lösen. Werksseitig ist Auto eingestellt. Sie sollten diese Einstellung belassen sofern keine Problem mit PCs auftreten, welche keinen Zugriff auf das Internet haben.

IPv4 TOS Prioritätskontrolle (für erfahrene Anwender):
TOS, Type of Services, ist das zweite Oktett eines IP Paketes. Bits 6-7 dieses Oktetts sind reserviert und Bit 0-5 werden verwendet um die Priorität des Paketes festzulegen.

Diese Feature verwendet die Bits 0-5 um die Paket-Priorität zu klassifizieren. Wenn das Paket eine hohe Priorität hat wird dieses zuerst bearbeitet und ist nicht abhängig von einer Limitierung. Daher, wenn dieses Feature aktiviert ist, überprüft der Ethernet Switch des Routers das zweite Oktett jedes einzelnen IP Paketes. Wenn der Wert im TOS Feld mit den aktivierten Werten übereinstimmt (0 bis 63), wird dieses Paket mit hoher Priorität behandelt.

3.1.10 DHCP Server

Der DHCP (Dynamic Host Control Protocol) Dienst bietet die Möglichkeit, dass alle lokal mit dem Router verbundene Geräte automatisch eine IP-Adresse (inkl. DNS- und Gateway-IP) zugewiesen bekommen können. Hierzu muss natürlich auch am Endgerät die IP-Adresse per DHCP bezogen werden.



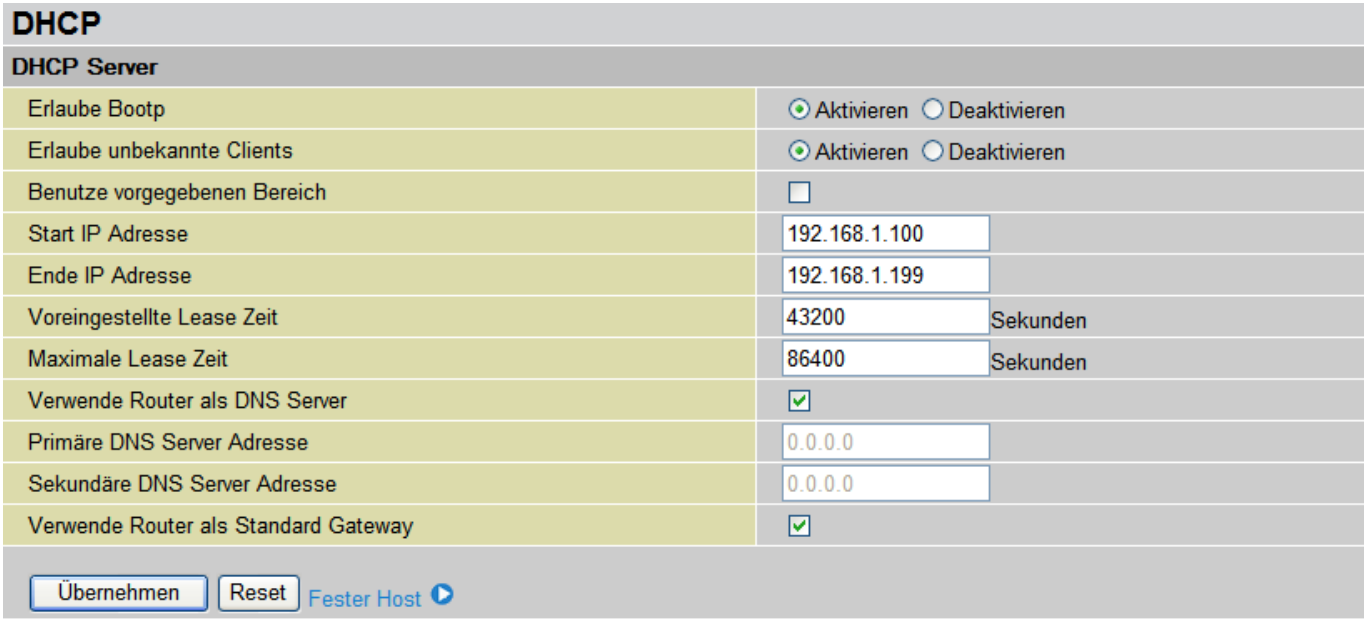
DHCP Server Status	
Erlaube Bootp	wahr
Erlaube unbekannte Clients	wahr
Aktivieren	wahr
Subnetz Definitionen	
Subnetz Wert	192.168.1.0
Subnetzmaske	255.255.255.0
Maximale Lease Zeit	86400 Sekunden
Voreingestellte Lease Zeit	43200 Sekunden
Benutze lokale Host Adresse als DNS Server	wahr
Benutze lokale Host Adresse als voreingestelltes Gateway	wahr
Beziehe Subnetz von der IP-Schnittstelle	iplan
IP Bereich *192.168.1.100- 192.168.1.199*	
Option *domain-name-servers= 0.0.0.0*	

Konfiguration:

DHCP Server Modus:

- **Deaktiviert:** Es wird kein DHCP verwendet, somit muss jedem Gerät im LAN eine IP-Adresse manuell zugewiesen werden. Ebenso müssen den Geräten die Router IP-Adresse als Gateway sowie als DNS-Server zugewiesen werden, damit eine Kommunikation auch ins Internet erfolgen kann

- **DHCP Server:** Wenn der DHCP-Dienst des Routers verwendet wird, dann können die Parameter des DHCP Servers konfiguriert werden. Diese Nachrichten werden an den DHCP Client gesendet, wenn er eine IP-Adresse vom DHCP Server anfordert



Folgende Einstellungen können bei Auswahl des Modus „DHCP Server" konfiguriert werden:

- **Erlaube Bootp:**
  Erlaubt die Nutzung des Bootstrap Protocols zum Booten eines (z.B. festplattenlosen) Computers über das Netzwerk

- **Erlaube unbekannte Clients:**
  Erlaubt nur Clients eine IP-Adresse zu beziehen, die bereits mit dem DHCP-Server mind. einmal verbunden waren

- **Benutze vorgegebenen Bereich:**
  Erlaubt dem Router nur IP-Adressen aus dem vorgegebenen Bereich zu verteilen. Werden darüber hinaus Adressen angefordert, werden diese Anfragen verworfen

- **Start IP Adresse:**
  Erste Adresse des Bereiches aus dem IP-Adressen vergeben werden dürfen durch den DHCP-Server

- **Ende IP Adresse:**
  Letzte Adresse des Berichtes aus dem IP-Adressen vergeben werden dürfen durch den DHCP-Server

- **Voreingestellte Lease Zeit:**
  Gültigkeitsdauer, für den ein Client seine IP-Adresse mindestens behält

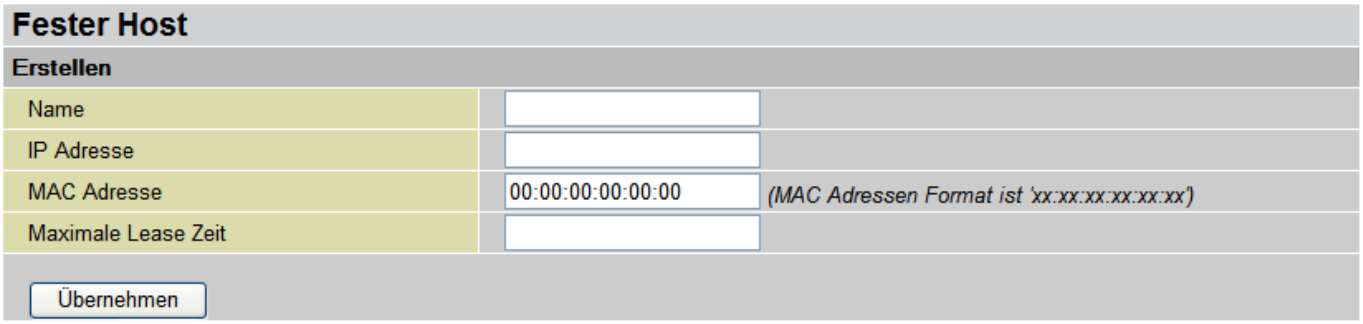
- **Maximale Lease Zeit:**
  Gültigkeitsdauer, für den ein Client seine IP-Adresse maximal behält

- **Verwende Router als DNS Server:**
  Der Router selbst übernimmt die Rolle als DNS-Server. Alle Anfragen einer Domain (z.B. www.google.de) von Clients aus dem LAN werden dann an den Router gestellt, der stellvertretend diese Anfrage an den DNS-Server des ISP weiterleitet. Ist diese Option deaktiviert, so muss ein mindestens ein gültiger primärer DNS-Server im Netzwerk für den Router angegeben werden. Ein sekundärer DNS-Server wird nur verwendet, wenn der primäre Server nicht erreichbar ist, diese Angabe bleibt somit optional.

- **Verwende Router als Standard Gateway:**
  Wird diese Option deaktiviert, so wird beim Bezug einer IP-Adresse durch einen Client im Netzwerk diesem kein Standard-Gateway mehr mit zugewiesen.

  ACHTUNG: Dem Client ist es dann nicht mehr möglich mit dem Internet zu kommunizieren!

- **Fester Host:**
  Diese Option ermöglicht es anhand einer vorgegebenen Hardware MAC-Adresse einem bestimmten Gerät immer die gleiche IP-Adresse zuzuweisen. Diesem kann auch eine eigene maximale Gültigkeitsdauer der IP-Adresse zugeteilt werden



DHCP Relay Agent:

In diesem Modus vergibt der Router selbst keine IP-Adressen und verwaltet diese, sondern tritt nur als Stellvertreter für einen anderen im LAN vorhandenen DHCP-Server in Kraft. Er leitet somit alle Anfragen eines Clients an den Ursprünglichen Server weiter und gibt die dort zugeteilten IP-Adressen an den anfragenden Client zurück.

DHCP Server IP Adresse: IP-Adresse des eigentlichen DHCP-Servers, für den alle Anfragen stellvertretend angenommen und weitergeleitet werden

3.2 WAN (Wide Area Network)

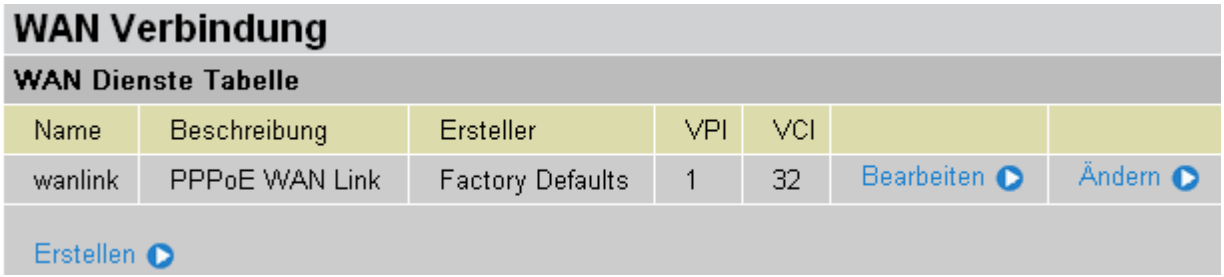
In dieser Kategorie lassen sich alle Einstellungen bezüglich der WAN-Schnittstelle ins Internet tätigen. Hierbei wird diese Schnittstelle auch häufig „ipwan" oder „wanlink" im Routerkonfigurations-menü genannt. Das Wide Area Network beschreibt die Verbindung vom Router zum Internet.

Diese Kategorie enthält folgende Untermenüs:

- **ISP**
- **DNS**
- **ADSL**

3.2.2 ISP (Internet Service Provider)

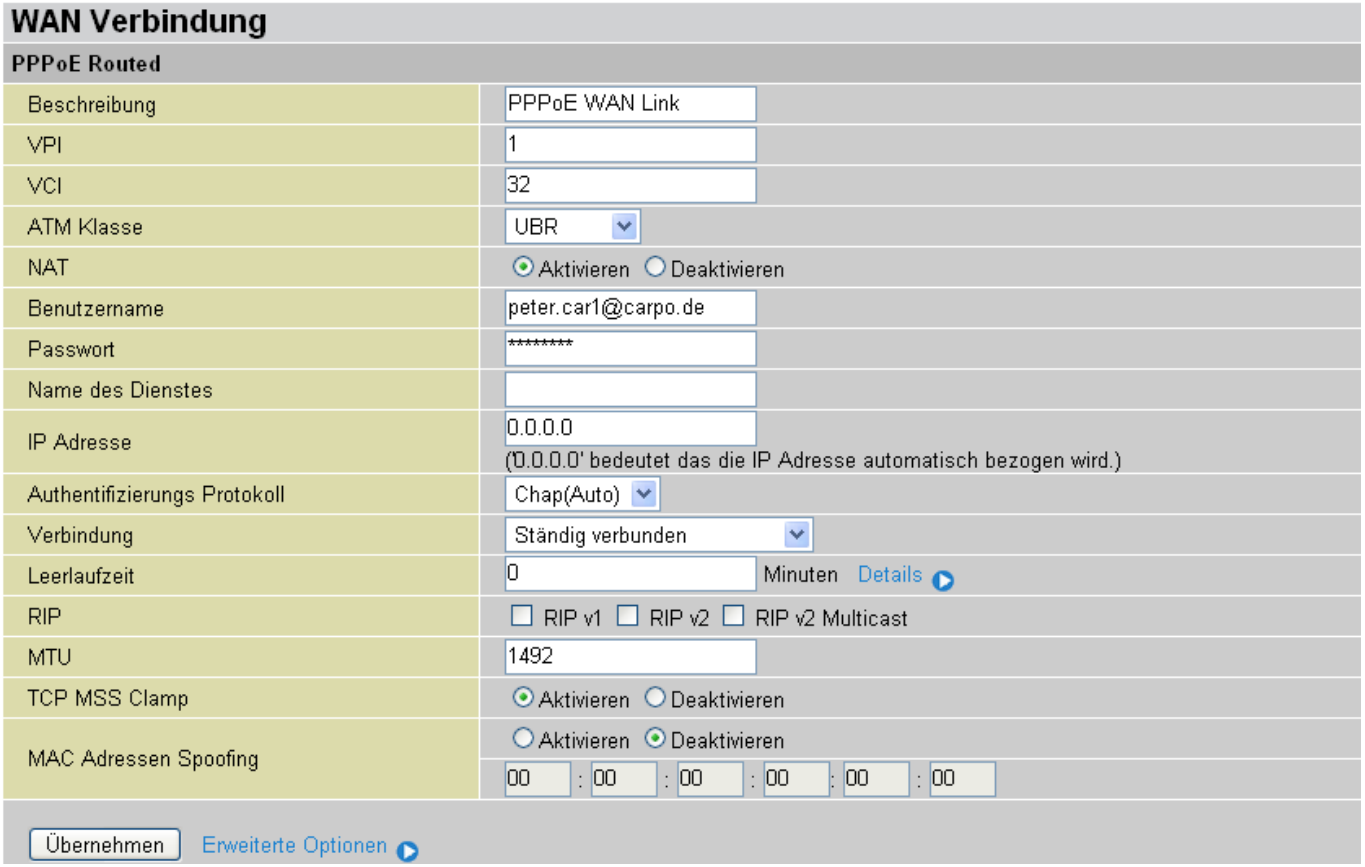
Die Werkseinstellung ist: **PPPoE**



- Wenn der verwendete ISP das gleiche Protokoll verwendet, können mit einem Klick auf **[BEARBEITEN]** weitere Einstellung zu dieser Verbindung vorgenommen werden

- Wenn Carpo oder ein anderer ISP PPPoE nicht unterstützt, kann mit einem Klick **[ÄNDERN]** das Verbindungsprotokoll geändert und weitere Einstellungen hierzu angepasst werden

- Mit einem Klick auf **[ERSTELLEN]** kann auch eine komplett neue WAN-Verbindung erstellt werden



Folgende Einstellungen können verändert werden:

- **Beschreibung:**
  Name der Verbindung, ergibt sich automatisch aus dem gewählten WAN-Verbindungsprotokoll

- **VPI:**
  Virtual Path Identifier, wird vom ISP vorgegeben

- **VCI:**
  Virtual Channel Identifier, wird vom ISP vorgegeben

- **ATM Klasse:**
  Hier kann die entsprechende ATM Klasse für den „Quality of Service" ausgewählt werden

- **NAT (Network Address Translation):**
  NAT erlaubt mehreren Nutzern mit einem einzigen IP-Account und einer einzigen IP-Adresse Zugang zum Internet. Falls LAN-User öffentliche IP-Adressen haben und direkt auf das Internet zugreifen, kann NAT abgeschaltet werden.

- **Benutzername:**
  Hier wird der Benutzername eingetragen, der vom ISP zugewiesen wurde. Es können bis zu 128 alphanumerische Zeichen eingeben werden (Gross- und Kleinschreibung beachten). Sehr oft in der Form „benutzername@ispname" anstelle "Benutzername"

- **Passwort:**
  Hier wird das zum Benutzername dazugehörige Passwort eingegeben, welches der ISP vergeben hat. Es können bis zu 128 alphanumerische Zeichen eingeben werden (Gross- und Kleinschreibung beachten)

- **Dienstname:**
  Dieser Punkt ist nur zur Identifizierung gedacht. Wenn benötigt, wird Ihnen Ihr ISP weitere Informationen mitteilen. Maximal können Sie 20 alphanumerische Zeichen eingeben.

- **IP Adresse:**
  Externe WAN IP-Adresse des ISP, ein leeres bzw. mit **0.0.0.0** ausgefülltes Feld bedeutet, dass die IP-Adresse automatisch nach der Einwahl bezogen wird

- **Authentifizierungs Protokoll:**
  Standard ist Chap(Auto). Dieser Wert wird vom ISP vorgegeben, ob alternativ Chap oder Pap benutzen werden muss

- **Verbindung:**
  - **Ständig Verbunden:** der Router startet eine PPPoE Sitzung sobald er eingeschaltet ist und diese nach Verbindungsabbruch durch den ISP automatisch wieder aufbaut (z.B. bei Zwangstrennung)

  - **Verbindung auf Anforderung:** Wenn Sie eine PPPoE Sitzung nur dann möchten, wenn ein Paket Zugang zum Internet verlangt (z.B.: wenn ein Programm auf Ihrem Computer Zugriff zum Internet verlangt)

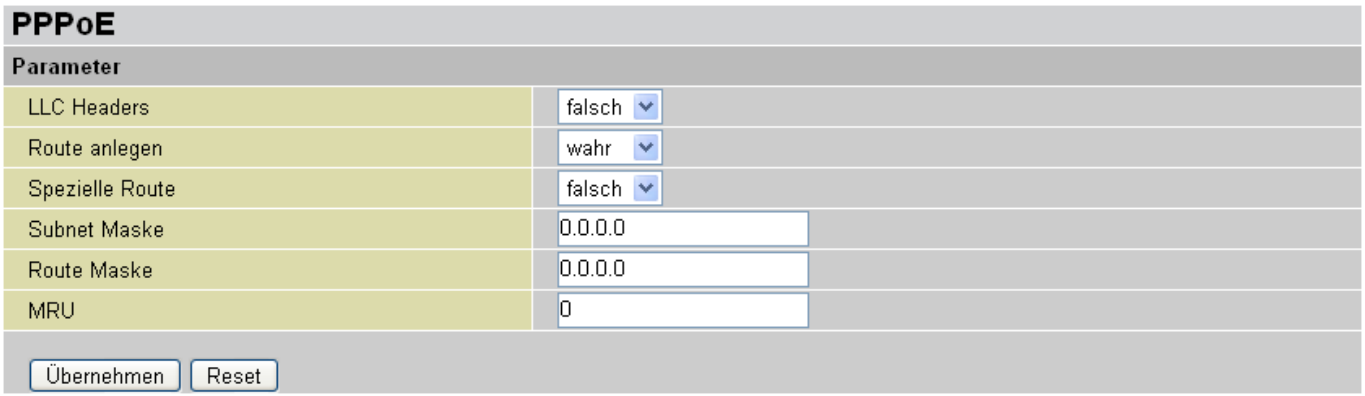
- **Leerlaufzeit:**
  Automatischer Verbindungsabbau des Routers, wenn keine Aktivität für eine voreingestellte Zeit stattfindet
  - **Details:** Hier können Sie die Ziel Ports und die Paket Typen angeben (TCP/UDP) welche von der Leerlaufzeit nicht überprüft werden. Dies erlaubt Ihnen

- **RIP v1, RIP v2, und RIP v2 Multicast:**
  Wählen Sie dies aus, um die RIP Funktion zu aktivieren, so dass der Router andere Router in seinen angeschlossenen Netzwerken erkennt und berücksichtigt

- **MTU:**
  Maximum Transmission Unit, beschreibt die maximale Paketgröße, die über ein Netzwerk übertragen werden kann, ohne dass das Datenpaket fragmentiert (geteilt) werden muss

- **TCP MSS Clamp:**
  Werksseitig ist diese Funktion aktiviert. Sämtlicher TCP Datenverkehr wird durch den Router geprüft. Wenn eine TCP Verbindungsanforderung den MTU-Wert im Router überschreitet, schreibt die MSS Funktion die Pakete so um, dass dennoch keine Fragmentierung dieser stattfinden muss

Erweiterte Optionen (PPPoE)



- **LLC Header:**
  Wählt den Encapsulation Modus aus, „true" für LLC bzw. „false" für VC-Mux

- **Route erstellen:**
  Diese Einstellung gibt an ob eine Route zum System hinzugefügt wird nachdem die IPCP (Internet Protocol Control Protocol) Verhandlung beendet ist. Wenn dies wahr ist, wird eine Route angelegt, welche Pakete direkt an das Remote Ende des PPP Link leitet.

- **Spezielle Route:**
  Gibt an ob eine Route angelegt wird wenn ein PPP Link eine gezielte oder Standard route ist. Wenn dies wahr ist, wird die Route nur für Pakete gültig sein für das Subnetz am Remote End des PPP Link. Die Adresse dieses Subnetz wird während der IPCP Verhandlung bezogen

- **Subnet Maske:**
  Stellt die Subnetz Maske, die für das lokale IP Interface zum PPP Transport verwendet wird zur Verfügung. Wenn die Angabe 0.0.0.0 ist wird die Netzmaske automatisch anhand der IP Adresse während der IPCP Verhandlung ausgerechnet.

- **Route Maske:**
  Stellt die Subnetz Maske, die für die Route benutzt wird, wenn ein PPP Link aufkommt, zur Verfügung. Wenn die Angabe 0.0.0.0 ist wird die Netzmaske automatisch anhand der IP Adresse während der IPCP Verhandlung ausgerechnet

- **MRU - Maximum Receive Unit:**
  Dies wird vereinbart während der LCP Protokoll Phase

- **Finde Primären / Sekundären DNS:**
  Diese Einstellung aktiviert / deaktiviert ob die primäre/sekundäre DNS Server Adresse vom Remote PPP Peer über IPCP angefragt wird. Die Standardeinstellung hierbei ist „wahr"

- **Übergebe DNS an Relay:**
  Kontrolliert ob das PPP Internet Protocol Control Protocol (IPCP) die DNS Server IP Adresse für einen remote Peer erfragen kann. Nachdem IPCP die DNS Server IP Adresse erfahren hat, wird es diese automatisch an das lokale DNS Relay weitergeben so dass die Verbindung aufgebaut werden kann

- **Übergebe DNS an Client:**
  Kontrolliert ob das PPP Internet Protocol Control Protocol (IPCP) die DNS Server IP Adresse für einen Remote Peer erfragen kann. Nachdem IPCP die DNS Server IP Adresse erfahren hat, wird es diese automatisch an die lokalen Clients weitergeben so das die Verbindung aufgebaut werden kann

- **Übergebe DNS an DHCP Server:** Ähnlich wie oben, aber gibt die DNS Server Adresse an den DHCP Server weiter

- **Finde Primären NBNS / Sekundären NBNS:**
  Diese Einstellung aktiviert / deaktiviert ob die primäre / sekundäre NBNS Server Adresse vom Remote Peer über IPCP angefragt wird. Der Standardwert dafür ist „falsch"

- **Finde Subnet Maske:**
  Gibt an, ob die Subnetzmaske während der IPCP Verhandlung benutzt wird oder nicht

- **Übergebe Subnet Maske an DHCP Server:**
  Aktiviert um Ihre DHCP Server Einstellungen zu verändern mit den Informationen die Sie während des IPCP Verhandlung erhalten

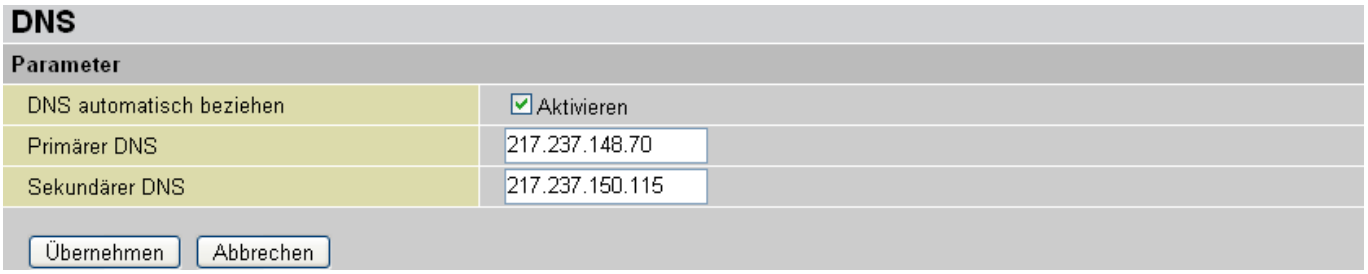
3.2.2 DNS (Domain Name System)

Das Domain-Name-System (DNS) beinhaltet ein Verzeichnis für Domain-Namen und deren IP-Adressen. Im Internet hat jeder Host einen Namen, z.B. www.billion.com/de, den man sich meist gut merken kann und eine IP-Adresse. Da man sich die IP-Adresse hingegen schlecht merken kann, reicht es, den Domain-Namen einzugeben, der vom DNS in die entsprechende IP-Adresse konvertiert wird. Eine IP Adresse ist eine 32-bit Nummer in der Form xxx.xxx.xxx.xxx, zum Beispiel 192.168.1.254. Sie können Sich eine IP Adresse wie eine Telefonnummer für ein Gerät im Internet vorstellen und der DNS erlaubt es Ihnen die Telefonnummer für jeden speziellen Namen zu finden. Weil man sich eine IP Adresse schwer merken kann, konvertiert das DNS diese in einen Benutzerfreundlichen Namen mit Ihrer dazugehörigen IP Adresse.

Sie können die Domain Name System (DNS) IP Adresse automatisch von Ihrem ISP bekommen, wenn er dies beim Login anbietet. Normalerweise wenn Sie PPPoE oder PPPoA als Ihr WAN – ISP Protokoll wählen, wird Ihr ISP Ihnen die notwendigen DNS IP Adressen automatisch übermitteln. Sie können das Konfigurationsfeld leer lassen.

Alternativ kann Ihr ISP Ihnen die IP Adressen seines DNS mitteilen. In diesem Falle geben Sie die DNS IP Adressen hier ein.

Wenn Sie ein anderes der drei weiteren Protokoll auswählen – RFC1483 Routed/Bridged und IPoA prüfen Sie bitte bei Ihrem ISP, ob Sie die IP Adressen für deren DNS Server erhalten. Diese DNS Server IP Adressen müssen Sie eingeben, wenn Sie die DNS Ihres PC auf die LAN IP des Routers einstellen.



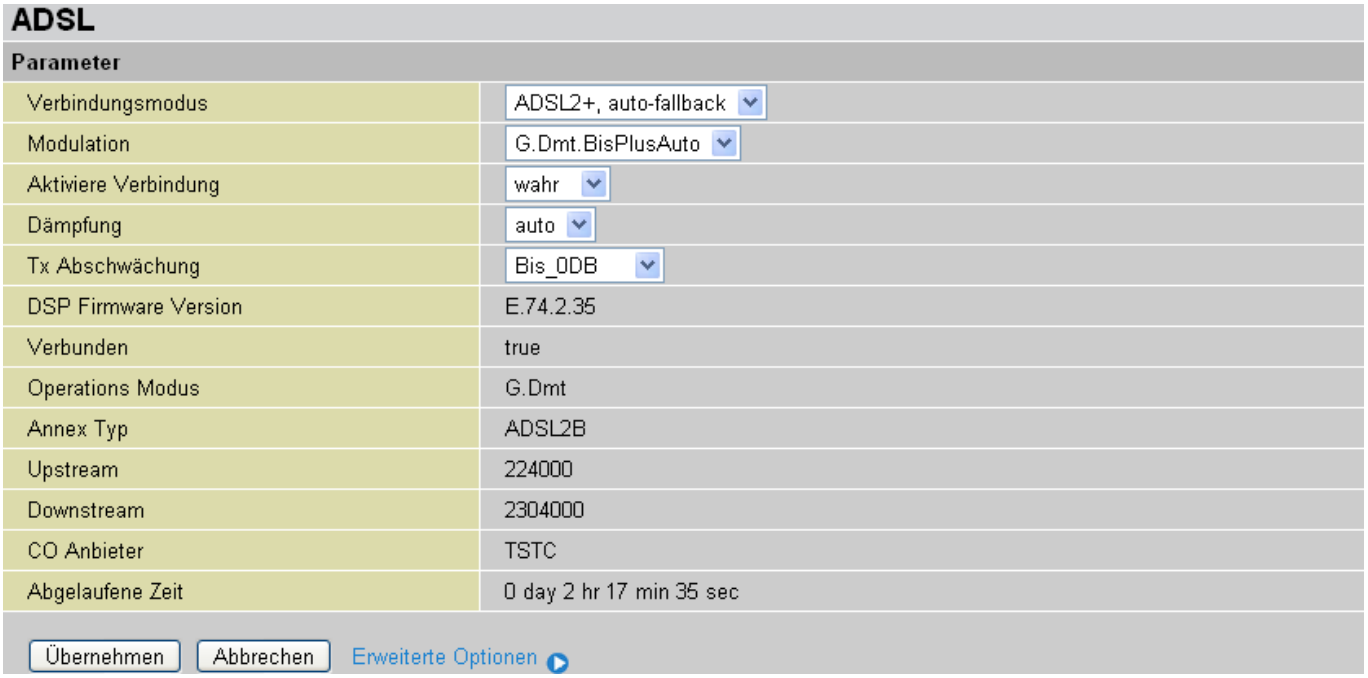
DNS automatisch beziehen: Bestimmt, ob der Router die IP-Adresse des DNS-Servers bei der Interneteinwahl vom ISP automatisch beziehen soll

Primärer DNS: Hier kann alternativ ein fester DNS Server eingetragen werden

Sekundärer DNS: Ein Sekundärer DNS-Server wird verwendet, wenn der primäre Server nicht mehr antwortet

3.2.2 ADSL (Asymmetric Digital Subscriber Line)

ADSL steht für Asymmetric Digital Subscriber Line und beschreibt die physikalische Leitung, über die sämtliche Daten aus und in das Internet übertragen werden. Asymmetrisch, da die Leitung meist eine höhere Bandbreite zum Herunterladen als zum Hochladen von Dateien bietet.



- **Verbindungsmodus:**
  Die Standardeinstellung ist Mulitmode. Dieser Modus wird automatisch den ADSL Line Code erkennen (G.dmt, G.lite, und T1.413). In manchen Gegenden kann es den ADSL Verbindungsmodus nicht erkennen. Stellen Sie hierfür den ADSL Verbindungsmodus zuerst auf T1.413 oder G.Dmt. Falls es weiterhin fehlschlägt, versuchen Sie andere Einstellungen wie ALCTL, ADI, etc.

- **Aktiviere Verbindung:**
  Unterbrechen (falsch) Ihrer ADSL Leitung und Aktivierung (wahr) Ihrer ADSL Leitung wenn Sie den Verbindungsmodus verändert haben

- **Coding Gain:**
  Konfiguriert den ADSL Coding Gain von 0 dB bis 7dB, oder automatisch

- **Tx Abschwächung:**
  Stellt den ADSL transmission gain ein, der Wert ist zwischen 0~12

- **DSP Firmware Version:**
  Aktuelle ADSL Line Code Firmware Version.

- **Verbunden:**
  Zeigt den aktuellen ADSL Leitungs-SYNC Status an

- **Operations Modus:**
  Zeigt den aktuellen ADSL Modus Standard (Verbindungsmodus) Ihres Routers an sobald die ADSL Leitung synchronisiert ist

- **Annex Typ:**
  ADSL Annex A, welches über einen normalen Telefonanschluss arbeitet. Annex B welches über eine ISDN Leitung arbeitet

- **Upstream:**
  Zeigt die aktuelle Upstream Rate Ihrer ADSL Leitung an

- **Downstream:**
  Zeigt die aktuelle Downstream Rate Ihrer ADSL Leitung an

3.3 System

In dieser Kategorie können verschiedenste Einstellungen getroffen werden, die sich auf das eigene Konfigurationssystem des Routers beziehen.

Diese Kategorie enthält folgende Untermenüs:

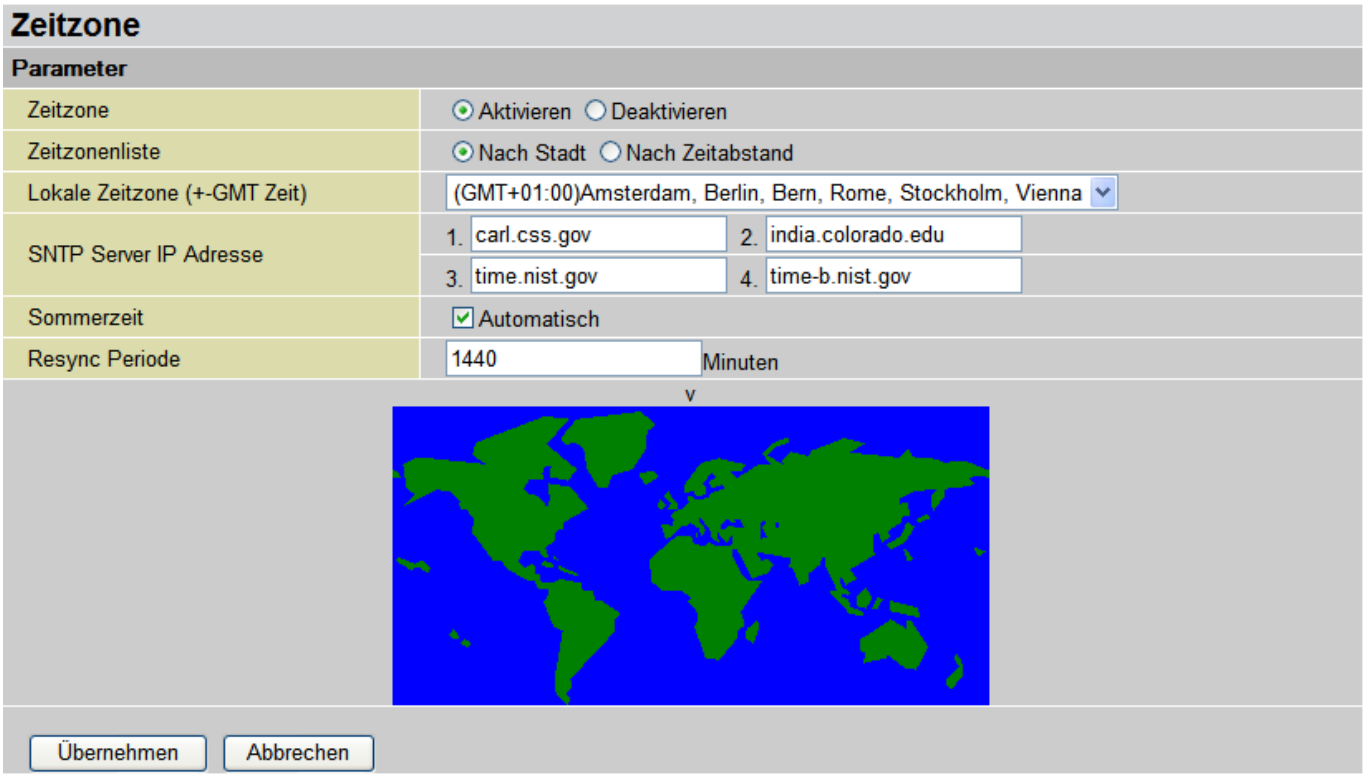
- **Zeitzone**
- **Remote Zugriff**
- **Firmware Upgrade**
- **Sichern/Wiederherstellen**
- **Neustart**
- **Benutzer Verwaltung**

3.3.2 Zeitzone

Der Router verfügt nicht über eine Echtzeit-Uhr, sondern über das Simple Network Time Protocol (SNTP), um über den SNTP Server im äußeren Netzwerk die richtige Uhrzeit vermittelt zu bekommen. Bitte wählen Sie die entsprechende Zeitzone und klicken dann auf „Übernehmen". Sie erhalten die korrekte Zeitangabe, wenn Sie mit dem Internet verbunden sind. Die Uhrzeit wird im Status-System-Fenster angezeigt. Wenn Sie es vorziehen, Ihren eigenen SNTP Server einzurichten, geben Sie diesen bitte ein und wählen ihn aus. Ihr ISP bietet möglicherweise auch einen SNTP Server zur Benutzung an.

Sommerzeit: Viele Orte auf der Welt stellen die Zeit um, damit eine Stunde des Tageslichtes vom morgen auf den Abend verschoben wird. Aktivieren Sie das Kontrollkästchen damit dies automatisch umgestellt wird.

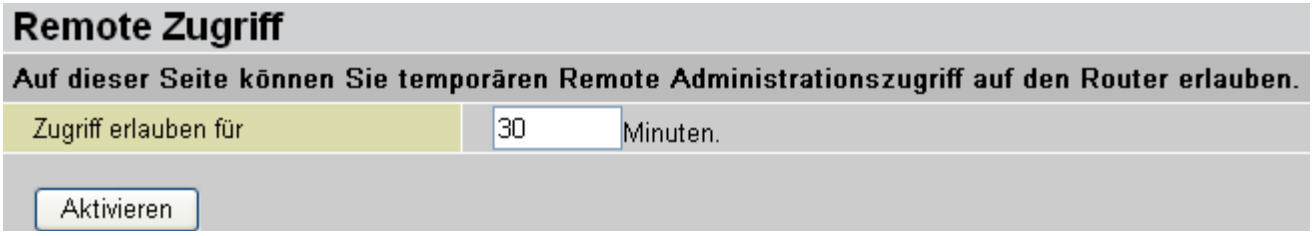
Resync Periode (in Minuten) ist das periodische Intervall in der der Router die Zeit erneut mit dem SNTP Server synchronisiert. Um einen erhöhten Verkehr zu Ihrem SNTP Server zu vermeiden, sollten Sie das Intervall so hoch wie möglich einstellen – zumindest alle paar Stunden oder sogar mehrere Tage.



3.3.2 Remote Zugriff

Um vorläufigen Fernzugriff auf den Router zu ermöglichen (z.B. außerhalb des LAN) wählen Sie die Zeitspanne wo Fernzugriffe erlaubt sind und klicken Sie auf Aktiviert. Sie können auch andere Konfigurationsoptionen für die Web Administration im Abschnitt Geräte Management im Menüpunkt Erweitert im GUI festlegen. Aktivieren sie bitte diese Funktion wenn ein Carpo Mitarbeiter sie dazu auffordert.

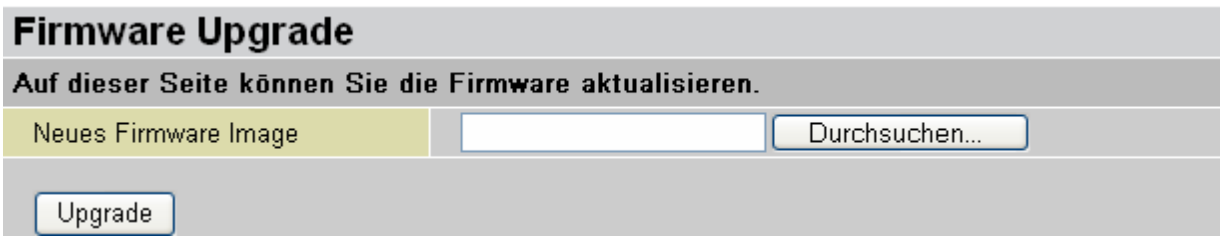
Wenn Sie den Fernzugriff permanent ermöglichen wollen, so geben Sie bitte 0 Minuten ein



3.3.2 Firmware Upgrade

Die Firmware des Routers ist eine Software die alle Funktionen ermöglicht. Stellen Sie sich den Router als einen Computer vor und die Firmware ist die Software womit der Router arbeitet. Nach einiger Zeit wird möglicherweise die Software für den Router verbessert und modifiziert und er kann aktualisiert werden um diese Neuheiten und Vorzüge zu nutzen.

HINWEIS: Eine aktuelle Firmware finden Sie unter *www.carpo.de* oder *www.carpo.com*. Benutzen Sie nur diese Firmware, da eine andere Firmware den Router zerstören kann. In diesem Fall übernimmt Carpo keine Gewährleistung.



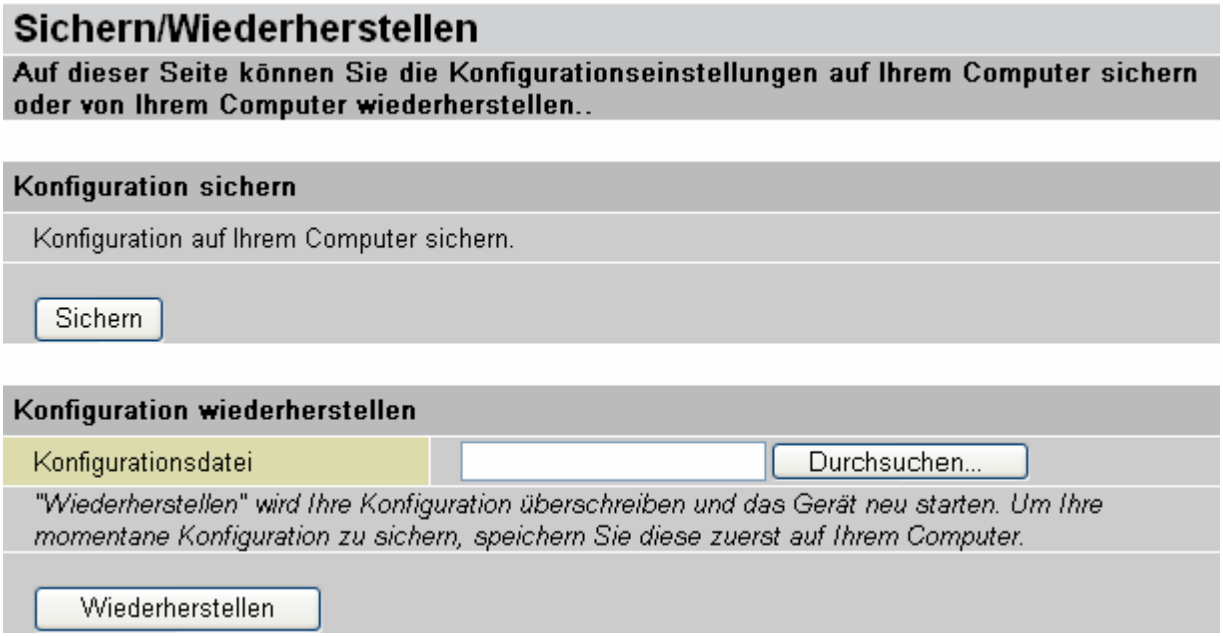
Klicken Sie auf Durchsuchen und Sie können die neue Firmware Version auswählen, welche Sie sich heruntergeladen haben. Klicken Sie auf „Upgrade" um die Firmware des Routers zu aktualisieren.

ACHTUNG: Schalten Sie Ihren Router NICHT aus oder unterbrechen den Firmware Upgrade Prozess. Dies kann den Router beschädigen!

Nachdem die Firmware aktualisiert wurde, empfehlen wir Ihnen einen Reset auf Standard Werkseinstellungen durchzuführen, um die volle Funktionalität der neuen Firmware Version zu erhalten. Verwenden Sie ebenfalls keine gespeicherte Konfiguration, sondern geben Ihre alte Konfiguration erneut ein. Schauen Sie im Abschnitt Neustart für weitere Informationen dazu nach.

3.3.2 Sichern / Wiederherstellen

Diese Funktion erlaubt es Ihnen die aktuellen Einstellungen des Router zu sichern oder ein Sicherung wiederherzustellen. Dies ist sehr nützlich, wenn Sie mit verschiedenen Einstellungen arbeiten oder experimentieren wollen. Wir empfehlen, die Einstellungen zu sichern, bevor Sie irgendwelche signifikanten Veränderungen an den Einstellungen des Routers vornehmen wollen.



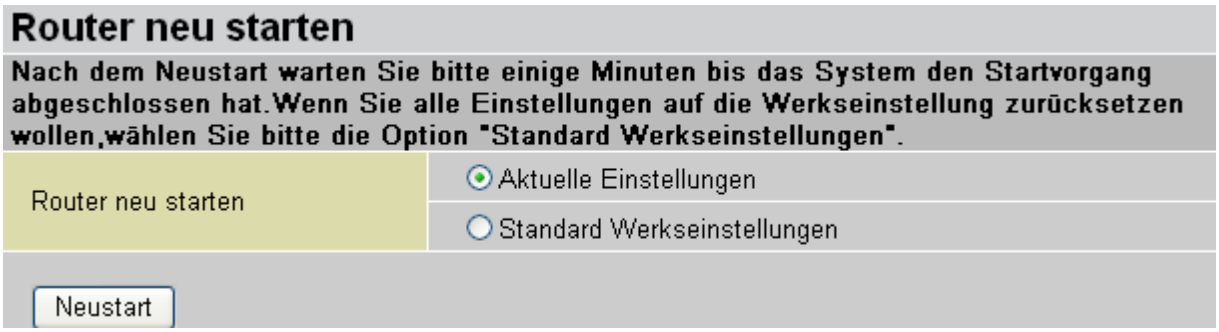
Klicken auf **[SICHERUNG]** um auszuwählen, wohin die Sicherungsdatei auf dem PC lokal abgespeichert werden soll. Die Datei kann auch nach Belieben umbenannt werden, z.B. wenn mehrere Sicherungen durchgeführt werden sollen.

Klicken auf **[DURCHSUCHEN]** um eine Sicherungsdatei auszuwählen, welche von dem PC wiederhergestellt werden soll. Es dürfen nur Sicherungsdateien, die von der Backupfunktion des Routers selber erzeugt worden sind und die von der gleichen Firmware Version des Router Sind, verwendet werden. Die Sicherungsdatei darf auf keinem Fall auf einem PC editiert oder anderweitig verändert werden.

Nachdem die Sicherungsdatei ausgewählt wurde, kann mit einem Klick auf **[WIEDERHERSTELLEN]** die gesicherten Einstellungen wiederhergestellt werden.

3.3.2 Neustart

Klicken Sie auf **[NEUSTART]** mit der Option **[AKTUELLE EINSTELLUNGEN]** um den Router neu zu starten und um die letzte im Router gespeicherte Einstellung wiederherzustellen.

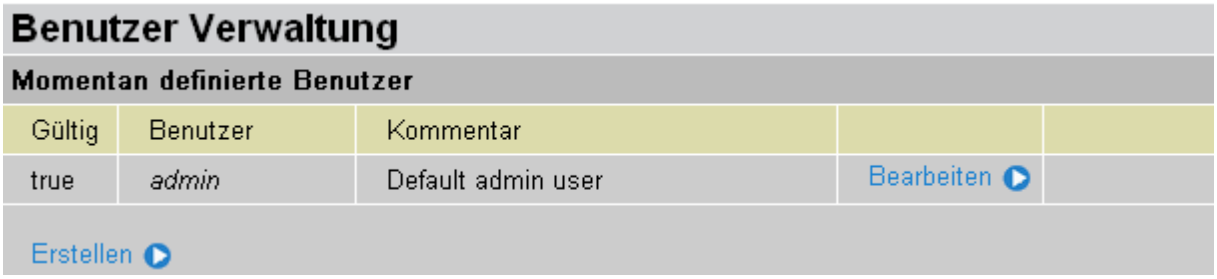


Wenn Sie den Router mit den Werkeinstellungen neu starten wollen (z.B. nach einem Firmware Upgrade oder einer defekten Konfiguration) so klicken Sie die **[STANDARD WERKSEINSTELLUNGEN]** Box an.

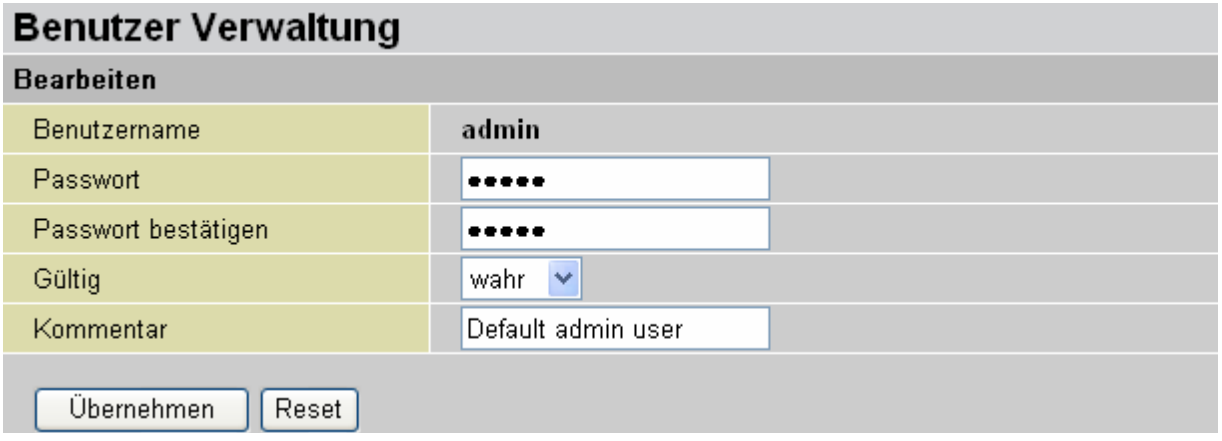
Sie können auch einen Reset auf die Werkeinstellungen durchführen, indem Sie den kleinen Resetschalter auf der Rückseite des Routers länger als 6 Sekunden drücken wenn der Router eingeschaltet ist.

3.3.2 Benutzer Verwaltung

Um nicht autorisierte Zugriffe auf die Router Konfiguration zu unterbinden, benötigen alle Benutzer ein Login mit Passwort. Sie können mehrere Benutzerkonten einrichten, mit jeweils individuellem Passwort.



Sie können bestehende Benutzer Bearbeiten und neue Benutzer Erstellen, welche auf die Konfiguration des Gerätes zugreifen können. Wenn Sie Bearbeiten gewählt haben, erhalten Sie folgende Optionen:

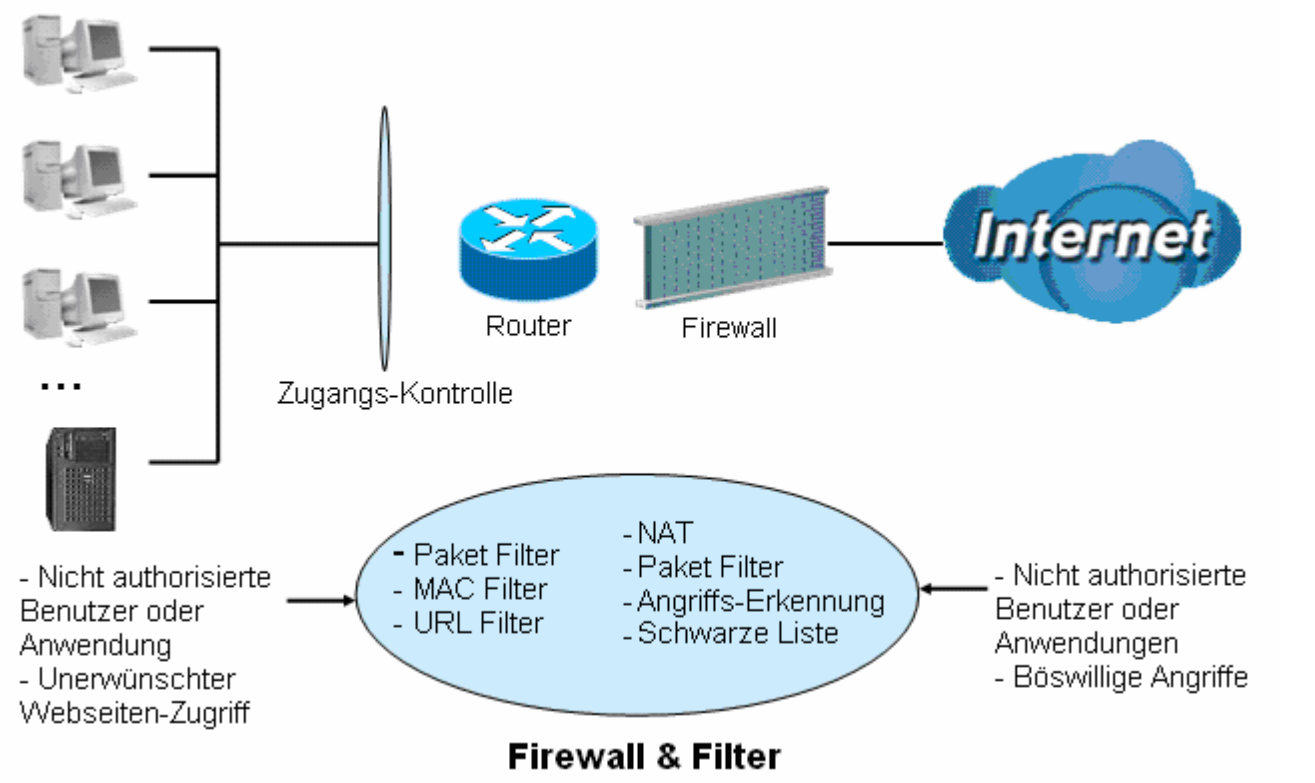


Folgende Einstellungen können in der Benutzer Verwaltung angepasst werden:

- **Benutzername:** Name des jeweiligen Benutzers, kann für die vordefinierten Standardnutzer nicht geändert werden.
- **Passwort:**Dazugehörige Passwort des jeweiligen Benutzers
- **Passwort bestätigen:** Erneute Eingabe des gewählten Passworts (zur Sicherheit gegen Tippfehler)
- **Gültig:** wahr = Benutzer ist aktiv und kann genutzt werden falsch = Benutzer ist inaktiv und kann nicht genutzt werden
- **Kommentar:** Hier kann ein beliebiger Kommentar zum Account hinterlegt werden

3.4 Firewall

Ihr Router hat eine SPI (Stateful Packet Inspection) Firewall um den Internetzugang von Ihrem LAN zu kontrollieren und um Hackerattacken zu verhindern. Zusätzlichen wenn Sie NAT (Network Address Translation. Schauen Sie im Abschnitt WAN Konfiguration für weitere Details nach) nutzen, fungiert der Router als eine Art „natürliche" Firewall, weil all Ihre PCs im LAN private IP Adressen nutzen, die nicht direkt aus dem Internet angesprochen werden können.



- **Firewall:**
  Unterbindet Zugang von außerhalb auf Ihr Netzwerk. Der Router bietet 4 Sicherheitsstufen an:
  - Alle blockiert/Benutzerdefiniert
  - Hohe Sicherheitsstufe
  - Mittlere Sicherheitsstufe (Werkseinstellungen)
  - Niedrige Sicherheitsstufe

- **NAT natural Firewall:**
  Diese maskiert die LAN Nutzer IP Adressen, die nach außen hin unsichtbar sind und es ist sehr viel schwieriger für einen Hacker ein Ziel in Ihrem Netzwerk auszumachen. Diese natürliche Firewall ist aktiv, sobald Sie NAT aktiviert haben.

HINWEIS: Wenn Sie Virtuelle Server (manuelle Portweiterleitung) für Ihren PC nutzen, wird Ihr PC entsprechend soweit geöffnet, wie Sie dies in den Virtuellen Server Einstellungen vorgenommen haben. Diese Ports sind dann in Ihrem Firewall Filter geöffnet.

Die Kategorie hat folgende Untermenüs:

- **Generelle Einstellungen:**
  Die Firewall kann generell aktiviert und deaktiviert werden, sowie eine allgemeine Sicherheitsstufe ausgewählt werden

- **Paket Filter:**
  Paket Filter Regeln verhindern unerlaubten Computern oder Programmen Zugriff auf das Lokale Netzwerk vom Internet aus oder in das Internet hinein

- **Angriffserkennung:**
  Aktiviere Angriffserkennung um boshafte Angriffe zu bemerken, verhindern und loggen

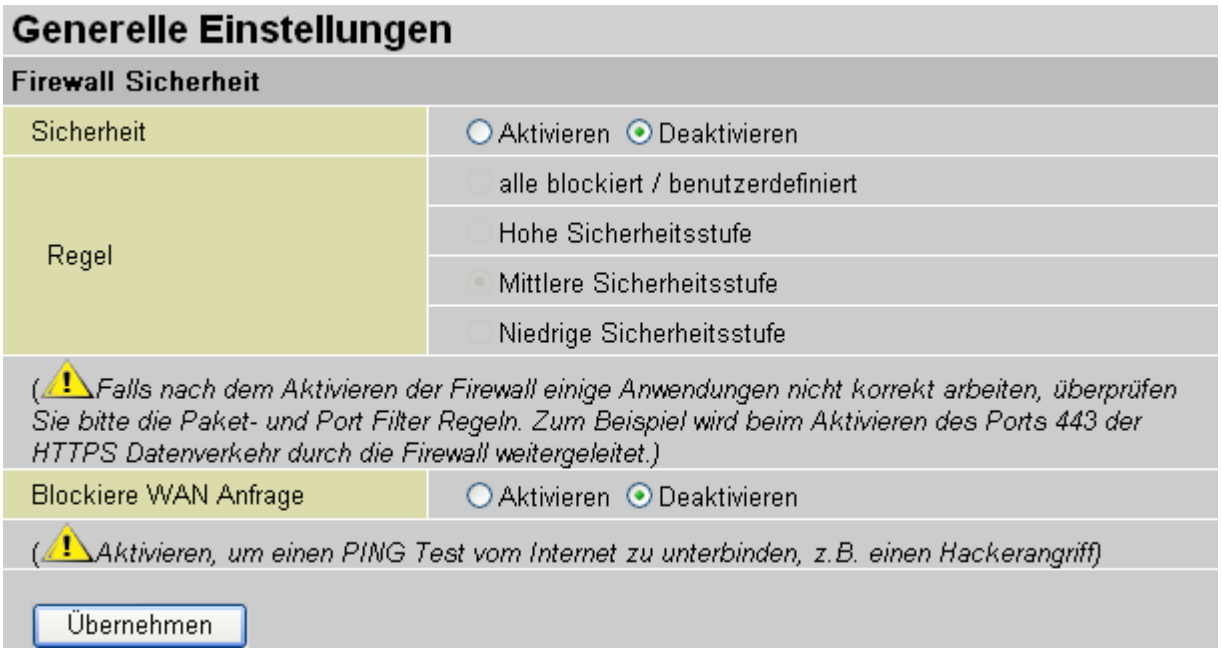
- **URL Filter:**
  Um bestimmte Webseiten zu blockieren, die vom lokalen Netzwerk besucht werden wollen

- **IM/P2P Blocking:**
  Erlaubt die Blockierung der Instant-Messenger MSN und Yahoo sowie die Blockierung der Peer-2-Peer Dienste BitTorrent und eMule/eDonkey

- **Firewall Log:**
  Hier kann definiert werden, ob die Tätigkeiten der Firewall mit im Ereignisprotokoll angezeigt werden sollen

3.4.1 Generelle Einstellungen

Sie können die Firewall deaktivieren, alle Filterregeln selber einstellen oder die Firewall aktivieren und damit die voreingestellten regeln nutzen, diese aber selber noch modifizieren so wie Sie es wünschen. Der Paket Filter kann verwendet werden um Port basierte Anwendungen und IP Adressen zu filtern.
Es gibt vier Optionen wenn Sie die Firewall aktivieren, diese sind:



Es gibt vier Optionen wenn Sie die Firewall aktivieren, diese sind:

- **Alle blockiert/Benutzerdefiniert:**
  keine vordefinierten Port- oder Adressregeln. Jedes hereinkommende (Internet nach LAN) und herausgehende (LAN nach Internet) Paket wird blockiert. Benutzer müssen Ihre eigenen Filterregeln aufstellen, um ins Internet gehen zu können.

- **Hohe/Mittlere/Niedrige Sicherheitsstufe:**
  Die vordefinierten Paket Filter Regeln für Hohe, Mittlere und Niedrige Sicherheitsstufe werden als Paket Filter Regeln im Menüabschnitt Paket Filter angezeigt.

Wählen Sie entweder Hohe, Mittlere oder Niedrige Sicherheitsstufe um die Firewall zu aktivieren.

Der einzige Unterschied zwischen diesen 3 Sicherheitsstufen, ist die Voreinstellungen der Paket Filter Regeln im Abschnitt **[PAKET FILTER]**. Die Firewall Funktionalität ist die gleiche für alle Einstellungen; es ist nur die Liste der Voreingestellten Paket Filter die sich dabei ändert.

Wenn Sie die Voreingestellten Sicherheitsstufen wählen und dann eigene Filter hinzufügen, können Sie vorläufig die Firewall deaktivieren und Ihre eigenen Einstellungen wiederherstellen wenn Sie den gleichen Sicherheitslevel wählen.

- **"Blockiere WAN Anfrage"**
  Dies ist eine eigene Funktion und steht nicht im Zusammenhang mit einer generell aktivierten oder deaktivierten Firewall. Hauptsächlich ist es um einen Scan von einer WAN Seite durch Hacker zu unterbinden.

HINWEIS: Jeder Remote Benutzer der versucht obige Einstellung vorzunehmen, kann eine Blockade der Konfiguration und des Router Management vom Internet aus hervorrufen. Daher nehmen Sie diese Einstellungen bitte vom LAN vor.

3.4.2 Paket Filter

Diese Funktion steht nur zur Verfügung wenn die Firewall aktiviert ist und eine der vier Sicherheitsstufen ausgewählt wurde (Alle blockiert, Hohe, Mittlere und Niedrige Sicherheitsstufe).

Paket Filter

TCP/UDP Filter hinzufügen | Raw IP Filter hinzufügen

Paket Filter Regeln

Regel-Name	Zeitplan	Quell IP / Netzmaske Ziel IP / Netzmaske	Protokoll	Quell Port(s) Ziel Port(s)	Eingehend Ausgehend		
mei_http	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Blockieren Erlauben	Bearbeiten	Löschen
mei_dns	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Blockieren Erlauben	Bearbeiten	Löschen
mei_tdns	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Blockieren Erlauben	Bearbeiten	Löschen
mei_ftp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Blockieren Erlauben	Bearbeiten	Löschen
		0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Blockieren	Bearbeiten	Löschen

Die vordefinierten Paket Filter Regeln in der Paket Filter Liste sind der Sicherheitsstufe angepasst und können der folgenden Tabelle entnommen werden.

Diese Tabelle hilft Aufschluss darüber zu geben, welche Regeln in welcher Sicherheitsstufe greifen:

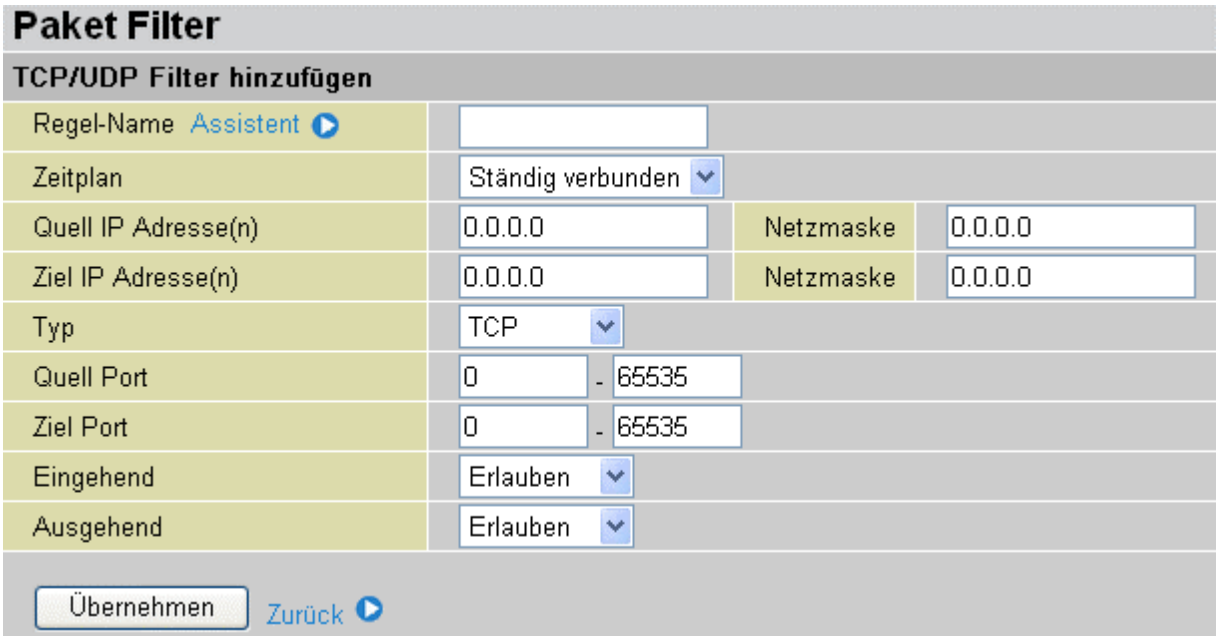
Sicherheitsabstufungen der Firewall: Voreingestellte Paket Filter

Anwendung	Protokoll	Port Nummer		Hohe Sicherheit		Mittlere Sicherheit		Niedrige Sicherheit	
		Start	End	Eingehend	Ausgehend	Eingehend	Ausgehend	Eingehend	Ausgehend
HTTP(80)	TCP(6)	80	80	NEIN	JA	NEIN	JA	NEIN	JA
DNS (53)	UDP(17)	53	53	NEIN	JA	NEIN	JA	JA	JA
DNS (53)	TCP(6)	53	53	NEIN	JA	NEIN	JA	JA	JA
FTP(21)	TCP(6)	21	21	NEIN	NEIN	NEIN	JA	NEIN	JA
Telnet(23)	TCP(6)	23	23	NEIN	NEIN	NEIN	JA	NEIN	JA
SMTP(25)	TCP(6)	25	25	NEIN	JA	NEIN	JA	NEIN	JA
POP3(110)	TCP(6)	110	110	NEIN	JA	NEIN	JA	NEIN	JA
NEWS(119) (Network News Transfer Protocol)	TCP(6)	119	119	NEIN	NEIN	NEIN	JA	NEIN	JA
RealAudio/ RealVideo (7070)	UDP(17)	7070	7070	NEIN	NEIN	JA	JA	JA	JA
PING	ICMP(1)	N/A	N/A	NEIN	JA	NEIN	JA	NEIN	JA
H.323(1720)	TCP(6)	1720	1720	NEIN	NEIN	NEIN	JA	JA	JA
T.120(1503)	TCP(6)	1503	1503	NEIN	NEIN	NEIN	JA	JA	JA
SSH(22)	TCP(6)	22	22	NEIN	NEIN	NEIN	JA	JA	JA
NTP(123)	UDP(17)	123	123	NEIN	JA	NEIN	JA	NEIN	JA
HTTPS(443)	TCP(6)	443	443	NEIN	NEIN	NEIN	JA	NEIN	JA
ICQ (5190)	TCP(6)	5190	5190	NEIN	NEIN	NEIN	NEIN	JA	JA

Eingehend: Internet zum LAN
Ausgehend: LAN zum Internet

TCP/UDP Filter hinzufügen:

Werden über die Tabelle hinaus weitere Anwendungen mit eigenen Protokollen genutzt, so müssen diese mit Angabe der verwendeten Portadressen über eine separat definierte Regel der Firewall bekannt und frei gegeben werden.



- **Regelname:**
  Beschreibung der Regel durch den Benutzer

- **Zeitplan:**
  Sie können den Zeitplan selber definieren. So können Sie bestimmte Regeln zu bestimmten Tageszeiten aktivieren. Für weitere Informationen hierfür lesen Sie bitte das Kapitel Zeitplan

- **Quell IP Adresse(n) / Ziel IP Adresse(n):**
  Dies ist der IP Adressen Filter, mit welchem Sie Datenverkehr von/zu bestimmten IP-Adressen erlauben/blockieren. Tragen Sie ebenfalls die Subnet Maske des IP Adressen Bereiches ein. Tragen Sie bei den IP Adressen und der Subnet Maske 0.0.0.0 wird der IP Adressen Filter nicht angewandt bzw. gilt für alle Adressen.

Tipp: Um einen Zugang zu blockieren von/zu einer einzigen IP Adresse, tragen Sie die gewünschte IP Adresse ein und geben als Subnet Maske "255.255.255.255" an.

- **Typ:**
  Ist der Paket Protokoll Typ. Wählen Sie TCP, UDP oder beide TCP/UDP

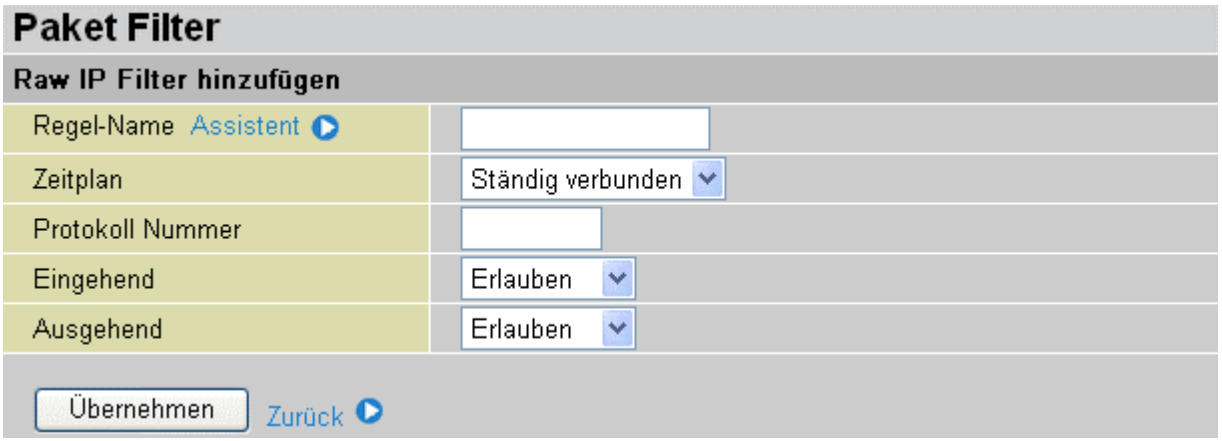
- **Quell Port:**
  Dieser Port oder der Port Bereich definiert den Port welcher von Remote/WAN (Internet) die Verbindung zur der lokalen Anwendung erhält oder nicht. Die Werkseinstellung lautet 0 ~ 65535. Es wird empfohlen dass diese Option von einem erfahren Anwender vorgenommen wird

- **Ziel Port:**
  Dieser Port oder der Port Bereich definiert die Anwendung

- **Eingehend / Ausgehend:**
  Wählen Sie Erlauben/Blockieren für den Zugriff zum Internet (Ausgehend) oder vom Internet (Eingehend)

- Klicken Sie auf **[ÜBERNEHMEN]** damit die Einstellungen übernommen werden

RAW IP Filter hinzufügen



- **Regelname:**
  Beschreibung der Regel durch den Benutzer

- **Zeitplan:**
  Sie können den Zeitplan selber definieren. So können Sie bestimmte Regeln zu bestimmten Tageszeiten aktivieren. Für weitere Informationen hierfür lesen Sie bitte das Kapitel Zeitplan

- **Protokoll Nummer:**
  Tragen Sie die Port Nummer ein, z.B. GRE 47

- **Eingehend / Ausgehend:**
  Wählen Sie Erlauben/Blockieren für den Zugriff zum Internet (Ausgehend) oder vom Internet (Eingehend)

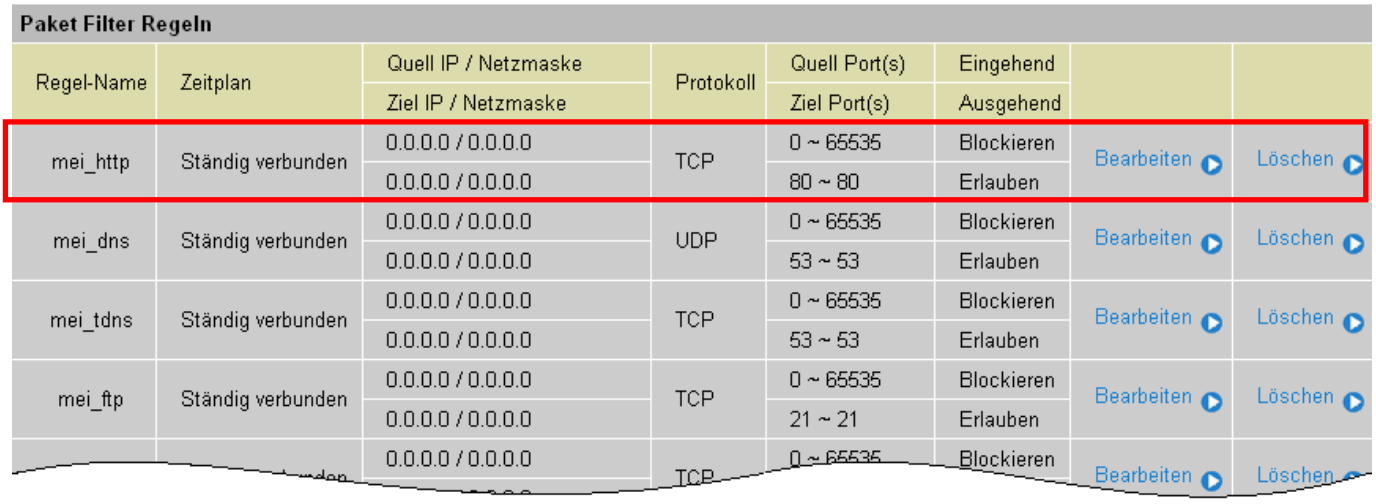
- Klicken Sie auf **[ÜBERNEHMEN]** damit die Einstellungen übernommen werden

Beispielkonfiguration: Konfiguration der Firewall für einen Zugriff vom Internet auf einen Computer im LAN, auf dem ein Webserver über Port 80 läuft.

Die voreingestellte Paket Filter Regel für HTTP (TCP Port 80) ist jeweils die gleiche, egal ob die Sicherheitsstufe auf Hohe, Mittlerer oder Niedrige Sicherheitsstufe eingestellt ist. Wenn Sie vom Internet auf den Webserver des Routers in Ihrem lokalen Netzwerk (LAN) zugreifen wollen und die Firewall aktiviert ist, müssen Sie die Paket Filter Regel für HTTP bearbeiten.

Wie Sie unten sehen können, sobald die Firewall aktiviert ist mit einer der drei Sicherheitsstufen (Hohe/Mittlere/Niedrige), ist der eingehende Zugang über HTTP nicht erlaubt.

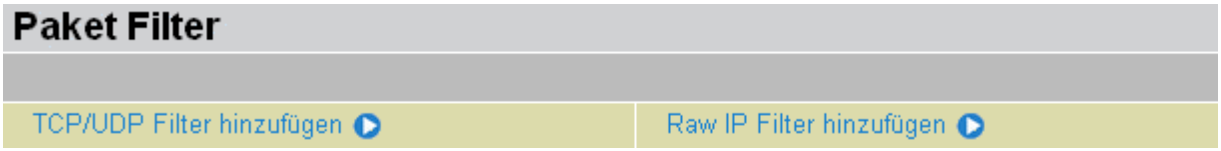
HINWEIS: Eingehend bedeutet vom Internet zum LAN, Ausgehend vom LAN zum Internet



Konfiguration der Paket Filter:

1. Klicken Sie auf Paket Filter:
   Sie sehen nun die Seite Paket Filter Regeln (in diesem Fall Niedrige Sicherheitsstufe)

HINWEIS: Sie können auch auf **[BEARBEITEN]** klicken, anstelle auf **[LÖSCHEN]**. Das Beispiel zeigt wie eine Paket Filter Regel hinzugefügt wird. Daher wird der vorhandene Eintrag zuerst gelöscht.

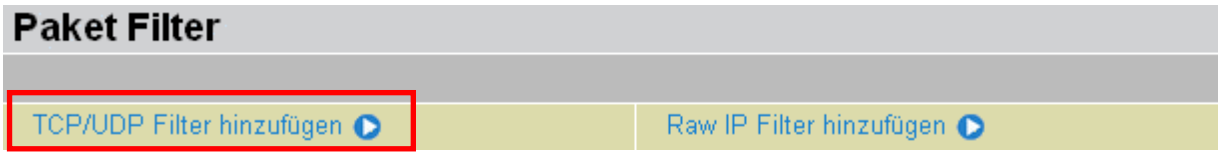


Paket Filter Regeln

Regel-Name	Zeitplan	Quell IP / Netzmaske Ziel IP / Netzmaske	Protokoll	Quell Port(s) Ziel Port(s)	Eingehend Ausgehend		
mei_http	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Blockieren Erlauben	Bearbeiten	Löschen
mei_dns	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Blockieren Erlauben	Bearbeiten	Löschen
mei_tdns	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Blockieren Erlauben	Bearbeiten	Löschen
mei_ftp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Blockieren Erlauben	Bearbeiten	Löschen
mei_tnet	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 23 ~ 23	Blockieren Erlauben	Bearbeiten	Löschen
mei_smtp	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 25 ~ 25	Blockieren Erlauben	Bearbeiten	Löschen
mei_pop3	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 110 ~ 110	Blockieren Erlauben	Bearbeiten	Löschen

2. Klicken Sie auf **[LÖSCHEN]** damit die existierende Paket Filter Regel für HTTP entfernt wird

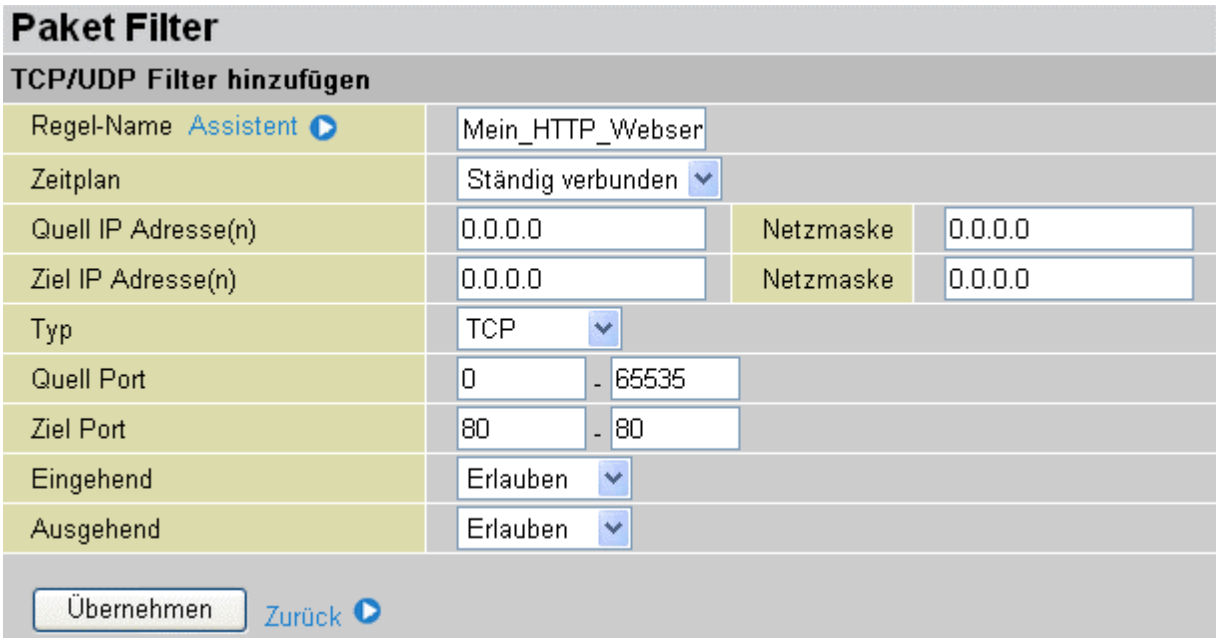
3. Klicken Sie auf **[TCP/UDP Filter hinzufügen]**



4. Tragen Sie einen Regel Namen ein, Wählen Sie den Zeitplan, Quell und Ziel IP Adressen, Typ, Quell und Ziel Port, Eingehend und Ausgehend.

Beispiel:

- **Regel Name:** *Mein_HTTP_Webserver*
- **Zeitplan:** *Always On*
- **Quelle / Ziel IP Adresse(n):** *0.0.0.0*
  (Damit jeder vom Internet auf den Webserver des Router zugreifen kann, wird hier 0.0.0.0 eingetragen)
- **Typ:** *TCP* ***(Siehe auchTabelle1: Voreingestellte Paket Filter)***
- **Quell Port:** *0-65535* ***(Jeder Port erhält die Erlaubnis sich zu verbinden)***
- **Ziel Port:** *80-80* ***(Dieser Port definiert HTTP)***
- **Eingehend / Ausgehend:** *Erlauben*



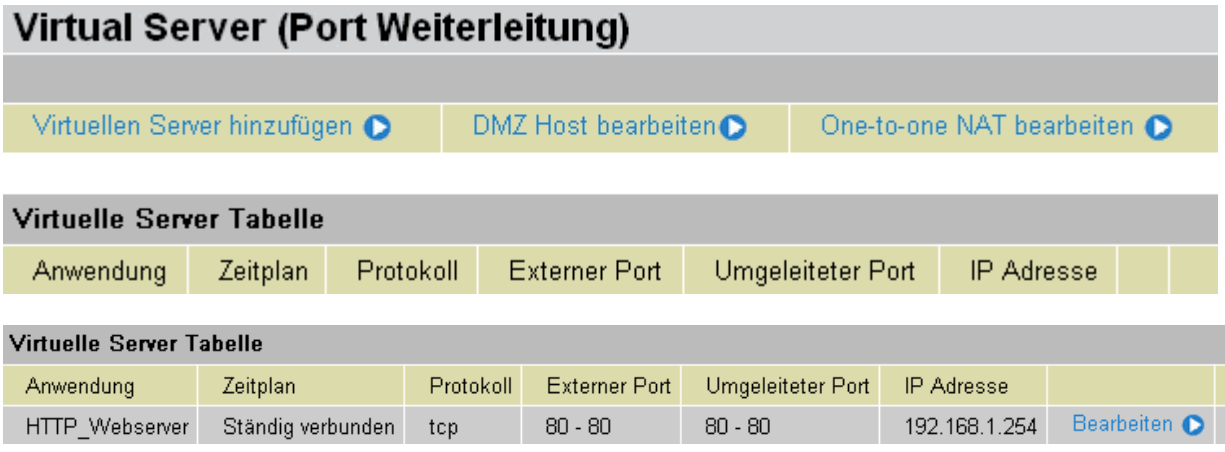
5. Die neue Paket Filter Regel sieht wie folgt aus:

Mein_HTTP_Webserver	Ständig verbunden	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Erlauben Erlauben	Bearbeiten	Löschen

6. Die Konfiguration des Virtuellen Servers (port forwarding/Portweiterleitung) muss nun vorgenommen werden, damit die HTTP Anfragen auf Port 80 zu dem lokalen Router weitergeleitet werden.

HINWEIS: Wie Sie die Portweiterleitung für HTTP vornehmen, entnehmen Sie bitte dem Kapitel **[VIRTUELLE SERVER]**

.



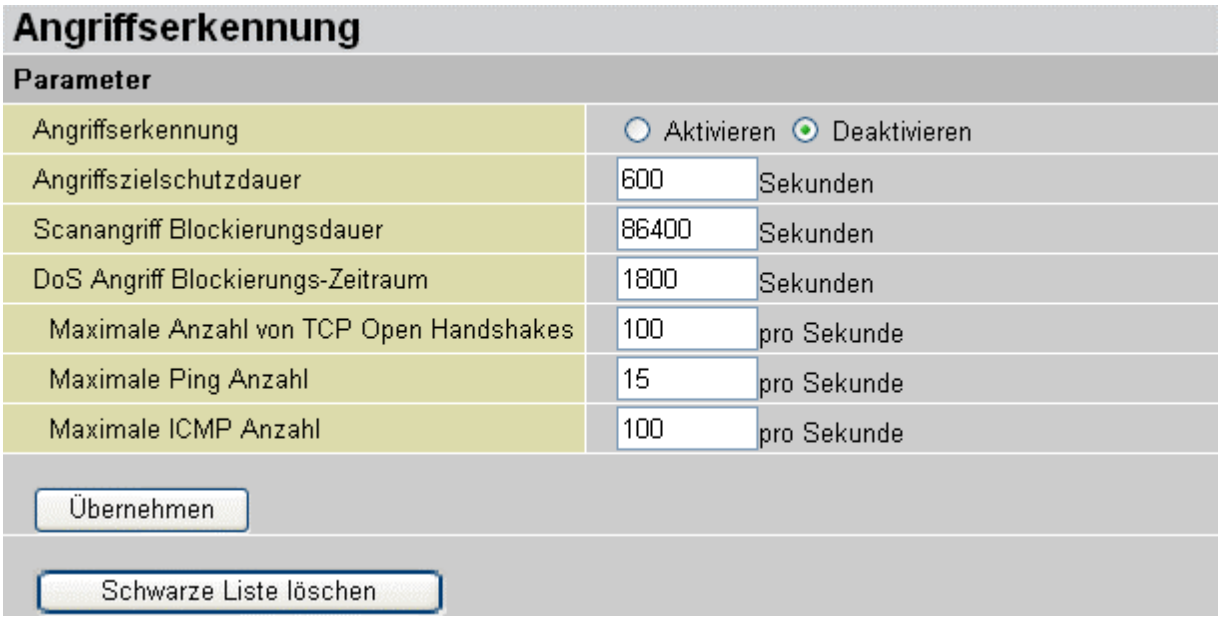
Virtuelle Server Tabelle

Anwendung	Zeitplan	Protokoll	Externer Port	Umgeleiteter Port	IP Adresse		
HTTP_Webserver	Ständig verbunden	tcp	80 - 80	80 - 80	192.168.1.254	Bearbeiten	Löschen

3.4.3 Angriffserkennung

Die Angriffserkennung (Intrusion Detection System / IDS) des Routers wird benutzt, um Hacker Attacken und ein Eindringen aus dem Internet zu verhindern. Wenn die Angriffserkennung Funktion der Firewall aktiviert ist, werden hereinkommende Pakete gefiltert und blockiert, je nachdem ob Sie als eine mögliche Hackerattacke, Eindringversuch oder andere Verbindungen gilt, die dem Router verdächtig vorkommt.

Schwarze Liste: Wenn der Router eine mögliche Attacke erkennt, wird die Verursacher IP oder Ziel IP in die Schwarze Liste (Blacklist) eingetragen. Jeder weitere Versuch diese IP zu nutzen wird so lange blockiert, wie die Zeiteinstellung in der Blockierungsdauer. Die Standardeinstellung dieser Funktion ist deaktiviert. Einige Angriffstypen werden direkt abgeblockt ohne die Schwarze Liste Funktionen zu nutzen, wie z.B. Land attack und Echo/CharGen Scan.



- **Angriffserkennung**:
  Wenn aktiviert, IDS blockiert Smurf Attacken. Werkseinstellung ist deaktiviert.

Blockierungsdauer:

- **Angriffszielschutzdauer**:
  Die Dauer für die Blockierung von *Smurf* attacks. Standardwert ist 600 Sekunden

- **Scanangriff Blockierungsdauer**:
  Dies ist die Dauer für den Host der einen möglichen Scan Angriff gestartet haben. Scan Angriffstypen einschließlich X'mas scan, IMAP SYN/FIN scan und andere. Standardwert ist 86400 Sekunden

- **DoS Angriff Blockierungs-Zeitraum**:
  Dies ist die Dauer des Blockens eines Hosts der einen möglichen Denial of Service (DoS) Angriff unternommen hat, inklusive Ascend Kill und WinNuke. Standardwert ist 1800 Sekunden.

- **Maximale Anzahl von TCP Open Handshakes**:
  Dies ist ein Schwellwert, der entscheidet, ob ein SYN Flood Angriff stattfindet oder nicht. Standardwert ist 100 TCP SYN per second.

- **Maximale PING Anzahl**:
  Dies ist ein Schwellwert, der entscheidet, ob ein ICMP Echo Storm stattfindet oder nicht. Standardwert ist 15 ICMP Echo Requests (PING) pro Sekunde

- **Maximale ICMP Anzahl**:
  Dies ist ein Schwellwert, der entscheidet, ob ein ICMP flood stattfindet oder nicht. Standartwert ist 100 ICMP Packets pro Sekunde mit der Ausnahme von ICMP Echo Requests (PING).

Für SYN Flood, ICMP Echo Storm und ICMP flood, warnt IDS den Benutzer im Event Log, es kann aber solche Attacken nicht verhindern.

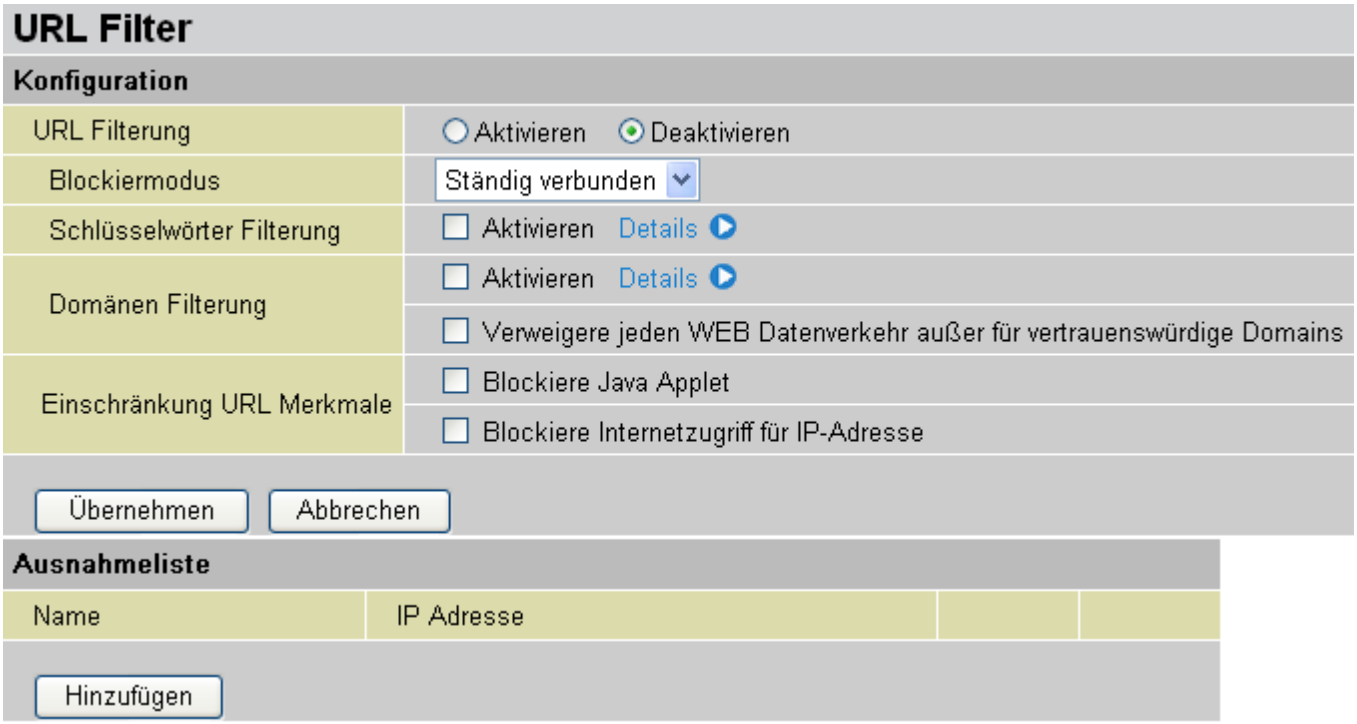
Hacker Attack Typen welche vom IDS erkannt werden

Angriff Name	Erkennungs Parameter	Schwarze Liste	Typen der Blockierungsdauer	Paket verwerfen	Anzeige im Protokoll
Ascend Kill	Ascend Kill data	Src IP	DoS	Ja	Ja
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Ja	Ja
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Ja	Ja
Land attack	SrcIP = DstIP			Ja	Ja
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Ja	Ja
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Ja	Ja
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Ja	Ja
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Ja	Ja
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Ja	Ja
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Ja	Ja
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Ja	Ja
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Ja	Ja
SYN Flood	Max TCP Open Handshaking Count(Default 100 c/sec)				Ja
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Ja
ICMP Echo	Max PING Count (Default 15 c/sec)				Ja

Src IP (Source IP): Quell IP
Src Port (Source Port): Quell Port
Dst Port (Destination IP): Ziel Port
Dst IP (Destination Port): Ziel IP

3.4.4 URL Filter

URL (Uniform Resource Locator – eine Adresse in der Form von http://www.carpo.com) Filter Regeln erlauben es Benutzer aus dem Netzwerk bestimmte Internetseiten anzusteuern. Es gibt keine Vordefinieren URL Filterregeln; Sie können diese Ihren Bedürfnissen anpassen.



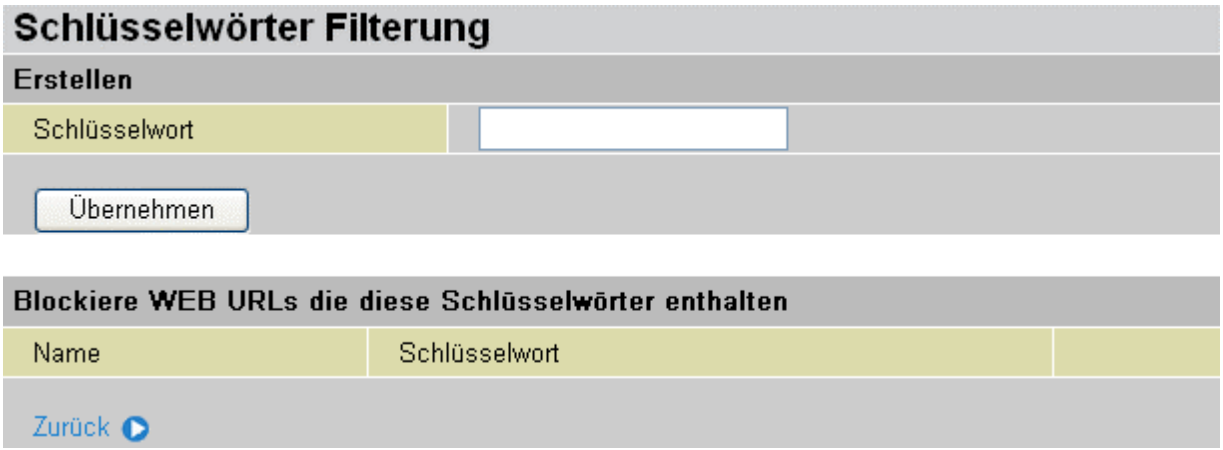
- **Aktivieren/Deaktivieren:** URL Filter aktivieren bzw. deaktivieren.

- **Blockiermodus:** Auflistung der verschieden URL Filter Modi. Die Voreinstellung ist deaktiviert

    - **Deaktiviert:**
      Der URL Filter ist deaktiviert
    - **Ständig verbunden:**
      Der URL Filter ist aktiviert und überprüft permanent die Anfragen
    - **TimeSlot1 ~ TimeSlot16:**
      Der von Ihnen gewählte Zeitplan. Sie können den URL Filter zu bestimmten Zeiten aktivieren, z.B. während den Bürozeiten. Für weitere Informationen hierfür lesen Sie bitte das Kapitel Zeitplan

- **Schlüsselwörter Filterung:** Erlaubt es bestimmte Schlüsselwörter in einer URL zu blockieren anstelle einer kompletten URL. (z.B. ein Bild namens "werbung.gif"). Wenn aktiviert, wird Ihre spezielle Schlüsselwörter Liste überprüft, ob ein Wort davon in der URL vorhanden ist und dadurch blockiert wird. Bitte beachten Sie dass der URL Filter nur den Web Browser (HTTP) blockiert, die den Port 80 nutzen

Zum Beispiel, die URL ist „**http://www.carpo.com/abcde.html**", und wird fallen gelassen weil das Schlüsselwort "**abcde**" dort erscheint.



Diese Funktion überprüft, ob der Domain Name in der URL in der Liste der erlaubten oder verbotenen URLs ist. Wenn dies zutrifft, wird die URL Anforderung gesendet (Trust) oder fallen gelassen (Forbidden). Für diese Funktion müssen beide Kontrollkästchen aktiviert sein.

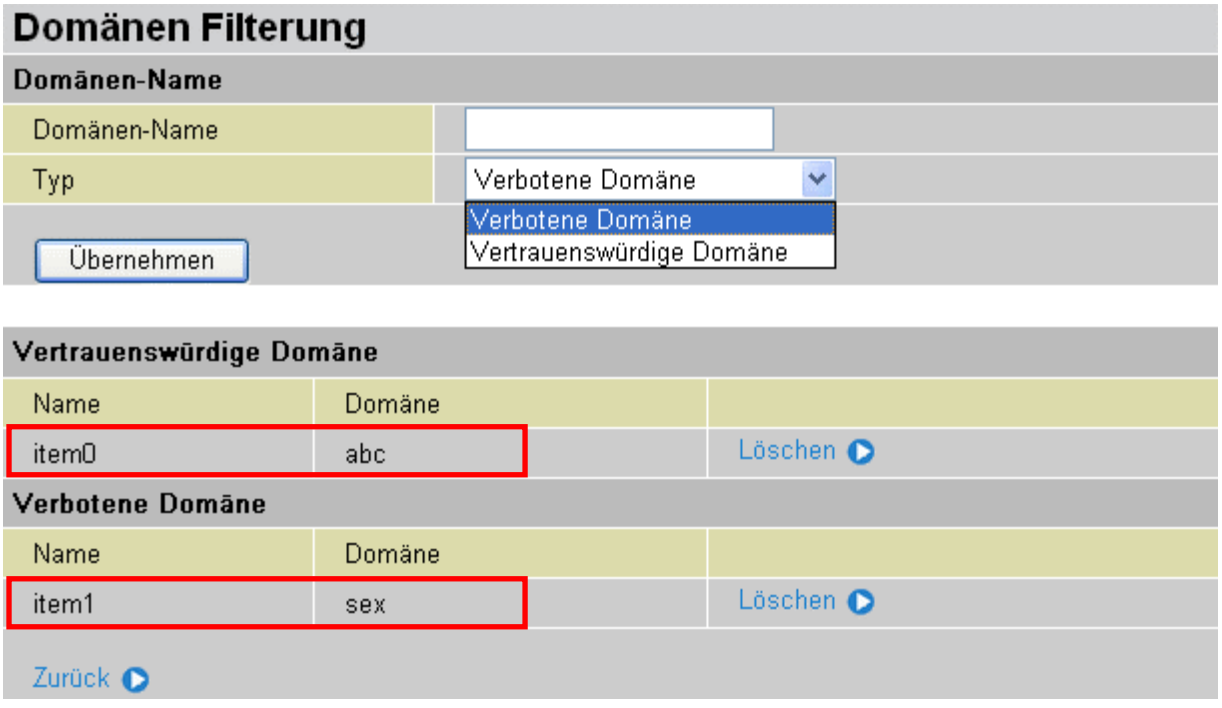
Die Prozedur ist wie folgt:

1. Prüft ob die Domain in der URL in der vertrauenswürdigen Liste ist. Wenn ja, wird die Verbindungsanfrage an den entfernten Server gesendet.

2. Wenn nicht, wird die verbotene Liste überprüft und die Verbindungsanfrage wird fallen gelassen.

3. Wenn ein Paket keines der beiden Bedingungen erfüllt, wird die Anfrage an den entfernten Server gesendet.

4. Bitte beachten Sie das die Domain spezifiziert wird und nicht die volle URL. Zum Beispiel um Verkehr nach **www.sex.com**, geben Sie "**sex**" oder "**sex.com**" anstelle von "**www.sex.com**". Im folgenden Beispiel wird die URL Anfrage für **www.abc.com** an den entfernten Server gesendet weil diese in den erlaubten Seiten enthalten ist während die URL Anfrage für **www.sex** oder **www.sex.com** nicht ausgeführt wird, weil **sex.com** in der verbotenen Liste enthalten ist.



- **Einschränkung URL Merkmale:** Diese Funktion erweitert die Einschränkung der URL Regeln

  Beispiel: Andy möchte jeden WEB Datenverkehr deaktivieren, ausgenommen denen in der vertrauenswürdigen Domäne, damit verhindert wird das Bobby auf andere Webseiten zugreifen kann. Andy wählt beide Funktionen der Domänen Filterung und denkt Bobby hat nun keinen Zugriff auf andere Webseiten. Aber Bobby kennt die Funktion Domänen Filterung und weiß dass er auf eine Webseite über deren IP Adresse zugreifen kann. Wenn dies der Fall ist, so ist die Funktion, Blockiere Internetzugriff für IP Adresse sehr hilfreich für Andy. Nun kann Andy verhindern dass Bobby Zugriff auf andere Seiten hat.

- **Blockiere Java Applet:** Diese Funktion kann Web Inhalte blockieren welche Java Applets beinhalten. Dies ist zum Schutz Ihres Systems wenn jemand einen Angriff über ein HTTP Protokoll versucht

- **Blockiere Internetzugriff für IP Adresse:** Verhindert das jemand die IP Adresse als URL benutzt um die Domain Filterung Funktion zu umgehen

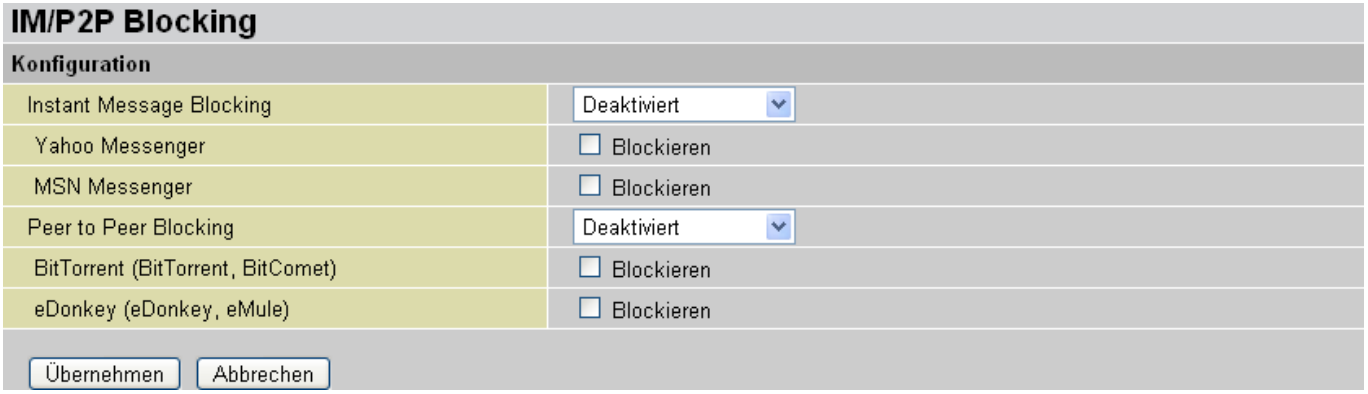
3.4.5 P2P/IM Blocking

In diesem Menü kann der Betrieb von Peer-2-Peer Diensten sowie Instant Messenger eingeschränkt werden. Hierbei sind folgende Dienste genau betroffen:

- **Instant Messenger:**
  - Windows Live Messenger (MSN)
  - Yahoo Messenger

- **Peer To Peer Tauschbörsen:**
  - Bittorrent
  - eDonkey

Mit einem Haken vor den jeweiligen Dienst aktiviert man die Sperrung hierfür. Wird der Haken wieder entfernt so deaktiviert man auch die Sperrung des jeweiligen Service.



Folgende Einstellungsmöglichkeiten sind gegeben:

- **Instant Message Blocking:** Hier lässt sich Sperrung zeitlich auf ein zuvor unter ERWEITERT – ZEITPLAN definierten Zeitraum eingrenzen

- **Peer To Peer Blocking:** Hier lässt sich die Sperrung der Peer To Peer Dienste zeitlich eingrenzen. Es können auch zuvor unter ERWEITERT – ZEITPLAN definierte Zeiträume gewählt werden

3.4.6 Firewall Protokoll

Firewall Protokoll zeigt die Informationen jeder unerwartenden Aktion Ihrer Firewall Einstellungen an.

Klicken Sie auf **[AKITIVEREN]** damit diese Protokolle angezeigt werden.

Nachdem das Protokoll aktiviert wurde, kann dies unter **[Status]** → **[Ereignisanzeige]** einsehen werden.

3.5 VoIP (Voice over Internet Protocol)

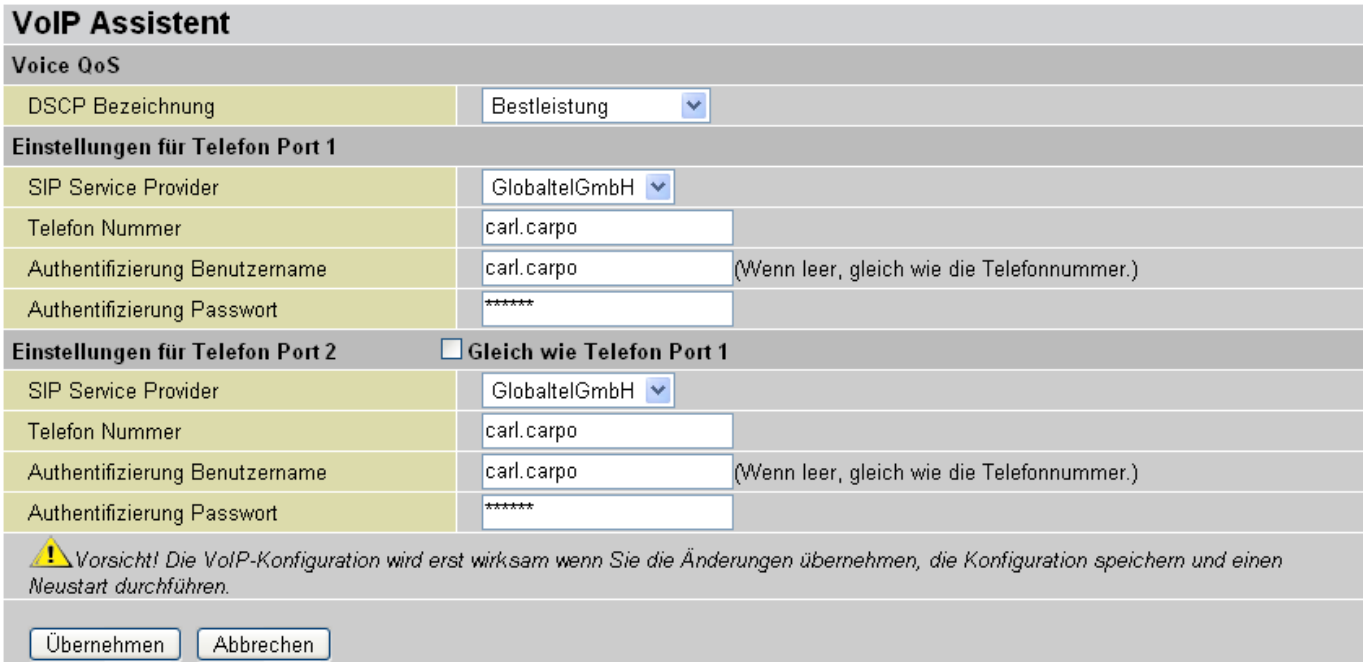
VoIP ermöglicht es Ihnen Telefongespräche über das Internet anstelle dem Festnetz (PSTN = Public Switched Telephone Network) zu führen. Die Gespräche sind nicht nur kosteneffektiv, gerade für Ferngespräche geeignet, sondern auch qualitativ hochwertig.

In dieser Kategorie befinden sich folgende Untermenüs:

- **Assistent**
- **Generelle Einstellungen**
- **Telefon Port**
- **PSTN Dial Plan**
- **VoIP Wählplan**
- **Anruffunktionen**
- **Klingeln & Rufton**

3.5.1. Assistent

Dieser Menüpunkt ermöglicht eine einfache Konfiguration Ihres VoIP Dienstanbieters. Telefon Port 1 und 2 können bei unterschiedlichen SIP Providern registriert sein.



Voice QoS

- **DSCP Bezeichnung:**
  Differentiated Services Code Point (DSCP), dies sind die ersten 6 Bits im ToS Byte. DSCP Marking erlaubt dem Anwender anhand des DSCP Wertes den Verkehr zu klassifizieren bevor die Pakete zum nächsten Router gesendet werden

Einstellungen für Telefon Port 1

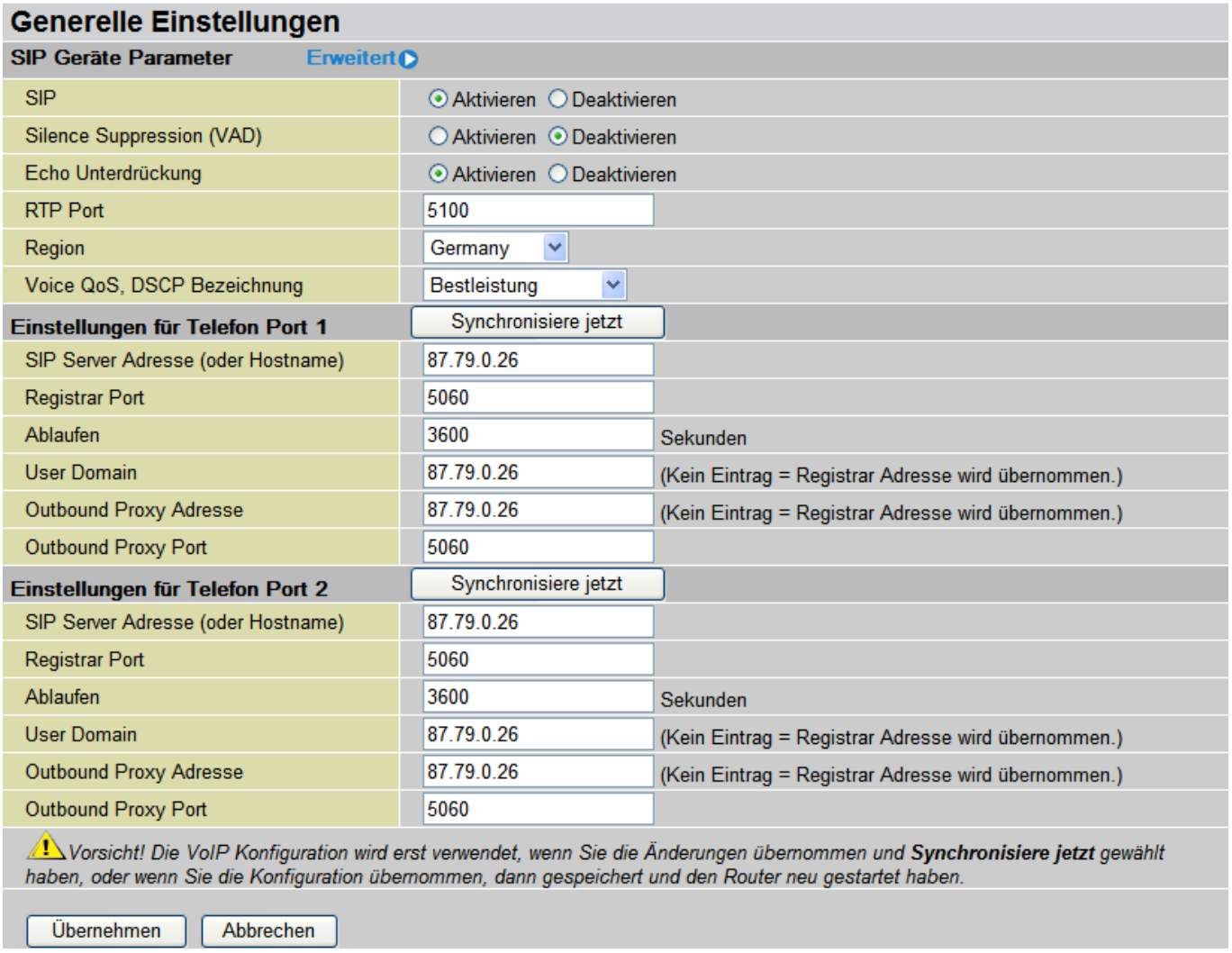
- **SIP Service Provider:**
  Hier können Sie den Service Provider auswählen. Wenn Sie eine Auswahl getroffen haben, werden die Werte in den Generellen Einstellungen (siehe weiter unten) automatisch eingetragen
- **Profil wählen:**
  Hier können Sie selber einen SIP Provider auswählen, sofern er nicht in der SIP Service Provider Auswahlliste steht. Zuerst müssen Sie aber unter VoIP (benutzerdefinierte Profile) ein Profil erstellen. Weitere Informationen finden Sie unter VoIP Benutzerdefinierte Profile
- **Telefon Nummer:**
  In diesem Feld tragen Sie die Benutzerkennung Ihres SIP Accounts ein
- **Authentifizierung Benutzername:**
  Der gleiche Eintrag wie bei der Telefon Nummer
- **Authentifizierung Passwort:**
  In diesem Feld tragen Sie das Passwort Ihres SIP Accounts ein

Einstellungen für Telefon Port 2

- **Gleich wie Telefon Port 1:**
  Nutzt die gleichen Einstellungen wie am Telefon Port 1. Eingehende Gespräche werden zeitgleich an beiden Telefon Ports signalisiert
- Restliche Einstellungsmöglichkeiten gleichen denen von Telefon Port 1

3.5.2. Generelle Einstellungen

Dieser Abschnitt spiegelt Einstellungen aus den Basiseinstellungen des VoIP Modules und dem ausgewählten Service Provider wieder.



SIP Geräte Parameter

- **SIP:**
  SIP als VoIP Anruf/Signal Protokoll verwenden. Werksseitig ist SIP deaktiviert
- **Silence Suppression (VAD):**
  Voice Activation Detection verhindert, dass bei einer Gesprächspause die "natürliche" Stille übertragen wird und Bandbreite verbraucht wird. Es ist auch bekannt als Silence Suppression, eine Software Anwendung welche die Bandbreite nur reserviert wenn Sprachaktivitäten erkannt werden. Werksseitig ist die Funktion **[Aktiviert]**
- **Echo Unterdrückung:**
  G.168 Echo Canceller ist ein ITU-T Standard. Es wird benutzt damit das Echo isoliert wird während Sie am Telefon sind. Dies hilft, dass Ihre eigene Stimme nicht zu sehr reflektiert wird, während Sie ein Telefongespräch führen. Werksseitig ist die Funktion **[Aktiviert]**
- **RTP Port:**
  Geben Sie hier den RTP Port an, welcher für verschiedene Endpunkte zugewiesen werden kann und unterschiedliche Gespräche, sofern vorhanden, dem Endpunkt zuweist. (Bereich von 5100 bis 65535, Werkseinstellung ist 5100)
- **Region:**
  Hier können Sie aus dem Drop-Down Menü das Land auswählen in welchem das VoIP Gerät arbeiten muss. Wenn ein Land ausgewählt wurde, werden automatisch die Länder-spezifischen Parameter verwendet
- **Voice QoS, DSCP Bezeichnung:**
  Differentiated Services Code Point (DSCP), dies sind die ersten 6 Bits im ToS Byte. DSCP Marking erlaubt dem Benutzer den Datenverkehr zu klassifizieren basierend auf dem DSCP Wert und dementsprechend die Pakete an den Router zu senden. Diese Einstellung sollte

immer auf **[Bestleistung]** belassen werden, da es anderenfalls zu Beeinträchtigungen während der Internettelefonie kommen kann

Einstellungen für Telefon Port 1

- **Registrar Adresse (oder Hostname):**
  Geben Sie hier die SIP Registrar IP Adresse an
- **Registrar Port:**
  Geben Sie hier den SIP Registrar Port an, über welchen die Registrieranfragen des VoIP Gerätes abgehört werden
- **Ablaufen:**
  Verfallszeit für das Senden der Registrierungsnachricht
- **User Domain/Realm:**
  Falls vorhanden können Sie einen unterschiedliche Domain für den SIP Proxy Server angeben
- **Outbound Proxy Adresse:**
  Geben Sie hier die SIP Outbound Proxy Server IP Adresse an. Dieser Parameter ist sehr hilfreich wenn das VoIP Gerät hinter NAT verwendet wird
- **Outbound Proxy Port:**
  Geben Sie hier den SIP Outbound Proxy Port an, über welchen Mitteilungen abgehört werden

Einstellungen für Telefon Port 2:

- Einstellungsmöglichkeiten gleichen denen von Telefon Port 1

HINWEIS: Wenn die Einstellungen für VoIP verändert werden, ist es wichtig diese Änderungen unter **[Generelle Einstellungen]** über die Funktion **[SYNCHRONISIERE JETZT]** direkt zu übernehmen. Anderenfalls werden weiterhin die alten Einstellungen beibehalten. Um die Veränderungen dauerhaft zu speichern muss die Funktion **[KONFIGURATION SPEICHERN]** verwendet werden!

Generelle Einstellungen - Erweitert

Klickt man in den Generellen Einstellungen auf den Punkt „Erweitert" so erhält man zusätzliche Einstellungsmöglichkeiten.

Parameter

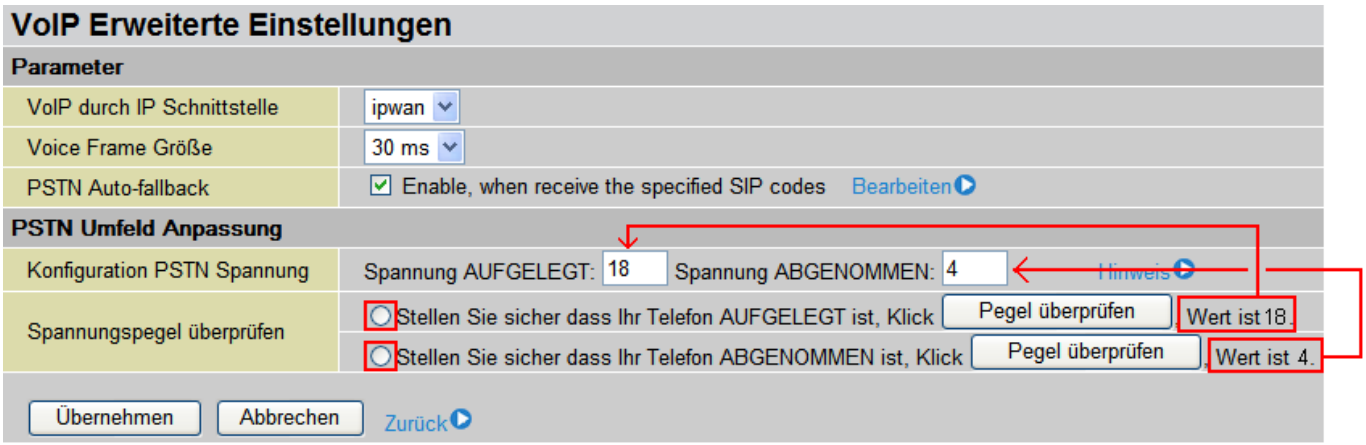
Folgende Möglichkeiten zur Konfiguration sind gegeben:

- **VoIP durch IP Schnittstelle:**
  - **ipwan:** Die VoIP-Registrierung wird über den WAN Port am Router vorgenommen. Die Daten vom SIP Server werden also darüber bezogen.
  - **iplan:** Die VoIP-Registrierung wird über einen LAN Port am Router vorgenommen. Die Daten vom SIP Server werden also darüber bezogen.

- **Voice Frame Größe:** Bestimmt den Zeitraum, für denen Daten der menschlichen Sprache gesammelt und in einem Datenpaket (Frame) verschickt werden

- **PSTN Auto-fallback:** Schaltet die automatische Wahl der Festnetzleitung ein, wenn über die VoIP Verbindung kein Gespräch aufgebaut werden konnte.

  Über den Button **„Bearbeiten"** können SIP Responsecodes bestimmt werden, bei denen die alternative Wahl der Festnetzleitung genutzt werden soll!



PSTN Umfeld Anpassung:

Die Festnetz (PSTN) Umfeld Anpassung hilft, die Spannung für ABGENOMMEN bzw. AUFGELEGT für Ihr Umfeld zu erkennen. Diese Funktion sollte verwendet werden, sofern die werksseitig eingestellten Werte falsch sind und daraus resultierend Anrufe nicht richtig erkannt werden, z.B. Anrufe nach 5 Sekunden beendet werden bevor der andere Teilnehmer abgenommen hat. Die aktuellen Pegel werden anhand des Umfeldes ermittelt inklusive der Anzahl und Art der Telefone.

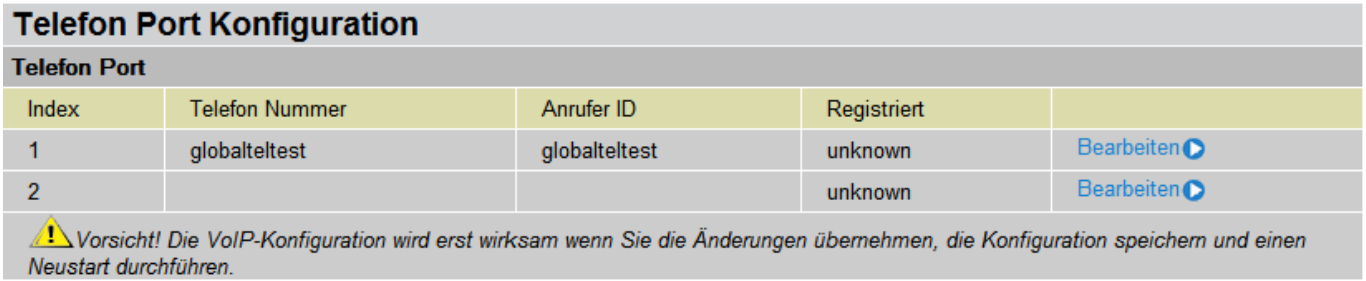
Damit Sie Ihr Telefon auf **ABGENOMMEN** (OFFHOOK) setzen, nehmen Sie den Hörer ab und drücken Sie Hook/Flash (Gabel oder R-Taste) bis Sie den normalen PSTN Wählton hören, nicht den VoIP Wählton. Warten Sie einige Sekunden und klicken dann auf die Schaltfläche Pegel überprüfen. Sie sollten den ABGENOMMEN/OFFHOOK Wert für jedes an dem Router angeschlossene Telefon überprüfen. Setzen Sie den Wert für die Spannung ABGENOMMEN auf den niedrigsten Wert von allen ermittelten Werten, z.B. wenn Ihre Telefone die Werte 4, 5 und 7 melden sollten Sie den Wert für Spannung ABGENOMMEN auf 4 setzen.

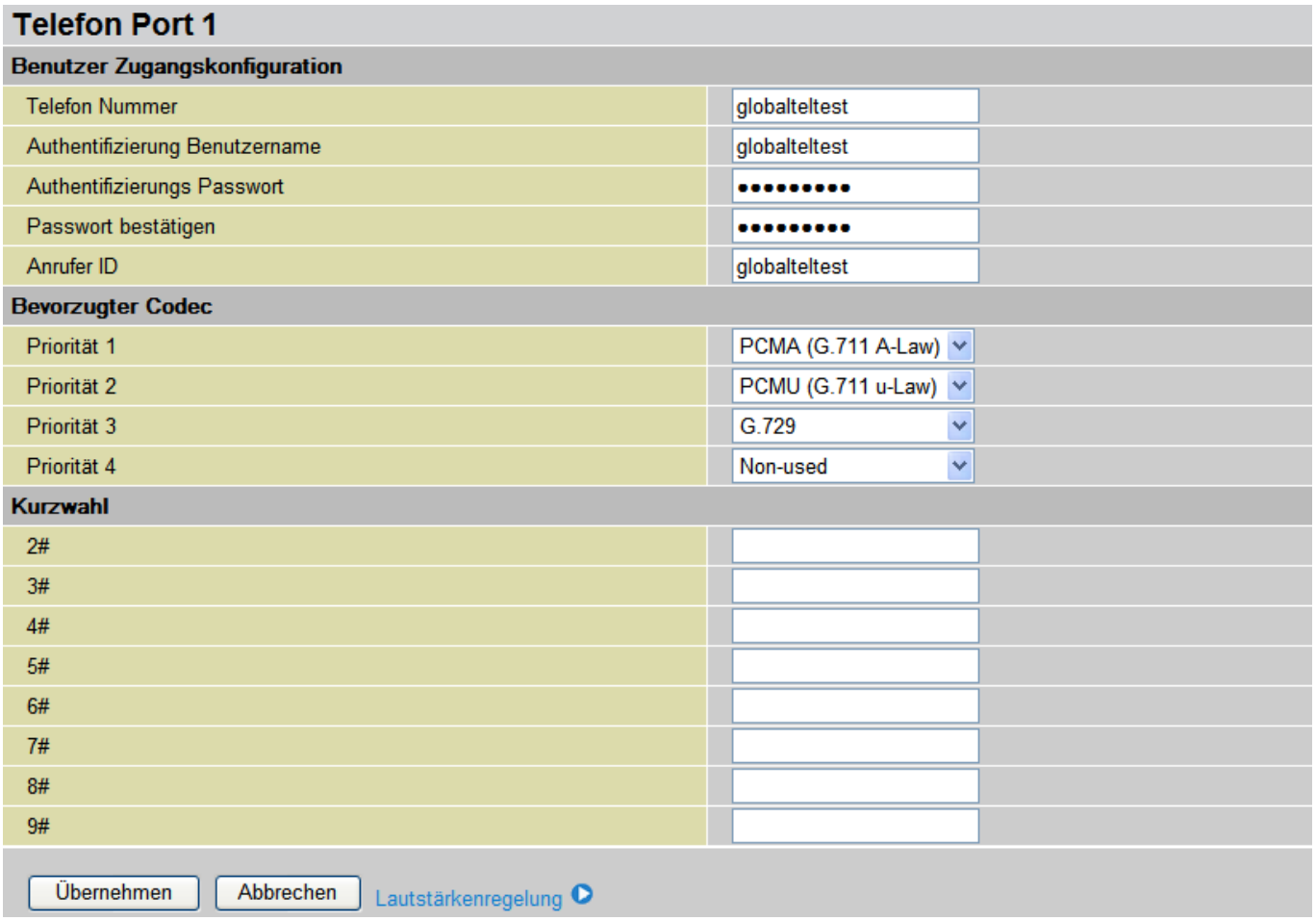
Wiederholen Sie den Vorgang für den Spannungspegel „**AUFGELEGT**".

Hinweis: Die ermittelten Werte werden nicht automatisch durch die Pegel Überprüfung gesetzt, Sie müssen den niedrigsten Wert selber eintragen nachdem Sie alle Ihre Telefone getestet haben. Die **Werte sind nur bei angeschlossener Festnetzleitung (Line) messbar!**

3.5.3 Telefon Port

Dieser Abschnitt zeigt Ihnen den Status des jeweiligen Telefon Ports an und erlaubt es Ihnen weitere Einstellungen vorzunehmen. Klicken Sie auf **[BEARBEITEN]** damit Sie weitere Einstellungen vornehmen können.





Folgende Einstellungen können verändert werden:

Benutzer Zugangskonfiguration

- **Telefon Nummer:**
  In diesem Feld tragen Sie die Benutzerkennung Ihres SIP Accounts ein
- **Authentifizierung Benutzername:**
  Der gleiche Eintrag wie bei der Telefon Nummer
- **Authentifizierung Passwort:**
  In diesem Feld tragen Sie das Passwort Ihres SIP Accounts ein
- **Passwort bestätigen:**
  Wiederholen Sie das Passwort
- **Anrufer ID:**
  Der Eintrag wird als Rufnummer übermittelt

Bevorzugter Codec

Codec (Engl. Akronym aus coding und decoding), codieren und decodieren der analogen Audiodaten. Stellen Sie die Priorität der Sprachkompression ein. Priorität 1 hat die höchste Priorität.

- **G.729: Audio Codec:**
  wird verwendet um Sprachinformationen in einem einzigen Paket zu codieren und decodieren. 8kbit/s Bandbreite wird benötigt.
- **G.711µ-LAW:**
  Audio Codec ohne Komprimierung, µ-LAW verwendet PCM (Pulse Code Modulation) zum codieren und decodieren und in ein 14-bit lineares Sample zu konvertieren. 64kbit/s Bandbreite wird benötigt.
- **G.711A-LAW:**
  Audio Codec ohne Komprimierung, µ-LAW verwendet PCM (Pulse Code Modulation) zum codieren und decodieren und in ein 13-bit lineares Sample zu konvertieren. 64kbit/s Bandbreite wird benötigt.
- **Non-used:**
  Nur unter Priorität 2 und 3 wählbar. Wenn nur der Codec unter Priorität 1 verwendet werden soll

HINWEIS: Werksseitig ist folgende Reihenfolge zugeordnet:
G.729 > G.711µ-LAW > G.711A-LAW

Kurzwahl
Vorgesehen für die Speicherung von Rufnummern welche Sie häufig verwenden.

- Sie können die Nummern 2 bis 9 verwenden
- Nach betätigen der Nummer 2 - 9 drücken Sie nur die Raute-Taste (#) um die Kurzwahl zu verwenden.
  z.B.: Kurzwahl zu der Nummer 9, drücken Sie einfach die 9, dann die Raute-Taste #. Der Router wählt nun automatisch die Nummer welche Sie unter dem Eintrag 9 eingegeben haben.
- Anstelle der Rufnummer können Sie auch IP Adressen oder Domainnamen bei der Kurzwahl eintragen

Beispiele:
Ihr Freund Tim gibt Ihnen eine SIP URL als sip: 89755@192.246.69.223, dann können Sie folgendes Eintragen 89755@192.246.69.223

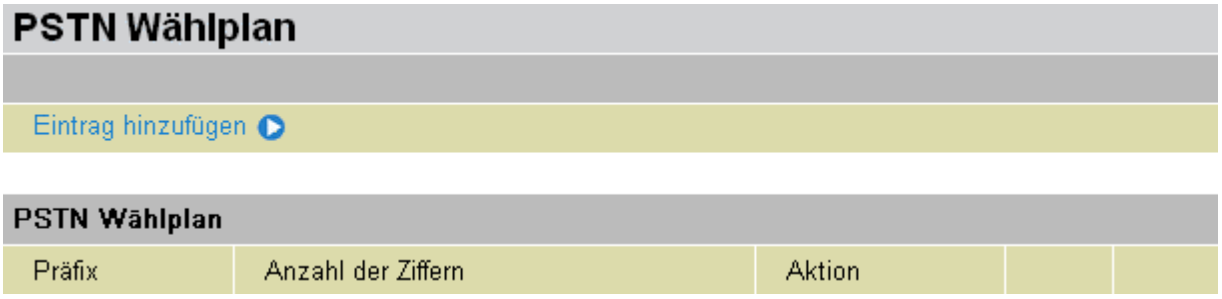
Ihr Freund Felix gibt Ihnen eine SIP URL als sip: felix@iptel.org, dann können Sie folgendes Eintragen „felix@iptel.org"

Wenn Ihr Freund Greg Ihnen nur eine IP Adresse "192.246.56.56" gibt, dann können Sie diese Eintragen "192.246.56.56". Im Falle, dass der Benutzer DDNS verwendet, können Sie auch die Domain eingeben, z.B. „sipname@dyndns.org".

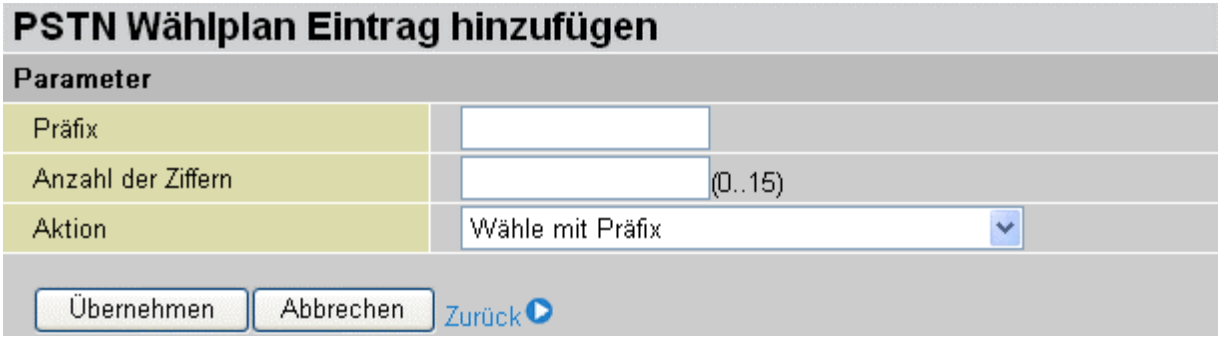
3.5.4 PSTN Wählplan

Dieser Abschnitt beschreibt wie Sie den Wechsel zwischen "VoIP und PSTN/Festnetz" konfigurieren. Sie können Wählpläne erstellen damit reguläre Gespräche nicht über VoIP sondern über PSTN/Festnetz hergestellt werden. Der Präfix ist erforderlich, damit eine Unterscheidung zwischen VoIP und den Festnetz Anrufen getätigt werden kann. Wenn die gewählte Nummer mit dem Präfix übereinstimmt welcher im Wählplan eingetragen ist, wird die anzurufende Nummer über das Festnetz verbunden. Andernfalls wird über das VoIP Netzwerk verbunden.
Erinnerung!

HINWEIS: Damit dieses Feature genutzt werden kann, müssen Sie mit einem SIP Server verbunden sein.



Klicken Sie auf **[Eintrag hinzufügen]** und eine neue Wählregel für das Festnetz zu definieren:



- **Präfix:** Geben Sie die Nummer(n) ein die den Wechsel zum PSTN/Festnetz festlegen

- **Anzahl der Ziffern:** Geben Sie die Anzahl der Ziffern ein mit den Sie raus wählen wollen. Maximal 15 Ziffern

- **Aktion:** Wählen Sie die Wählmethode für den PSTN/Festnetz Anrufe

    - **Wähle mit Präfix:**
      Die gewählte Rufnummer inkl. des Präfix wird für den PSTN/Festnetzanruf verwendet
      Hinweis: Die aktuell gewählte Rufnummer muss mit der Anzahl der Ziffern übereinstimmen.

    - **Wähle ohne Präfix:**
      Die gewählte Rufnummer ohne Präfix wird für den PSTN/Festnetzanruf verwendet.
      Hinweis: Die aktuell gewählte Rufnummer muss mit der Anzahl der Ziffern übereinstimmen.

    - **Wählen nach Zeitüberschreitung:**
      Die gewählte Rufnummer wird über PSTN/Festnetz gesendet inkl. dem Präfix wenn die Zeitüberschreitung erreicht wird. Die Zeitüberschreitung wird aktiviert wenn in einer bestimmten Zeit nicht mehr gewählt wurde.
      Hinweis: Die aktuell gewählte Rufnummer darf NICHT die Anzahl der Ziffern übertreffen.

    - **Wählen nach Zeitüberschreitung ohne Präfix:**
      Die gewählte Rufnummer wird über PSTN/Festnetz gesendet ohne dem Präfix wenn die Zeitüberschreitung erreicht wird. Die Zeitüberschreitung wird aktiviert wenn in einer bestimmten Zeit nicht mehr gewählt wurde.
      Hinweis: Die aktuell gewählte Rufnummer darf NICHT die Anzahl der Ziffern übertreffen.

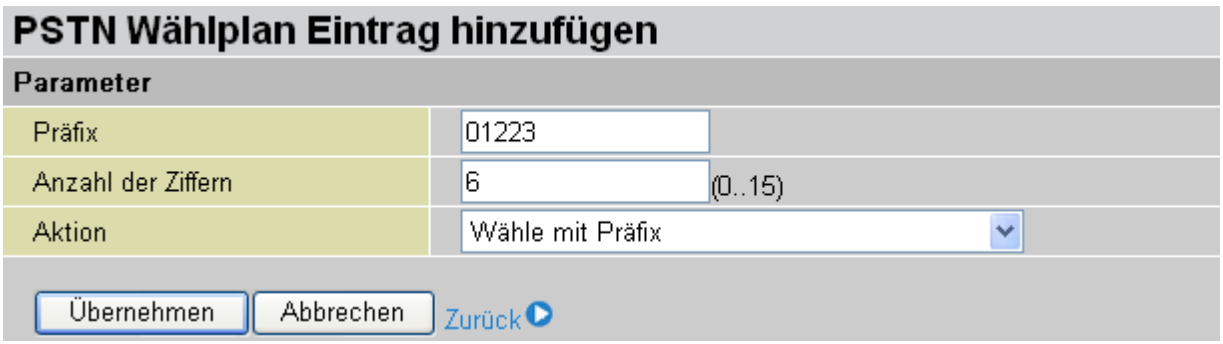
HINWEIS: Folgende Situationen veranlassen Telefon Port 1 und 2 direkt über PSTN/Festnetz zu wählen.

- ***Stromausfall. Gerät ist aus.***
- ***Ausfall der Internetverbindung, z.B. keine WAN IP Adresse***
- ***SIP Service ist nicht erreichbar.***

Ausgenommen:
- Benutzer hat manuell die Registrierung deaktiviert
- Benutzer hat einen falschen Benutzernamen und/oder Passwort eingetragen
- Benutzer wählt eine falsche SIP Nummer

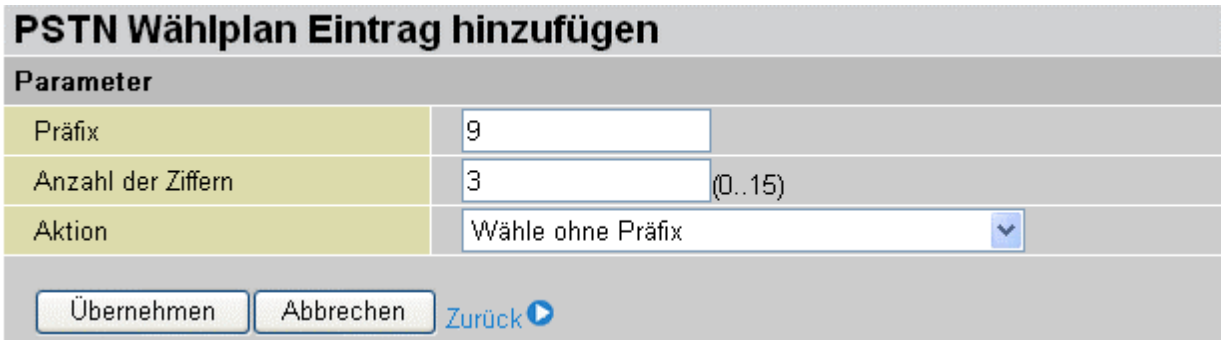
PSTN Wählplan Beispiele:

1) Wählen mit Präfix



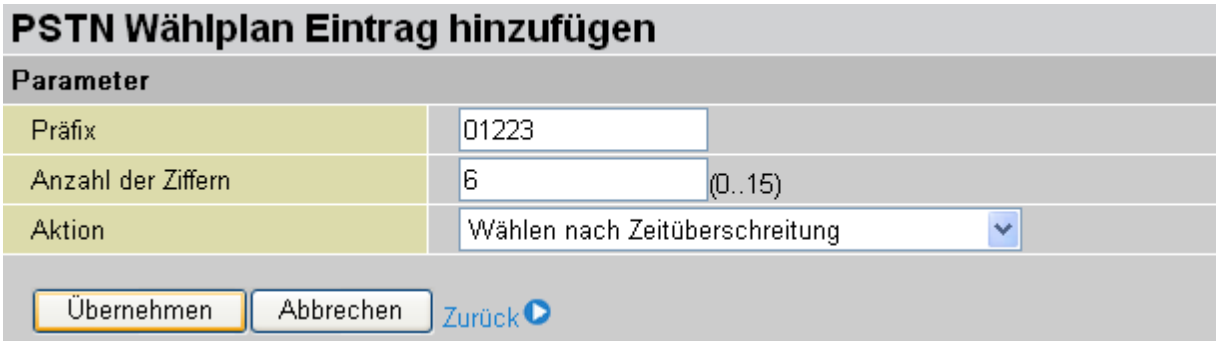
Wenn Sie 01223 707070 wählen, wird die Nummer 01223707070 für einen regulären Anruf über den FXO Port (Festnetz) gewählt.

2) Wählen ohne Präfix



Wenn Sie 9102 wählen, wird die Nummer 102 für einen regulären Anruf über den FXO Port (Festnetz) gewählt.

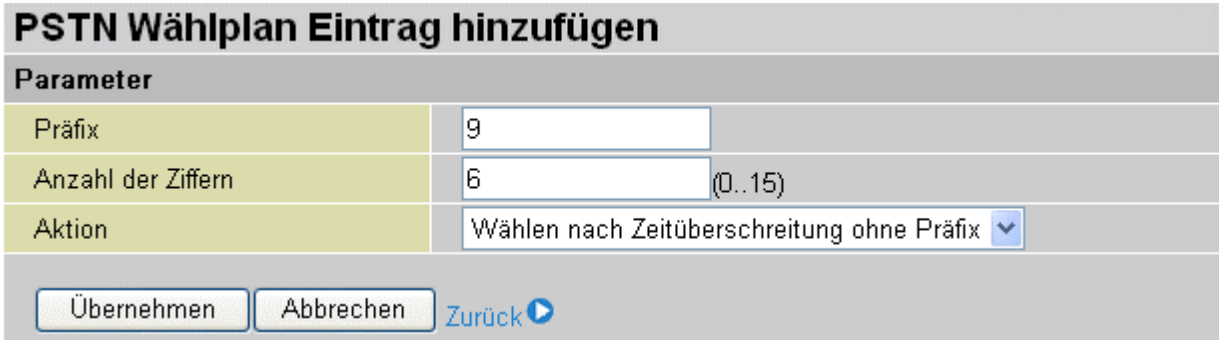
3) Wählen nach Zeitüberschreitung



Wenn Sie nur 01223 7070 wählen und keine weitere Nummer, wird nach der Zeitüberschreitung die Nummer 012237070 für einen regulären Anruf über den FXO Port (Festnetz) gewählt.

Obwohl 7070 (nur 4 Nummern) nicht übereinstimmt mit den im Feld Anzahl der Ziffern eingetragenen 6 Ziffern, ist 7070 eine gültige Nummer da nicht die angegebene Anzahl von 6 Ziffern übertroffen wird.

4) Wählen nach Zeitüberschreitung ohne Präfix

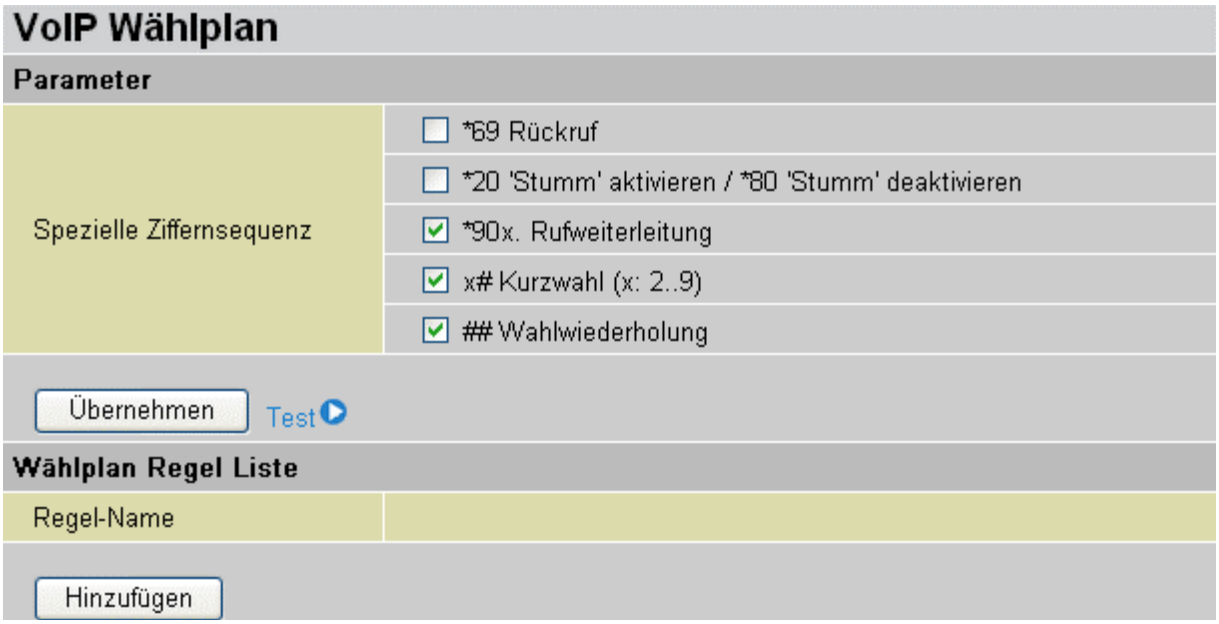


Wenn Sie nur 9 7070 wählen und keine weitere Nummer, wird nach der Zeitüberschreitung die Nummer 7070 für einen regulären Anruf über den FXO Port (Festnetz) gewählt.

Obwohl 7070 (nur 4 Nummern) nicht übereinstimmt mit den im Feld Anzahl der Ziffern eingetragenen 6 Ziffern, ist 7070 eine gültige Nummer da nicht die angegebene Anzahl von 6 Ziffern übertroffen wird.

3.5.5 VoIP Wählplan

Dieser Abschnitt beschreibt wie eine Rufnummer als direkter VoIP Anruf gewählt wird. Sie müssen dann nicht mehr eine lange VoIP Rufnummer für einen VoIP Anruf merken.



Folgende Einstellungen können in diesem Menü angepasst werden:

- **Parameter:**
  Eine Liste mit vordefinierten Wählplänen hilft Ihnen wenn Sie einen Anruf verpasst oder wenn Sie eine Rufweiterleitung tätigen wollen. Erläuterung zu den speziellen Ziffernsequenzen:
- ***69 (Rückruf):**
  Wählen Sie *69 um den letzten verpassten Anruf zurück zu rufen. Diese Funktion ist nur für SIP Anrufe verfügbar.
- ***20 (Stumm aktivieren):**
  Wählen Sie *20 wenn Sie nicht gestört werden wollen. Ihr Telefon wird nicht klingeln wenn Sie angerufen werden.
- ***80 (Stumm deaktivieren):** Wählen Sie *80 wenn Sie Stumm deaktivieren wollen. Ihr Telefon wird klingeln wenn Sie angerufen werden.
- ***90x (Rufweiterleitung):** Wählen Sie *90 und dann die Telefonnummer zu welchem der Anruf weitergeleitet werden soll. Diese Funktion ist Werksseitig aktiviert.
- **x# Kurzwahl (x:2..9):** Bitte schauen Sie unter Telefon Port Konfiguration -> Kurzwahl zur Erklärung dieses Merkmal nach. Diese Funktion ist Werksseitig aktiviert.
- **## Wahlwiederholung:** Drücken Sie ## damit Sie die zuletzt gewählte Rufnummer erneut wählen. Diese Funktion ist Werksseitig aktiviert.

Hinweis: Für weitere Informationen lesen Sie auch den Abschnitt Spezielle

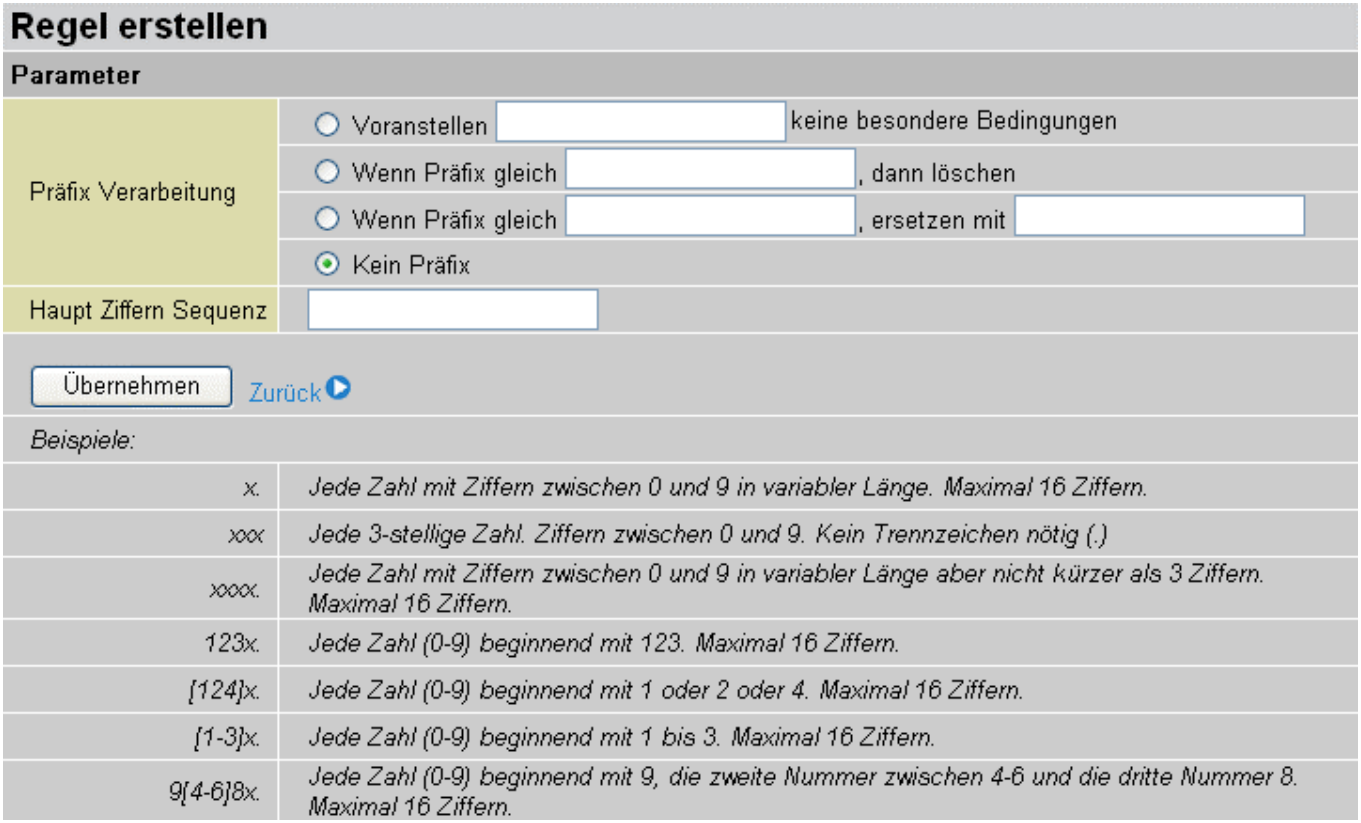
Ziffernsequenz.

- **Test:** Test zeigt Ihnen die aktuelle Nummer welche über VoIP angerufen wird.

Klicken Sie auf **[Übernehmen]** damit die Einstellungen wirksam werden

Wählplan Regel Liste

Klicken Sie auf **[Hinzufügen]** und erstellen Sie eine neue VoIP Wählplan Regel



Präfix Verarbeitung:

- **Voranstellen xxx keine besonderen Bedingungen:**
  Die Nummer xxx wird ohne besondere Bedingungen vorangestellt wenn ein Anruf getätigt wird
- **Wenn Präfix gleich xxx, dann löschen:**
  Präfix xxx wird gelöscht bevor die Nummer gewählt wird
- **Wenn Präfix gleich xxx, ersetzen mit xxx:**
  Präfix xxx wird ersetzt mit dem Präfix im zweiten Feld
- **Kein Präfix:**
  Kein Präfix wird der Nummer vorangestellt. Dies ist die Werkseinstellung.

Haupt Ziffern Sequenz:

- **x:** Jede Ziffern zwischen 0 und 9.
- **. (Punkt):** Tragen Sie die Nummer(n) ein, zwischen 0 und 9

Beispiele:

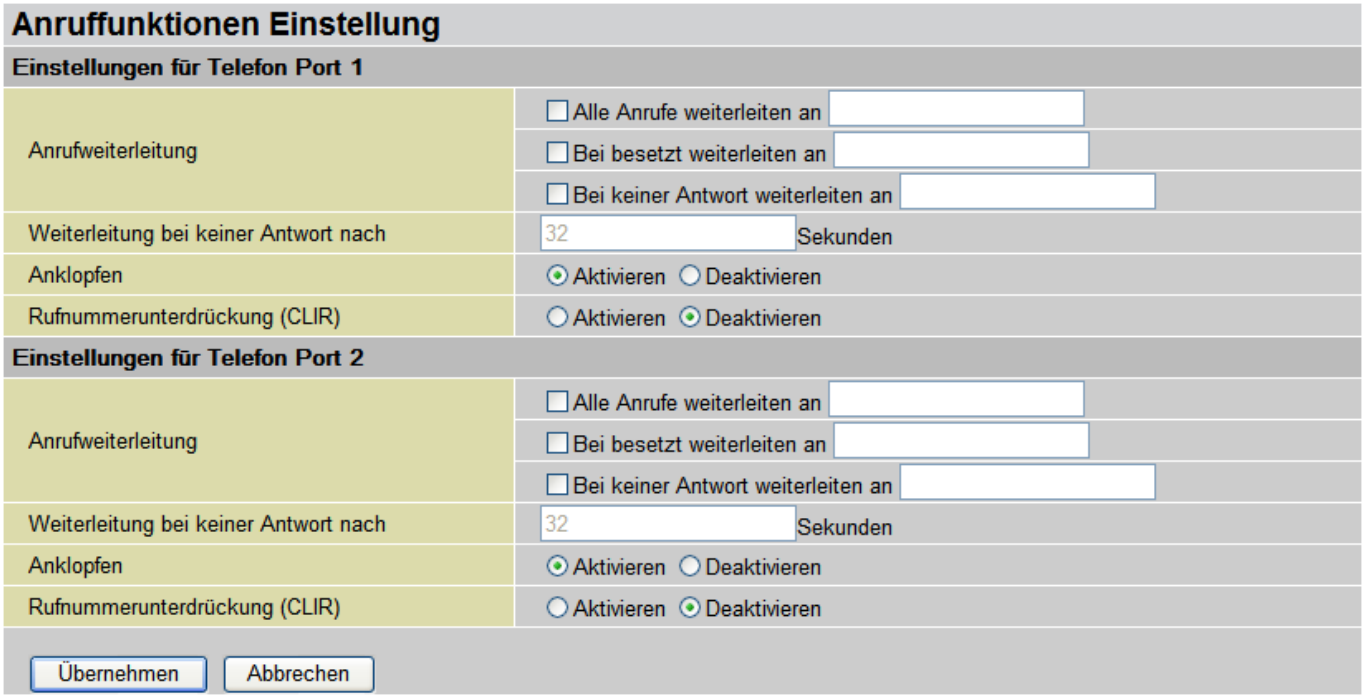
Haupt Ziffern Sequenz Liste	**Beschreibung**
x**.**	Jede Zahl mit Ziffern zwischen 0 und 9 in variabler Länge. Maximal 16 Ziffern.
xxx	Jede 3-stellige Zahl. Ziffern zwischen 0 und 9. Kein Trennzeichen nötig (.)
xxx**.**	Jede Zahl mit Ziffern zwischen 0 und 9 in variabler Länge aber nicht kürzer als 3 Ziffern. Maximal 16 Ziffern.
123x**.**	Jede Zahl (0-9) beginnend mit 123. Maximal 16 Ziffern.
[x…x]x. z.B.: [124]x**.**	Jede Zahl (0-9) beginnend mit 1 oder 2 oder 4. Maximal 16 Ziffern.
[x-x]x**.** z.B.: [1-3]x**.**	Jede Zahl (0-9) beginnend mit 1 bis 3. Maximal 16 Ziffern.
x[x-x]x. z.B.: 9[4-6]8x**.**	Jede Zahl (0-9) beginnend mit 9, die zweite Nummer zwischen 4-6 und die dritte Nummer 8. Maximal 16 Ziffern.

Die folgende Tabelle zeigt die speziellen Ziffernsequenzen die im System integriert sind:

Option	Beschreibung
Flash-hook „R-Taste"	**Umschalten zum PSTN/Festnetz** **Hinweis:** Ein kurzer klick auf die Gabel des Telefons. Bei einigen Telefonen gibt es auch eine Taste für diese Funktion. Diese Taste hat die Bezeichnung „FLASH" oder "Rückfragetaste".
***69**	**Nur für SIP, letzten Anruf in Abwesenheit zurück rufen** **Hinweis:** Wählen Sie *69 wird die Nummer angerufen welche zuletzt versucht hat Sie zu erreichen. Z.B., A ruft B an, legt aber auf bevor B abnimmt. Wenn B *69 wählt, wird A angerufen.
##	**Wahlwiederholung**
***20**	**Nicht stören aktivieren** **Hinweis:** Es ist möglich "nicht stören" zu aktivieren. Jeder Anrufer hört dann ein Besetztzeichen und das Telefon klingelt nicht. Z.B., B wählt *20 und legt auf. A ruft B an und hört nur ein Besetztzeichen währen da Telefon von B nicht klingelt.
***80**	**Nicht stören deaktivieren**
***74<x><Nummer>#**	**Kurzwahl Nummern speichern, wobei 'x' eine Nummer zwischen 2 und 9 ist.** **Hinweis:** <x> ist eine Nummer zwischen 2 und 9, und <Nummer> ist die Telefonnummer des Anrufzieles. Um die den Teilnehmer unter der angegebenen Kurzwahl zu erreichen wählen Sie: <**x**>#, wobei **<x>** eine Nummer zwischen 2 und 9 ist. Die Einstellungen werden in der Konfiguration unter Kurzwahl übernommen.
***90<Telefon-Nummer>**	Nur für SIP , tragen Sie die **Rufweiterleitung** ein, wobei <Telefon-Nummer> die Nummer ist zu der der aktuelle Anruf weitergeleitet werden soll. **Hinweis:** **Rufweiterleitung**, Sie führen ein Gespräch (eingehend oder ausgehend) und entscheiden dass dieses Gespräch zu einem anderen Telefon weitergeleitet werden soll. Dann führen Sie folgende Schritte aus: 1. Drücken Sie die „Flash" bzw. „Rückfragetaste" 2. Wählen Sie *90<Telefon-Nummer> (z.B. *907401) Sie hören einen Bestätigungston. Der andere Teilnehmer hört ein Freizeichen und das Telefon des dritten klingelt. Wenn der dritte abnimmt wird das Gespräch mit dem ersten verbunden. Wenn der dritte nicht abnimmt kann derjenige, der weitergeleitet werden soll einfach auflegen und den Anruf beenden.

3.5.6 Anruffunktionen

Hier können generelle Anruffunktion eingestellt werden, die unabhängig vom eingehenden Teilnehmer und eingehender Leitung (VoIP oder PSTN).



Folgende Einstellungen können hier verändert werden:

Einstellungen für Telefon Port 1

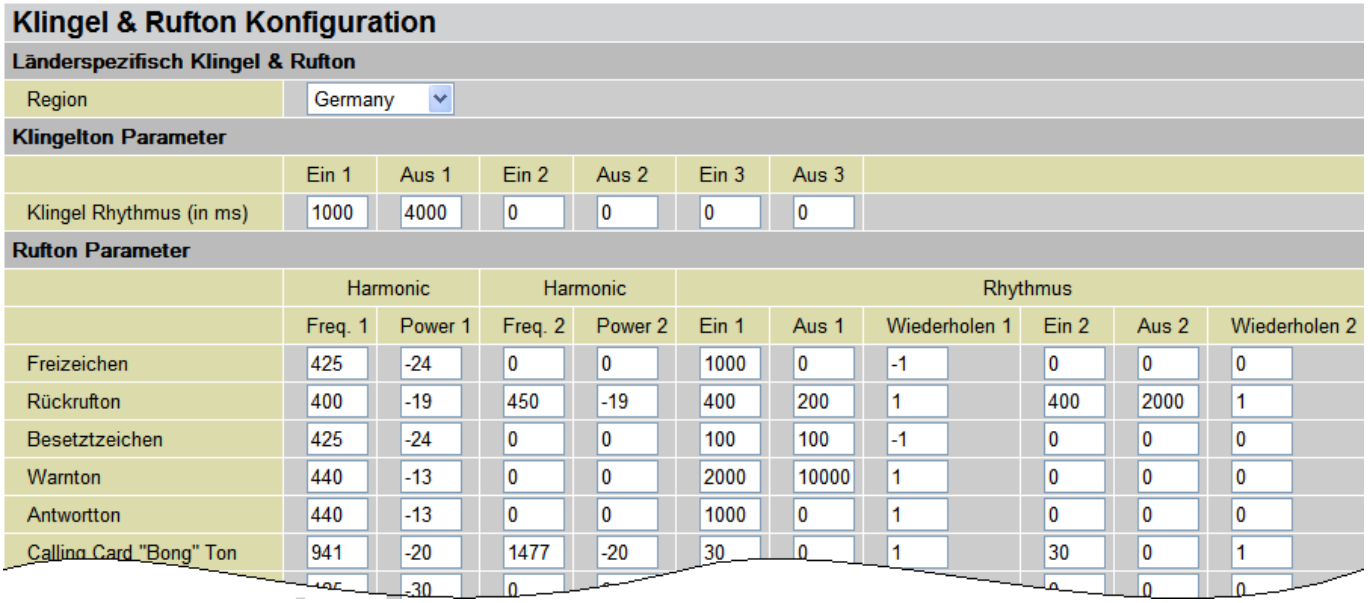
- **Anrufweiterleitung:**
  - **Alle Anrufe weiterleiten an *xxx*:**
    Leitet ausnahmslos alle eingehenden Anrufe an eine zuvor unter „xxx" definierte Nummer weiter
  - **Bei besetzt weiterleiten an *xxx*:**
    Leitet alle Anrufe nur bei besetzter Leitung an eine zuvor unter „xxx" definierte Nummer weiter
  - **Bei keiner Antwort weiterleiten an *xxx*:**
    Leitet alle Anrufe nach einer unter dem nächsten Punkt definierten Zeit an eine zuvor unter „xxx" definierte Nummer weiter
  - **Weiterleitung bei keiner Antwort nach *xxx* Sekunden:**
    Leitet alle Anrufe, die innerhalb dieser Zeit nicht angenommen werden, an eine unter dem vorherigen Punkt definierten Nummer weiter
  - **Anklopfen:**
    Gibt die Möglichkeit während eines bereits geführten Gesprächs weitere eingehende Anrufe nicht abzuweisen, sondern im Telefonhörer mit einem Anklopfton kenntlich zu machen
  - **Rufnummernunterdrückung (CLIR):**
    Unterdrückt die eigene Rufnummer bei ausgehenden Gesprächen, soweit dieses Merkmal vom Anbieter unterstützt wird

Einstellungen für Telefon Port 2

- Einstellungsmöglichkeiten gleichen denen von Telefon Port 1

3.5.7 Klingeln & Rufton

Dieser Abschnitt erlaubt es erfahrenen Anwendern die vorhandenen Ton-Parameter zu verändern (Freizeichen, Besetztzeichen, Antwortton etc.)



Klingel & Rufton Konfiguration

Länderspezifisch Klingel & Rufton

Region	Germany

Klingelton Parameter

	Ein 1	Aus 1	Ein 2	Aus 2	Ein 3	Aus 3
Klingel Rhythmus (in ms)	1000	4000	0	0	0	0

Rufton Parameter

	Harmonic		Harmonic		Rhythmus					
	Freq. 1	Power 1	Freq. 2	Power 2	Ein 1	Aus 1	Wiederholen 1	Ein 2	Aus 2	Wiederholen 2
Freizeichen	425	-24	0	0	1000	0	-1	0	0	0
Rückrufton	400	-19	450	-19	400	200	1	400	2000	1
Besetztzeichen	425	-24	0	0	100	100	-1	0	0	0
Warnton	440	-13	0	0	2000	10000	1	0	0	0
Antwortton	440	-13	0	0	1000	0	1	0	0	0
Calling Card "Bong" Ton	941	-20	1477	-20	30	0	1	30	0	1
		-30	0						0	0

Folgende Einstellungen können hier verändert werden:

Länderspezifisch Klingel & Rufton

- **Region:** Wählen Sie das Land aus der Drop-Down Liste aus in welchem Sie das Gerät einsetzen. Dieser VoIP Router unterstützt die vorgegebenen Klingel & Ruftöne für verschieden Länder. Sollte Ihr Land nicht in der Liste aufgeführt sein, müssen Sie unter umständen die Ton-Parameter selber eingeben

Klingelton Parameter

- **Klingel Rhythmus (in ms):** Der Klingel Rhythmus ist in drei Felder unterteilt, Frequenz: Ein Zeit1, Aus Zeit1, Ein Zeit2, Aus Zeit2 und Ein Zeit3, Aus Zeit3. Die Frequenz ist in Hertz, die Zeit in Millisekunden angegeben
- **Rufton Parameter**
  Für die richtigen Werte sollten Sie Ihren Telefonanbieter kontaktieren. Es wird ausdrücklich empfohlen diese Einstellungen nur von einem erfahrenen Anwender zu verändern!

Klicken Sie auf **[Übernehmen]** damit die Einstellungen wirksam werden

3.6 QoS (Quality of Service)

Die QoS Funktion hilft Ihnen, den Netzwerkverkehr für jedes Programm vom LAN (Ethernet und/oder Wireless) zum WAN (Internet) zu kontrollieren. Es ermöglicht Ihnen eine unterschiedliche Priorität und Datendurchsatz für jedes Programm zu konfigurieren, insbesondere wenn das System mit der vollen Upstream Geschwindigkeit arbeitet.

Diese Kategorie beinhaltet folgende Untermenüs:

- **Priorisation**
- **IP Throttling ausgehend**
- **IP Throttling eingehend**

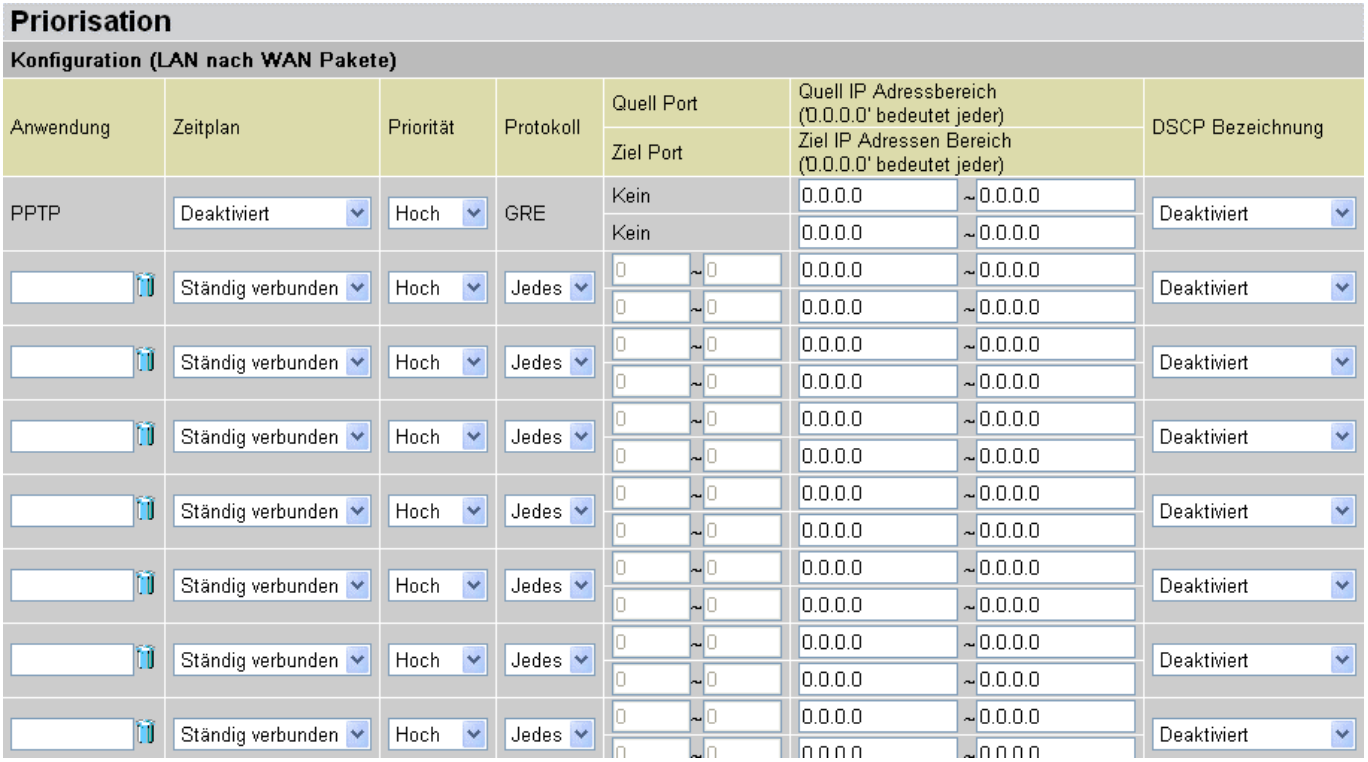
3.6.1 Priorisation

Es gibt drei Priorisationseinstellungen, welche im Router angeboten werden:

- **Hoch**
- **Normal** (Werksseitig, ohne Priorisierung des Datenverkehrs)
- **Niedrig**

Die Balance der Ausnutzung jeder Priorität ist wie folgt eingestuft:

- **Hoch** = **60%**
- **Normal** = **30%**
- **Niedrig** = **10%**



Folgende Einstellungen können hier verändert werden:

- **Anwendung**: Der Name, der eine existierende Regel identifiziert

- **Zeitplan**: Zeitvorgabe für die Regel

- **Priorität**: Priorität für die Regel/Anwendung. Jeder Verkehr hat eine normale Priorität, so lange bis Sie dies ändern, also Hoch oder Niedrig einstellen

- **Protokoll**: Der Name des zu verwenden Protokolls

- **Quell Port**: Der Quell Port dessen Pakete überwacht werden

- **Ziel Port**: Der Ziel Port dessen Pakete überwacht werden

- **Quell IP Adressbereich**: Die Quell IP Adresse, bzw. Adressbereiches dessen Pakete überwacht werden sollen

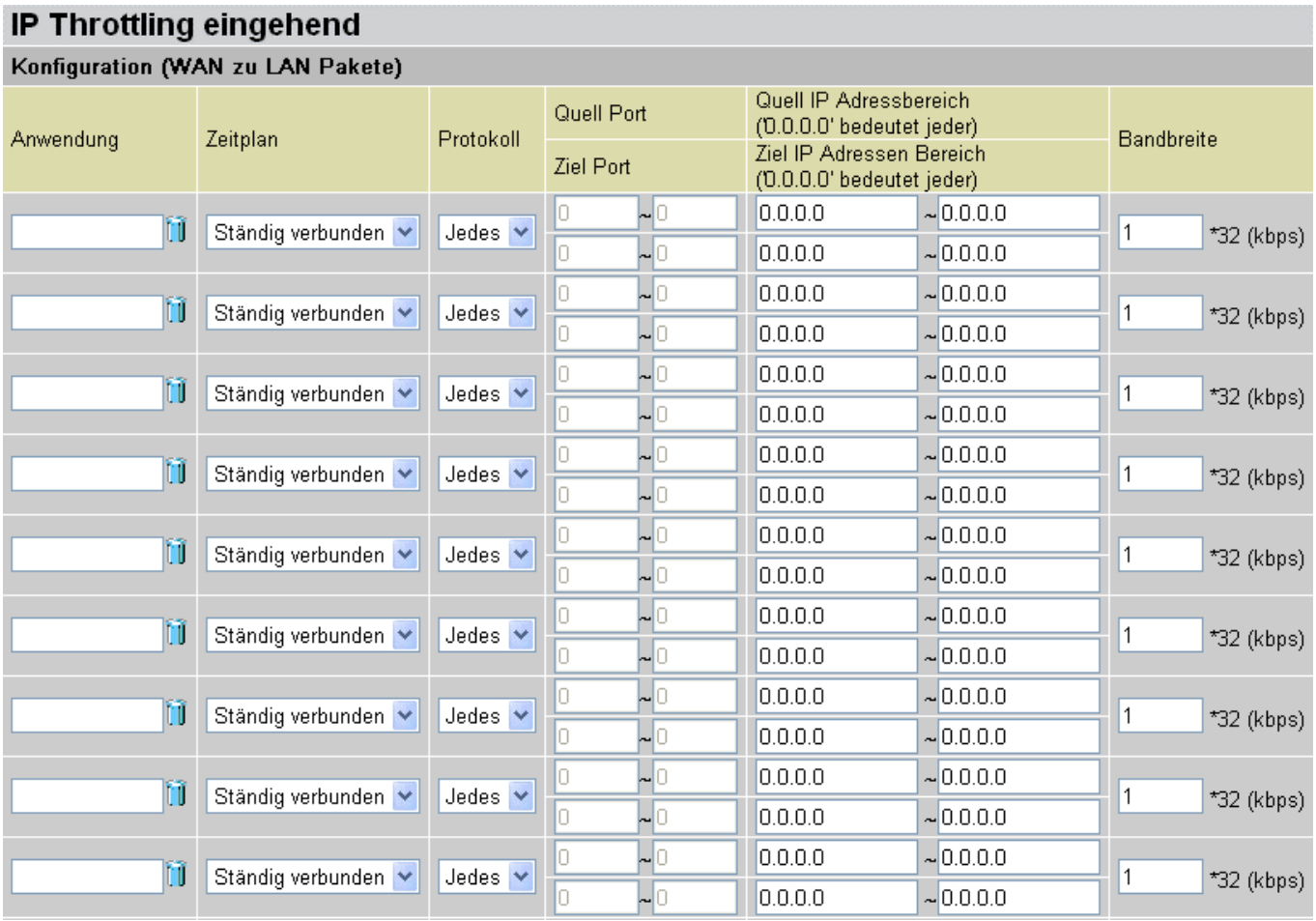
- **Ziel IP Adressbereich**: Die Ziel IP Adresse, bzw. Adressbereiches dessen Pakete überwacht werden sollen

- **DSCP Bezeichnung**: Differentiated Services Code Point (DSCP), dies sind die ersten 6 Bits im ToS Byte. DSCP Marking erlaubt dem Anwender anhand des DSCP Wertes den Verkehr zu klassifizieren bevor die Pakete zum nächsten Router gesendet werden. Weitere Informationen sind in der folgenden Tabelle hinterlegt:

DSCP Mapping Tabelle	
(Wireless) ADSL Router	**Standard DSCP**
Deaktiviert	Kein
Bestleistung	Bestleistung (000000)
Premium	Express Weiterleitung (101110)
Gold Service (L)	Class 1, Gold (001010)
Gold Service (M)	Class 1, Silber (001100)
Gold Service (H)	Class 1, Bronze (001110)
Silber Service (L)	Class 2, Gold (010010)
Silber Service (M)	Class 2, Silber (010100)
Silber Service (H)	Class 2, Bronze (010110)
Bronze Service (L)	Class 3, Gold (011010)
Bronze Service (M)	Class 3, Silber (011100)
Bronze Service (H)	Class 3, Bronze (011110)

3.6.2 Priorisation (eingehend) (WAN zu LAN)

IP Throttling erlaubt Ihnen die Geschwindigkeit des IP Verkehrs zu limitieren. Den Wert den Sie eintragen, multipliziert mit 32kbps, ergibt die limitierte Geschwindigkeit der Anwendung.



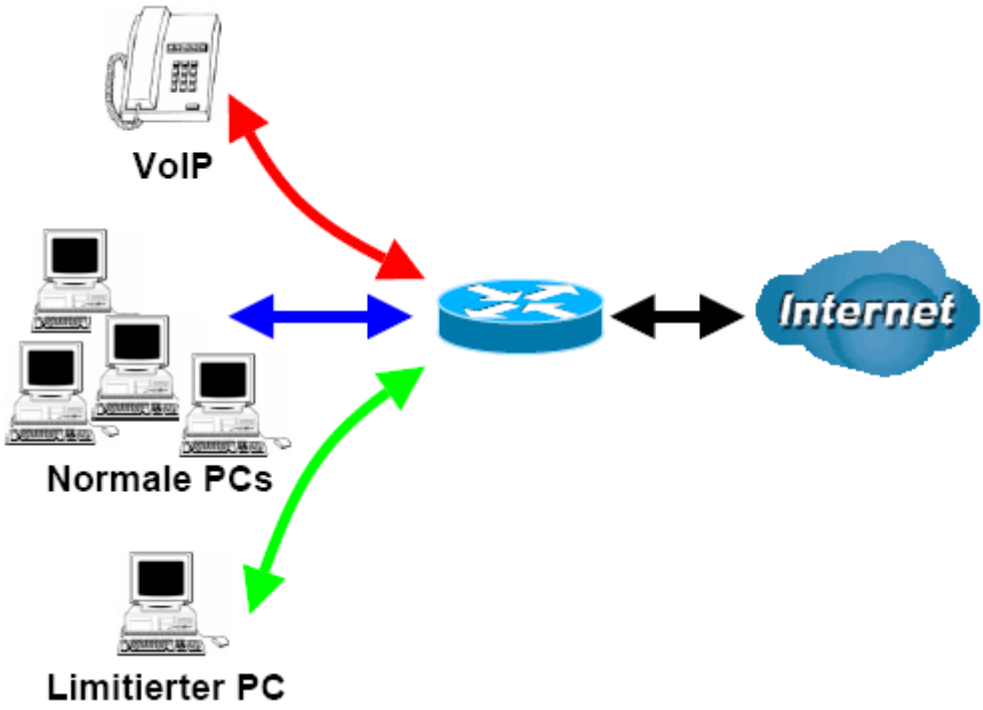
Folgende Einstellungen können verändert werden:

- **Anwendung**:
  Der Name, der eine existierende Regel identifiziert

- **Zeitplan**:
  Zeitvorgabe für die Regel
- **Priorität**:
  Priorität für die Regel/Anwendung. Jeder Verkehr hat eine normale Priorität, so lange bis Sie dies ändern, also Hoch oder Niedrig einstellen
- **Protokoll**:
  Der Name des zu verwenden Protokolls
- **Quell Port**:
  Der Quell Port dessen Pakete überwacht werden
- **Ziel Port**:
  Der Ziel Port dessen Pakete überwacht werden
- **Quell IP Adressbereich**:
  Die Quell IP Adresse, bzw. Adressbereiches dessen Pakete überwacht werden sollen
- **Ziel IP Adressbereich**:
  Die Ziel IP Adresse, bzw. Adressbereiches dessen Pakete überwacht werden sollen
- **Bandbreite**:
  Die limitierte Geschwindigkeit für den eingehenden IP Verkehr

Beispiel: QoS für Ihr Netzwerk

Verbindungsdiagramm



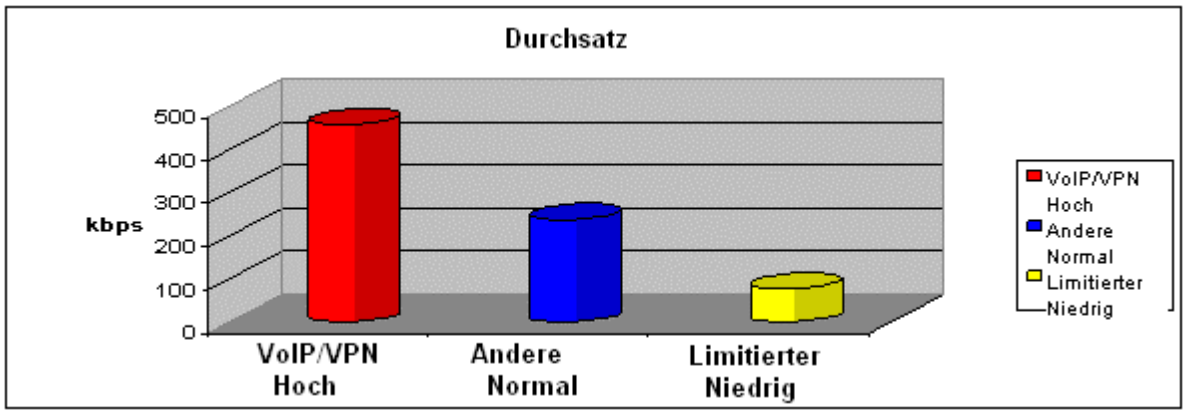
Information und Einstellungen

Upstream:	928 kbit/s
Downstream:	8 Mbit/s
VoIP Benutzer:	192.168.1.1
Normaler Benutzer :	192.168.1.2 ~ 192.168.1.5
Limitierter Benutzer :	192.168.1.100

Prioritization

Configuration (from LAN to WAN packet)

Application	Time Schedule	Priority	Protocol	Source Port / Destination Port	Source IP Address Range ('0.0.0.0' means Any) / Destination IP Address Range ('0.0.0.0' means Any)	DSCP Marking
PPTP	Always On	High	GRE	none none	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	Gold service (L)
VoIP	Always On	High	any	0 ~ 0 0 ~ 0	192.168.1.1 ~ 192.168.1.1 0.0.0.0 ~ 0.0.0.0	Gold service (L)
Restricted	TimeSlot1	Low	any	0 ~ 0 0 ~ 0	192.168.1.100 ~ 192.168.1.100 0.0.0.0 ~ 0.0.0.0	Gold service (L)



Missionskritische Anwendungen
Missionskritische Anwendungen müssen reibungslos gesendet werden, ohne dass Pakete verworfen werden. Setzen Sie hierfür die Priorität Hoch, damit andere Anwendungen nicht die Bandbreite belegen.

Sprach Anwendung
Sprach Anwendungen (VoIP) sind Latenz-Empfindlich. Die meisten VoIP Geräte verwenden das SIP Protokoll und die Port Nummer wird vom SIP Modul automatisch zugewiesen. Besser ist es feste IP Adressen für diese Geräte zu verwenden, damit die VoIP Pakete eine hohe Priorität erhalten.

VoIP	Ständig verbunden	Hoch	Jedes	0 ~ 0 0 ~ 0	192.168.1.1 ~ 192.168.1.1 0.0.0.0 ~ 0.0.0.0	Gold Service (L)

Die oben verwendeten Einstellungen verbessern die Qualität Ihres VoIP Dienstes auch bei hoher Last des Datenverkehrs.

Limitierte Anwendungen
Einige Firmen verwenden einen FTP Server für Ihre Kunden zum Download diverser Dateien oder Heimanwender verwenden FTP Server um Dateien auszutauschen.

Limitierter	TimeSlot1	Niedrig	Jedes	0 ~ 0 0 ~ 0	192.168.1.100 ~ 192.168.1.100 0.0.0.0 ~ 0.0.0.0	Gold Service (L)

Die oben verwendeten Einstellungen limitieren die Auslastung des Upstream vom FTP Server. Der Zeitplan unterstützt Sie des Weiteren dass diese Limitierung nur zu bestimmten Tageszeiten in Kraft tritt.

Erweiterte Einstellungen unter Verwendung von IP Throttling
Mittels IP Throttling können Sie Bandbreiten genauer zuteilen, selbst wenn die Anwendung den gleichen Status wie eine andere Anwendung hat.

Upstream: 928kbps (29*32kbps)
Missionskritische Anwendung: 192kbps (6*32kbps)

Sprach Anwendung: 128kbps (4*32kbps)
Limitierte Anwendung: 160kbps (5*32kbps)
Andere Anwendungen: 448kbps (14*32kbps)

6+4+14+5 = 29, 29*32kbps = **928kbps**

IP Throttling ausgehend

Konfiguration (LAN nach WAN Pakete)

Anwendung	Zeitplan	Protokoll	Quell Port / Ziel Port	Quell IP Adressbereich ('0.0.0.0' bedeutet jeder) / Ziel IP Adressen Bereich ('0.0.0.0' bedeutet jeder)	Bandbreite
PPTP	Ständig verbunden	gre	0 ~ 0	0.0.0.0 ~ 0.0.0.0	6 *32 (kbps)
			0 ~ 0	0.0.0.0 ~ 0.0.0.0	
VoIP	Ständig verbunden	Jedes	0 ~ 0	0.0.0.0 ~ 0.0.0.0	4 *32 (kbps)
			0 ~ 0	0.0.0.0 ~ 0.0.0.0	
Limitierter	TimeSlot1	Jedes	0 ~ 0	192.168.1.100 ~ 192.168.1.100	5 *32 (kbps)
			0 ~ 0	0.0.0.0 ~ 0.0.0.0	
Andere	TimeSlot1	Jedes	0 ~ 0	192.168.1.2 ~ 192.168.1.5	14 *32 (kbps)
			0 ~ 0	0.0.0.0 ~ 0.0.0.0	

Manchmal laden Ihre Kunden oder Freunde Dateien auf Ihren FTP Server und beeinträchtigen somit Ihren Downstream. Die Einstellungen unten helfen Ihnen die Bandbreite diesbezüglich zu limitieren.

IP Throttling eingehend

Konfiguration (WAN zu LAN Pakete)

Anwendung	Zeitplan	Protokoll	Quell Port / Ziel Port	Quell IP Adressbereich ('0.0.0.0' bedeutet jeder) / Ziel IP Adressen Bereich ('0.0.0.0' bedeutet jeder)	Bandbreite
Limitierter	TimeSlot1	Jedes	0 ~ 0	0.0.0.0 ~ 0.0.0.0	64 *32 (kbps)
			0 ~ 0	192.168.1.100 ~ 192.168.1.100	

3.6.4 Priorisation (ausgehend) (LAN zu WAN)

Diese Einstellungsmöglichkeiten gleichen denen des vorangegangenen Kapitels **3.6.2. Priorisation (eingehend)** und können adaptiv von dort übernommen werden.

3.7 Virtual Server (Manuelle Portweiterleitung)

In TCP/IP und UDP Netzwerken ist ein Port eine 16-bit Nummer, welche benutzt wird, um ein Anwendungsprogramm zu identifizieren (normalerweise ein Server) wohin hereinkommende Verbindungen zugeordnet werden. Manche Anwendungen haben vordefinierte Ports von IANA (Internet Assigned Numbers Authority), und diese werden als "well-known ports" bezeichnet. Server folgen den „well-known ports" Zuordnungen, so dass Clients diese lokalisieren können.

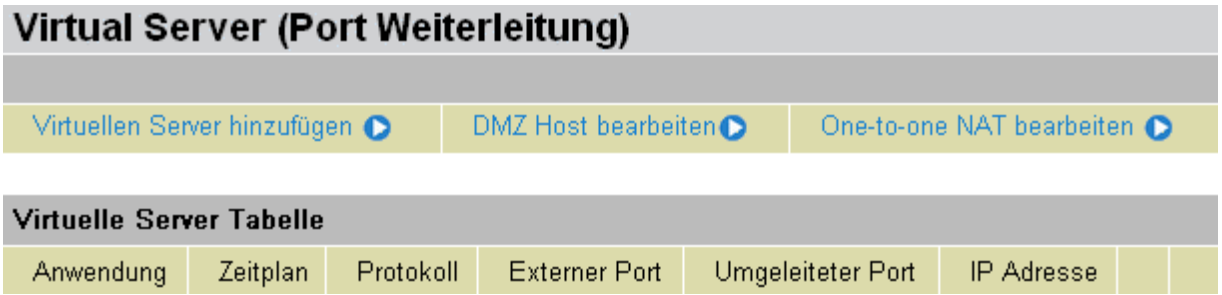
Wenn Sie einen Server auf Ihrem Netzwerk laufen lassen wollen, welcher vom WAN (z.B. von anderen Computern außerhalb Ihres Netzwerks) aus zugreifbar sein soll oder andere Programme, die hereinkommende Verbindungen akzeptieren (z.B. Peer-to-Peer/P2P Software wie Instant Messenger oder P2P File Sharing Programme) und NAT (Network Address Translation) nutzen, dann müssen Sie Ihren Router so konfigurieren, dass er die hereinkommenden Verbindungen an den entsprechenden Computer weiterleiten kann, auf dem dieses Programm läuft. Sie können ebenfalls Port Forwarding nutzen, wenn Sie einen Online Spiele Server hosten.

Der Grund dafür ist, wenn Sie NAT nutzen, dass Ihre öffentliche IP Adresse vom Router benutzt wird und auch dorthin zeigt, welcher allen Verkehr anschließend an die Private IP Ihrer PCs weiterleitet. Schauen Sie im Abschnitt WAN Konfiguration dieser Anleitung nach für weitere Informationen zu NAT.

Die Internet Assigned Numbers Authority (IANA) ist ein zentraler Koordinator für die Zuweisung der einzigartigen Parameterwerte für die Internet Protokolle. Port Nummern gehen von 0 bis 65535, aber nur Portnummern von 0 bis 1023 sind für privilegierte Services bestimmt und werden als "Well-Known Ports" bezeichnet. Die registrierten Ports sind von 1024 bis 49151 nummeriert. Die restlichen Ports werden als dynamische Ports oder private Ports bezeichnet, gehen von 49152 bis 65535.

Beispiele von Well-Known und registrierten Portnummern finden Sie in Tabelle 5, für weitere Informationen schauen Sie bitte auf http://www.iana.org/assignments/port-numbers nach.

Der Router kann als Virtual Server konfiguriert werden, so dass externe Benutzer dienste wie WEB oder FTP Server über die öffentliche IP Adresse des Routers (WAN) automatisch zu dem Server in Ihrem LAN weitergeleitet werden, welcher weiterhin eine private IP Adresse hat.



Virtuellen Server hinzufügen

NAT kann als eine natürliche Firewall dienen, Ihr Router schützt Ihr Netzwerk vor Nutzung von fremden Personen, da alle hereinkommenden Verbindungen auf den Router zeigen, außer Sie nutzen einen Virtuellen Server, der die Einträge an PCs in Ihrem Netzwerk weiterleitet. Wenn Ihr Router anderen Internet Nutzern den Zugang zu Internen Servern erlauben soll, z.B. Webserver, Email Server, FTP Server oder Spielserver, fungiert der Router als ein Virtueller Server. Sie können einen lokalen Server mit einer speziellen Port Nummer diesen Service zuordnen z.B. web/HTTP (Port 80), FTP (Port 21), Telnet (Port 23), SMTP (Port 25), oder POP3 (Port 110), Wenn eine Anfrage von außerhalb an den Router kommt, leitet der Router die Anfrage an den dafür vorgesehenen internen Server weiter.

Folgende Einstellungen können hier verändert werden:

- **Zeitplan:**
  Hier können Sie einen selbst definierten Zeitplan für die Aktivierung Ihres Virtuellen Servers angeben. Wählen Sie den Zeitplan aus oder Ständig verbunden für den Virtuellen Server. Für die Einstellungen und weitere Information zum Zeitplan sehen Sie im Abschnitt Zeitplan nach

- **Anwendung**:
  Tragen Sie hier einen Namen für die Anwendung ein oder klicken Sie auf **[Assistent]** um einen vorgegebene Anwendung auszuwählen

- Assistent **:**
  20 vorgegebene Regeln haben Sie zur Auswahl. Wählen Sie eine Anwendung aus werden die Anwendung, das Protokoll sowie die externen und umgeleiteten Ports in die entsprechenden Felder übernommen.

- **Protokoll**:
  Das für den Virtuellen Server zu verwendende Protokoll. Zusätzlich zu dem benötigten Port müssen Sie auch das benötigte Protokoll angeben. Welches Protokoll wird von der Anwendung festgelegt. Die meisten Anwendungen verwenden TCP oder UDP.

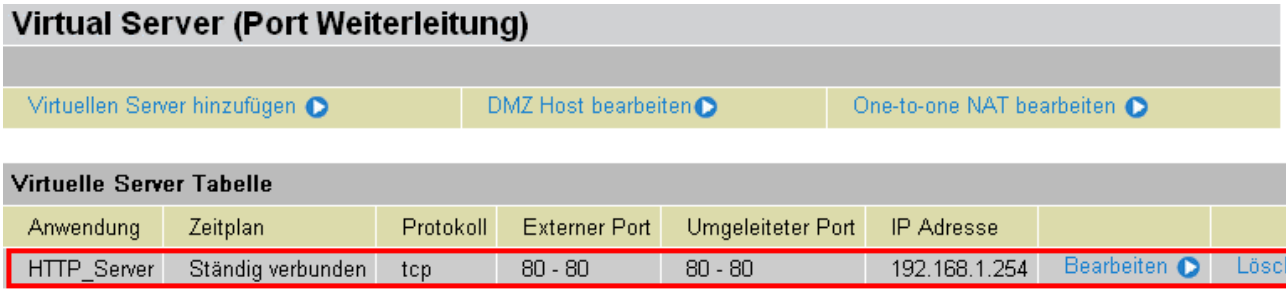
- **Externer Port:**
  Die Port Nummer welche auf der Remote/WAN Seite für den Virtuellen Server verwendet wird

- **Umgeleiteter Port:**
  Die Port Nummer welche vom lokalen Server im LAN verwendet wird

- **Interne IP Adresse:** Die private IP Adresse im LAN, auf welcher die Anwendung für den Virtuellen Server vorhanden ist. **[Aktive PC]** listet alle existierenden PCs in Ihrem Netzwerk auf.

Beispiel:
Wenn Sie z.B. jederzeit auf Ihren Router per Fernwartung mittels Web/HTTP zugriff haben wollen, müssen Sie den Port 80 (Web/HTTP) aktivieren und auf die IP Adresse des Routers umleiten. Dann werden alle eingehenden HTTP Anfragen zu dem Router mit der IP Adresse 192.168.1.254 weitergeleitet. Da der Port 80 schon zur Auswahl steht, müssen Sie nur neben **Anwendung** auf **Assistent** klicken. Ein Fenster mit voreingestellten Regeln erscheint und Sie müssen nur **HTTP_Server** auswählen.

Anwendung: *HTTP_Server*
Zeitplan: *Ständig verbunden*
Protokoll: *tcp*
Externer Port: *80-80*
Umgeleiteter Port: *80-80*
IP Adresse: *192.168.1.254*



- **Bearbeiten:** Klicken Sie hier wenn Sie diesen Eintrag bearbeiten möchten
- **Löschen:** Klicken Sie hier wenn Sie diesen Eintrag löschen möchten

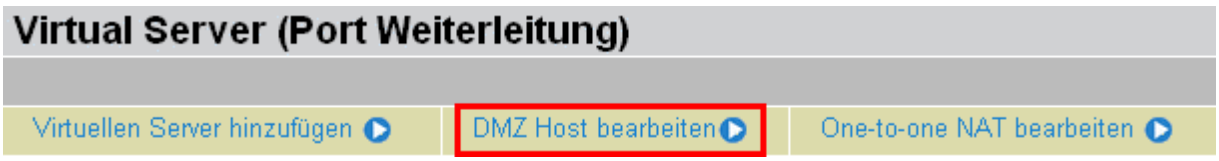
HINWEIS: Die Port Weiterleitung birgt auch Sicherheitsrisiken, da außenstehende Benutzer die Möglichkeit haben sich mit Ihrem Netzwerk zu verbinden. Daher empfehlen wir nur die Ports zu öffnen, welche Sie für die jeweilige Anwendung benötigen. Tragen Sie nicht einfach einen Rechner als DMZ Host ein.

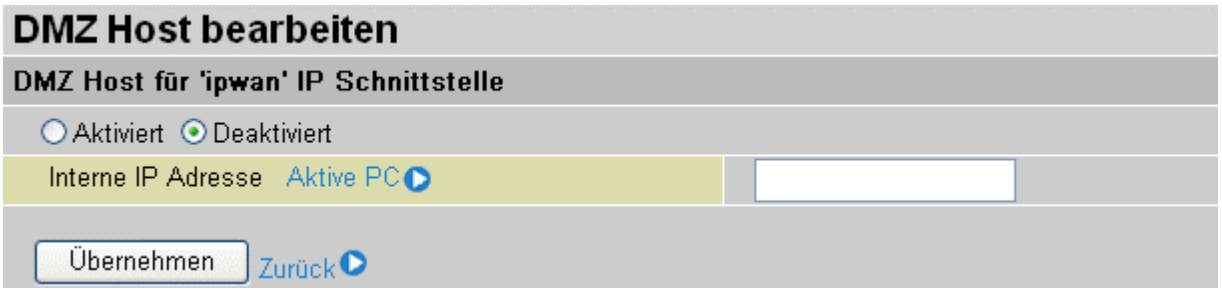
Wenn Sie NAT unter WAN Verbindung deaktiviert haben sind die Einstellungen im Bereich Virtueller Server ungültig. Wenn Sie DHCP Server aktiviert haben, achten Sie darauf dass die IP Adressen für die Virtuellen Server außerhalb des IP-Bereiches des DHCP Servers liegen. Verwenden Sie für die Virtuellen Server statische IP-Adressen. Diese müssen aber im gleichen Subnetz liegen wie die IP Adresse des Routers.

DMZ Host bearbeiten

Der DMZ Host ist ein lokaler Computer der offen im Internet ist. Wenn Sie eine spezielle interne IP Adresse als DMZ Host festlegen, werden alle hereinkommenden Pakete von der Firewall und dem NAT Algorithmus überprüft und dann an den DMZ Host weitergeleitet, solange es keinen Konflikt mit einer anderen Portnummer des virtuellen Servers besteht.

Vorsicht: Der lokale Computer, welcher als DMZ Host festgelegt wird, kann ein Sicherheitsrisiko darstellen





- **Deaktiviert:** Die Funktion DMZ ist werksseitig deaktiviert.
- **Aktiviert:** Aktiviert die Funktion DMZ

Interne IP Adresse: Tragen Sie die statische IP Adresse für den DMZ Host ein wenn Sie DMZ **Aktiviert** haben. Bedenken Sie dass diese IP Adresse vor dem WAN/Internet ungeschützt ist.

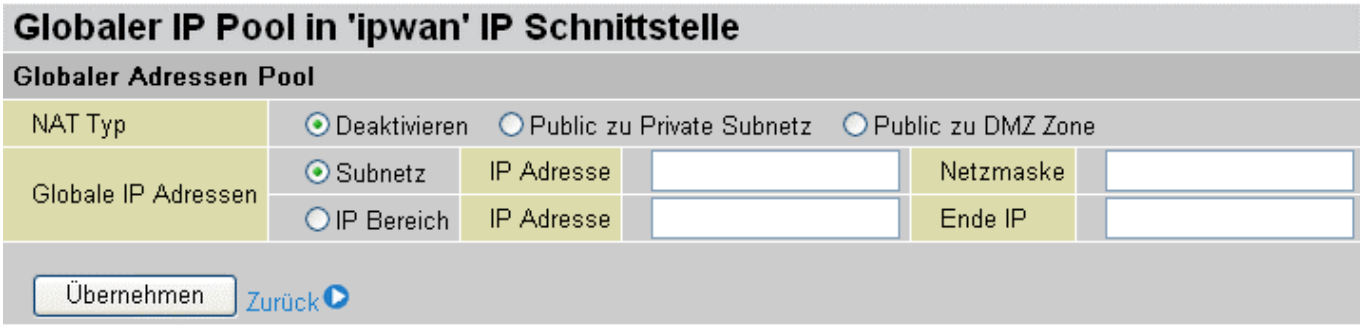
- Assistent:
  20 vorgegebene Regeln haben Sie zur Auswahl. Wählen Sie eine Anwendung aus werden die Anwendung, das Protokoll sowie die externen und umgeleiteten Ports in die entsprechenden Felder übernommen.

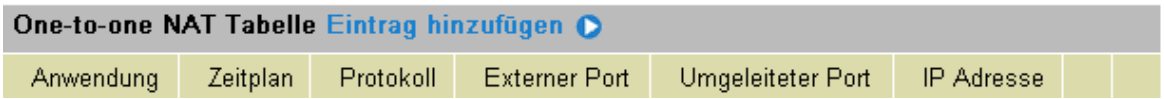
Klicken Sie auf **Übernehmen** damit die Einstellungen wirksam werden

One-to-One NAT (Network Address Translation) bearbeiten

One-to-One NAT verbindet eine spezifische private/lokale IP Adresse mit einer globalen/öffentlichen IP Adresse.

Wenn Sie mehrere öffentliche WAN IP Adressen von Ihrem ISP (Internet-Service-Provider) erhalten, erfüllen Sie die Voraussetzung One-to-One NAT mit diesen IP Adressen zu nutzen.





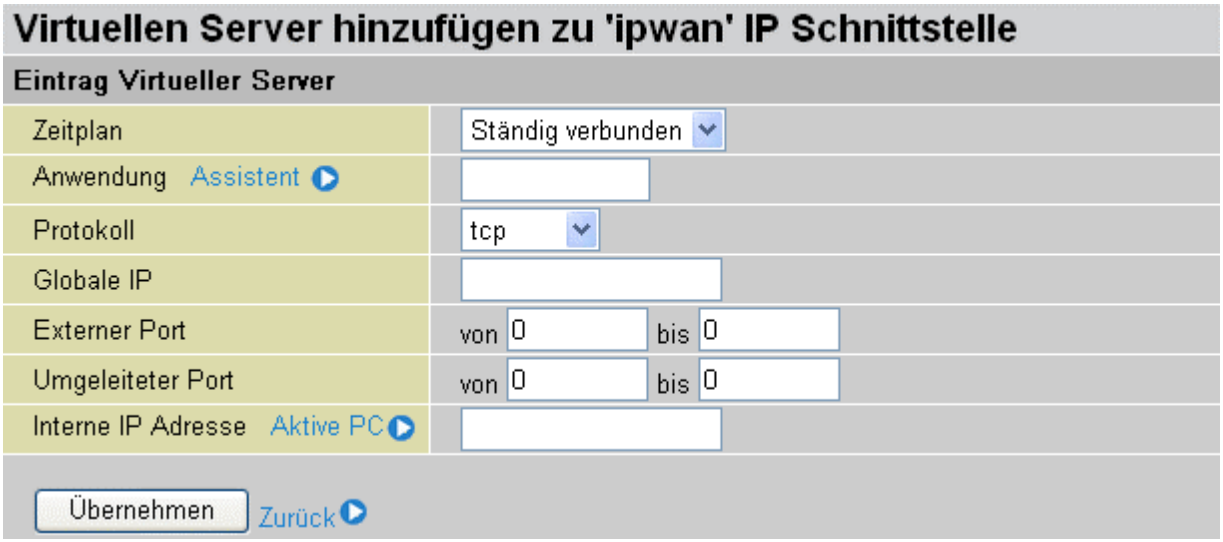
NAT Typ: Wählen Sie den gewünschten NAT Typ. Die Funktion One-to-One NAT ist werksseitig deaktiviert.

Globale IP Adressen:

- **Subnetz:** Das Subnetz der öffentlichen WAN IP Adresse welche Sie von Ihrem ISP erhalten haben. Wenn Sie diese Information von Ihrem ISP erhalten haben, so tragen Sie diese hier ein. Andernfalls wählen Sie die Option IP Bereich.
- **IP Bereich:** Der IP Adressen Bereich Ihrer öffentlichen WAN IP Adressen. Z.B., IP: 192.168.1.1, Ende IP: 192.168.1.10

Klicken Sie auf **Übernehmen** damit die Einstellungen wirksam werden.

Klicken Sie auf **[Eintrag hinzufügen]** für eine neue One-to-One NAT Regel



- **Zeitplan:**
  Hier können Sie einen selbst definierten Zeitplan für die Aktivierung Ihres Virtuellen Servers angeben. Wählen Sie den Zeitplan aus oder Ständig verbunden für den Virtuellen Server. Für die Einstellungen und weitere Information zum Zeitplan sehen Sie im Abschnitt Zeitplan nach.

- **Anwendung**:
  Tragen Sie hier einen Namen für die Anwendung ein oder klicken Sie auf **[Assistent]** um einen vorgegebene Anwendung auszuwählen.

- Assistent **:**
  20 vorgegebene Regeln haben Sie zur Auswahl. Wählen Sie eine Anwendung aus werden die Anwendung, das Protokoll sowie die externen und umgeleiteten Ports in die entsprechenden Felder übernommen.

- **Protokoll**:
  Das für den Virtuellen Server zu verwendende Protokoll. Zusätzlich zu dem benötigten Port müssen Sie auch das benötigte Protokoll angeben. Welches Protokoll wird von der Anwendung festgelegt. Die meisten Anwendungen verwenden TCP oder UDP.

- **Globale IP:**
  Geben Sie die öffentliche WAN IP Adresse für diese Anwendung an. Diese globale IP Adresse muss als **Globale IP Adresse** eingetragen sein.

- **Externer Port:**
  Die Port Nummer welche auf der Remote/WAN Seite für den Virtuellen Server verwendet wird.

- **Umgeleiteter Port:**
  Die Port Nummer welche vom lokalen Server im LAN verwendet wird.

- **Interne IP Adresse:**
  Die private IP Adresse im LAN, auf welcher die Anwendung für den Virtuellen Server vorhanden ist. listet alle existierenden PCs in Ihrem Netzwerk auf.

Beispiele: Liste einiger Well-Known und registrierten Port Nummern

Die Internet Assigned Numbers Authority (IANA) ist ein zentraler Koordinator für die Zuweisung der einzigartigen Parameterwerte für die Internet Protokolle. Port Nummern gehen von 0 bis 65535, aber nur Portnummern von 0 bis 1023 sind für privilegierte Services bestimmt und werden als "Well-Known Ports" bezeichnet. Die registrierten Ports sind von 1024 bis 49151 nummeriert. Die restlichen Ports werden als dynamische Ports oder private Ports bezeichnet, gehen von 49152 bis 65535.

Beispiele von Well-Known und registrierten Portnummern finden Sie unten, für weitere Informationen schauen Sie bitte auf http://www.iana.org/assignments/port-numbers nach.

Port Nummer	Protokoll	Beschreibung
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

3.8 Zeitplan

Der Zeitplan unterstützt bis zu 16 Zeit Fenster welche Ihnen für Ihre Internetverbindung zur Verfügung stehen. In jedem Zeitprofil können Sie den Zeitplan anhand von Tag(en) und Zeiten festlegen, damit z.B. von Montags bis Samstags nur bestimmte Anwender oder Applikationen das Internet verwenden dürfen.

Der Zeitplan arbeitet in Verbindung mit der Zeit des Routers. Da der Router selbst keine Echtzeituhr integriert hat, bezieht er die Zeit mittels Simple Network Time Protocol (SNTP) von einem SNTP Server im Internet. Schauen Sie im Abschnitt **Zeitzone** für weitere Informationen nach. Die Zeit des Routers muss mit Ihrer lokalen Zeit übereinstimmen. Wenn die Zeit nicht übereinstimmt wird die Funktion Zeitplan nicht einwandfrei funktionieren (Zeitverschiebungen).

Zeitplan

Zeitfenster

ID	Name	Wochentag	Startzeit	Endzeit		
1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
4	TimeSlot4	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
5	TimeSlot5	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
6	TimeSlot6	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
7	TimeSlot7	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
8	TimeSlot8	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
9	TimeSlot9	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
10	TimeSlot10	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
11	TimeSlot11	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
12	TimeSlot12	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
13	TimeSlot13	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
14	TimeSlot14	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
15	TimeSlot15	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
16	TimeSlot16	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen

Konfiguration des Zeitplans

Zeitfenster bearbeiten

1. Wählen Sie ein Zeitfenster (Time Slot 1 bis 16) aus um es zu bearbeiten, klicken Sie auf **[Bearbeiten].**

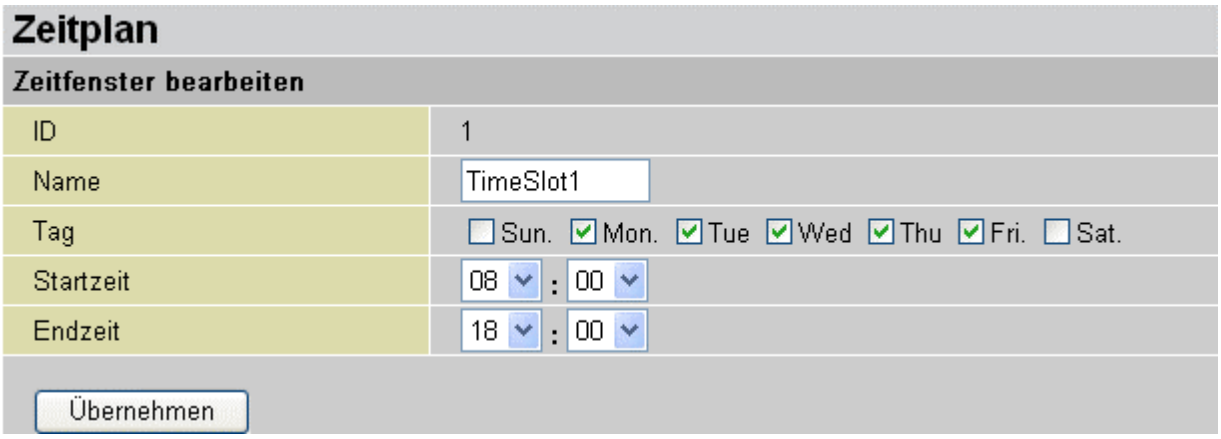
Zeitplan

Zeitfenster

ID	Name	Wochentag	Startzeit	Endzeit		
1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen
2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	Bearbeiten	Löschen

Hinweis: Die Tage welche selektiert wurden werden in Großbuchstaben angegeben. Tage in Kleinbuchstaben wurden nicht selektiert und dementsprechend wird die Regel auch nicht an diesen Tagen angewendet.

2. Die detaillierten Einstellungen des Zeitfensters werden angezeigt.



Folgende Einstellungen können hier verändert werden:

- **ID:** Die ID des Zeitfenster
- **Name:** Hier können Sie einen Namen für das Zeitfenster eintragen
- **Tag:** Werksseitig sind die Tage von Montag bis Freitag selektiert. Sie können selber die Tage festlegen, an welchen die Regel angewendet werden soll
- **Startzeit:** Werksseitig ist 8:00 eingestellt. Sie können die Startzeit selber festlegen
- **Endzeit:** Werksseitig ist 18:00 eingestellt. Sie können die Endzeit selber festlegen
- Klicken Sie auf **Übernehmen** damit die Einstellungen wirksam werden.

Löschen eines Zeitfenster

- Klicken Sie auf **Löschen** damit das entsprechende Zeitfenster gelöscht wird. Die Tage werden alle deaktiviert.

3.9 Erweitert

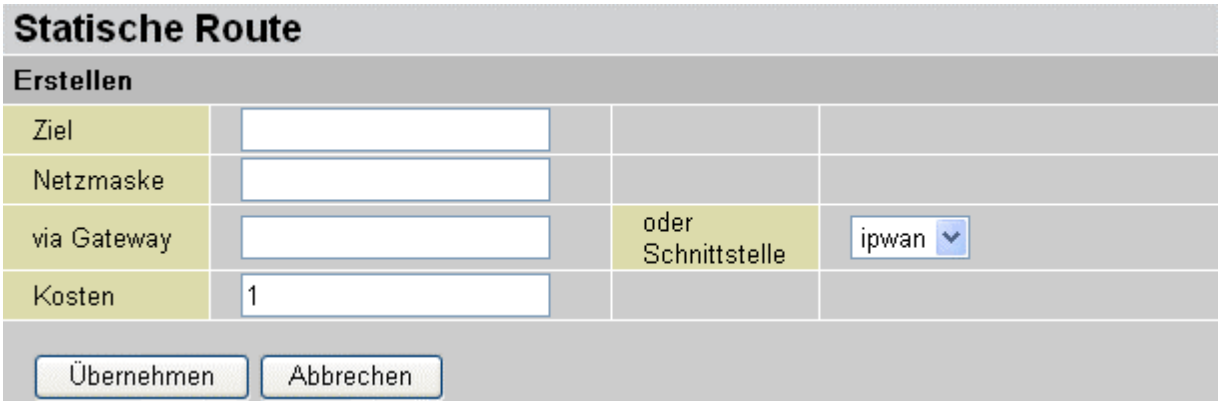
Die Konfigurationen innerhalb des Menüs **Erweitert** sind primär für erfahrene Anwender gedacht, welche die hier angebotenen Funktionen benötigen. Nicht erfahrene Anwender sollten diese Funktionen und deren Einstellungen nicht verändern.

Diese Kategorie bietet folgende Untermenüs:

- Statische Route
- Dynamischer DNS
- Prüfe Email
- Geräte Management
- IGMP
- VLAN Bridge

3.9.1 Statische Route

Klicken Sie auf **Erstellen** um eine Statische Route hinzuzufügen

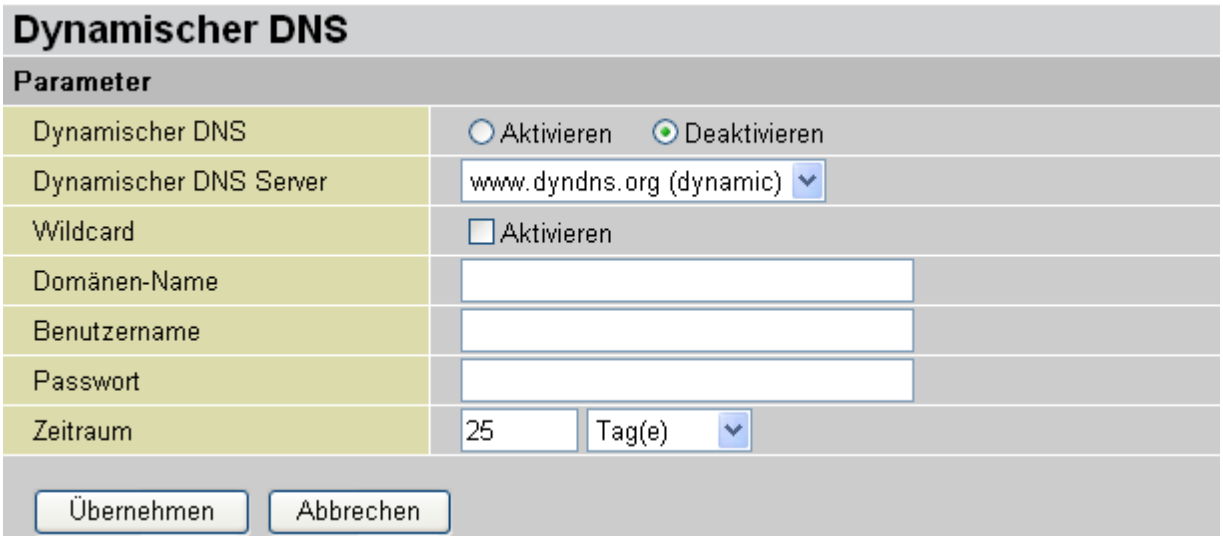


Folgende Einstellungen können hier verändert werden:

- **Ziel:** Tragen Sie die Ziel IP Adresse ein
- **Netzmaske:** Tragen sie die Netzmaske zu der Ziel IP Adresse ein
- **Via Gateway:** Tragen Sie die Gateway IP Adresse über welche die Pakete weitergeleitet werden sollen
- **Schnittstelle:** Geben Sie die Schnittstelle an über welche die Pakete weitergeleitet werden sollen
- **Kosten:** Auch Hop genannt. Normalerweise wird die 1 übernommen

3.9.2 Dynamischer DNS

Die Dynamische DNS Funktion erlaubt Ihnen, einen Alias für eine dynamische IP Adresse als einen statischen Hostname darzustellen, indem Sie einen Domainnamen dazu nutzen. Dies ist besonders nützlich, wenn Sie einen Server über Ihre ADSL Verbindung hosten, so das jeder der sich mit dem Server verbinden will, einfach Ihren Domainnamen nutzt, anstelle der sich regelmäßig wechselnden IP Adresse. Diese dynamische IP Adresse ist die WAN IP des Routers, welche Ihnen von Ihrem ISP zugewiesen wird.



Zuerst müssen Sie sich bei einem Dynamischen DNS Provider registrieren und einen Account einrichten, z.B. bei http://www.dyndns.org

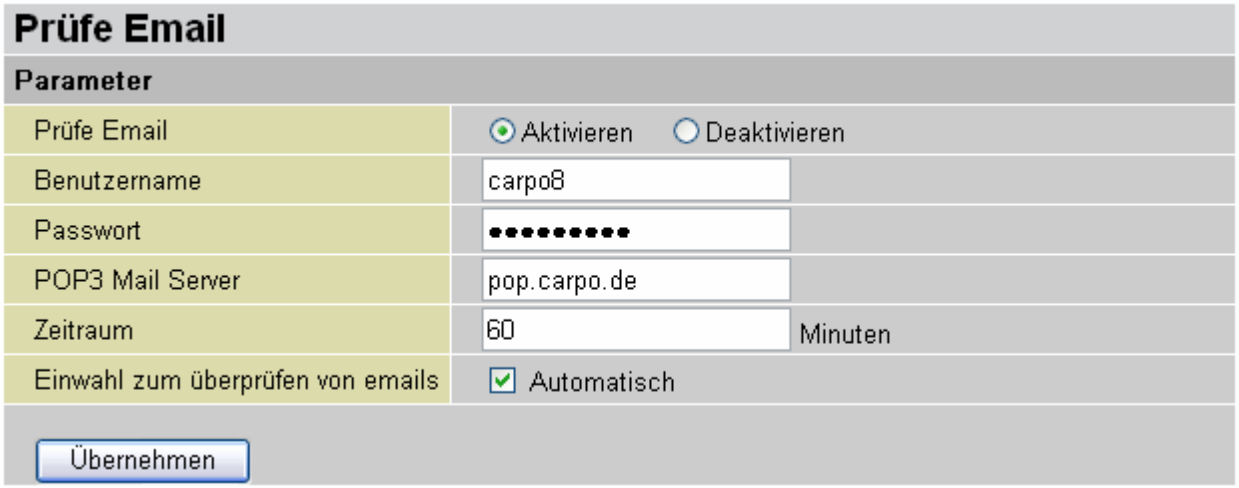
Es werden mehr als 10 DDNS Dienste unterstützt.

- www.dyndns.org (custom)
- www.dyndns.org (dynamic)
- www.dyndns.org (static)
- www.zoneedit.com
- www.dtdns.com
- www.dhs.org
- www.3domain.hk
- www.no-ip.com
- www.3322.org
- dyndns.dk
- www.tzo.com
- www.enom.com
- vdyn.b2e.co.za
- dyndns.adept.co.za
- www.dy.fi
- ddns.mweb.net

Folgende Einstellungen können verändert werden:

- **Deaktivieren:**
  Klicken um die Funktion Dynamischer DNS zu deaktivieren
- **Aktivieren:**
  Klicken um die Funktion Dynamischer DNS zu aktivieren. Die folgenden Felder müssen die notwendigen Informationen beinhalten, ansonsten wird die Funktion Dynamischer DNS wieder deaktiviert
- **Dynamischer DNS Server:**
  Wählen Sie den DDNS Dienst bei welchem Sie einen Account haben
- **Wildcard:**
  Wenn Wildcard aktiviert wird, kann z.B. die Homepage xyz.dyndns.org auch über Aliase erreicht werden. Dies kann hilfreich sein, wenn für die Homepage weitere Sub-Domains angelegt werden, z.B. support.xyz.dyndns.org oder guestbook.xyz.dyndns.org
- **Domänen Name, Benutzername und Passwort:**
  Tragen Sie den registrierten Domänennamen sowie den dazugehörigen Benutzernamen und das Passwort ein
- **Zeitraum:**
  Geben Sie den Zeitraum an, wann der Router mit dem DDNS Server die erforderlichen Informationen austauschen soll. Unabhängig von dieser Einstellung, teilt der Router dem DDNS Server die IP Adresse mit sobald diese vom ISP geändert wurde
- **Via WAN Schnittstelle:**
  Auswahl über welche WAN Schnittstelle Sie die DDNS Anfrage heraus senden wollen

3.9.3 Prüfe Email



Diese Funktion erlaubt es Ihnen, über den Router Ihr POP3 Postfach nach neuen E-Mails zu überprüfen. Die Mail LED an Ihrem Router wird blinken, sobald neue Nachrichten auf den Download warten. Sie können den Status ebenfalls überprüfen im Abschnitt Status – E-Mail Status des Webinterfaces, welches zusätzlich genauere Informationen über die Anzahl der neuen E-Mails bereithält. Schauen Sie im Abschnitt Status dieser Anleitung für weitere Informationen nach.

- **Deaktivieren:** Klicken um die Funktion Prüfe Email zu deaktivieren
- **Aktivieren:** Klicken um die Funktion Prüfe Email zu aktivieren

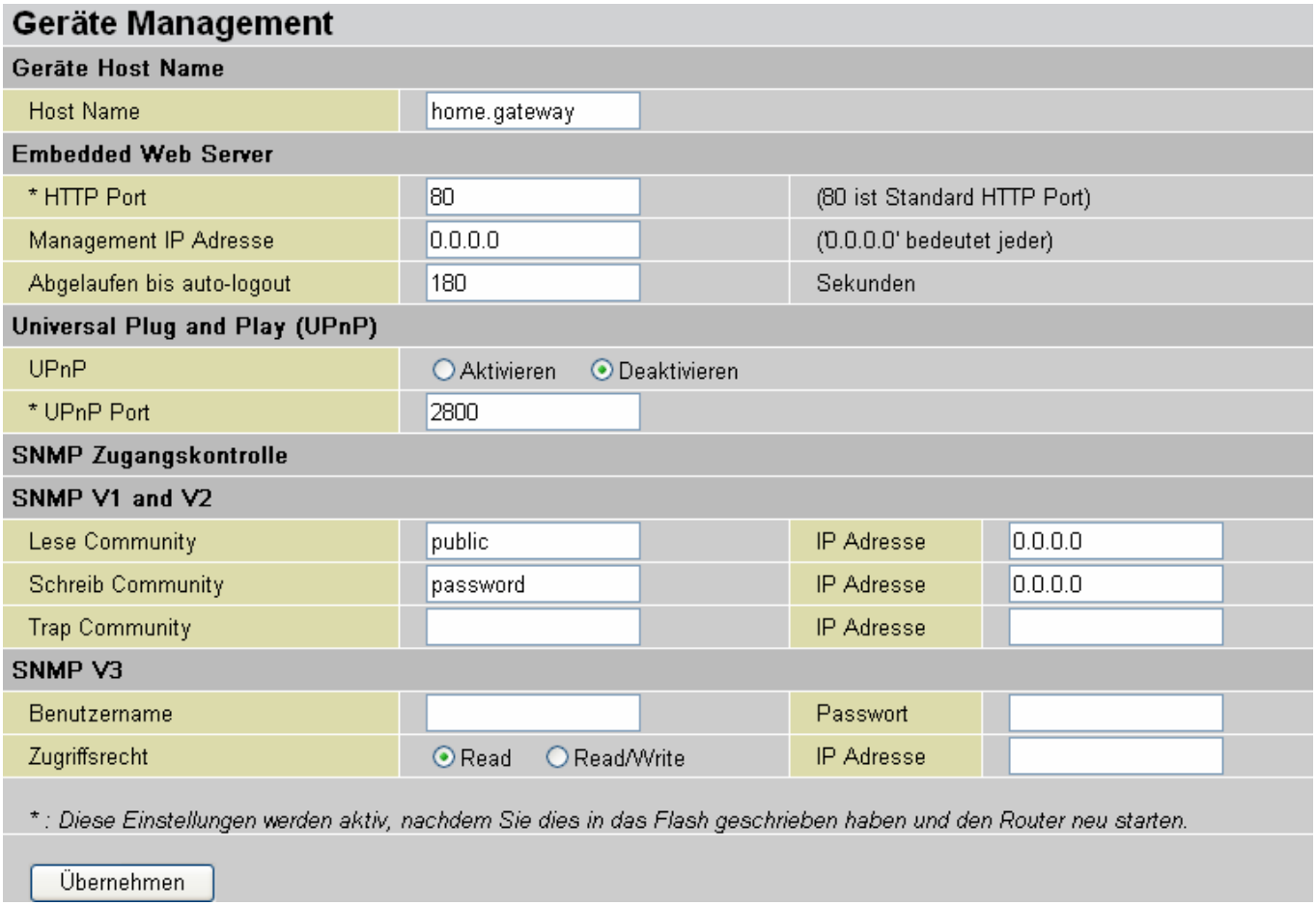
Die folgenden Felder müssen die notwendigen Informationen beinhalten:

Benutzername: Tragen Sie den den Login-Namen des POP3 Accounts ein welchen Sie überprüfen wollen. Es ist die E-Mail-Adresse die Sie von Carpo erhalten haben. Normalerweise ist die Adresse Benutzername@carpo.de, resp. Benutzername@carpo.ch aufgebaut. Sollten Sie Probleme mit dem Login Account haben, kontaktieren Sie bitte Carpo.

- **Passwort:** Passwort des Email Accounts
- **POP3 Mail Server:** Namen des (POP3) Mail Server
- **Zeitraum:** Intervall (Minuten) für die Prüfung des Email Accounts
- **Einwahl zum überprüfen von Emails:**
  Wenn diese Funktion aktiviert ist, wird Ihr ADSL Router automatisch eine Verbindung ins Internet aufbauen, um zu prüfen, ob neue E-Mails vorhanden sind. Seien Sie bitte vorsichtig, wenn Ihre ADSL Nutzung über einen Zeittarif abgerechnet wird

3.9.4 Gerätemanagement

Die Geräte Management Konfigurationseinstellungen erlauben Ihnen die Sicherheitsoptionen und Überwachungsfunktionen des Routers einzustellen.



Eingebauter Web Server

HTTP Port: Dies ist der Port des integrierten Webservers (für Web-basierende Konfiguration) der benutzt wird. Der Standardwert ist der HTTP Port 80. Benutzer können einen alternativen Port festlegen, wenn Sie zum Beispiel einen zusätzlichen Webserver auf Ihrem PC laufen lassen.

- Management IP Adresse: Sie können die IP Adresse angeben, von der ein Log-in gestattet ist und die auf den Web Server des Routers zugreifen kann. Wenn Sie die IP Adresse als 0.0.0.0 festlegen, kann jeder Benutzer Sie sich von jeder IP Adresse einloggen.

- Abgelaufen bis auto-logout: Gibt den Zeitrahmen an bis zum automatischen Ausloggen des Benutzers.

Zum Beispiel: Benutzer A ändert die HTTP Port Nummer auf 100, angegeben durch die eigene IP Adresse 192.168.1.55, und gibt die auto-logout Zeit mit 100 Sekunden an. Der Router wird nur Benutzer A von der IP Adresse 192.168.1.55 zugriff auf das Web GUI über: http://192.168.1.254:100 erlauben. Nach 100 Sekunden wird der Router Benutzer A automatisch ausloggen.

Universal Plug and Play (UPnP)

UPnP bietet Peer-to-Peer Netzwerkanschlussfähigkeit für PCs und andere Netzwerkgeräte an. Es erleichtert die Konfiguration unterschiedlicher Programme und den Datentransfer zwischen den Geräten. UPnP bietet viele Vorzüge für Nutzer von NAT Router über UPnP NAT Traversal und erleichtert die Arbeit für Port Forwarding mit unterstützten Systemen sehr, da die benutzten Programme dies automatisch kontrollieren und konfigurieren. Dadurch entfällt die zusätzliche Konfigurationsarbeit des Benutzers.

Das Betriebssystem und das relevante Programm müssen UPnP neben dem Router unterstützen. Windows XP und Windows ME unterstützen UPnP (wenn die Komponente schon installiert ist) von Anfang an, und Windows 98 Benutzer müssen die Internet Verbindungsfreigabe von Windows XP installieren, um UPnP zu unterstützen. Windows 2000 unterstützt kein UPnP.

- **Deaktivieren:** Klicken Sie hier, um die UPnP Funktion des Routers zu deaktivieren
- **Aktivieren:** Klicken Sie hier, um die UPnP Funktion des Routers zu aktivieren
- **UPnP Port:** Der Standardwert ist 2800. Es wird empfohlen diesen Standardwert zu nutzen

Wenn dieser Port mit anderen einem anderen benutzen Port einen Konflikt verursacht, so ändern Sie diesen Port.

SNMP Zugangskontrolle

(Entsprechende Software auf einem PC im gleichen LAN wird vorausgesetzt, um diese Funktion zu nutzen) – Simple Network Management Protocol.

SNMP V1 und V2:

- **Lese Community:**
  Gibt einen Namen und eine IP Adresse an, die als Read Community identifiziert wird. Dieser Community String wird gegenüber dem String im Konfigurationsfile verglichen. Sobald der String richtig ist, können sich Benutzer die Daten ansehen

- **Schreib Community:**
  Gibt einen Namen und eine IP Adresse an, die als Write Community identifiziert wird. Dieser Community String wird gegenüber dem String im Konfigurationsfile verglichen. Sobald der String richtig ist, können sich Benutzer die Daten ansehen und modifizieren

- **Trap Community:**
  Gibt einen Namen und eine IP Adresse an, die als Trap Community identifiziert wird. Dieser Community String wird gegenüber dem String im Konfigurationsfile verglichen. Sobald der String richtig ist, werden die SNMP Traps an diese IP Adresse gesendet

SNMP V3:

Spezifiziert Name und Passwort für die Authentifizierung und definiert die Zugriffsrechte von einer überprüfen IP Adresse. Nachdem die Autorisierung erfolgreich war, können Benutzer mit dieser IP Adresse Daten ansehen und modifizieren.

SNMP Version: SNMPv2c und SNMPv3

SNMPv2c kombiniert die gemeinschaftlich-basierende Annäherung von SNMPv1 mit dem Protokoll-Funktionen von SNMPv2, lässt dabei aber alle Sicherheits-Mechanismen von SNMPv2 weg. Das "c" stammt von der Tatsache dass SNMPv2c den SNMPv1 Community String für die “Sicherheit” verwendet. SNMPv2c ist weit verbreitet und akzeptiert.

SNMPv3 beinhaltet starke Authentifizierungs-Mechanismen, mit Berechtigungen für Fern-Überwachung.

Unterstützte Traps: Cold Start, Authentication Failure.
Folgende MIBs werden unterstützt:

- Vom RFC 1213 (MIB-II):
  - System group
  - Interfaces group
  - Address Translation group
  - IP group
  - ICMP group
  - TCP group
  - UDP group
  - EGP (not applicable)
  - Transmission
  - SNMP group

- Vom RFC1650 (EtherLike-MIB):
  - dot3Stats

- Vom RFC 1493 (Bridge MIB):
  - dot1dBase group
  - dot1dTp group
  - dot1dStp group (konfiguriert als spanning tree)

- Vom RFC 1471 (PPP/LCP MIB):
  - pppLink group
  - pppLqr group

- Vom RFC 1472 (PPP/Security MIB):
  - PPP Security Group)

- Vom RFC 1473 (PPP/IP MIB):
  - PPP IP Group

- Vom RFC 1474 (PPP/Bridge MIB):
  - PPP Bridge Group

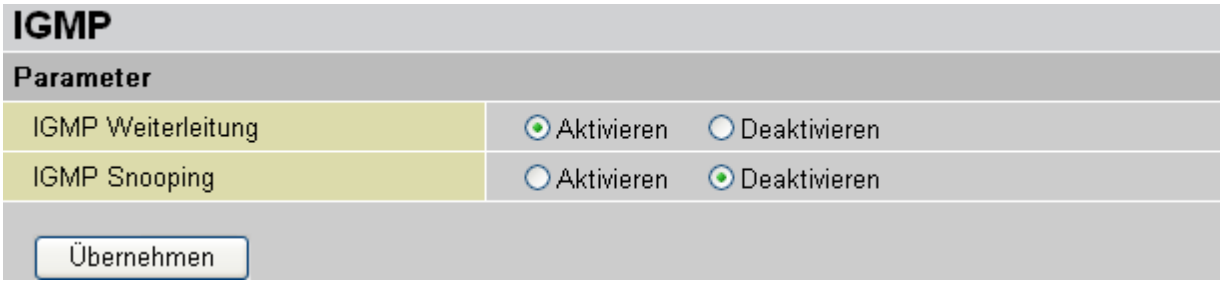
- Vom RFC1573 (IfMIB):
  - ifMIBObjects Group

- Vom RFC1695 (atmMIB):
  - atmMIBObjects

- Vom RFC 1907 (SNMPv2):
  - only snmpSetSerialNo OID

3.9.5 IGMP

IGMP, bekannt als Internet Group Management Protocol, dient zur Organisation von Multicast Gruppen.

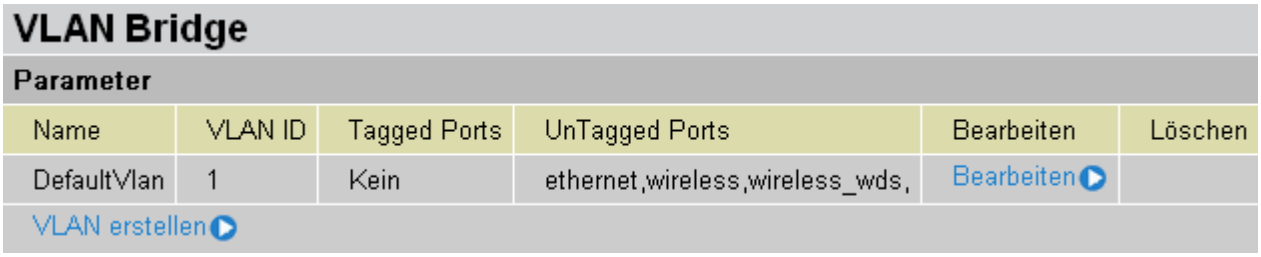


Folgende Einstellungen können hier verändert werden:

- **IGMP Weiterleitung:** Akzeptiere Multicast Pakete. Werkseinstellung Aktiviert
- **IGMP Snooping:** Erlaube dem Switched Ethernet die Weiterleitung zu überprüfen und zu entscheiden. Werkseinstellung Aktiviert.

3.9.6 VLAN Bridge

Ein Virtual Local Area Network (VLAN) ist ein virtuelles lokales Netz innerhalb eines physischen Netzes. Dieser Abschnitt erlaubt es eine VLAN Gruppe zu erstellen und die Mitglieder zu spezifizieren.



Folgende Einstellungen können hier verändert werden:

- **VLAN erstellen:** Erstellt eine neue VLAN Gruppe
- **Bearbeiten:** Bearbeitet die Mitglieder der vorhandene VLAN Gruppe

Beispiele für erweiterte VLAN Einstellungen (Triple Play)

VLAN_Data:
Ethernet Port 1, Wireless und Wireless WDS sind für das Internet reserviert

- Ethernet Port 1 benötigt VC 0/40 Bridged.

VLAN_Video:

Ethernet Ports: 2 und 3:

- 0/33 Bi-direktional IP
- 0/34 Video
- 0/35 Video
- 0/36 Video Subscriber Services (EPG, EAS, etc.)
- 0/37 Video
- 0/38 Video
- 0/39 Spare

Schritt 1: Einstellungen Mitglieder Ports

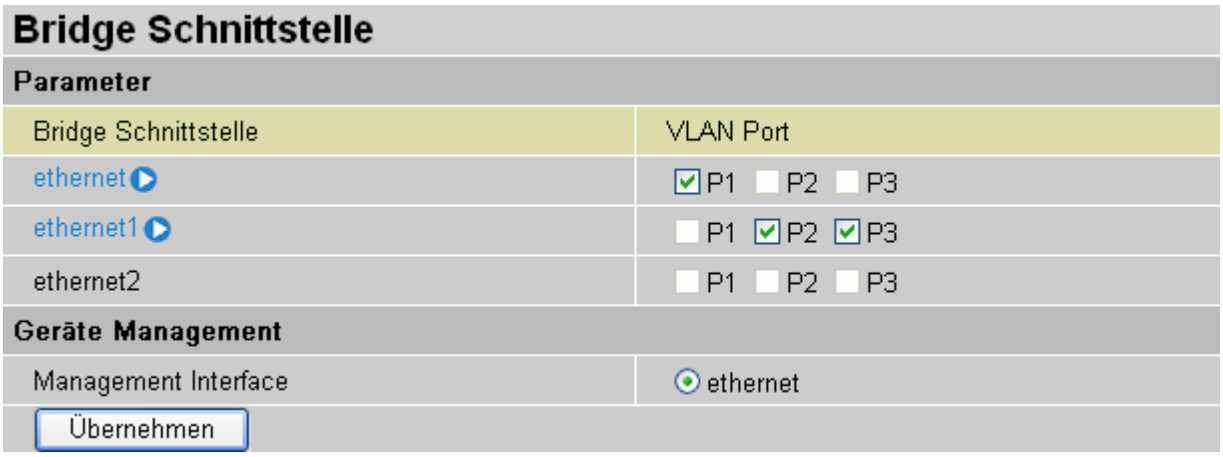
Gehen Sie in das Menü **KONFIGURATION → LAN → BRIDGE SCHNITTSTELLE**

Sie können unter **BRIDGE SCHNITTSTELLE** für jede VLAN Gruppe Mitglieder Ports wählen.
Im Beispiel werden zwei VLAN Gruppen erstellt.

- Ethernet: P1 (Port 1)
- Ethernet1: P2 und P3 (Port 2, 3)

HINWEIS: Bitte deaktivieren Sie zuerst P2, P3 vom Ethernet VLAN und aktivieren diese dann unter Ethernet1. Sie sollten jede VLAN Gruppe behutsam einstellen. Jede Bridge Schnittstelle ist wie folgt zugeordnet:

Bridge Schnittstelle	**VLAN Port (Startet immer mit)**
Ethernet	P1 / P2 / P3
Ethernet1	P2 / P3
Ethernet2	P3



Schritt 2: Erstellen der WAN Schnittstelle

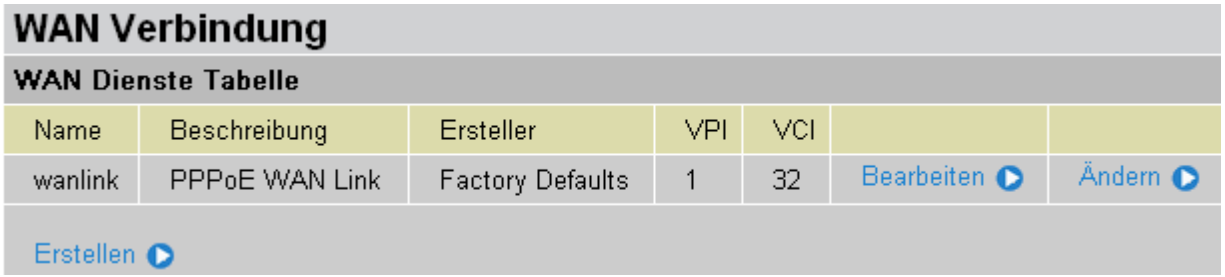
Gehen Sie in das Menü **KONFIGURATION → WAN → ISP**

wanlink ist die werksseitig eingestellte WAN Schnittstelle für Daten/Internet Dienste. Carpo verwendet diese dieses Protokoll. Wenn Sie einen anderen ISP haben und dieser das Protokoll verwendet, klicken Sie auf **BEARBEITEN** um weitere Parameter einzugeben, sofern nötig. Wenn Carpo oder Ihr anderer ISP PPPoE nicht verwendet, so können Sie die werksseitige WAN Verbindung über Ändern wechseln.

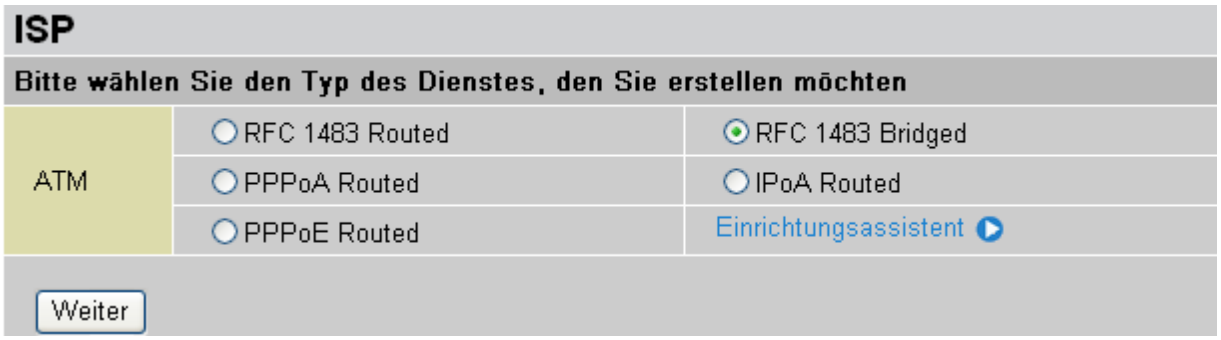
In dem Beispiel wird **1/32** für **Data/Internet** und **PPPoE** verwendet;

- Klicken Sie auf **BEARBEITEN** um die Einstellungen VPI/VCI auf 1/32 zu setzen
- Klicken Sie auf **ERSTELLEN** um eine weitere WAN Schnittstelle für Video Anwendungen einzurichten

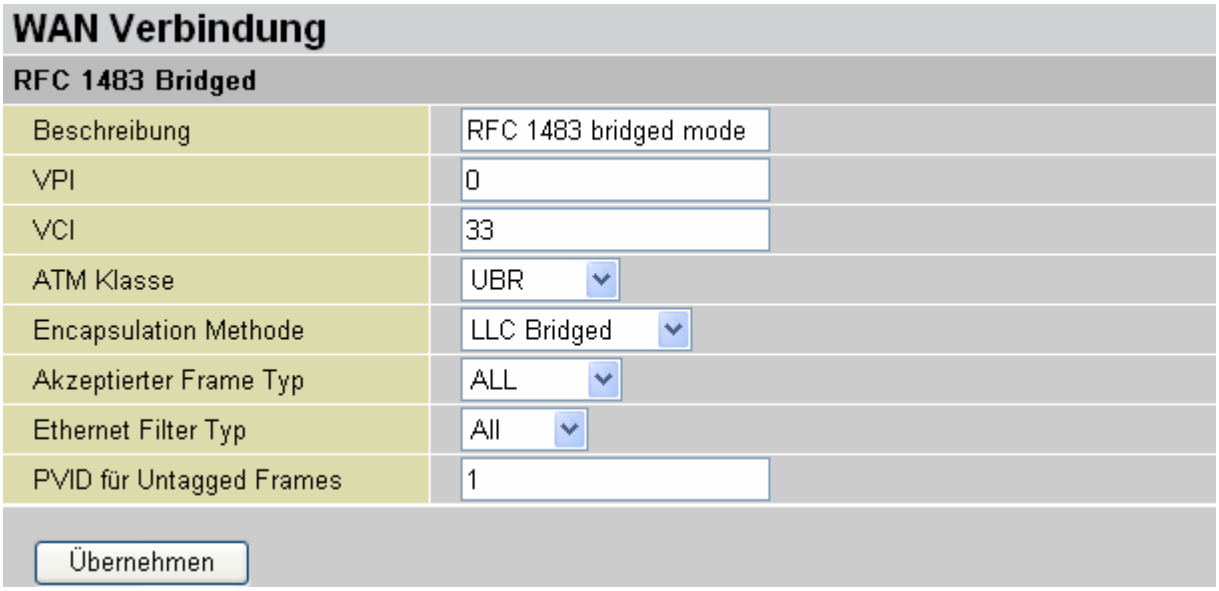
Im Ganzen werden 8 VLANs unterstützt, daher können maximal 8 WAN Schnittstellen erstellt werden.



Im Beispiel weisen wir PVC 0/33 bis 0/39 unter Verwendung vom 1483 Bridged Mode zu für die Video Anwendung zu. Aktivieren Sie RFC 1483 Bridged und klicken Sie auf Weiter um die Einrichtung fortzusetzen.



- Tragen Sie für VPI 0 und VCI 33 ein. Wählen Sie die ATM Klasse, Encapsulation Methode, Akzeptierter Frame Typ, Filter Typ und PVID für Untagged Frames



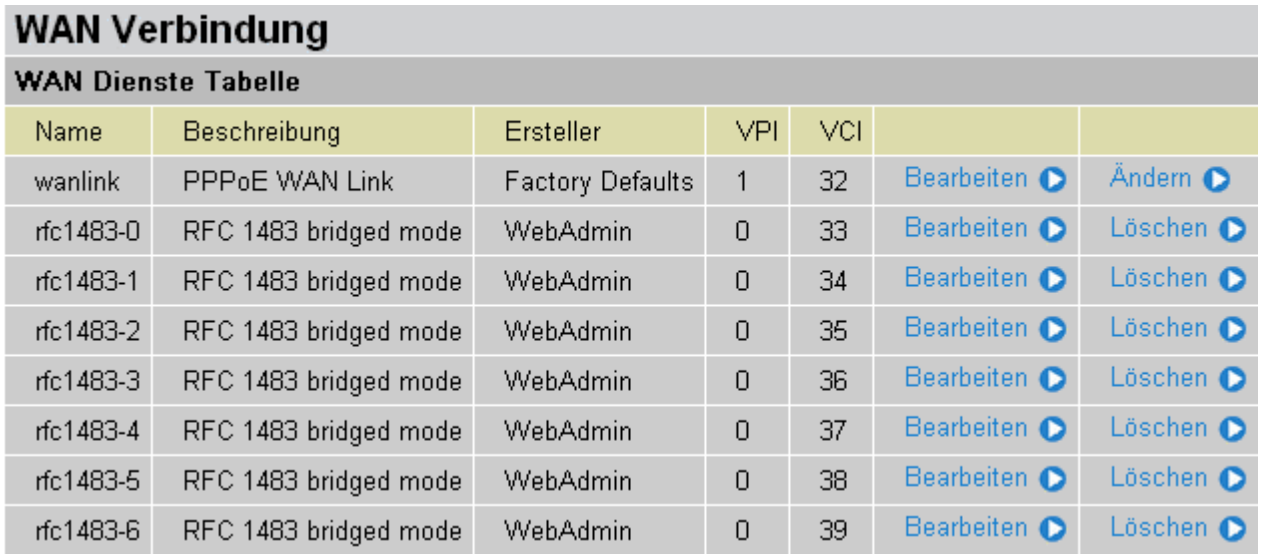
Folgende Einstellungen können hier verändert werden:

- **VPI und VCI:** Tragen Sie die Informationen von Carpo oder eines anderen ISP ein
- **ATM Klasse:** Der Quality of Service Ihres ATM Layers
- **Encapsulation Methode:** Wählen Sie das Encapsulation Format, dies wird Ihnen von Carpo oder einem anderen ISP mitgeteilt
- **Akzeptierter Frame Typ:** Geben Sie an welche Art von Datenverkehr diese Verbindung passieren soll, jeder Datenverkehr oder nur VLAN tagged Daten
- **Filter Typ:** Geben Sie an welcher Ethernet Filter Typ für diese Bridge Schnittstelle angewendet werden soll

All	Erlaubt allen Ethernet Paket Typen diesen Port zu verwenden.
IP	Erlaubt nur IP/ARP Ethernet Paket Typen diesen Port zu verwenden.
PPPoE	Erlaubt nur PPPoE Ethernet Paket Typen diesen Port zu verwenden.

- **PVID für Untagged Frames:** PVID ist bekannt als Port VLAN Identifier. Wenn ein nicht markiertes (untagged) Paket vom eingehenden Port(s) empfangen wird diese Paket markiert (tagged) mit der angegebenen PVID

Im Beispiel müssen Sie nur VPI und VCI wie angegeben ändern (0/33) – lassen Sie die anderen Einstellungen wie sie waren. Wiederholen sie diese Schritte indem Sie auf **Erstellen** → dann **RFC1483 Bridged** wählen → bis Sie von 0/34 bis 0/39 die **Bridged Schnittstellen** erstellt haben.



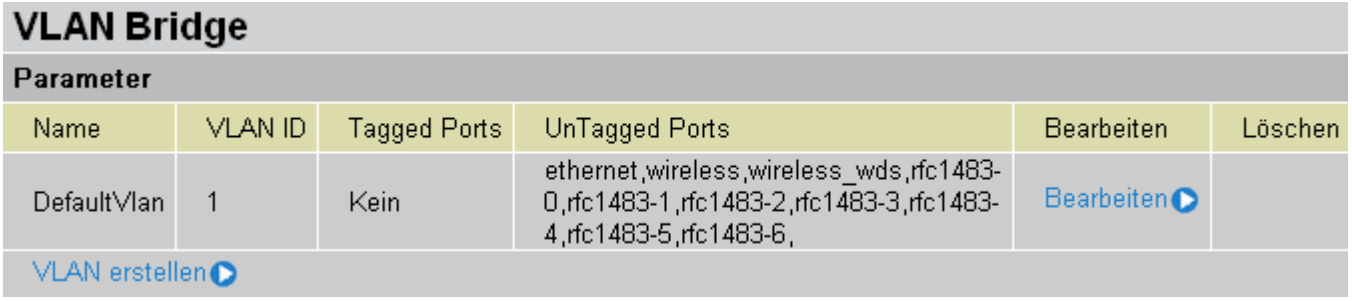
Schritt 3: VLAN Dienste einrichten

Gehen Sie in das Menü **KONFIGURATION → ERWEITERT → VLAN BRIDGE**

DefaultVlan listet alle Mitglieder Ports auf. Es ist notwendig dass Sie für jedes VLAN die Mitglieder Ports gruppieren.

Im Beispiel werden zwei VLAN Gruppen benötigt: Data und Video

- Klicken Sie auf **VLAN erstellen** um eine weitere VLAN Gruppe einzurichten

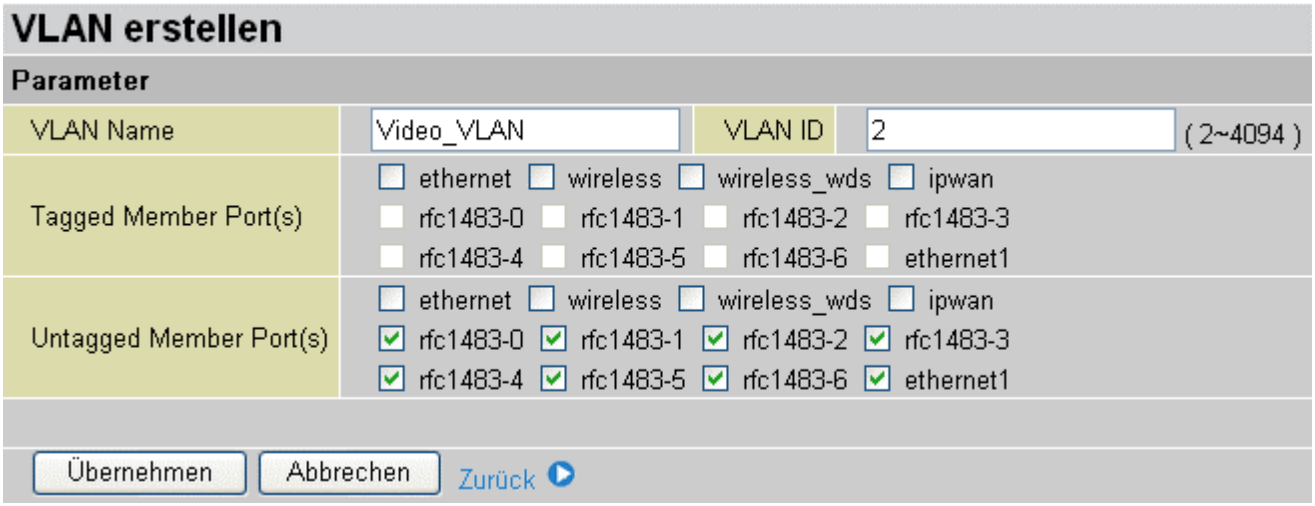


Geben Sie einen Namen und eine ID (PVID) an, damit die Video Gruppe identifiziert wird. Der gültig Bereich für PVID ist 1 ~ 4094.

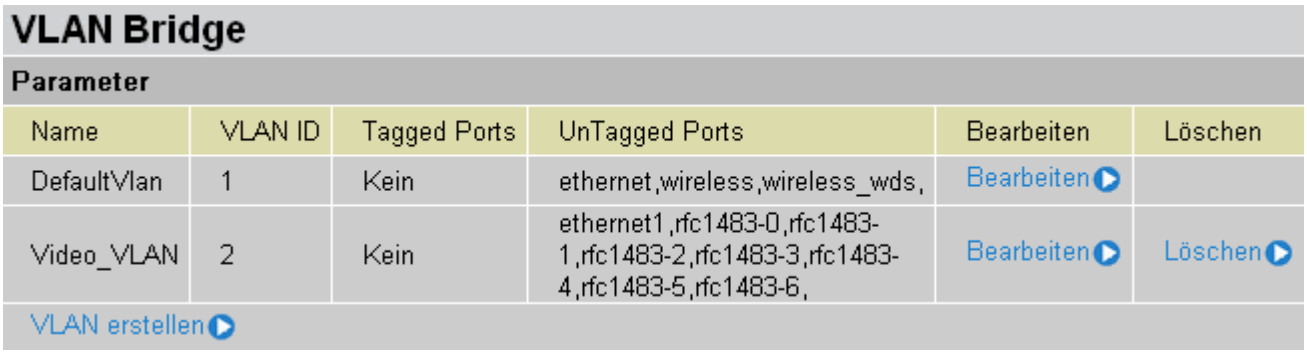
Im Beispiel:

- VLAN untagged Ports für Data/Internet: **ethernet**, **wireless** and **wireless_wds**
- VLAN untagged Ports für Video: **ethernet1**, **rfc-1483-0 ~ rfc-1483-6**

Klicken Sie auf **Übernehmen** damit die Einstellungen sofort wirksam werden.



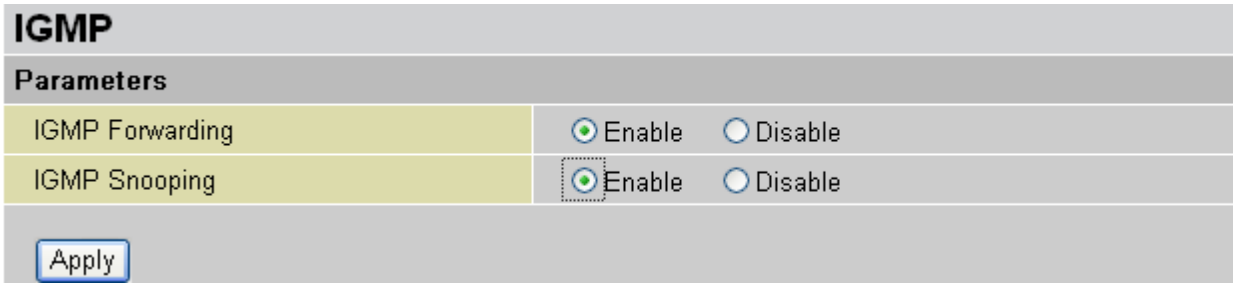
Nachdem Sie die **VLAN Bridge** und die **Bridge Schnittstelle** wie im Schritt 1 erstellt und verbunden haben, sehen Sie das konforme Verhältnis in diesem Fenster.



Schritt 4: IGMP Snooping Aktivieren

Gehen Sie in das Menü **Konfiguration → Erweitert → IGMP**.

- **IGMP Snooping** muss **aktiviert** damit der Video Stream korrekt weitergeleitet wird



4. Speichern der Konfiguration im Flash

Nachdem Sie die Einstellungen des Routers verändert haben, müssen Sie alle Konfigurationsparameter im FLASH speichern, um einen Datenverlust zu verhindern, wenn der Router ausgeschaltet oder ein Reset durchgeführt wird.

- Klicken Sie auf **Speichern der Konfiguration im Flash** und dann auf **Übernehmen** um die neue Konfiguration im Flash zu speichern

Nach erfolgreicher Speicherung der Konfiguration wird dies mit einem separat auftretendem Fenster bestätigt. Klicken Sie hier auf OK.

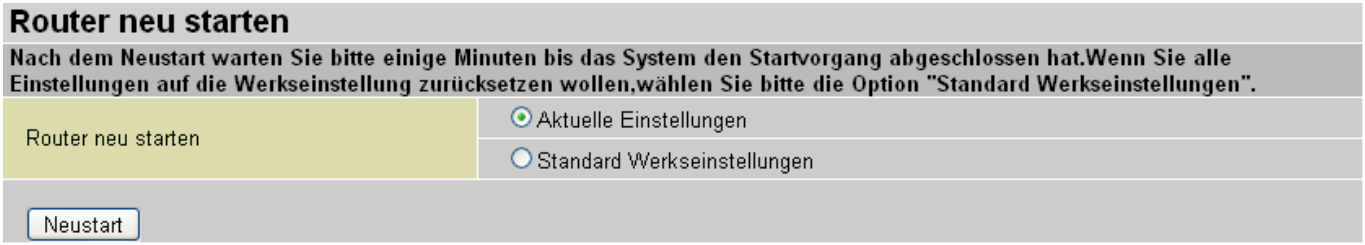
Es kann u.U. vorkommen, dass die getätigten Einstellungen nicht direkt übernommen und genutzt werden. Hier empfiehlt es sich, dass die Einstellungen zuvor wie oben beschrieben dauerhaft gespeichert werden und das Gerät anschließend neu gestartet wird.

Hierzu klickt man am unteren Rechten Fensterrand auf den Button NEUSTART

Bei einem Neustart des Routers können entweder
- die **aktuellen** Einstellungen

oder
- die **werksseitigen** Einstellungen (Router Reset)

weiterverwendet werden.

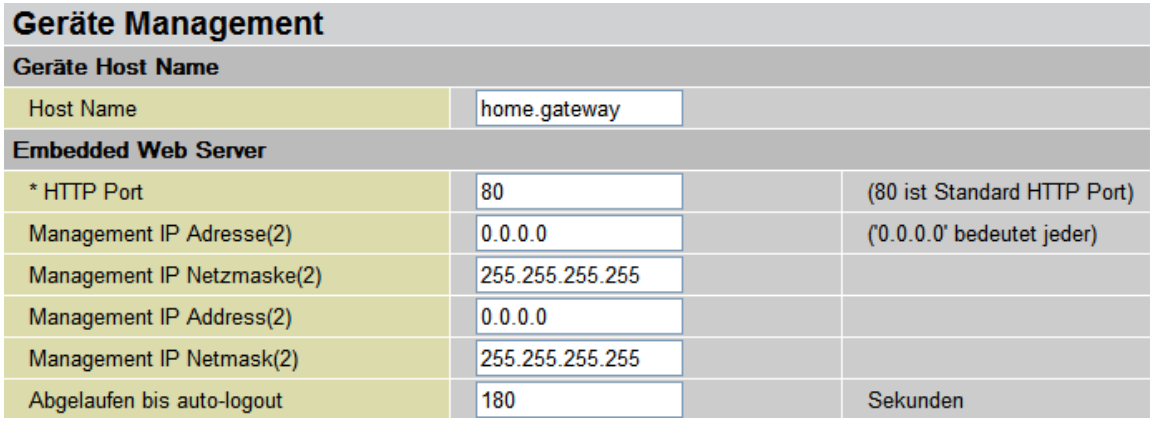


Nach einem Klick auf NEUSTART startet sich der Router komplett neu, synchronisiert sich anschließend erneut mit der DSL Leitung und ist dann erst wieder einsatzbereit. Ein Timer zeigt dies genau an, danach wird das Routerkonfigurationsmenü selbständig neu geöffnet:

Ausloggen

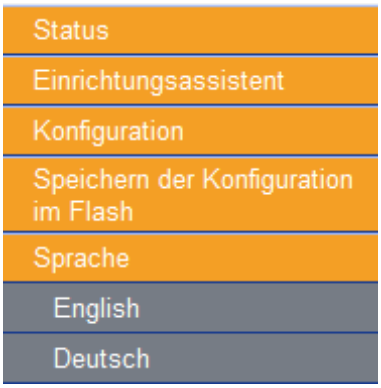
Um das Web Interface des Routers zu verlassen, wählen Sie **AUSLOGGEN**. Versichern Sie sich, dass Sie die Konfiguration gespeichert haben, bevor Sie ausloggen.

HINWEIS: Bedenken Sie, dass der Router sich nur von einem PC gleichzeitig konfigurieren lässt. Sobald ein PC auf den Router zugreift, kann kein anderer einen Zugriff darauf erhalten, solange der PC sich nicht ausgeloggt hat. Wenn der vorherige PC sich vergisst auszuloggen, so kann der zweite PC nach einer vorgegeben Zeit – Standardwert ist 3 Minuten - auf den Router zugreifen. Sie können diesen Wert modifizieren im Abschnitt **Erweitert – Geräte Management** des Web Interface. Schauen Sie im Abschnitt **Erweitert** in dieser Anleitung nach für weitere Informationen zu diesem Thema.



Geräte Management		
Geräte Host Name		
Host Name	home.gateway	
Embedded Web Server		
* HTTP Port	80	(80 ist Standard HTTP Port)
Management IP Adresse(2)	0.0.0.0	('0.0.0.0' bedeutet jeder)
Management IP Netzmaske(2)	255.255.255.255	
Management IP Address(2)	0.0.0.0	
Management IP Netmask(2)	255.255.255.255	
Abgelaufen bis auto-logout	180	Sekunden

5. Sprache



Im letzten Menüpunkt kann die jeweilige Sprache der Bedienoberfläche ausgewählt werden:

Zur Verfügung stehen folgende Sprachen:

- **Englisch**
- **Deutsch**