TP-LINK®

Handbuch

TL-MR3020

Tragbarer 3G/3,75G-Wireless-N-Router

Rev: 1.0.0
1910010533

COPYRIGHT & HANDELSMARKEN

Diese Spezifikationen können kurzfristigen Änderungen unterliegen. TP-LINK® ist eine registrierte Handelsmarke von TP-LINK TECHNOLOGIES CO., LTD. Andere Marken und Produktnamen sind Handelsmarken oder registrierte Handelsmarken ihrer entsprechenden Rechteinhaber.

http://www.tp-link.com

FCC-STATEMENT

Dieses Gerät wurde getestet und entspricht den Spezifikationen eines B-Klasse-Gerätes laut Teil 15 der FCC-Reglementierung. Diese Spezifikationen sollen gegen schädliche Einwirkungen des Geräts in einer häuslichen Umgebung schützen. Dieses Gerät erzeugt und benutzt Funksignale und kann, falls es nicht sachgemäß und den Anweisungen entsprechend installiert wird, Funkkommunikation stören. Jedoch kann nicht garantiert werden, dass solche Interferenzen bei einer bestimmten Installation nicht auftreten. Sollte dieses Gerät schädliche Interferenzen mit Radio- oder Fernsehgeräten verursachen, was einfach durch Aus- und Einschalten des Geräts nachgewiesen werden kann, wird geraten, mindestens eine der folgenden Maßnahmen durchzuführen:

- Empfängerantenne anders ausrichten oder deplatzieren.
- Den Abstand zwischen dem Gerät und dem Radio-/Fernsehempfänger vergrößern.
- Das Gerät an einem anderen Stromkreis als das Radio-/Fernsehgerät betreiben.
- Den Händler oder einen Radio-/TV-Techniker zu Rate ziehen.

Dieses Gerät entspricht Teil 15 der FCC-Reglementierung. Der Betrieb unterliegt den folgenden beiden Bedingungen:

1) Das Gerät darf keine schädlichen Interferenzen verursachen.
2) Dieses Gerät muss jegliche eindringende Interferenz tolerieren, einschließlich solcher, die unerwünschtes Verhalten hervorruft.

Sämtliche nicht von TP-LINK genehmigten Änderungen am Gerät können die Betriebserlaubnis erlöschen lassen.

Hinweis: Der Hersteller ist nicht verantwortlich für Interferenzen an anderen Geräten, die aus unbefugten Veränderungen an diesem Modell resultieren Sämtliche nicht von TP-LINK genehmigten Änderungen am Gerät können die Betriebserlaubnis erlöschen lassen.

FCC-Funkfrequenzaussendungsstatement

Dieses Gerät entspricht den FCC-Funkfrequenzaussendungsgrenzen, die für eine unkontrollierte Umgebung gelten. Dieses Gerät und seine Antenne dürfen nicht in der unmittelbaren Nähe anderer radiowellenaussendenden Geräte/Antennen betrieben werden.

„Um den FCC-Radiofrequenzaussendungsanforderungen gerecht zu werden, gilt dies nur für mobile Konfigurationen. Die für diesen Sender benutzten Antennen müssen so installiert werden, dass sie sich mindestens 20cm von Personen und nicht in der unmittelbaren Nähe anderer radiowellenaussendenden Geräte/Antennen befinden."

CE- Warnung

CE 1588 !

Dies ist ein B-Klasse-Produkt. In einer häuslichen Umgebung kann dieses Produkt Interferenzen verursachen, welche für den Benutzer entsprechende Maßnahmen erfordern können.

Nationale Restriktionen

Dieses Gerät ist für den Betrieb zu Hause und im Büro in allen EU-Ländern (und anderen Ländern, die die EU-Direktive 1999/5/EC befolgen) zugelassen. Folgende Betriebseinschränkungen gelten:

Land	Restriktion	Grund/Bemerkung
Bulgarien	keine	Für öffentlichen Betrieb und Betrieb im Freien ist eine allgemeine Betriebserlaubnis erforderlich
Frankreich	Betrieb im Freien begrenzt auf 10mW im Band von 2454 bis 2483,5MHz	Militärische Nutzung. Eine Umstrukturierung des 2,4-GHz-Bandes hat in der Vergangenheit die bis dahin geltende Regelung gelockert. Volle Implementierung ist im Jahr 2012 geplant
Italien	keine	Für den Betrieb außerhalb des eigenen Domizils ist eine allgemeine Betriebserlaubnis erforderlich
Luxemburg	keine	Allgemeine Betriebserlaubnis erforderlich für Netz- und Diensteanbieter
Norwegen	Implementiert	Dies gilt nicht für den Bereich im Umkreis von 20km um das Zentrum von Ny-Ålesund
Russische Föderation	keine	Nur Indoor-Betrieb gestattet.

Bemerkung: Bitte benutzen Sie das Produkt in Frankreich nicht im Freien.

KONFORMITÄTSERKLÄRUNG

Für das Gerät:

Produktbeschreibung: Tragbarer 3G/3,75G-Wireless-N-Router

Modellnr.: **TL-MR3020**

Handelsmarke: **TP-LINK**

erklären wir eigenverantwortlich, dass dieses Produkt alle darauf anwendbaren technischen Regelungen nach folgender Richtlinie erfüllt:

Direktiven 1999/5/EC

Das oben angegebene Produkt entspricht den folgenden Standards/Normen:

ETSI EN 300 328 V1.7.1: 2006

ETSI EN 301 489-1 V1.8.1:2008& ETSI EN 301 489-17 V2.1.1:2009

EN60950-1:2006

Empfehlung 1999/519/EC

EN62311:2008

Direktiven 2004/108/EC

Das oben angegebene Produkt entspricht weiterhin den folgenden Standards/Normen:

EN 55022:2006 +A1:2007

EN 55024:1998+A1:2001+A2:2003

EN 61000-3-2:2006

EN 61000-3-3:1995+A1:2001+A2:2005

Direktiven 2006/95/EC

Das oben angegebene Produkt entspricht weiterhin den folgenden Standards/Normen:

EN60950-1:2006

Direktiven (ErP) 2009/125/EC

Audio/Video-, informations- und kommunikationstechnische Geräte mit umweltbewusstem Design

EN62075:2008

Für diese Erklärung verantwortlich:

Yang Hongliang

Internationaler Produktmanager

TP-LINK TECHNOLOGIES CO., LTD.

South Building, No.5 Keyuan Road, Central Zone, Science & Technology Park, Nanshan, Shenzhen, P. R. China

INHALTSVERZEICHNIS

Verpackungsinhalte

In der Verpackung sollten folgende Gegenstände zu finden sein:

- Tragbarer 3G/3,75G-Wireless-N-Router TL-MR3020
- AC/DC-Adapter für den tragbaren 3G/3,75G-Wirless-N-Router TL-MR3020
- USB-Kabel
- Ethernet-LAN-Kabel
- Schnellinstallationsanleitung
- Eine CD zum tragbaren 3G/3,75G-Wireless-N-Router TL-MR3020 mit:
    - Diesem Handbuch
    - Weiteren Informationen

☞ **Bemerkung:**

Stellen Sie sicher, dass die Verpackung obige Gegenstände beinhaltet. Ist etwas davon beschädigt oder nicht vorhanden, setzen Sie sich bitte mit Ihrem Händler in Verbindung.

Kapitel 1. Einführung

Vielen Dank, dass Sie den tragbaren 3G/3,75G-Wireless-N-Router TL-MR3020 gekauft haben.

1.1 Produktübersicht

TP-LINK versteht die Notwendigkeit unserer Gesellschaft, trotz hoher Mobilität stets erreichbar zu sein. Eine drahtlose Internetverbindung fast überall ermöglicht unser tragbarer Wireless-N-3G/3,75G-Router TL-MR3020. Im Nu ist ein drahtloser Internetzugang mit Datenraten von bis zu 150Mbps errichtet. Egal ob im Zug, beim Camping, auf Dienstreisen: Ihr WLAN-Internetzugang ist in Sekundenschnelle aufgebaut.

3G-/WAN-Breitbandverbindung

Der tragbare Wireless-N-3G/3,75G-Router TL-MR3020 unterstützt mit 3G-, WISP-Client- und Accesspoint-Modus eine flexible Verwendung. Der Router erlaubt Internetzugang über 3G und WAN (xDSL sowie statische oder dynamische IP-Adresse). Dank Failover-Funktion können Sie im Fehlerfall zwischen beiden umschalten und Ihre Internetverbindung aufrechterhalten.

Hohe Kompatibilität

Der tragbare Wireless-N-3G/3,75G-Router TL-MR3020 ist kompatibel zu iPad, iTouch, Android-Smartphones, Kindles und anderen portablen WiFi-Geräten. Über den USB2.0-Anschluss können Sie handelsübliche 3G-Modems verbinden, da der Router zu vielen UMTS-/HSPA-/EVDO-USB-3G/3,75G-Modems kompatibel ist.

Hohe Geschwindigkeit

TP-LINKs Wireless-N-3G/3,75G-Router ermöglichen WLAN-Datenraten mit 802.11n-Geschwindigkeit, bis zu 150Mbps, und damit mehr als die herkömmlichen 802.11g-Produkte, so dass sogar HD-Videostreaming möglich wird.

Niedrieger Stromverbrauch

Über den Mini USB-Anschluss kann der Router über einen Computer oder einen stromsparenden AC/DC-Adapter betrieben werden.

1.2 Konventionen

Die Begriffe „der Router“, „TL-MR3020” oder „das Gerät“ bezeichnen in diesem Handbuch den tragbaren Wireless-N-3G/3,75G-Router TL-MR3020, sofern nicht anders angegeben.

1.3 Hauptfunktionalitäten

- Mini-Desgn, ideal zum Mitnehmen

- 10/100M-RJ45-WAN-Port mit Autoabstimmung, USB2.0-Anschluss, Mini-USB-Anschluss
- Kompatibel zu den Standards IEEE802.11n/g/b sowie IEEE802.3/3u
- Kompatibel zu vielen UMTS-/HSPA-/EVDO-USB-3G-Modems
- Kompatibel zu iPad, iTouch, Android-Smartphones, Kindles und anderen portablen WiFi-Geräten
- Wireless-N-Geschwindigkeit von bis zu 150Mbps
- Drahtlose Sicherheit einfach einrichten durch Drücken der „WPS“-Taste
- Sicherheit mittels WPA/WPA2 und WPA-PSK/WPA2-PSK mit TKIP/AES
- Stromversorgung über Computer oder mitgelieferten AC/DC-Adapter, wenig Stromverbrauch
- Betriebsarten: 3G-Router, WISP-Client und WLAN-Accesspoint
- Internetzugriff über 3G und WAN (dynamische und statische IP-Adresse, PPPoE (DSL), L2TP und PPTP)
- VPN-Passthrough, Virtuelle Server, spezielle Applikationen und DMZ-Host
- UPnP, Dynamisches DNS und Statisches Routing
- Bietet automatisches und zeitgesteuertes Verbinden mit dem Internet
- NAT und DHCP-Server, der IP-Adressen auch statisch vergeben kann
- Kann eine PPPoE-Internetverbindung bei Bedarf herstellen und nach einer konfigurierbaren Leerlaufzeit trennen
- 64/128/152-Bit-WEP-Verschlüsselung und WLAN-ACL (Access Control List)
- Flussstatistiken
- Unterstützt Firmware-Upgrade und Konfiguration über Web

1.4 Routergehäuse

1.4.1 Oberseite

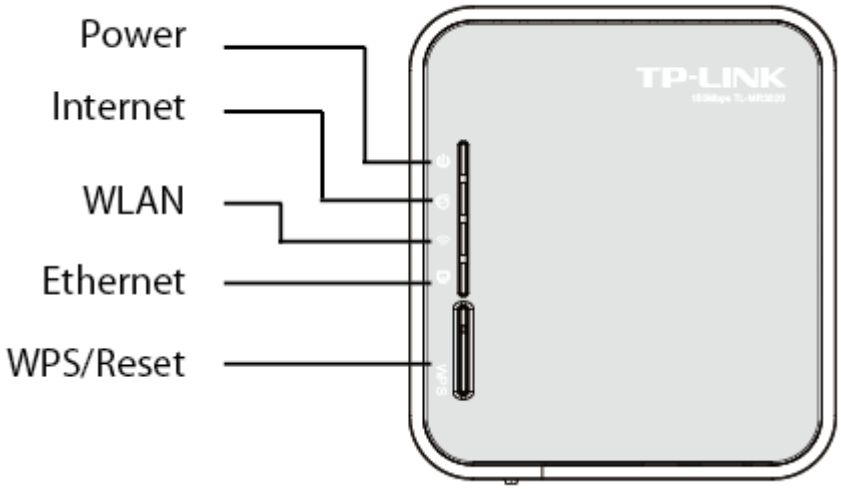


Bild 1-1 Gerätevorderseite

Die LEDs des Routers befinden sich auf der Vorderseite (von oben nach unten).

LED	Status	Bedeutung
Power	Ein	Der Router bekommt elektrische Spannung.
	Aus	Der Router ist ausgeschaltet.
Internet	Ein	Der Router ist mit dem Internet verbunden aber es werden keine Daten übertragen.
	Blinkt	Der Router ist mit dem Internet verbunden und Daten werden übertragen.
	Aus	Der Router ist nicht mit dem Internet verbunden.
WLAN	Ein	Die WLAN-Schnittstelle ist aktiviert.
	Blinkt	Die WLAN-Schnittstelle ist aktiviert und Daten werden übertragen.
	Aus	Die WLAN-Schnittstelle ist deaktiviert.
Ethernet	Ein	An dem Port besteht eine inaktive Verbindung.
	Blinkt	An dem Port werden Daten übertragen.
	Aus	Der Port ist nicht verbunden.

Tabelle 1-1 LEDs

- **WPS/Reset:** Haben Sie WLAN-Clients, die WPS (Wi-Fi Protected Setup) oder QSS (Quick Secure Setup) unterstützen, können Sie durch kurzes Drücken (kürzer als 5 Sekunden) dieser Taste schnell eine abgesicherte WLAN-Verbindung aufbauen. Wenn Sie die Taste länger als 10 Sekunden drücken, führt der Router einen Reset durch.

1.4.2 Seitenansicht

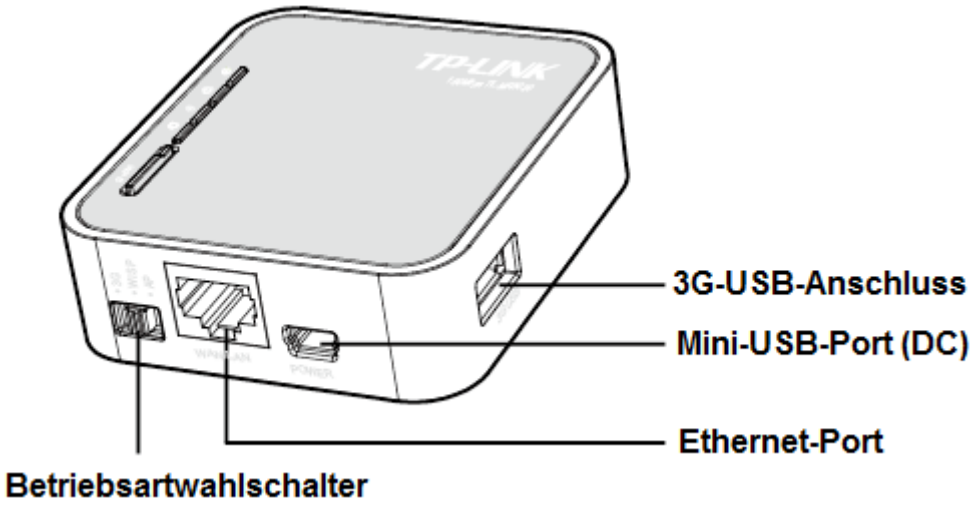


Bild 1-2 Geräteseitenansicht

Auf der Seite finden Sie folgende Teile (von links nach rechts).

- **3G-USB-Port:** Anschluss für das USB-Modem.
- **Mini-USB-Port:** Anschluss zur Stromversorgung.
- **Ethernet-Port:** Dieser Port kann als LAN- oder WAN-Verbindung genutzt werden.
- **Betriebsartwahlschalter:** Hiermit kann man zwischen den einzelnen Modi des Router wechseln.

Kapitel 2. Hardwareinstallation

2.1 Systemvoraussetzungen

- 3G/3,75G- oder Breitband-Internetzugang (DSL/Kabel/Ethernet)
- Jeder PC im LAN muss über einen funktionierenden Ethernet-Adapter und ein RJ45-Ethernetkabel verfügen
- TCP/IP muss auf jedem PC vorhanden sein
- Webbrowser, z.B. Microsoft Internet Explorer oder Mozilla Firefox

2.2 Anforderungen an die Installationsumgebung

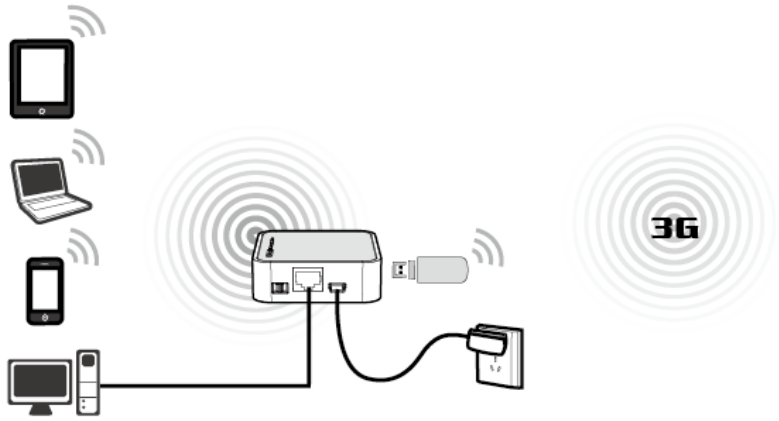
- Stellen Sie den Router an einer gut belüfteten Stelle auf, möglichst weit weg von Heizkörpern oder Radiatoren.
- Vermeiden Sie starken, direkten Lichteinfall (z.B. Sonnenlicht)
- Lassen Sie mindestens 5cm Platz auf allen Seiten des Routers.
- Betriebstemperatur: 0°C..40°C (32°F..104°F)
- Relative Luftfeuchtigkeit im Betrieb: 10%..90%, nicht kondensierend

2.3 Anschließen des Geräts

Dieser Router unterstützt drei Betriebsarten: 3G-Router, WISP-Cliebt und AP (Accesspoint). Somit können Sie das Gerät flexibel an Ihre Anforderungen anpassen. Bitte verfahren Sie bei der Installation nach den folgenden Schritten (abhängig vom gewünschten Modus):

a. 3G-Router-Modus

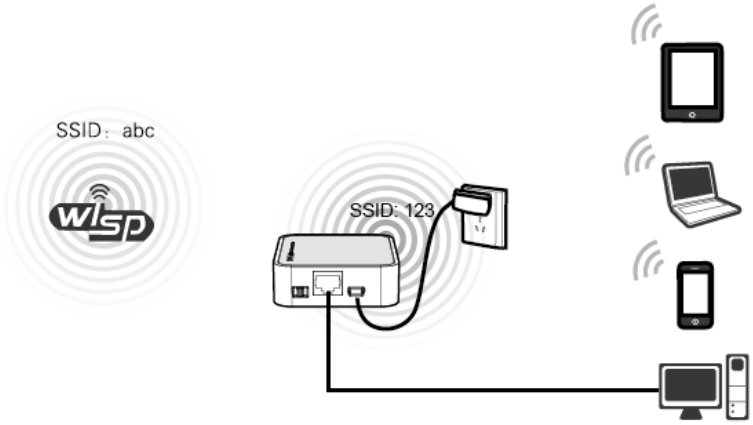
Als 3G-Router (mit 3G-Modem/-Karte) kann dieser Router sich mit einem 3G-Mobilfunknetz verbinden und dessen Internetkonnektivität unter einer eigenen WLAN-SSID bereitstellen.



1. Stellen Sie den Betriebsartwahlschalter des Routers auf „3G Router“.
2. Verbinden Sie Ihren Computer mit dem Ethernetport des TL-MR3020 mittels eines LAN-Kabels.
3. Verbinden Sie Ihr 3G-Modem mit dem 3G-USB-Port des Routers.
4. Schließen Sie das beiliegende USB-Kabel mit dem Mini-USB-Port des Routers und dem beiliegenden Spannungsadapter an und stecken Sie diesen dann in eine spannungsführende Steckdose.

b. WISP-Client-Modus

Als WISP-Client verbidnet der Router sich drahtlos mit einem „**W**ireless **ISP**” (Drahtloser Internetdiensteanbieter) und sendet lokal ein weiteres drahtloses Netz aus, mit dem Sie Ihre privaten Geräte ans Internet anbinden können.



1. Stellen Sie den Betriebsartwahlschalter des Routers auf „WISP“.
2. Verbinden Sie Ihren Computer mit dem Ethernetport des TL-MR3020 mittels eines LAN-Kabels.
3. Schließen Sie das beiliegende USB-Kabel mit dem Mini-USB-Port des Routers und dem beiliegenden Spannungsadapter an und stecken Sie diesen dann in eine

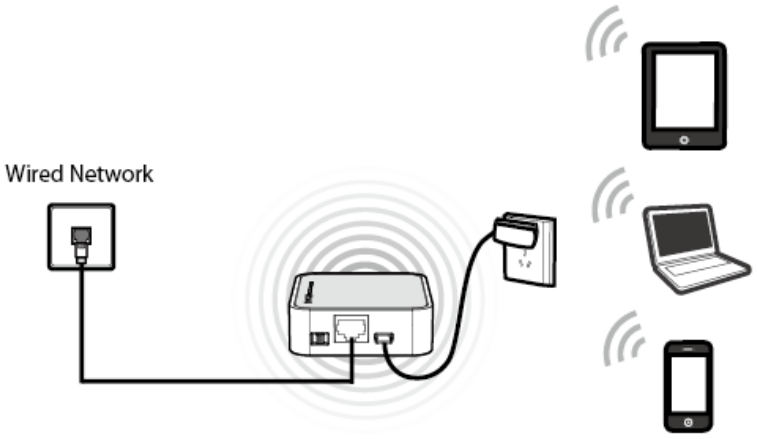
spannungsführende Steckdose.

c. AP-Modus

Im AP-Modus verhält der Router sich nicht als Router, sondern arbeitet an einem einzigen Netzsegment und erfüllt Aufgaben als WLAN-Accesspoint, Repeater, Bridge with AP und WLAN-Client. Bitte stellen Sie den Router in den gewünschten AP-Untermodus.

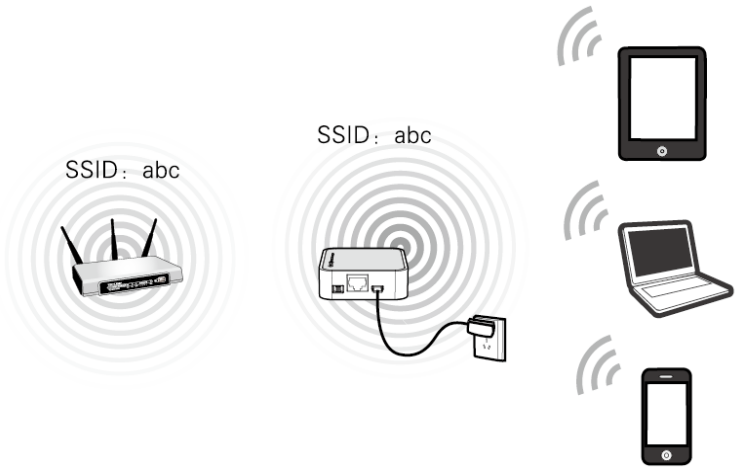
a) Accesspoint

Als Accesspoint stellt der TL-MR3020 drahtgebundene Konnektivität drahtlos bereit.



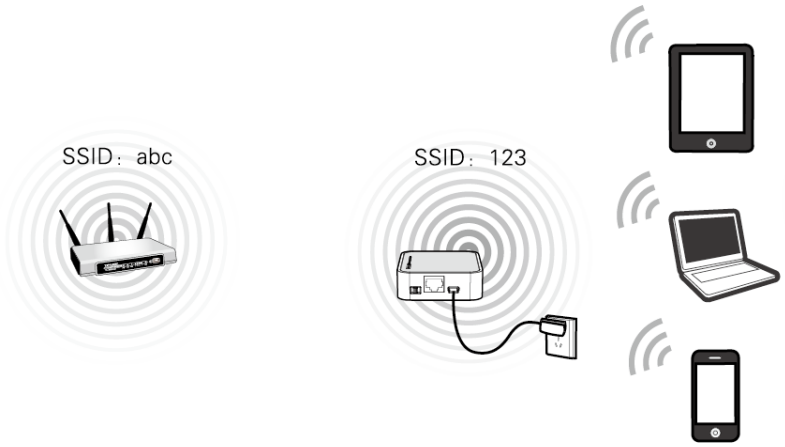
b) Repeater

Als Repeater kann der TL-MR3020 die Abdeckung eines weiteren WLANs erweitern.



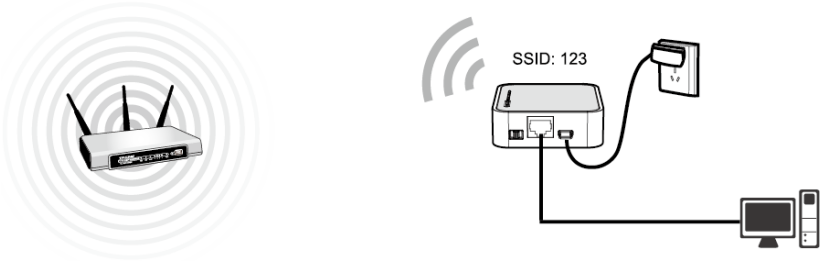
c) Bridge with AP

Als Bridge kann der TL-MR3020 zwei kabelbegundene Netze drahtlos miteinander verbinden (hierfür werden zwei TL-MR3020s benötigt).



d) Client

Als Client konfiguriert, verhält der Router sich wie eine WLAN-Karte und bringt somit nicht-WLAN-fähige Ethernetgeräte in ein drahtloses Netz.



Kapitel 3. Schnellinstallationsanleitung

Dieses Kapitel zeigt Ihnen, wie Sie die Basisfunktionalitäten Ihres tragbaren Wireless-N-3G/3,75G-Routers mit Hilfe der **Schnellinstallation** in wenigen Minuten konfigurieren.

3.1 3G-Router-Modus

Die Standard-IP-Adresse des tragbaren Wireless-N-3G/3,75G-Router lautet 192.168.0.254. Die Standard-Subnetzmaske ist 255.255.255.0. Diese Werte können nach Ihren Vorstellungen geändert werden. In diesem Dokument werden jedoch die Standardwerte als Beispiele benutzt.

Verbinden Sie den PC mit einem LAN-Port am Router. Dann können Sie die IP-Adresse Ihres PCs folgendermaßen konfigurieren.

3.1.1 TCP/IP-Konfiguration

Als Beispiel wird eine WLAN-Verbindung verwendet, um den Router zu konfigurieren. (Sie können ebenso eine LAN-Verbindung nutzen um die Konfiguration vorzunehmen. Wenn Sie dabei Hilfe benötigen schauen Sie bitte im Anhang B: PCs konfigurieren.)

1. Unter Windows XP (klassische Ansicht) gehen Sie bitte wie folgt vor: **Start** → **Einstellungen** → **Systemsteuerung** → **Netzwerk- und Internetverbindungen** → **Netzwerkverbindungen**; unter Windows 7 gehen Sie bitte wie folgt vor: **Start** → **Systemsteuerung** → **Netzwerk und Internet** → **Netzwerk- und Freigabecenter** → **Adaptereinstellungen ändern**

   Tätigen Sie einen Rechtsklick auf **Drahtlosnetzwerkverbindung** und wählen Sie **Eigenschaften**.

2. Bei Windows XP machen Sie in dem unterem Fenster einen Doppelklick auf **Internetprotokoll (TCP/IP)**; bei Windows 7 machen Sie in dem unterem Fenster einen Doppelklick auf **Internetprotokoll Version 4 (TCP/IPv4)**.

3. Wählen Sie **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen**.

3.1.2 Verbinden mit dem Router

1. Klicken Sie in der Taskleiste auf das Symbol  .

2. Klicken Sie auf **Liste aktualisieren** und wählen Sie das WLAN-Netz des Routers aus und klicken Sie auf **Verbinden**.

Bemerkung:

Die Standard SSID des Routers lautet TP-LINK_POCKET_3020_xxxxxx. (Die Werte xxxxxx sind die letzten 6 Stellen der MAC-Adresse des Routers.)

3. Wenn bei dem WLAN-Netz des Router **Verbunden** steht, sind Sie erfolgreich mit dem Router verbunden.

3.1.3 Routerkonfiguration

1. Um auf die webbasierte Konfiguration zuzugreifen, öffnen Sie einen Webbrowser und geben Sie die Adresse http://192.168.0.254 in die Adresszeile ein.

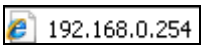


Bild 3-1 Einloggen in den Router

2. Das in Bild 3-2 gezeigte Login-Fenster erscheint. Geben Sie **admin** als Benutzernamen und als Passwort ein. Klicken Sie **OK** oder drücken Sie **Enter**.

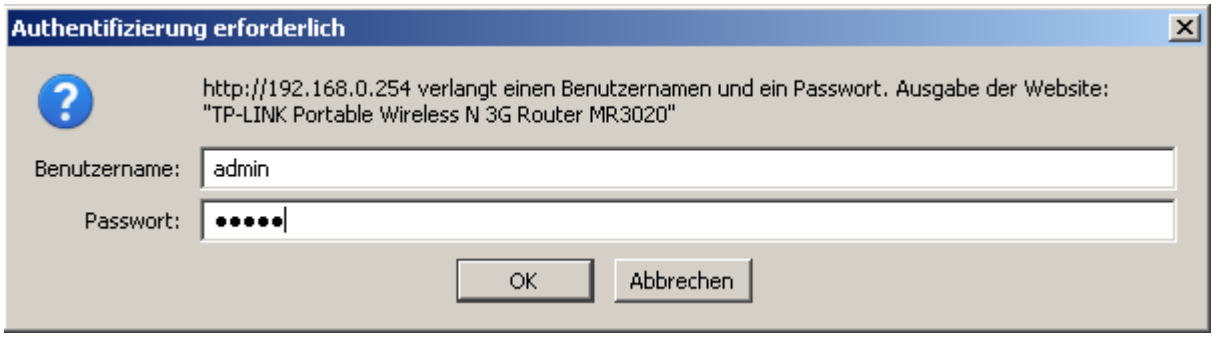


Bild 3-2 Login-Fenster

Bemerkung:

Erscheint dieses Fenster nicht, könnte Ihr Webbrowser für die Benutzung eines Proxys konfiguriert sein. Im Falle des Internet Explorers gehen Sie auf **Extras** > **Internetoptionen** > **Verbindungen** > **LAN-Einstellungen** und entfernen dort den Haken bei **Proxy-Server für LAN-Verbindungen benutzen**. Klicken Sie **OK**.

3. Bevor Sie die Konfiguration fortsetzen, kontrollieren Sie bitte unter **Status** den Status von 3G, um zu sehen ob Ihr 3G-Modem-Stick erkannt wird (Bild 3-3).

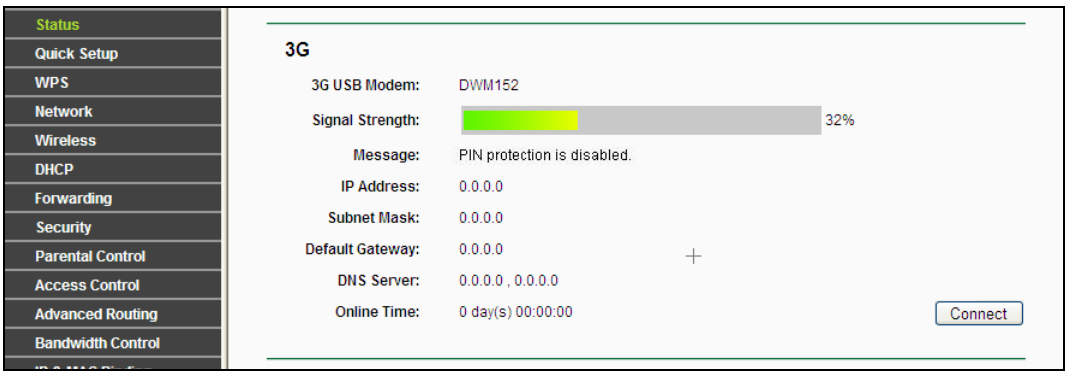


Bild 3-3 3G-Status

4. Gehen Sie im Menü auf **Quick Setup** klicken Sie auf **Next**.

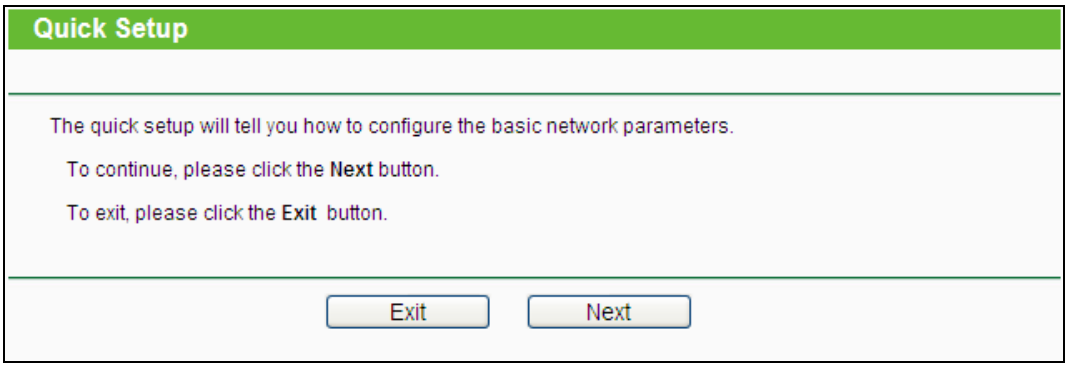


Bild 3-4 Quick Setup

5. Klicken Sie **Next**. Die Seite **Internet Access** erscheint (Bild 3-5). Wählen Sie den gewünschten Internetzugriff und klicken Sie **Next**. Die Konfigurationsvorgänge unterscheiden sich kaum für die verschiedenen Modi. Hier wird als Beispiel **3G Only (As Lan)** genommen.

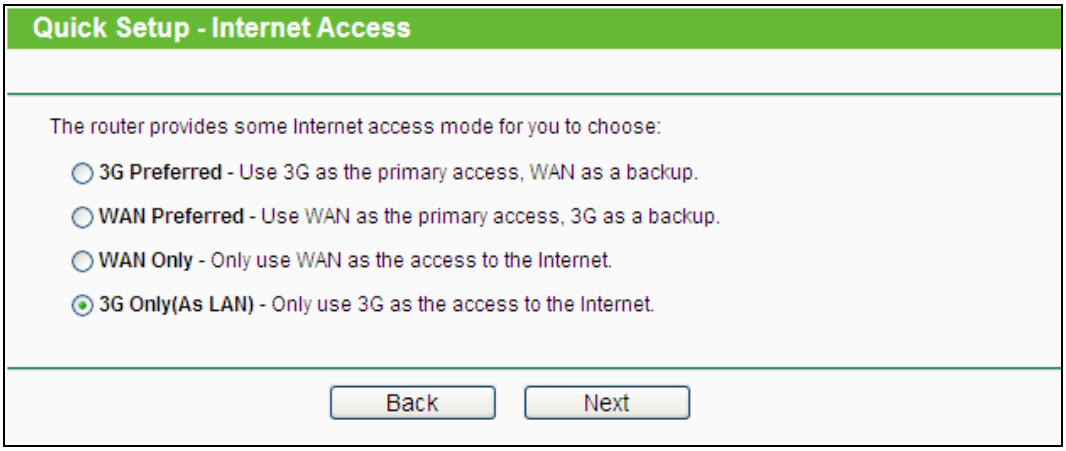


Bild 3-5 Internetzugriffsmodusauswahl

- **3G Preferred -** In diesem Modus versucht der Router zunächst, eine 3G-Verbindung aufzubauen. Schlägt dies fehl und am WAN-Port ist etwas angeschlossen oder wenn gar kein 3G-Modem angeschlossen ist, wird der WAN-Zugang benutzt. Kann irgendwann wieder eine 3G-Verbindung hergestellt werden, schaltet der Router auf diese zurück.
- **WAN Preferred -** In diesem Modus versucht der Router zunächst, eine WAN-Verbindung aufzubauen. Schlägt dies fehl und über den USB-Port kann eine Verbindung hergestellt werden, schaltet der Router auf 3G-Internetzugriff um. Kann irgendwann wieder eine WAN-Verbindung hergestellt werden, schaltet der Router auf diese zurück.
- **WAN Only -** Dieser Modus verwendet ausschließlich den WAN-Port. Der 3G-Zugang wird nicht verwendet.
- **3G Only (As LAN) -** Diese Betriebsart bedeutet, dass der Internetzugriff über WAN deaktiviert ist.

6. Es erscheint nun Bild 3-6. Tragen Sie auf dieser Seite Ihre Zugangsdaten ein und klicken Sie anschließend **Next**.

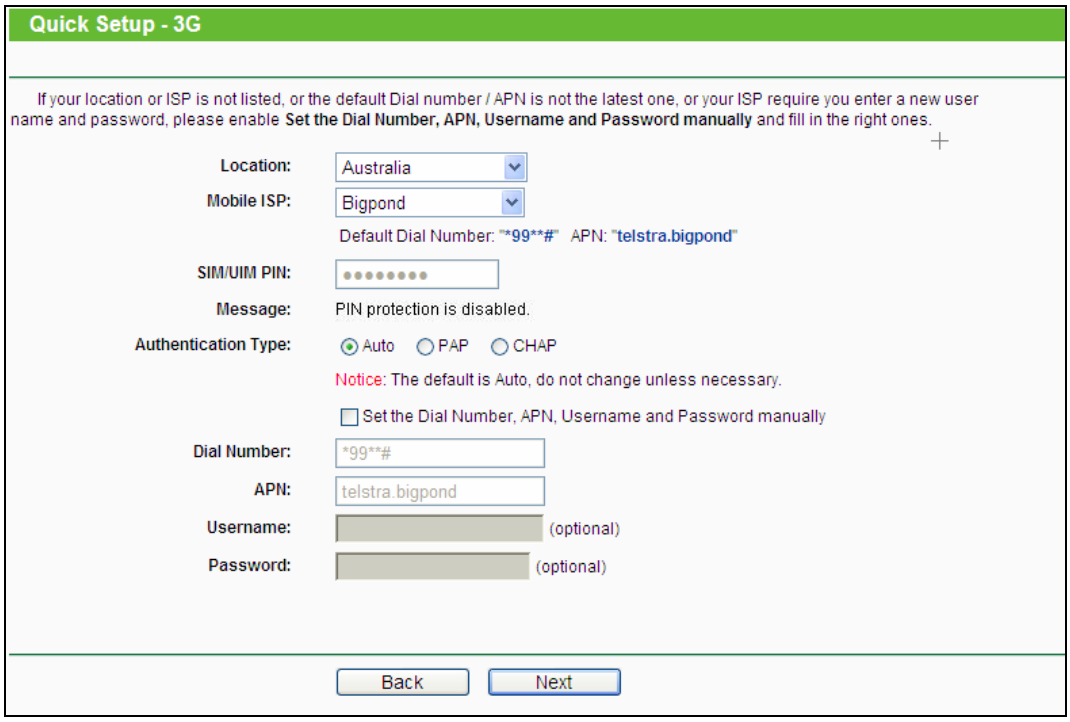


Bild 3-6 Verbindungsparameter

7. Klicken Sie **Next**. Die WLAN-Einstellungen erscheinen (Bild 3-7).

- **Wireless Radio -** Aktivieren (**Enable**) oder Deaktivieren (**Disable**) der WLAN-Einheit.
- **Wireless Network Name -** Geben Sie hier einen Namen aus bis zu 32 Zeichen ein. Mit diesem WLAN-Namen (SSID) arbeiten dann alle mit diesem WLAN verbundenen Drahtlosgeräte. Der Name lautet standardmäßig „TP-LINK_Pocket_XXXXXX“, wobei „XXXXXX“ die letzten 6 Ziffern der MAC-Adresse des Routers darstellen. Bei der SSID wird zwischen Groß- und Kleinschreibung unterschieden.
- **Region -** Der Standort des Routers. Diese Angabe ist wichtig bei Verwendung des WLANs. Machen Sie hier falsche Angaben, könnte der Routerbetrieb gültige Grenzwerte verletzen. Ist Ihre Region hier nicht aufgelistet, wenden Sie sich bitte an die lokalen Behörden. In Deutschland setzen Sie bitte **Germany**, in der Schweiz **Switzerland** und in Österreich **Austria** ein.
- **Channel -** Die Nummer des Kanals, den die WLAN-Einheit des Routers benutzt. Die Standardeinstellung ist **Auto**, so dass der Router automatisch den am wenigsten belegten Kanal benutzt. Es ist nicht erforderlich, dies zu ändern, es sei denn, Sie stellen Interferenzen von einem nahen Accesspoint fest.
- **Mode -** Legt fest, in welchem Drahtlos-Modus der Router arbeitet.
- **Channel Width -** Wählen Sie eine Kanalbreite aus. In der Standardeinstellung **Auto** wird diese automatisch eingestellt.

- **Max Tx Rate -** Hiermit können Sie die WLAN-Geschwindigkeit beschränken

- **Wireless Security -** Einstellen der WLAN-Sicherheitsoptionen.
  - **Disable Security -** Keine Sicherheit. So können alle WLAN-Geräte (auch fremde) sich ohne Weiteres mit Ihrem Netz verbinden. Aufgrund gesetzlicher Vorgaben wird Ihnen empfohlen, die stärkste verfügbare Verschlüsselung einzustellen.
  - **WPA-PSK/WPA2-PSK -** WPA basierend auf einem Passwort.
    - **PSK Password** - Hier können Sie **ASCII**- oder **Hexadezimal**-Zeichen eingeben.

      Im Fall von **ASCII** können Sie arabische Ziffern sowie lateinische Groß- und Kleinbuchstaben verwenden. Es werden 8 bis 63 Zeichen verlangt.

      Benutzen Sie ein **Hexadezimal**-Passwort, können Sie in Ihrem Passwort arabische Ziffern von 0 bis 9 und Buchstaben von A bis F benutzen. Als Länge sind 8 bis 64 Zeichen zugelassen.

    Bitte seien Sie sich im Klaren darüber, dass beim Passwort Groß- und Kleinschreibung entscheidend sind. Es wird empfohlen, das Passwort und die anderen WLAN-Einstellungen an sicherer Stelle aufzubewahren.

- **No Change -** Mit dieser Option übernehmen Sie die bisherigen WLAN-Einstellungen.

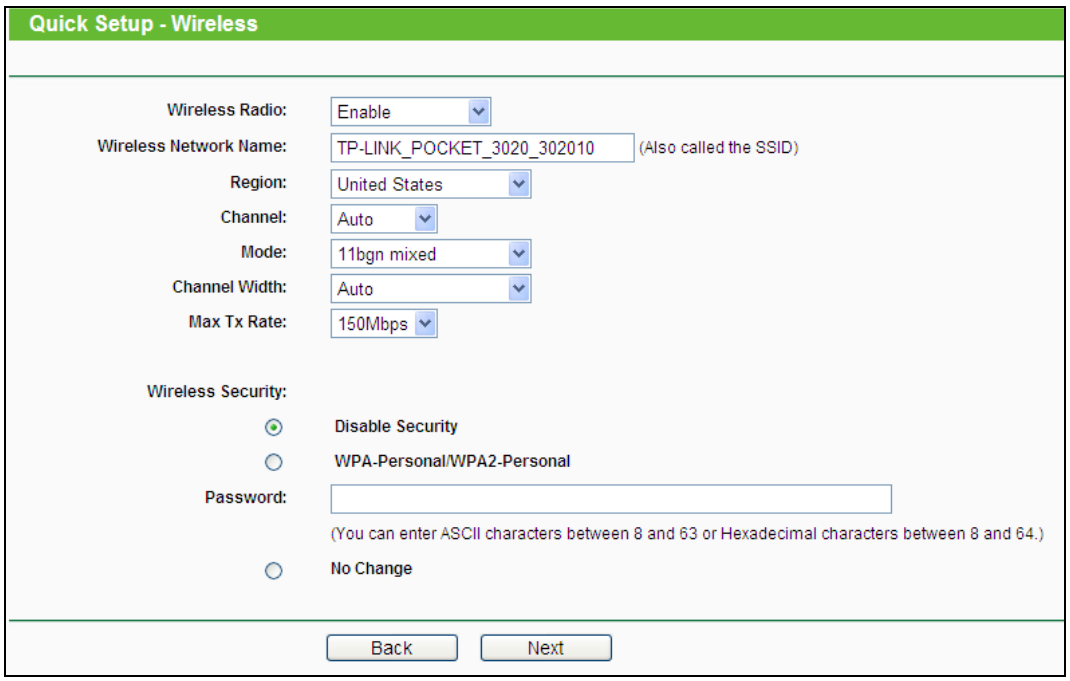


Bild 3-7 Quick Setup – WLAN-Einstellungen

8. Klicken Sie **Next** und auf **Reboot**, um die neue WLAN-Konfiguration zu übernehmen und **Quick Setup** abzuschließen. (Falls in den WLAN-Einstellungen nichts geändert wurde, klicken Sie **Finish**, um die **Schnellinstallation** abzuschließen.)

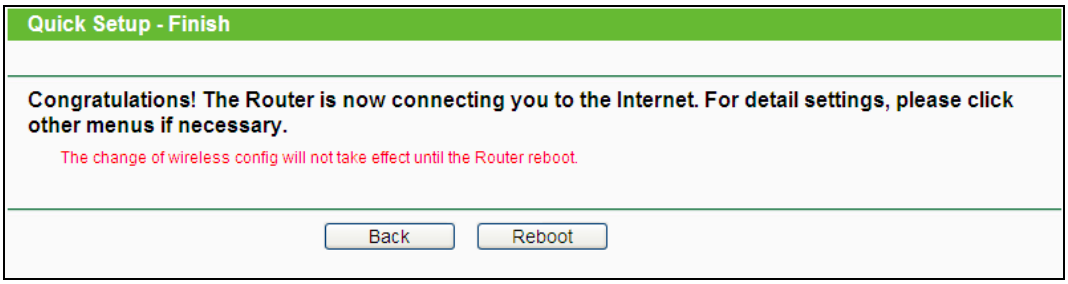


Bild 3-8 Quick Setup abgeschlossen

☞ **Bemerkung:**

Nach dem Neustart verbinden Sie sich erneut mit dem Netywerk (siehe Kapitel 3.1.2).

3.2 WISP-Modus

Die Standard-IP-Adresse des tragbaren Wireless-N-3G/3,75G-Routers lautet 192.168.0.254. Die Standard-Subnetzmaske ist 255.255.255.0. Diese Werte können nach Ihren Vorstellungen geändert werden. In diesem Dokument werden jedoch die Standardwerte als Beispiele benutzt.

3.2.1 TCP/IP-Konfiguration

Als Beispiel wird eine WLAN-Verbindung verwendet, um den Router zu konfigurieren. (Sie können ebenso eine LAN-Verbindung nutzen um die Konfiguration vorzunehmen. Wenn Sie dabei Hilfe benötigen schauen Sie bitte im Anhang B: PCs konfigurieren.)

1. Für Windows XP (klassische Ansicht) gehen Sie bitte wie folgt vor: **Start** → **Einstellungen** → **Systemsteuerung** → **Netzwerk- und Internetverbindungen** → **Netzwerkverbindungen**; für Windows 7 gehen Sie bitte wie folgt vor: **Start** → **Systemsteuerung** → **Netzwerk und Internet** → **Netzwerk- und Freigabecenter** → **Adaptereinstellungen ändern**

   Tätigen Sie einen Rechtsklick auf **Drahtlosnetzwerkverbindung** und wählen Sie **Eigenschaften**.

2. Bei Windows XP machen Sie in dem unterem Fenster einen Doppelklick auf **Internetprotokoll (TCP/IP)**; bei Windows 7 machen Sie in dem unterem Fenster einen Doppelklick auf **Internetprotokoll Version 4 (TCP/IPv4)**.

3. Wählen Sie **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen**.

3.2.2 Verbinden mit dem Router

1. Klicken Sie in der Taskleiste auf das Symbol .

2. Klicken Sie auf **Liste aktualisieren** und wählen das WLAN-Netz des Routers aus und klicken Sie auf **Verbinden**.

Bemerkung:

Die Standard SSID des Routers lautet TP-LINK_POCKET_3020_xxxxxx. (Die Werte xxxxxx sind die letzten 6 Stellen der MAC-Adresse des Routers.)

Wenn bei dem WLAN-Netz des Router **Verbunden** steht, sind Sie erfolgreich mit dem Router verbunden.

3.2.3 Routerkonfiguration

1. Um auf die webbasierte Konfiguration zuzugreifen, öffnen Sie einen Webbrowser und geben Sie die Adresse http://192.168.0.254 in die Adresszeile ein.

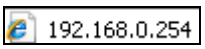


Bild 3-9 Einloggen in den Router

2. Das in Bild 3-10 gezeigte Login-Fenster erscheint. Geben Sie **admin** als Benutzernamen und als Passwort ein. Klicken Sie **OK** oder drücken Sie **Enter**.

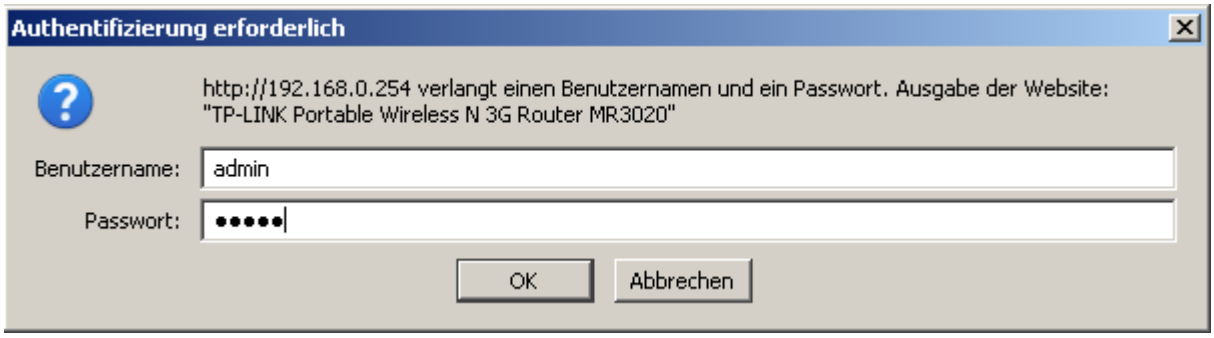


Bild 3-10 Login-Fenster

Bemerkung:

Erscheint dieses Fenster nicht, könnte Ihr Webbrowser für die Benutzung eines Proxys konfiguriert sein. Im Falle des Internet Explorers gehen Sie auf **Extras** > **Internetoptionen** > **Verbindungen** > **LAN-Einstellungen** und entfernen dort den Haken bei **Proxy-Server für LAN-Verbindungen benutzen**. Klicken Sie **OK**.

3. Gehen Sie im Menü auf **Quick Setup** klicken Sie auf **Next**.

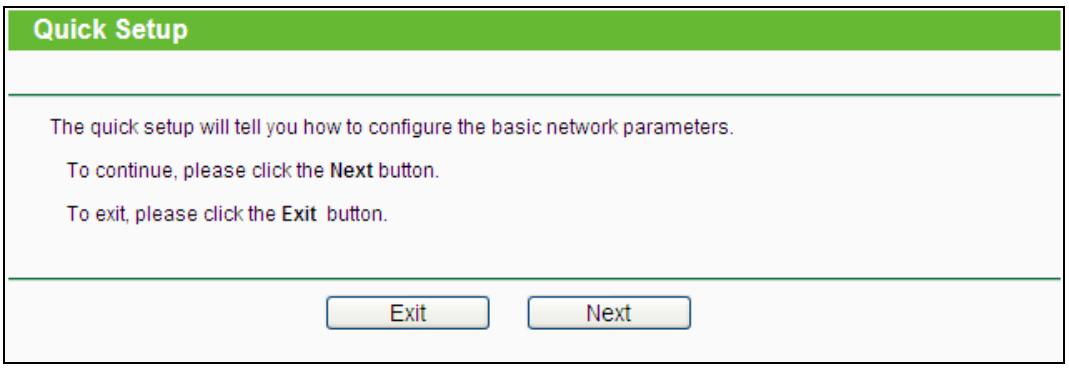


Bild 3-11 Quick Setup

4. Wählen Sie **WAN Connection Type** aus und klicken Sie auf **Next**.

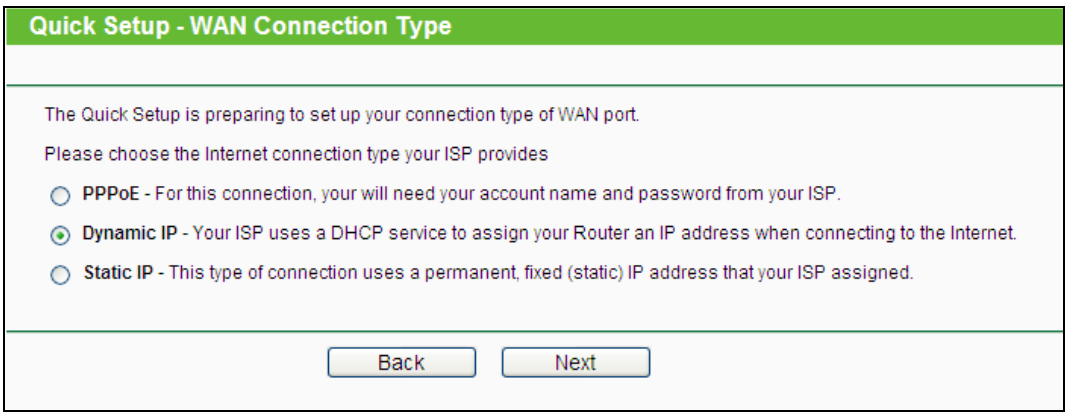


Bild 3-12 Quick Setup – WAN Connection Type

➢ Wenn Sie **PPPoE** wählen erhalten Sie das Bild 3-13.

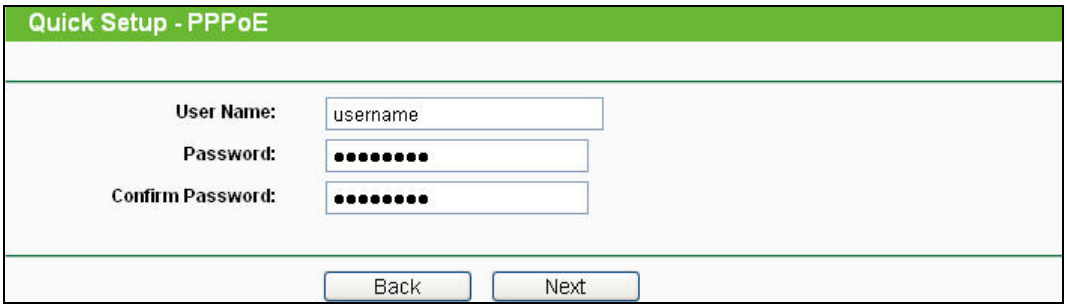


Bild 3-13 Quick Setup – PPPoE

- **User Name and Password -** Geben Sie Benutzernamen und Passwort ein, so wie Sie sie von Ihrem ISP erhalten haben. Hier wird zwischen Groß- und Kleinschreibung unterschieden.

➢ Wenn Sie **Dynamic IP** wählen erhalten Sie das Bild 3-14.

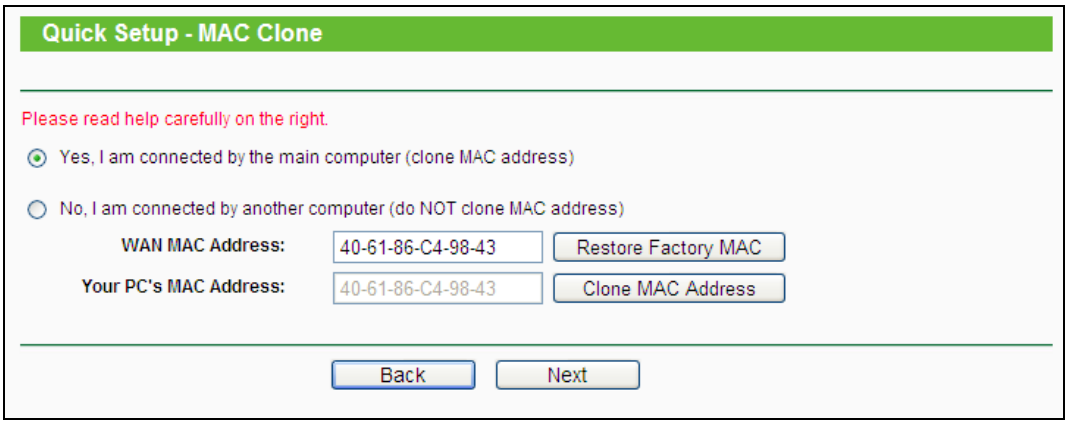


Bild 3-14 Quick Setup – MAC Clone

- Wenn Sie von Ihrem Hauptcomputer auf den Router zugreifen, klicken Sie bitte **Yes** und anschließend auf **Clone MAC Address**.
- Wenn Sie nicht von Ihrem Hauptcomputer auf den Router zugreifen, klicken Sie bitte **No** und tragen manuell die MAC-Adresse Ihres Hauptcomputers im Feld **WAN MAC Address ein**.

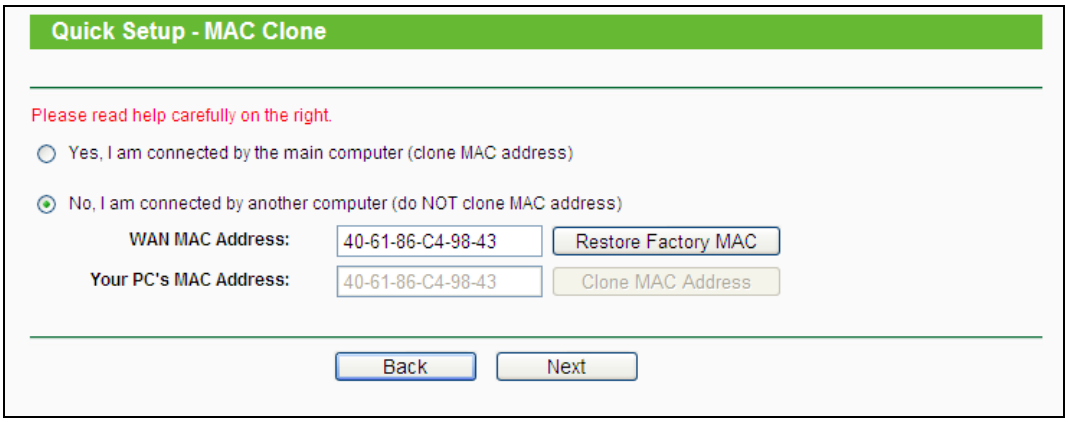


Bild 3-15 Quick Setup – MAC Clone

➢ Wenn Sie **Static IP**, wählen erhalten Sie das Bild 3-16.

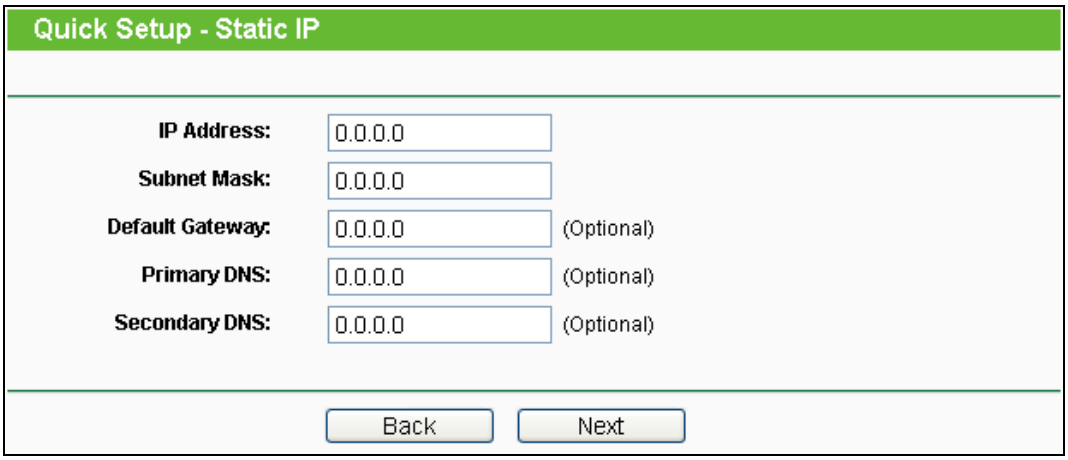


Bild 3-16 Quick Setup - Static IP

- **IP Address -** Die IP-Adresse, die Sie von Ihrem ISP erhalten haben.
- **Subnet Mask -** Die Subnetzmaske, gewöhnlich 255.255.255.0.
- **Default Gateway -** Die IP-Adresse des Gateways Ihres ISPs (optional).
- **Primary/Secondary DNS -** Geben Sie eine oder zwei DNS-Serveradressen ein (optional).

5. Klicken Sie auf **Next** und Sie erhalten das Bild 3-17. Klicken Sie auf **Survey** um vorhandene WLAN-Netze anzeigen zu lassen. Wählen Sie die SSID von Ihrem WLAN-Netz und klicken auf **Connect** und die SSID und BSSID wird automatisch ausgefällt. Wenn das WLAN-Netz verschlüsselt ist, stellen Sie die richtige Verschlüsselung mit Passwort ein.

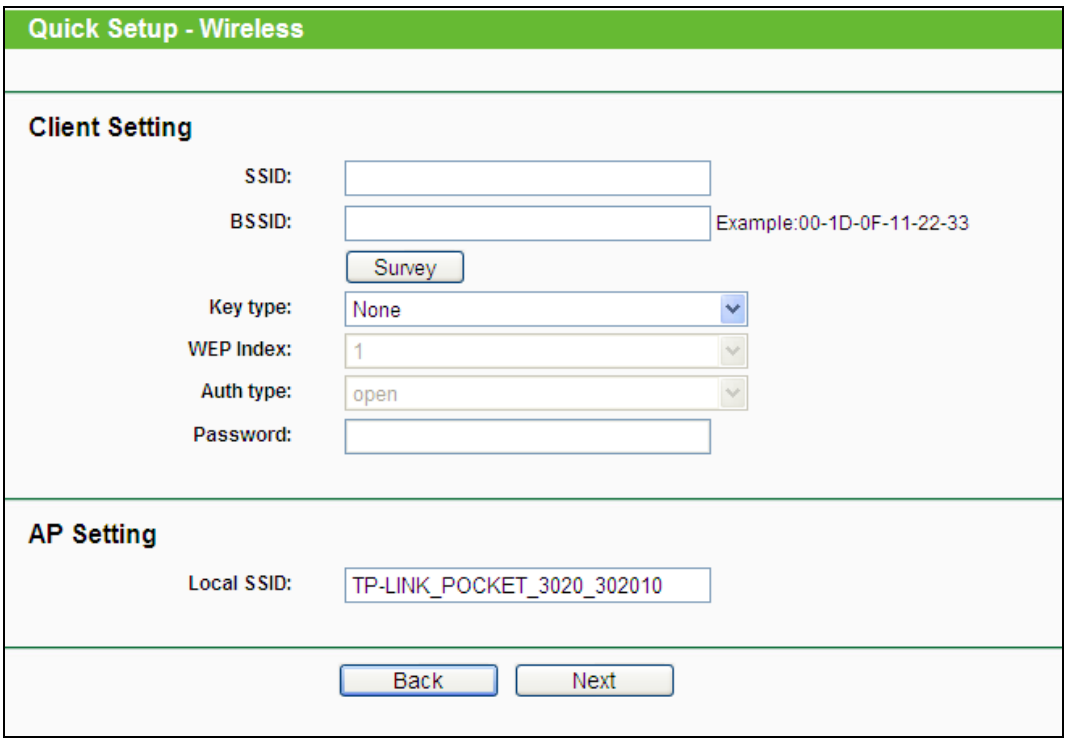


Bild 3-17 Quick Setup – Wireless

6. Klicken Sie auf **Next** und Sie erhalten das Bild 3-18. Klicken Sie auf **Reboot**, um die WLAN-Einstellungen zu übernehmen und die Schnellinstallation abzuschließen.

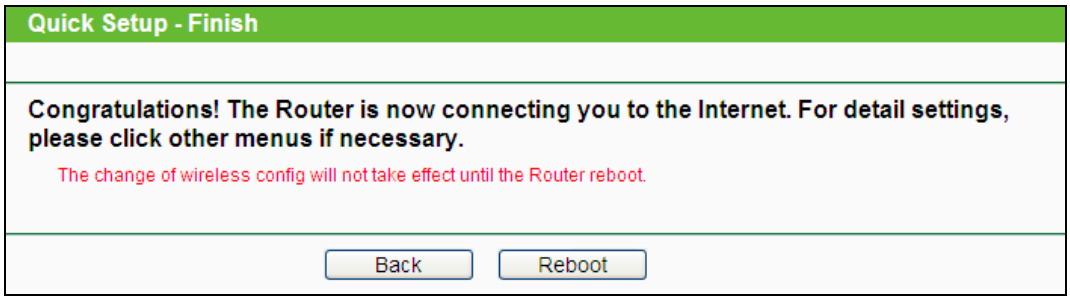


Bild 3-18 Quick Setup – Finish

Bemerkung:

Nach dem Neustart verbinden Sie sich erneut mit dem WLAN (siehe Kapitel 3.2.2).

3.3 AP-Modus

3.3.1 TCP/IP-Konfiguration

Als Beispiel wird eine WLAN-Verbindung verwendet, um den Router zu konfigurieren. (Sie können ebenso eine LAN-Verbindung nutzen um die Konfiguration vorzunehmen. Wenn Sie dabei Hilfe benötigen schauen Sie bitte im Anhang B: PCs konfigurieren.)

1. Für Windows XP (klassische Ansicht) gehen Sie bitte wie folgt vor: **Start** → **Einstellungen** → **Systemsteuerung** → **Netzwerk- und Internetverbindungen** → **Netzwerkverbindungen**; für Windows 7 gehen Sie bitte wie folgt vor: **Start** →

Systemsteuerung → Netzwerk und Internet → Netzwerk- und Freigabecenter → Adaptereinstellungen ändern

Tätigen Sie einen Rechtsklick auf **Drahtlosnetzwerkverbindung** und wählen Sie **Eigenschaften**.

2. Bei Windows XP machen Sie in dem unterem Fenster einen Doppelklick auf **Internetprotokoll (TCP/IP)**; bei Windows 7 machen Sie in dem unterem Fenster einen Doppelklick auf **Internetprotokoll Version 4 (TCP/IPv4)**.

3. Wählen Sie **Folgende IP-Adresse verwenden**, geben Sie eine IP-Adresse der Form 192.168.1.x ein. x bezeichnet eine Zahl von 2 bis 254 und **Subnetzmaske** ist 255.255.255.0. Wählen Sie **Folgende DNS-Server verwenden**. Als **Bevorzugten DNS-Server** geben Sie die DNS-Server-Adresse, die Sie von Ihrem ISP erhalten haben, ein.

4. Klicken Sie **OK**.

3.3.2 Mit dem AP verbinden

1. Klicken Sie in der Taskleiste auf das Symbol  .

2. Klicken Sie auf **Liste aktualisieren** und wählen das WLAN-Netz des Routers aus und klicken Sie auf **Verbinden**.

☞ **Bemerkung:**

Die Standard SSID des Routers lautet TP-LINK_POCKET_3020_xxxxxx. (Die Werte xxxxxx sind die letzten 6 Stellen der MAC-Adresse des Routers.)

Wenn bei dem WLAN-Netz des Router **Verbunden** steht, sind Sie erfolgreich mit dem Router verbunden.

3.3.3 Routerkonfiguration

1. Um auf die webbasierte Konfiguration zuzugreifen, öffnen Sie einen Webbrowser und geben Sie die Adresse http://192.168.0.254 in die Adresszeile ein.

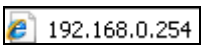


Bild 3-19 Einloggen in den Router

2. Das in Bild 3-20 gezeigte Login-Fenster erscheint. Geben Sie **admin** als Benutzernamen und als Passwort ein. Klicken Sie **OK** oder drücken Sie **Enter**.

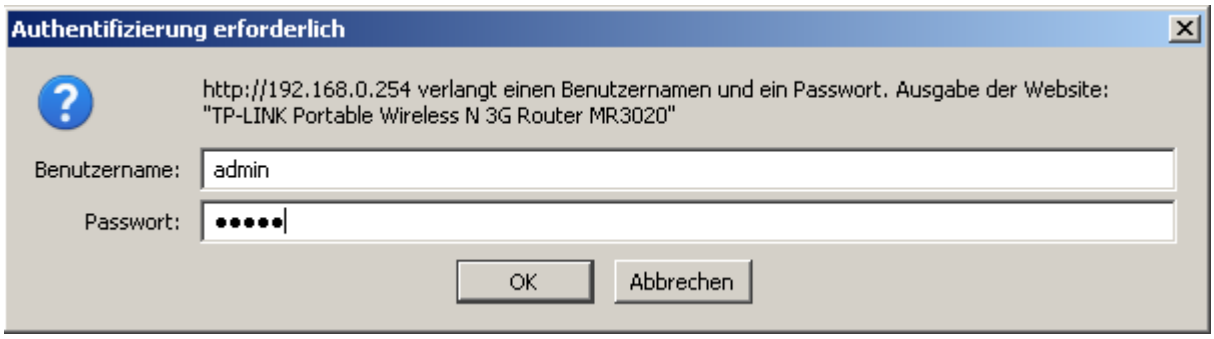


Bild 3-20 Login-Fenster

Bemerkung:

Erscheint dieses Fenster nicht, könnte Ihr Webbrowser für die Benutzung eines Proxys konfiguriert sein. Im Falle des Internet Explorers gehen Sie auf **Extras** > **Internetoptionen** > **Verbindungen** > **LAN-Einstellungen** und entfernen dort den Haken bei **Proxy-Server für LAN-Verbindungen benutzen**. Klicken Sie **OK**.

3. Gehen Sie im Menü auf **Quick Setup** klicken Sie auf **Next**.

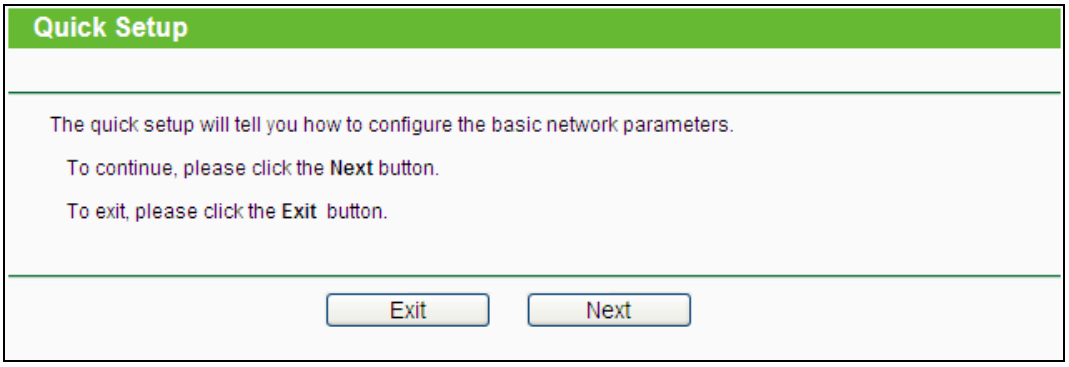


Bild 3-21 Quick Setup

4. Wählen Sie den **Wireless Operation Mode Type** und klicken Sie auf **Next**.

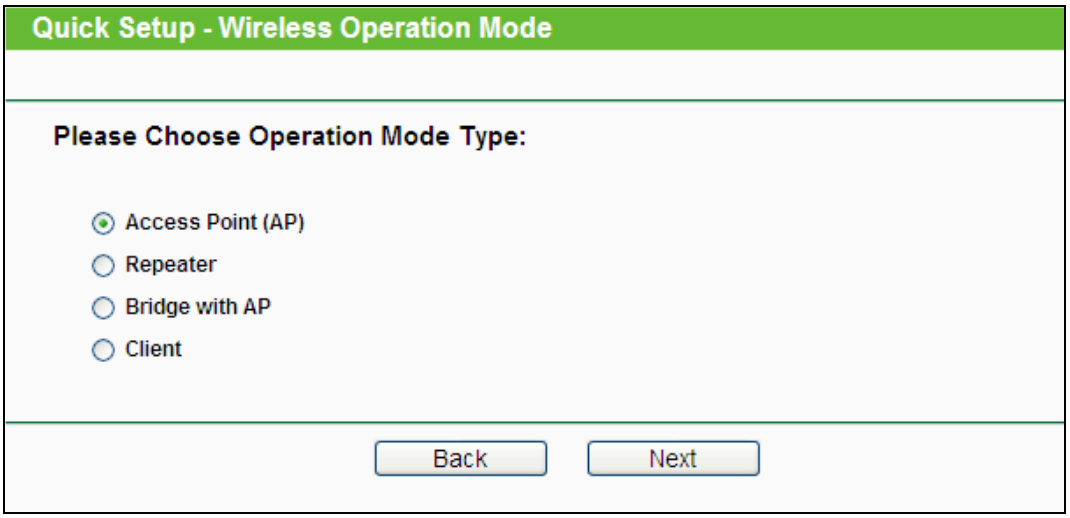


Bild 3-22 Quick Setup – Wireless Operation Mode

➢ Wenn Sie **Access Point (AP)** wählen erhalten Sie das Bild 3-23.

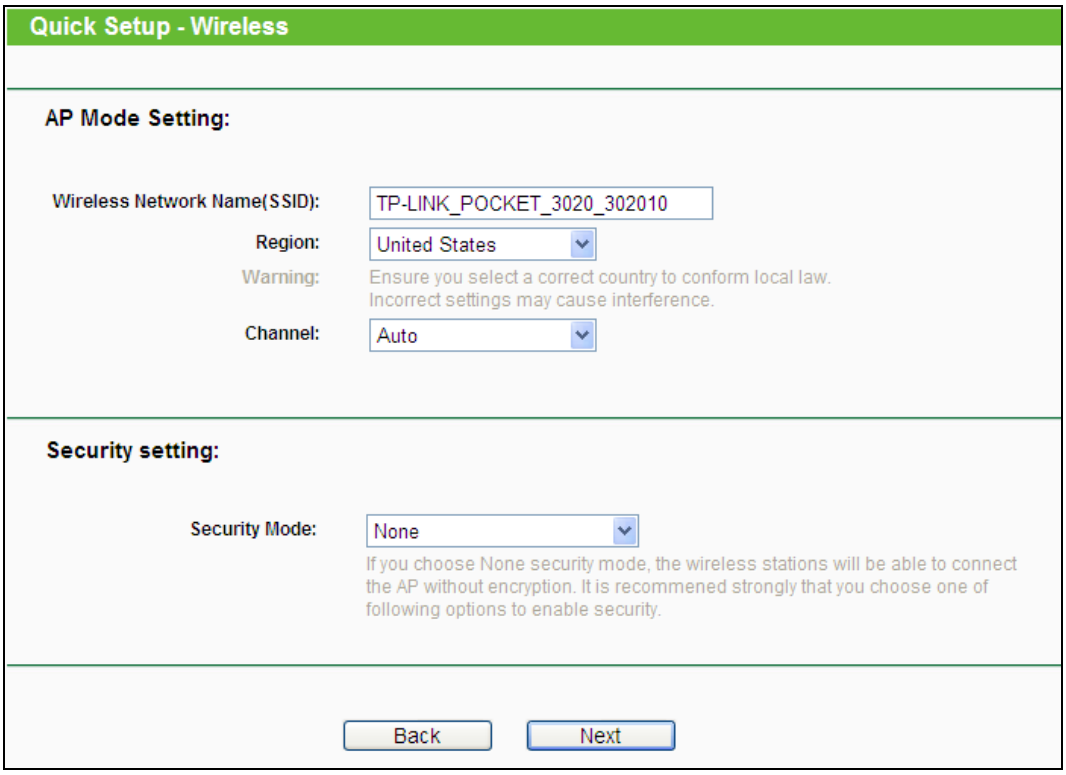


Bild 3-23 Quick Setup – AP

- **Wireless Network Name (SSID)** - Geben Sie einen Namen von bis zu 32 Zeichen an (SSID). Dieser muss von allen anderen Geräten in Ihrem WLAN verwendet werden. Standardwert ist TP-LINK, doch sollte dieser geändert werden. Hier wird zwischen Groß- und Kleinschreibung unterschieden, z.B. bezeichnen *TP-LINK* und *tp-link* unterschiedliche Netze.
- **Region** - Wählen Sie hier den Standort des Routers aus. Eine falsche Auswahl könnte gegen geltende Gesetze verstoßen. Ist Ihre Region nicht aufgeführt, wenden Sie sich bitte an die zuständigen Behörden. Standardeinstellung ist **United States**, so dass hier in der Regel eine Anpassung vorgenommen werden muss. In Deutschland setzen Sie bitte **Germany**, in der Schweiz **Switzerland** und in Österreich **Austria** ein
- **Channel** - Dieses Feld legt die Betriebsfrequenz des Routers fest. In der Standardeinstellung **Auto** wählt der Router automatisch einen Kanal aus. Es ist nicht erforderlich, diese zu ändern, es sei denn, Sie stellen Interferenzen von einem nahen Accesspoint fest.

➢ Wenn Sie **Repeater** wählen erhalten Sie das Bild 3-24. In diesem Modus gibt der AP Daten an einen verbundenen, WDS-fähigen Root-AP weiter. Der Repeater erweitert also die Reichweite des Root-APs.

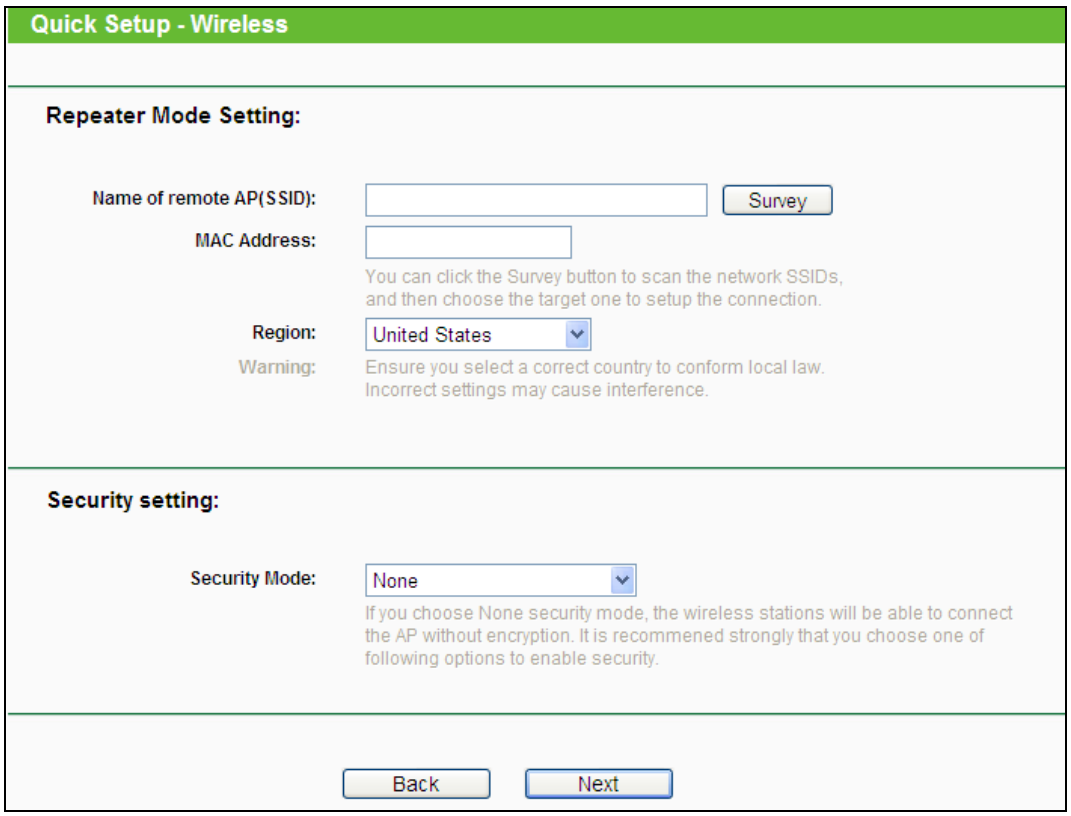


Bild 3-24 Quick Setup – Repeater

- **Name of remote AP (SSID)** - Geben Sie den Netzwerknamen (SSID) des AP ein mit dem Sie sich verbinden wollen oder klicken Sie auf **Survey**, um das WLAN-Netzwerk zu suchen und über **Connect** zu verbinden.
- **MAC Address** - Geben Sie die MAC-Adresse des Root-APs, dessen Reichweite Sie vergrößern möchten, in dieses Feld ein.
- **Region** - Wählen Sie aus der Drop-Down-Liste die Region aus, in der der AP sich befindet. Damit verbunden sind Spezifikationen für die vom AP verwendeten Kanäle und Weiteres. Daher kann hier eine falsche Einstellung einen nicht gesetzeskonformen Betrieb verursachen. Ist die Region, in der der Router steht, nicht in dieser Liste aufgeführt, wenden Sie sich bitte an die zuständigen Behörden.

➢ Wenn Sie **Bridge with AP** wählen, erhalten Sie das Bild 3-25. In diesem Modus können dieser AP und bis zu 4 weitere 4 APs, die sich ihrerseits im Bridgemodus befinden, benutzt werden, um mehrere kabelgebundene Netze miteinander zu verbinden.

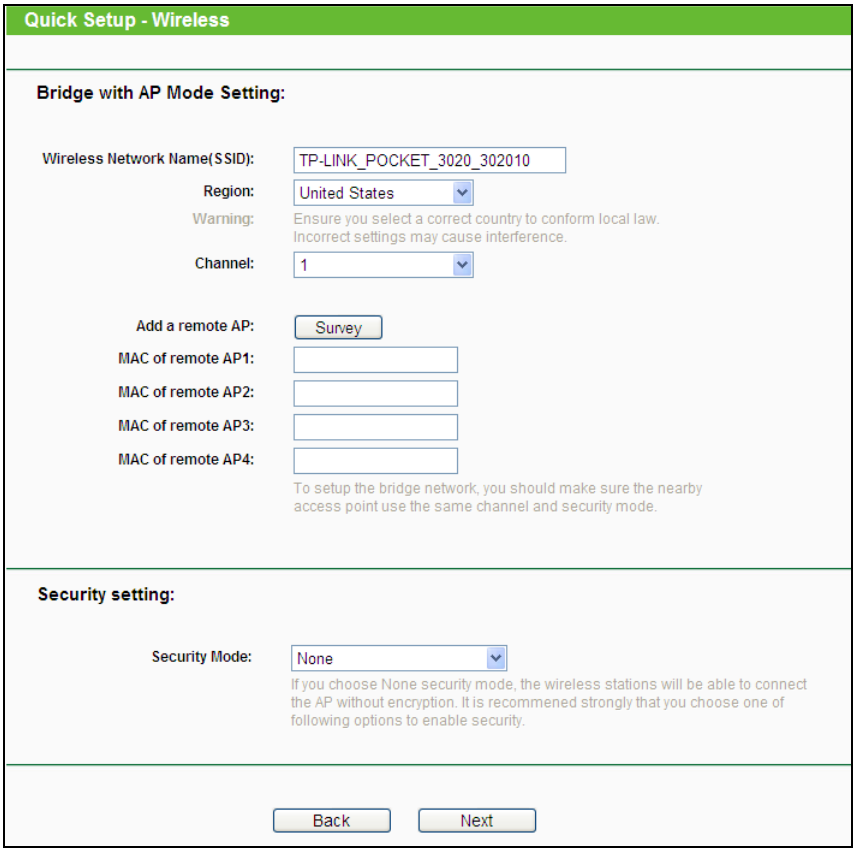


Bild 3-25 Quick Setup – Bridge with AP

- **Wireless Network Name (SSID)** - Dies ist der Name Ihres drahtlosen Netzes. Er darf bis zu 32 Zeichen lang sein. Alle Geräte, die zu Ihrem Netz gehören (sollen), müssen mit diesem Namen konfiguriert werden. Die Standard-SSID lautet „TP-LINK_XXXXXX“, wobei „XXXXXX“ für die letzten sechs Zeichen der MAC-Adresse des APs steht. Hierbei wird zwischen Groß- und Kleinschreibung unterschieden. Beispielsweise bezeichnen die SSIDs *TP-LINK* und *tp-link* unterschiedliche Netze.
- **Region** - Wählen Sie aus der Drop-Down-Liste die Region aus, in der der AP sich befindet. Damit verbunden sind Spezifikationen für die vom AP verwendeten Kanäle und Weiteres. Daher kann hier eine falsche Einstellung einen nicht gesetzeskonformen Betrieb verursachen. Ist die Region, in der der Router steht, nicht in dieser Liste aufgeführt, wenden Sie sich bitte an die zuständigen Behörden.
- **Channel** - Dieses Feld legt die Betriebsfrequenz des Routers fest. In der Standardeinstellung **Auto** wählt der Router automatisch einen Kanal aus. Es ist

nicht erforderlich, diese zu ändern, es sei denn, Sie stellen Interferenzen von einem nahen Accesspoint fest.

- **Add a remote AP** - Klicken Sie auf **Survey**, um die Felder **MAC of remote AP (1-4)** auszufüllen.
- **MAC of remote AP (1-4)** - Die MAC-Adresse des/der anderen AP(s).

➢ Wenn Sie **Client** wählen, erhalten Sie das Bild 3-26. In dieser Betriebsart dient der AP dazu, ein Ethernetgerät als WLAN-Station Ihrem drahtlosen Netz hinzuzufügen.

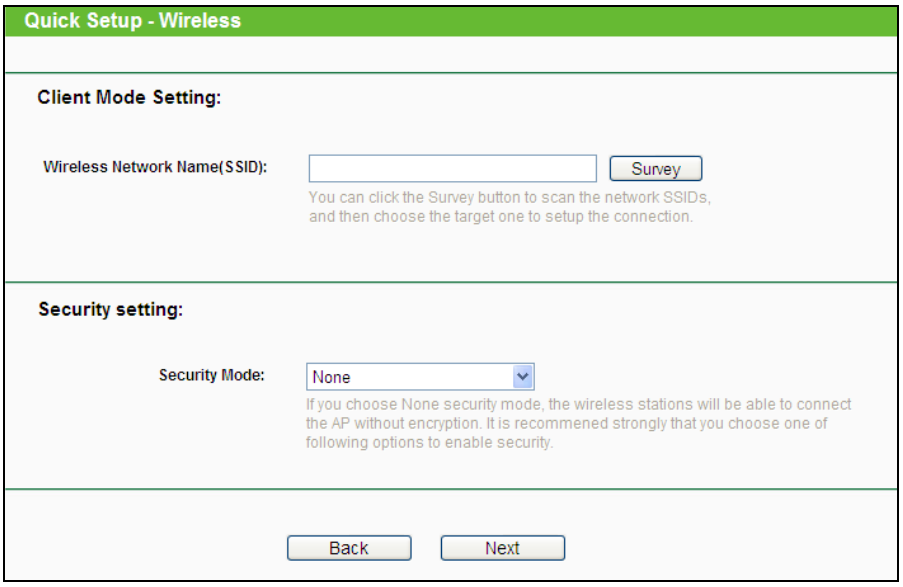


Bild 3-26 Quick Setup – Client

- **None** - Hiermit können Sie verfügen, dass der AP ganz ohne Verschlüsselung arbeitet. Damit kann jeder in Reichweite sich mit dem AP verbinden. Es wird wärmstens empfohlen, dass Sie statt dieser Option eine mit Sicherheit wählen.
- **WEP**

  Type - WEP-Sicherheit nach IEEE 802.11:

  - **Automatic** - Der WEP-Authentifizierungstyp kann auf **Automatic** (Standard), **Open System** oder **Shared Key** eingestellt werden. **Automatic** lässt den Client den Typ auswählen.

  WEP Key Format - Als Schlüsselformat können Sie zwischen **ASCII** und **Hexadecimal** wählen. Im Fall von **ASCII** können Sie mit beliebigen Zeichen arbeiten. Haben Sie **Hexadecimal** gewählt, können Sie nur Buchstaben von A bis F und arabische Ziffern verwenden. Der Wert 0 ist allerdings unzulässig. Bitte beachten Sie die vorgegebene Schlüssellänge.

  WEP Key settings - Wählen Sie einen der vier Schlüssel aus, um diesen zu verwenden.

Key Type - Hier können Sie die Schlüssellänge (64, 128 oder 152 Bit) auswählen. Der Wert „**Disabled**" bedeutet hier, dass der Schlüssel ungültig ist.

Bei **64-Bit**-Verschlüsselung sind 10 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 5 ASCII-Zeichen einzugeben.
Bei **128-Bit**-Verschlüsselung sind 26 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 13 ASCII-Zeichen einzugeben.
Bei **152-Bit**-Verschlüsselung sind 32 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 16 ASCII-Zeichen einzugeben.

- **WPA/WPA2-Personal**

  Version - WPA-PSK-Version. Die Standardeinstellung ist **Automatic**, womit entsprechend der Fähigkeiten/Anforderungen der Clients entweder mit **WPA-PSK** (Wi-Fi Protected Access) oder **WPA2-PSK** (WPA Version 2) gearbeitet wird.

  Encryption - Hier können Sie zwischen **Automatic**, **TKIP** und **AES** wählen.

  Password - Das Passwort kann 8 bis 63 ASCII- oder 8 bis 64 Hexadezimalzeichen lang sein.

  Group Key Update Period - Geben Sie die Dauer der Gültigkeit eines einzigen Gruppenschlüssels in Sekunden an. Dieser Wert sollte 0 (=deaktiviert) oder mindestens 30 betragen. Empfohlen sind Werte von 500 oder 600.

- **Not Change** - Wenn Sie die Option wählen, werden keine Änderungen an der WLAN-Verschlüsselung vorgenommen.

5. Klicken Sie auf **Next**, erhalten Sie das Bild 3-27. Klicken Sie auf **Reboot**, um den Router neu zu starten und die Einstellungen zu übernehmen.

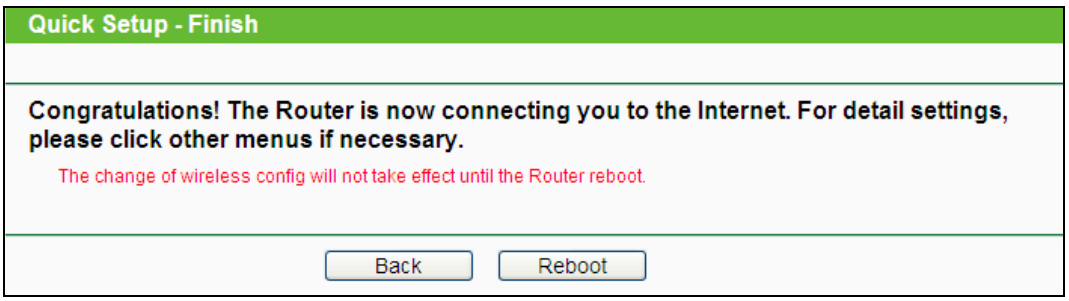


Bild 3-27 Quick Setup beendet

Hinweis:

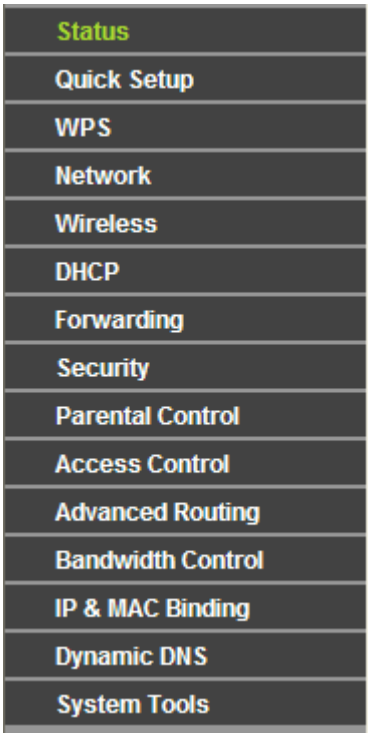
Nach dem Neustart des Routers ändern Sie die TCP/IT-Einstellungen Ihres Computers wieder auf **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen** (siehe Kapitel 3.3.1) und verbinden Sie sich mit dem Netzwerk (siehe Kapitel 3.3.2).

Kapitel 4. Konfiguration als 3G-Router

Dieses Kapitel zeigt Ihnen die Schlüsselfunktionalitäten und Konfigurationsmöglichkeiten jedes Menüs.

4.1 Login

Nachdem Sie sich erfolgreich eingeloggt haben, sehen Sie die fünfzehn Hauptmenüs auf der linken Bildschirmseite. Im rechten HTML-Frame ist der Hilfetext zu sehen.



Im Folgenden werden diese Hauptmenüs detailliert behandelt.

4.2 Status

Die Seite **Status** zeigt Statusinformationen zum Router. Diese Informationen können hier nicht geändert werden.

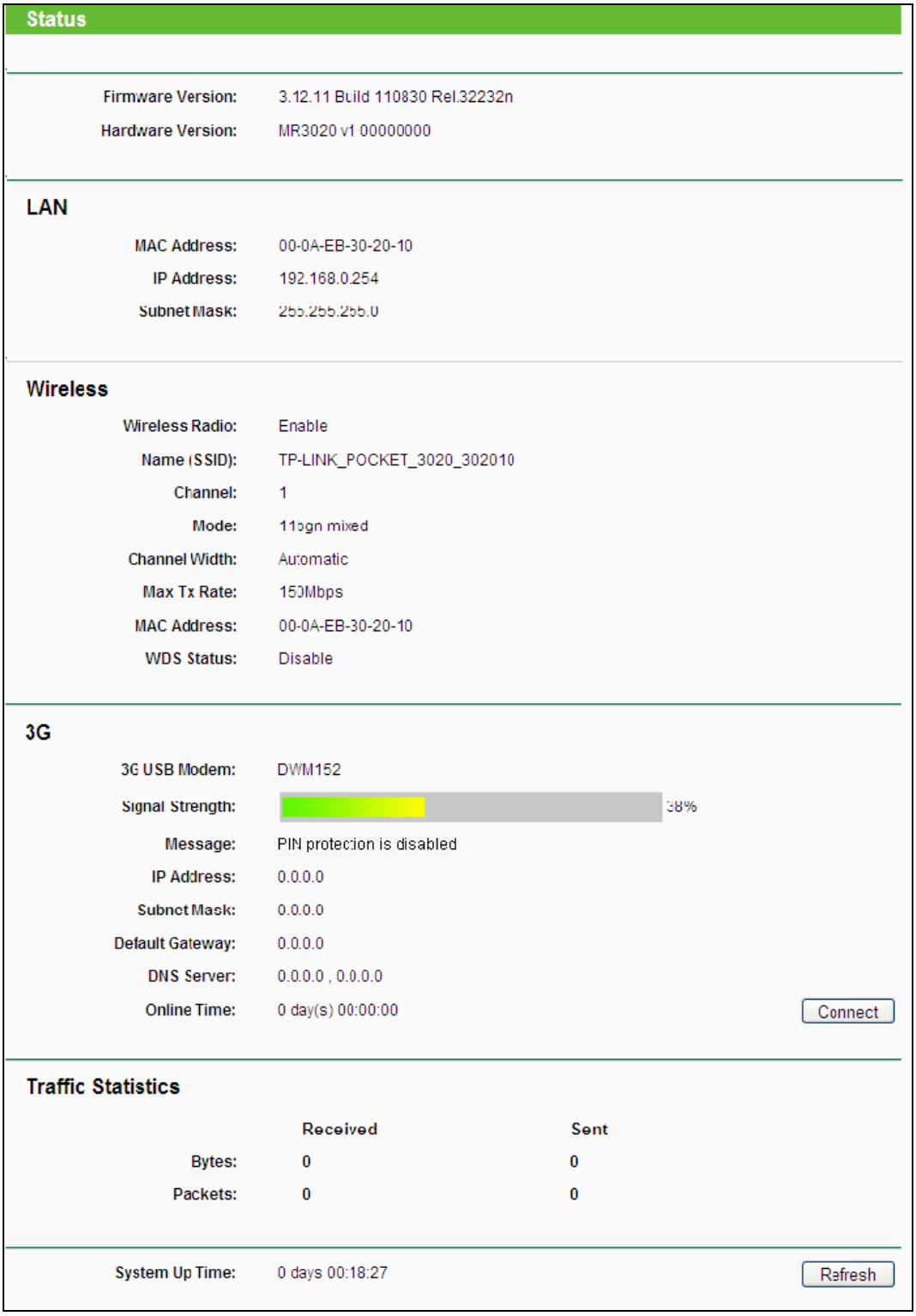


Bild 4-1 Statusseite

4.3 Quick Setup

Für die Schnellinstallation schauen Sie bitte im Kapitel 3.2 nach.

4.4 WPS

WPS (**Wi-Fi Protected Setup**), früher QSS **(Quick Secure Setup)** genannt, ermöglicht es

Ihnen, ohne viel Arbeit ein weiteres drahtloses Gerät Ihrem verschlüsselten WLAN hinzuzufügen.

Schritt 1: Gehen Sie in das Menü **WPS**. Sie sehen Folgendes (Bild 4-2).

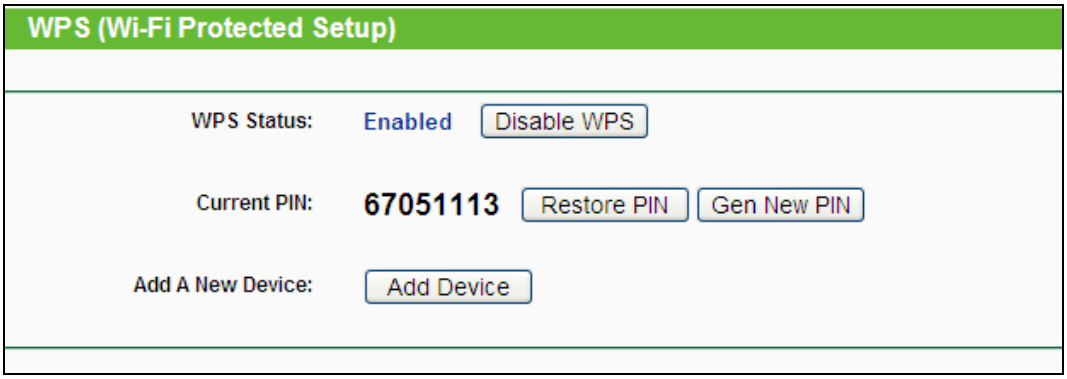


Bild 4-2 WPS

- Fehler! AutoText-Eintrag nicht definiert. **Status -** WPS aktivieren oder deaktivieren.
- **Current PIN -** Aktuelle Router-PIN. Die Standard-PIN kann auf dem Etikett auf der Geräterückseite oder auf dem Handbuch gefunden werden.
- **Restore PIN -** Standard-PIN des Routers wiederherstellen.
- **Gen New PIN -** Neue PIN per Zufallsgenerator erstellen. Damit können Sie die Sicherheit wiederherstellen, wenn die alte PIN Unbefugten bekannt wurde.
- **Add device -** Mit dieser Schaltfläche können Sie neue Geräte von Hand einbinden.

Schritt 2: Um ein neues Gerät hinzuzufügen, gehen Sie so vor:

Unterstützt der Drahtlosadapter WPS (Wi-Fi Protected Setup), können Sie die Verbindung entweder mit der Tastendruckmethode (PBC) oder der PIN-Methode herstellen.

☞ Bemerkung:

Um mittels WPS erfolgreich eine Verbindung herzustellen, sollten Sie zeitgleich die entsprechende WPS-Konfiguration des Adapters durchführen.

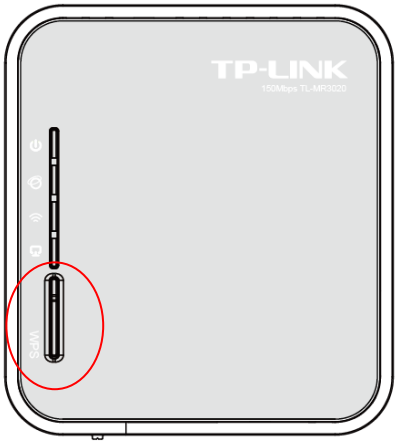
Als Beispiel dient im Folgenden ein WPS-fähiger TP-LINK-Adapter.

I. Mittels Tastendruck

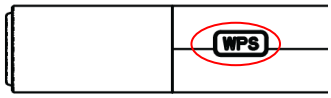
Verfügt Ihr WLAN-Client über eine „Wi-Fi Protected Setup“-Taste, verfahren Sie wie folgt.

Methode 1:

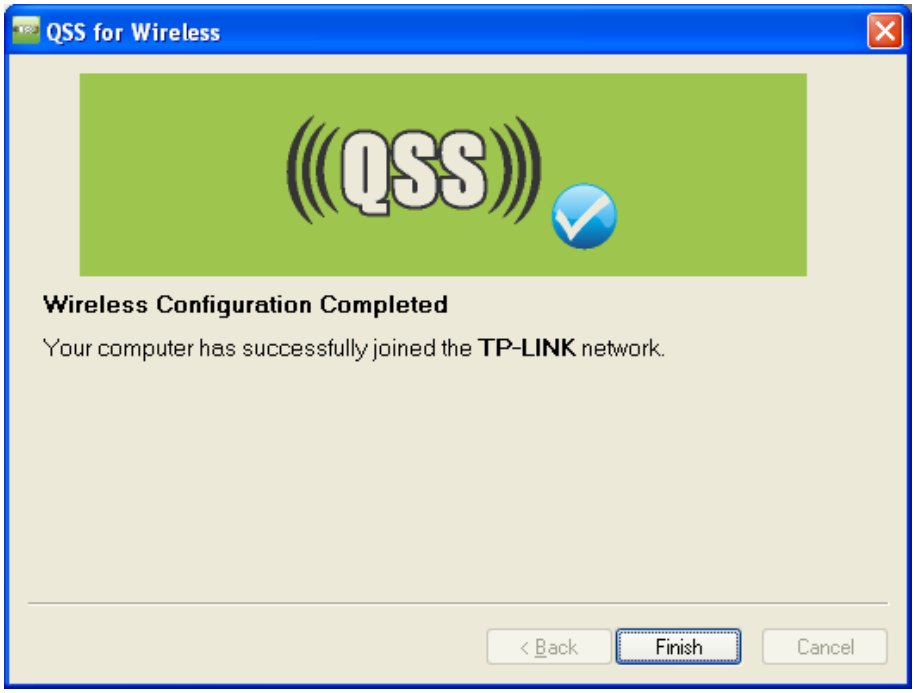
Schritt 1: Drücken Sie die WPS-Taste auf der Vorderseite des Routers.



Schritt 2: Drücken Sie die WPS-Taste Ihres Clientgerätes für mehrere Sekunden.



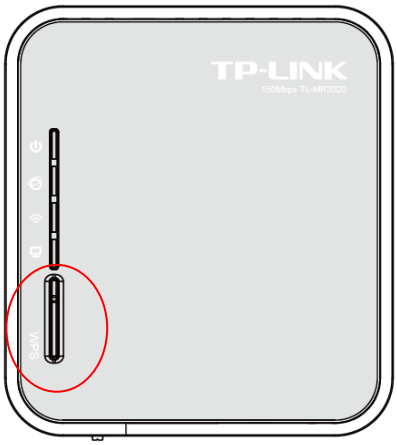
Schritt 3: Die „Wi-Fi Protected Setup“-LED des Routers blinkt für zwei Minuten, bis das Clientgerät sich erfolgreich mit dem Router verbunden hat und Sie vom WPS/QSS Tool folgende Meldung erhalten:



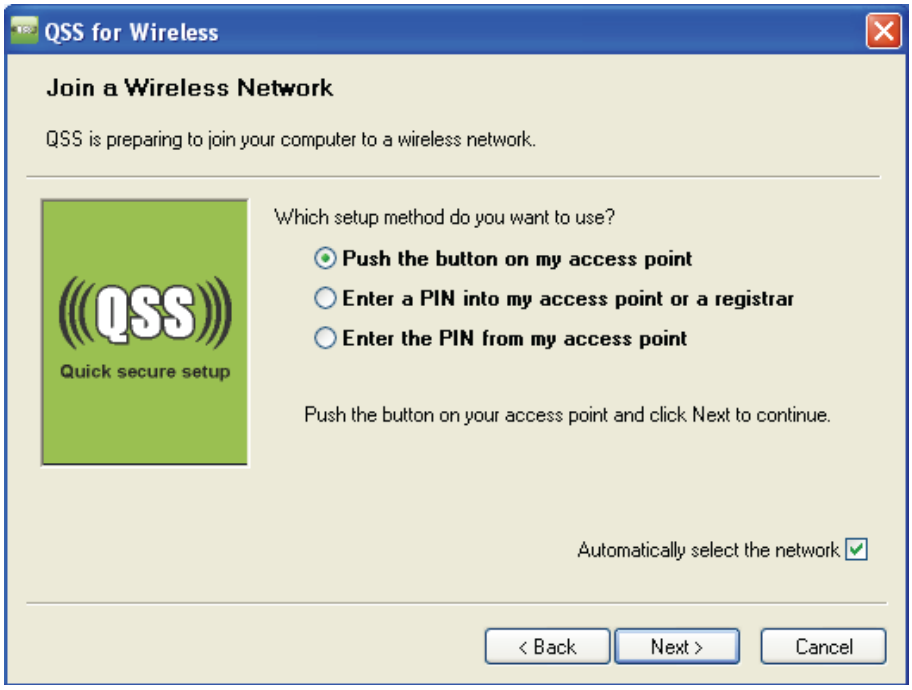
WPS/QSS-Konfigurationssoftware des WLAN-Adapters

Methode 2:

Schritt 1: Drücken Sie die WPS-Taste auf der Vorderseite des Routers.

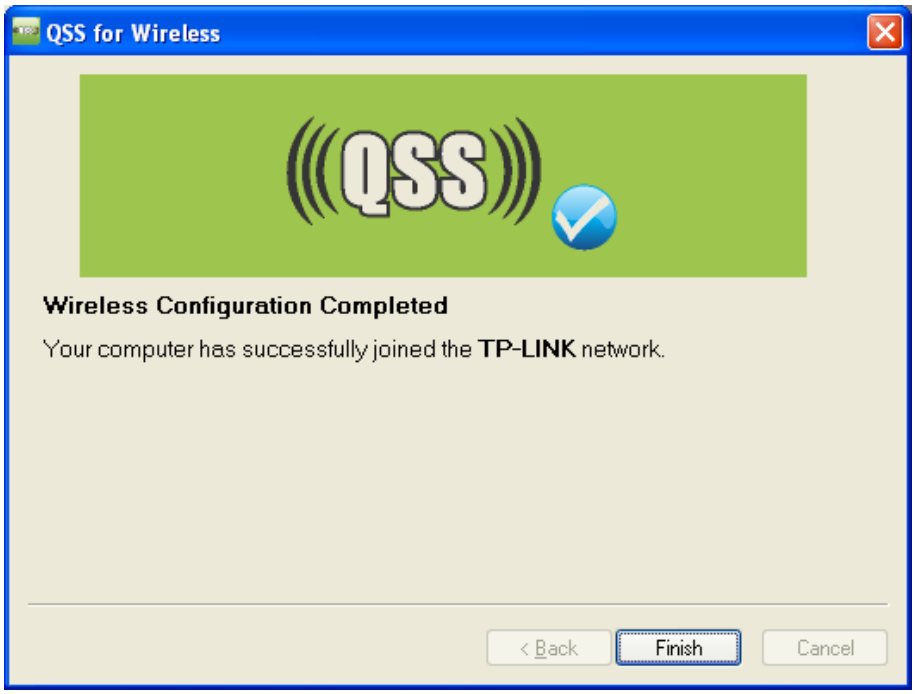


Schritt 2: Für die Konfiguration des WLAN-Adapters wählen Sie in der Software **Push the button on my access point und** klicken Sie auf **Next**.



Die WPS/QSS Konfigurationssoftware des WLAN-Adapters

Schritt 3: Warten Sie bis das nachfolgende Bild erscheint und klick Sie auf **Finish**.



WPS/QSS-Konfigurationssoftware des WLAN-Adapters

Methode 3:

Schritt 1: Klicken Sie im **WPS**-Menü **Add device** (Bild 4-2), Sie sehen dies.

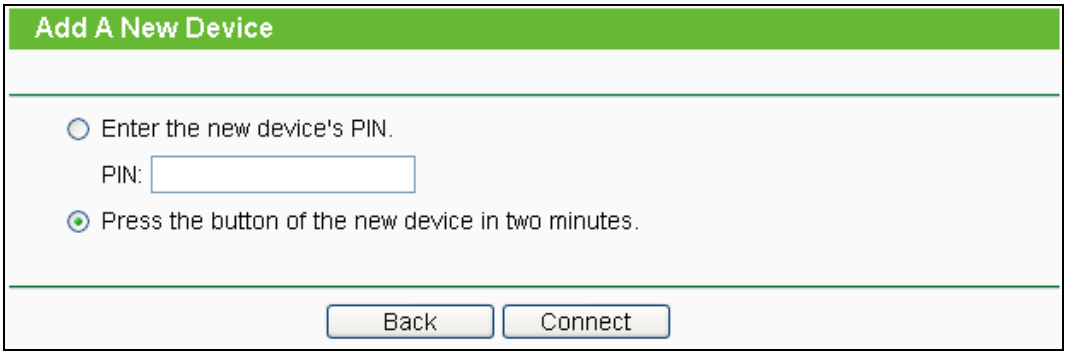
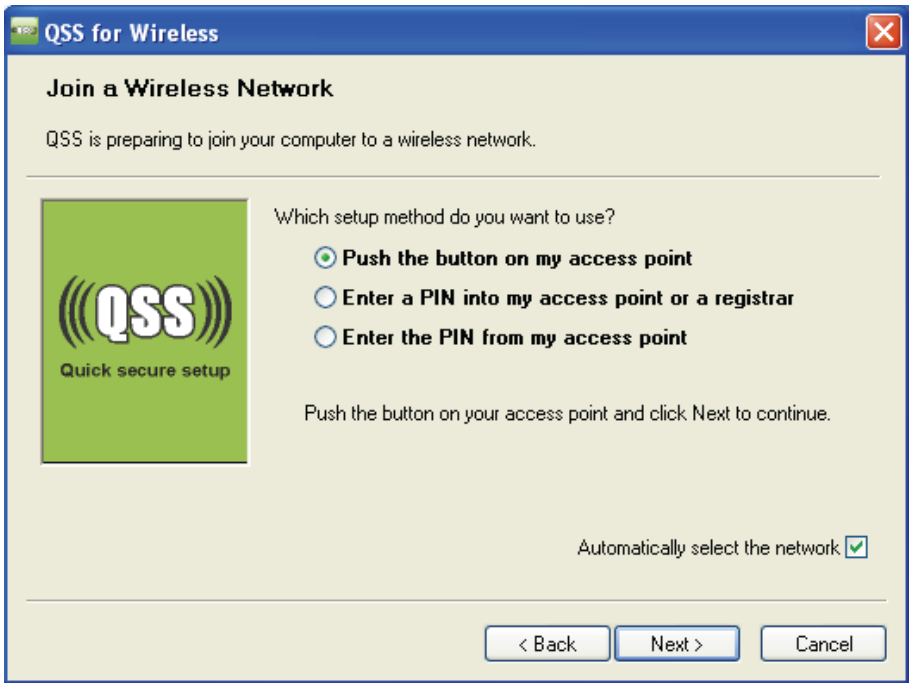


Bild 4-3 Gerät hinzufügen

Schritt 2: Wählen Sie **Press the button of the new device in two minutes** und klicken auf **Connect**.

Schritt 3: Für die Konfiguration des WLAN-Adapters wählen Sie in der Software **Push the button on my access point** und klicken Sie auf **Next**.



WPS/QSS-Konfigurationssoftware des WLAN-Adapters

Schritt 4: Warten Sie bis das nachfolgende Bild erscheint und klicken Sie auf **Finish**.

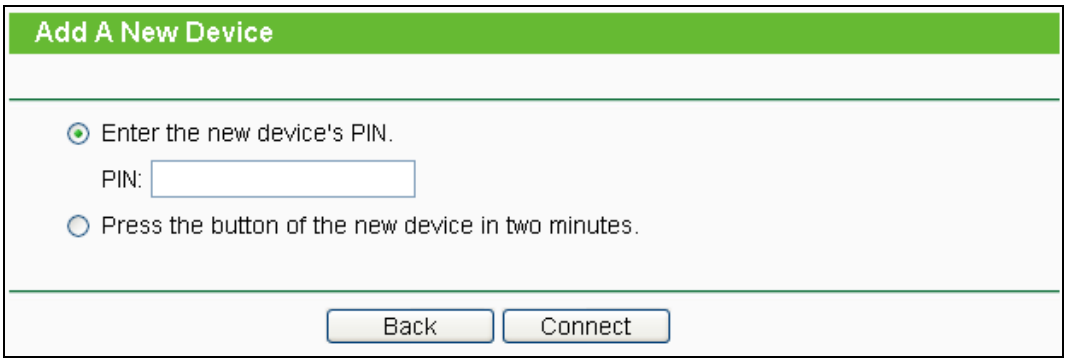
WPS/QSS-Konfigurationssoftware des WLAN-Adapters

II. Per PIN-Eingabe

Diese Methode können Sie anwenden, wenn Ihrem WLAN-Client eine WPS-PIN zugeordnet ist.

I. Methode 1: Eingabe der Client-PIN im Router

Schritt 1: Klicken Sie im **WPS**-Menü **Add device** (Bild 4-2). Sie sehen dies:

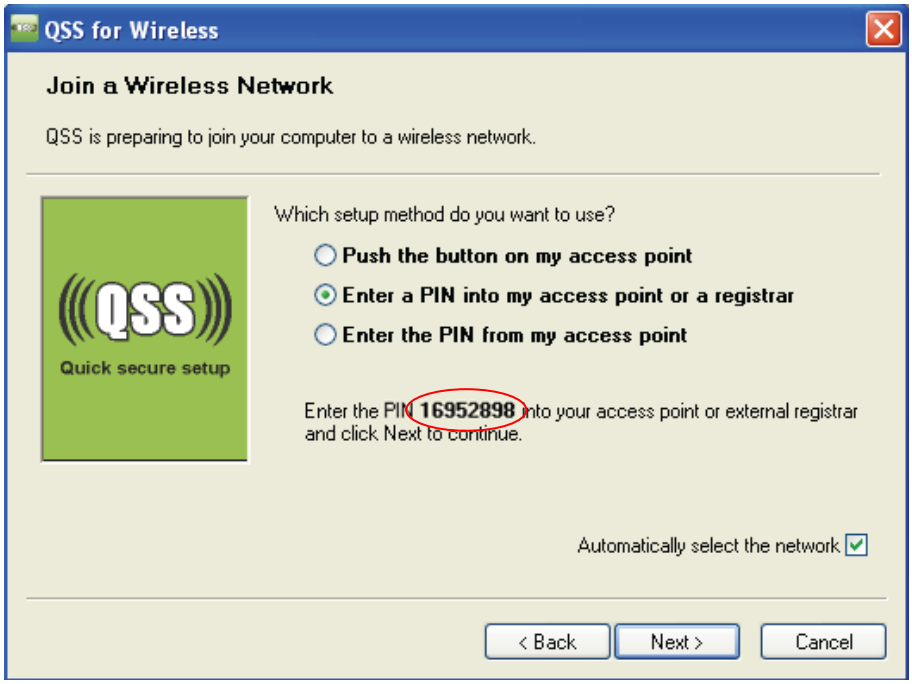


Schritt 2: Geben Sie die PIN Ihres WLAN-Clientgerätes in das Feld **PIN** ein und klicken Sie **Connect.**

Bemerkungen:

Die PIN des WLAN-Adapters finden Sie in der WPS/QSS-Konfigurationssoftware des WLAN-Adapters.

Schritt 3: Für die Konfiguration des WLAN-Adapters wählen Sie in der Software **Enter a PIN into my access point or a registrar** und klicken Sie auf **Next.**



Die WPS/QSS Konfigurationssoftware des WLAN-Adapters

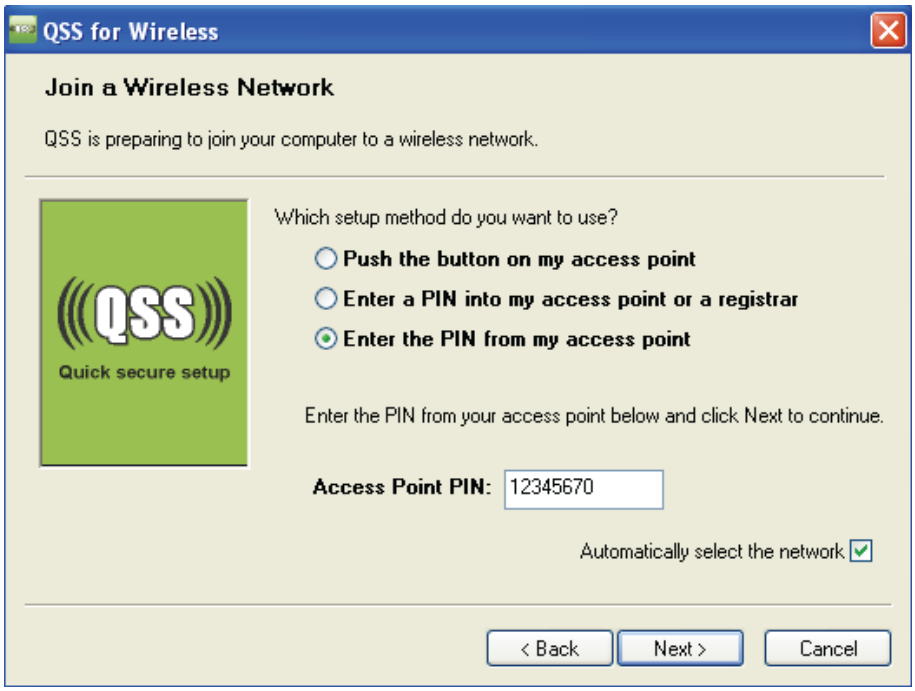
Bemerkungen:

In dem Beispiel lautet die Standard-PIN des WLAN-Adapters 16952898.

Methode 2: Eingabe der Router-PIN in Ihren WLAN-Client

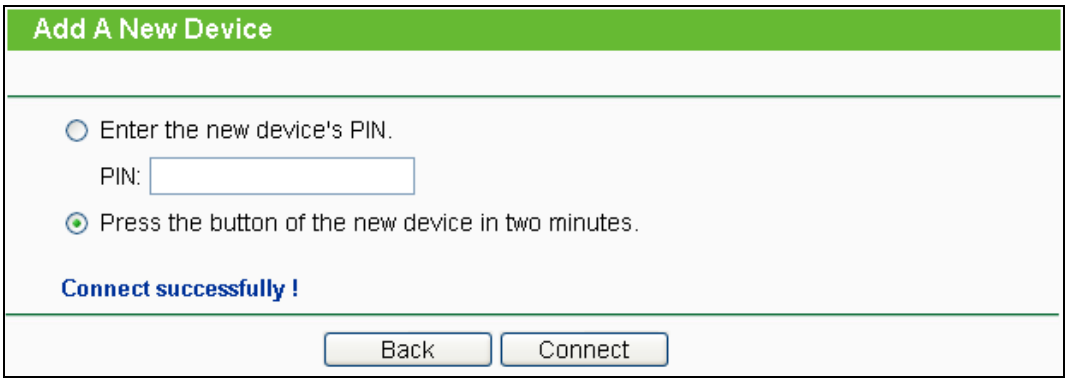
Schritt 1: Geben Sie die PIN, die Sie auf der WPS-Seite Ihres Routers und auf der Routerunterseite finden (Bild 4-2), in die Software Ihres Clientgerätes ein.

Schritt 2: Für die Konfiguration des WLAN-Adapters wählen Sie in der Software **Enter a PIN from my access point**, geben Sie die PIN des Routers ein und klicken Sie auf **Next.**



WPS/QSS-Konfigurationssoftware des WLAN-Adapters

Schritt 3: Wenn die Verbindung erfolgreich aufgebaut wurde, erhalten Sie folgende Meldung am Router:



Bemerkungen:

1) Die **Fehler! AutoText-Eintrag nicht definiert.**-LED des Routers leuchtet nach dem erfolgreichen Verbinden mit dem Netz für weitere 5 Minuten.

2) Die **Fehler! AutoText-Eintrag nicht definiert.**-Funktion kann nicht benutzt werden, wenn das WLAN des Routers deaktiviert ist.

4.5 Network

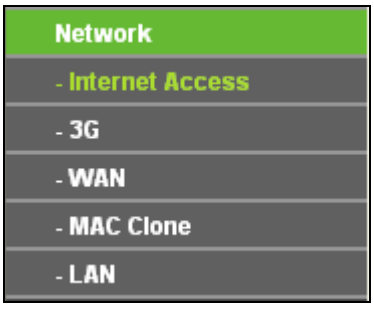


Bild 4-4 Das Menü **Network**

Im Netzwerk-Menü gibt es vier Untermenüs (Bild 4-4): **Internet Access**, **3G**, **WAN**, **MAC Clone** und **LAN**.

4.5.1 Internet Access

Wählen Sie **Network** → **Internet Access**. Hier können Sie die Art des Internetzugriffs konfigurieren. Der Router ist in der Lage, sich über den WAN-Anschluss und über 3G mit dem Internet zu verbinden.

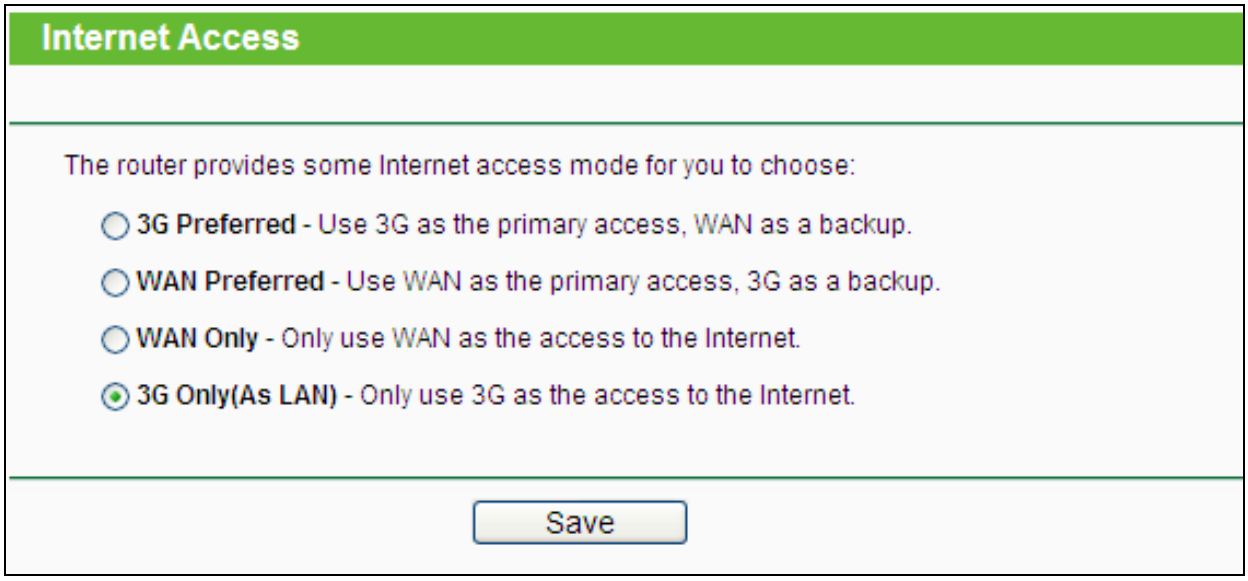


Bild 4-5 Internetzugriffsmodus

- **3G Preferred**
  In diesem Modus versucht der Router zunächst, eine 3G-Verbindung aufzubauen. Schlägt dies fehl und am WAN-Port ist etwas angeschlossen oder wenn gar kein 3G-Modem angeschlossen ist, wird der WAN-Zugang benutzt. Kann irgendwann eine 3G-Verbindung hergestellt werden, schaltet der Router auf diese um.

- **WAN Preferred**
  In diesem Modus versucht der Router zunächst, eine WAN-Verbindung aufzubauen. Schlägt dies fehl und über den USB-Port kann eine Verbindung hergestellt werden, schaltet der Router auf 3G-Internetzugriff um. Kann irgendwann eine WAN-Verbindung hergestellt werden, schaltet der Router auf diese um.

- **WAN Only**
  Dieser Modus verwendet ausschließlich den WAN-Port. Der 3G-Zugang wird nicht verwendet.

- **3G Only (As LAN)**
  Diese Betriebsart bedeutet, dass der Internetzugriff über WAN deaktiviert ist.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

☞ **Bemerkungen:**

1) Um den Failover nicht nur bei **PPPoE**, **Dynamic IP** und **Static IP**, sondern auch bei **BigPond Cable**, **PPTP** und **L2TP** nutzen zu können, ist eventuell ein Firmwareupdate nötig:
   Siehe **http://www.tp-link.com/support/download.asp**

2) Benutzen Sie **3G Preferred** oder **WAN Preferred**, kann der Router automatisch Verbindungen herstellen oder trennen. Dies ist bei Volumen- und besonders Zeittarifen zu beachten. Weiterhin steht die Schaltfläche **Connect** bzw. **Disconnect** (bei **3G**, **PPPoE**, **PPTP** und **L2TP**) nicht zur manuellen Bedienung zur Verfügung.

4.5.2 3G

Im Menü **Network** → **3G** können Sie die 3G-Verbindungsparameter konfigurieren (siehe unten). Um die 3G-Funktion zu benutzen, schließen Sie zunächst das USB-Modem an den Router an. Dem Gerät ist bereits eine Vielzahl 3G-USB-Modems bekannt. Ist Ihres unterstützt, werden die USB-Parameter automatisch gesetzt und in Bild 4-6 angezeigt (Beispiel hier: Modell DWM152). Im andern Fall wird Ihnen **Unknown Modem** angezeigt, wie in Bild 4-7. Auf unserer Homepage **http://www.tp-link.com** finden Sie die neueste UMTS-Modem-Kompatibilitätsliste.

☞ **Bemerkung:**

Die 3G-Einstellungen stehen nicht zur Verfügung, wenn als Internetzugangsart **WAN Only** konfiguriert ist. In diesem Fall müssten die Einstellungen auf der Seite Internet Access geändert werden.

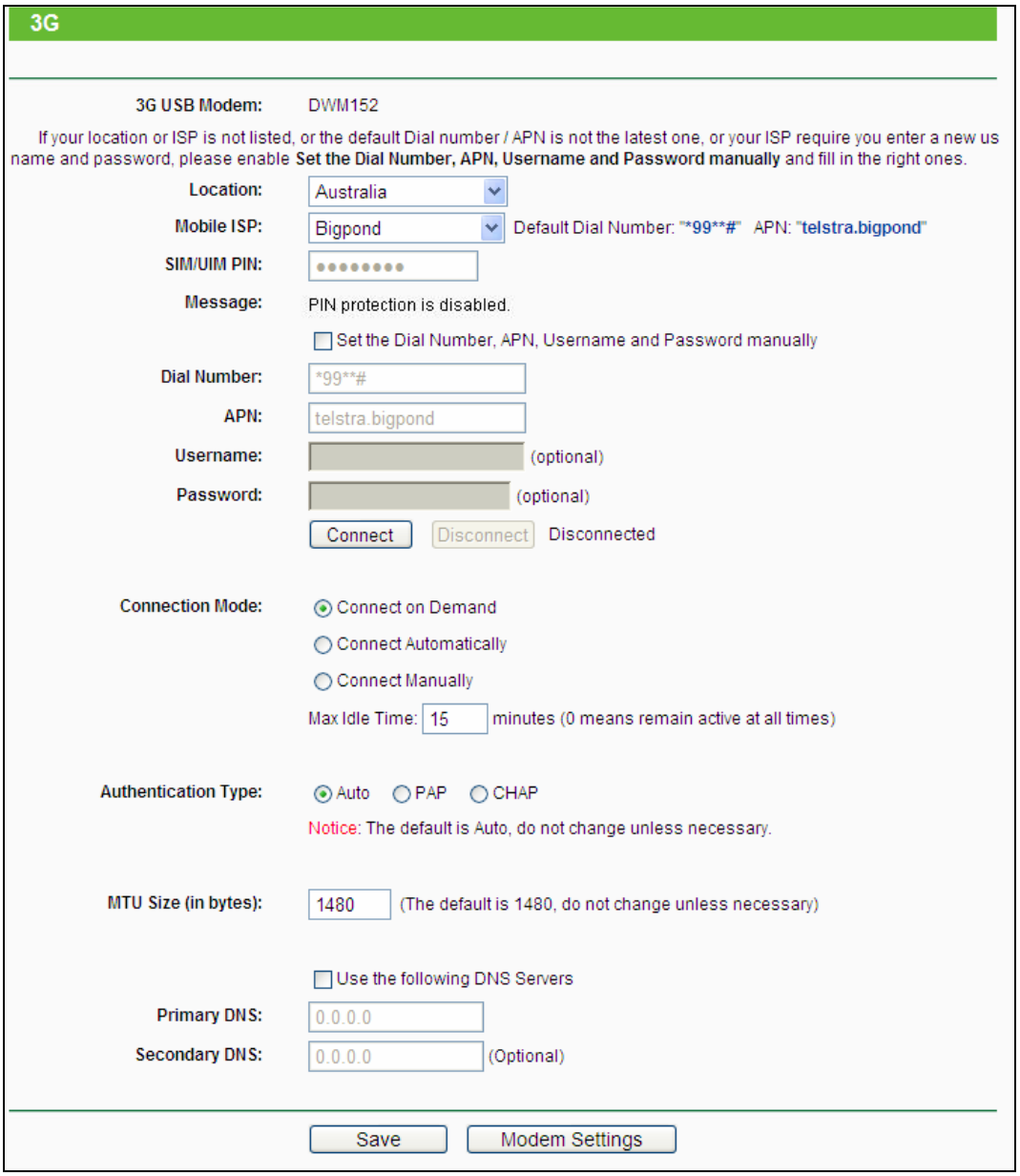


Bild 4-6 3G-Modem erkannt

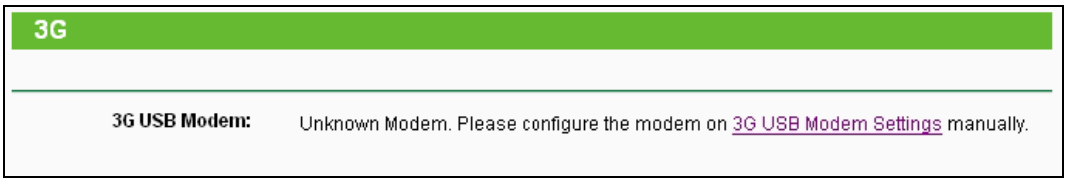


Bild 4-7

- **Location -** Das Land, in dem das zu benutzende Mobilfunknetz sich befindet.
- **Mobile ISP -** Der Mobilfunkdiensteanbieter, den Sie für Ihren 3G-Zugang benutzen wollen. Hier sind die wichtigsten Anbieter mit ihren APNs und ihren Einwahlnummern voreingestellt. Ist Ihr Anbieter nicht in der Liste enthalten, wählen Sie **Set the Dial Number and APN manually** und geben Sie Einwahlnummer (**Dial Number**) und **APN** von Hand ein.

- **Dial Number & APN -** Hier können Sie Einwahlnummer (**Dial Number**) und **APN** (Access Point Number) von Hand eingeben, wenn **Set the Dial Number and APN manually** markiert ist.
- **Username & Password -** Benutzername und Passwort zur Interneteinwahl (optional). Diese bekommen Sie von Ihrem Anbieter, falls erforderlich. Beachten Sie Groß-/Kleinschreibung.

Klicken Sie **Connect**, um sich mit dem 3G-Netz zu verbinden. Wurde die Verbindung erfolgreich hergestellt, sehen Sie auf der 3G-Seite etwas wie in Bild 4-8 („Connected“). Auf der Seite **Status** sehen Sie im Abschnitt **3G** etwas wie in Bild 4-9.

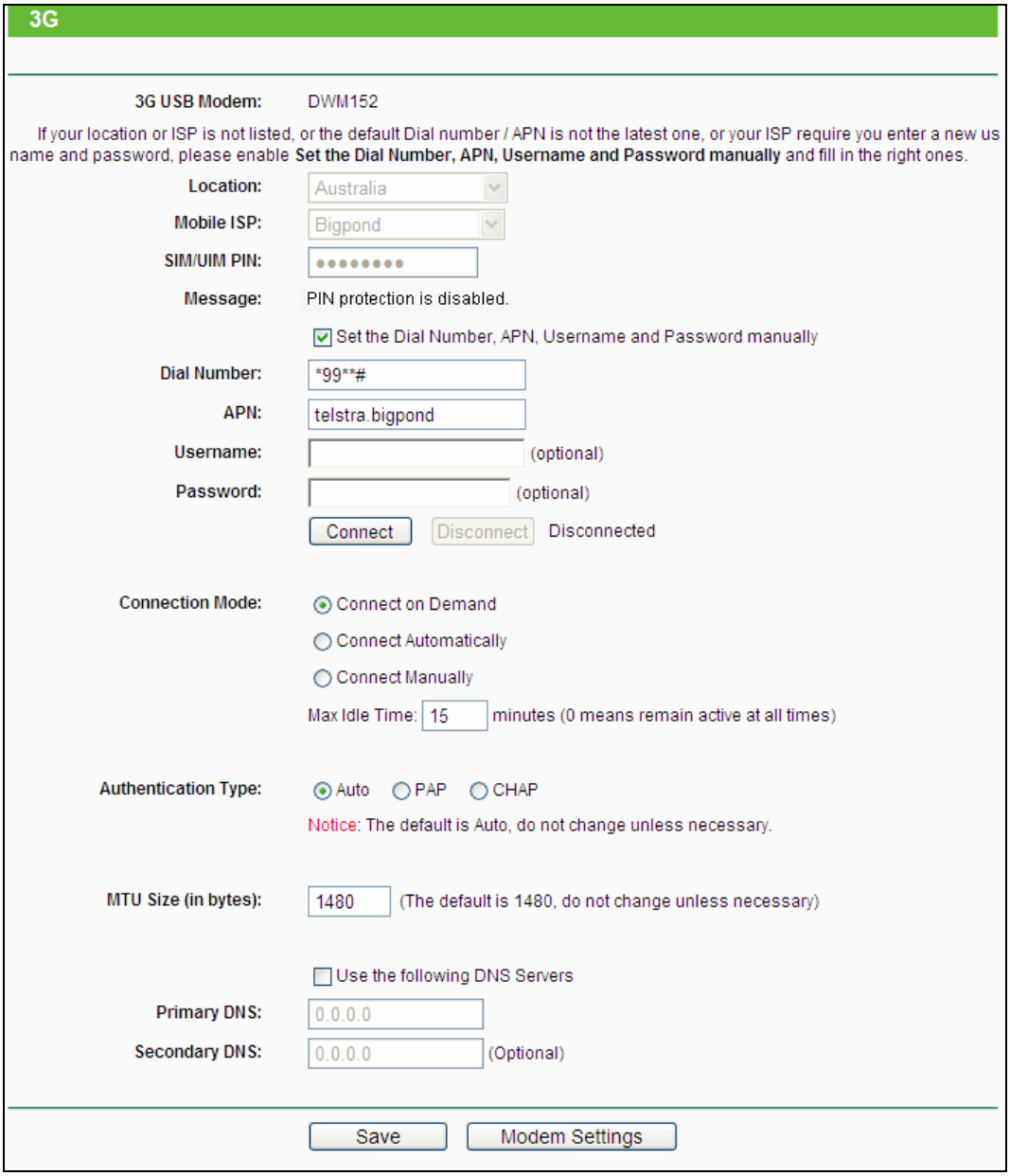


Bild 4-8 3G-Einstellungen

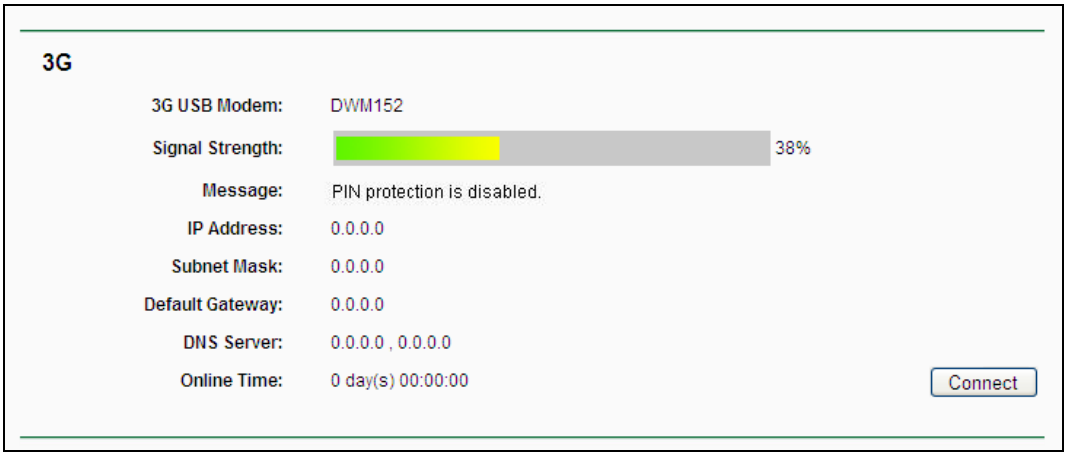


Bild 4-9 Abschnitt „3G“ auf der Statusseite

- **Connect on Demand -** Der Router verbindet sich bei Bedarf und trennt die Verbindung, nachdem sie die angegebene Zeit inaktiv war (**Max Idle Time**). Nach einer solchen Trennung wird sie bei Bedarf erneut hergestellt. Soll die automatische Trennung unterbleiben, setzen Sie als **Max Idle Time** den Wert **0**. Ansonsten geben Sie die Zeit in Minuten an, nach der die Verbindung getrennt werden soll.

☞ **Bemerkung:**

Die Verbindung wird bei Nichtbenutzung der Internetverbindung nach Ablauf der **Max Idle Time** nicht getrennt, wenn noch einige Prozesse im Hintergrund auf das Internet zugreifen.

- **Connect Automatically -** Verbindung automatisch herstellen und aufrechterhalten, soweit möglich.
- **Connect Manually -** Hiermit können/müssen Sie den Router stets von Hand einwählen. Nach Ablauf der **Max Idle Time** trennt der Router die Verbindung automatisch, wenn in diesem Zeitraum kein Internetdatenverkehr stattgefunden hat. Eine automatische Wiedereinwahl findet dann nicht statt. Soll die automatische Trennung unterbleiben, setzen Sie als **Max Idle Time** den Wert **0**. Ansonsten geben Sie die Zeit in Minuten an, nach der die Verbindung getrennt werden soll.

☞ **Bemerkung:**

Die Verbindung wird bei Nichtbenutzung der Internetverbindung nach Ablauf der **Max Idle Time** nicht getrennt, wenn noch einige Prozesse im Hintergrund auf das Internet zugreifen.

- **Authentication Type -** Einige Anbieter verlangen einen besonderen Authentifizierungstyp. Trifft dies bei Ihrem zu, machen Sie die entsprechende Angabe.
- **MTU Size -** Die Standard-MTU(Maximum Transmission Unit)-Größe beträgt 1480 Byte. In aller Regel ist dieser Wert korrekt. Bei einigen Anbietern jedoch muss dieser Wert angepasst werden.
- **Use the following DNS Servers -** Weist Ihr Mobilfunkanbieter Ihnen keine DNS-Serveradressen automatisch zu, können Sie diese Option aktivieren und unter

Primary DNS und **Secondary DNS** die entsprechenden Adressen von Hand eingeben. Die Eingabe in das Feld **Secondary DNS** ist optional.

- **Primary DNS -** IP-Adresse des ersten DNS-Servers.
- **Secondary DNS -** IP-Adresse des alternativen DNS-Servers (optional).

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

Wird Ihr USB-Modem nicht direkt vom Router unterstützt, öffnen Sie **Modem Settings**. Sie sehen Bild 4-10. Hier können Sie Ihr USB-Modem parametrieren.

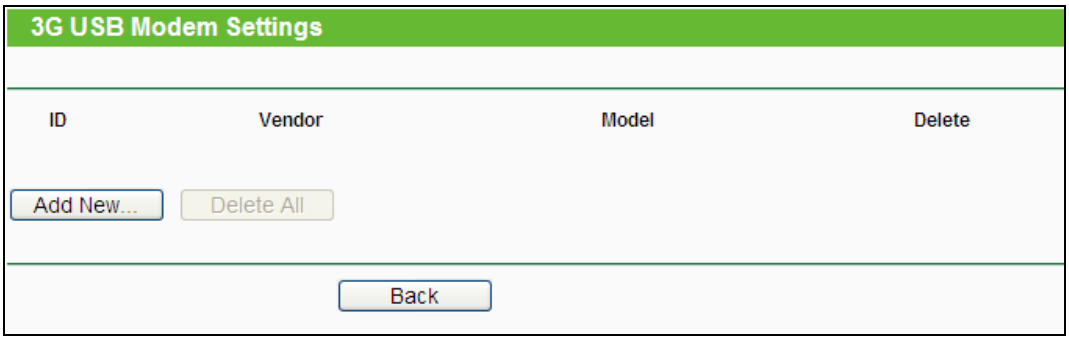


Bild 4-10 3G USB-Modem-Einstellungen

Dem Router sind bereits etliche 3G-USB-Modems bekannt. In diesem Fall findet die Parametrierung automatisch statt. Ansonsten, d.h. wenn **unknown** angezeigt wird, werden diese Parameter von Ihnen abgefragt. Wir empfehlen, in diesem Fall folgende Prozedur.

Um dem Router neue 3G-USB-Modems bekannt zu machen.

1. Laden Sie sich die neueste Modem-Konfigurationsdatei von **http://www.tp-link.com** herunter.
2. Klicken Sie **Add New...** (Bild 4-10) Sie sehen Bild 4-11.
3. Klicken Sie **Durchsuchen…**, um den Pfad zu der heruntergeladenen Datei anzugeben.
4. Klicken Sie **Upload**, um die Konfigurationsdatei in den Router zu laden.

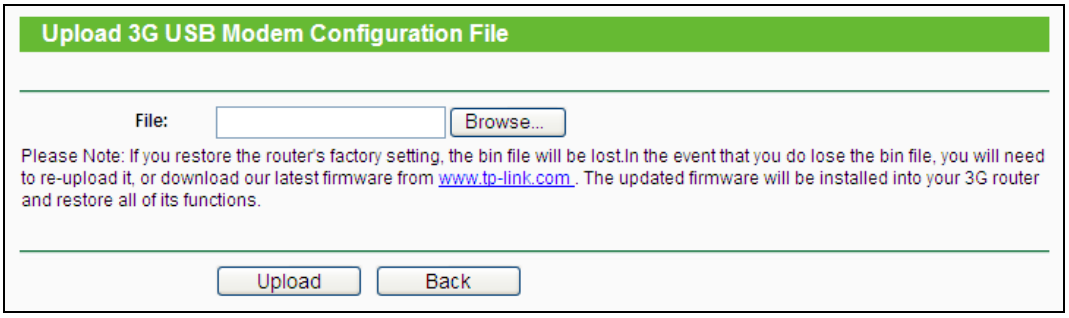


Bild 4-11 Modemparameter hinzufügen

4.5.3 WAN

Wählen Sie im Menü **Network** → **WAN**, können Sie die WAN-IP-Parameter einstellen.

Bemerkung:

Die WAN-Einstellungen stehen nicht zur Verfügung, wenn als Internetzugangsart **3G Only** konfiguriert ist. In diesem Fall müssten die Einstellungen auf der Seite Internet Access geändert werden.

1. Bietet Ihr ISP einen DHCP-Dienst (z.B. bei Verwendung eines Kabelmodems), wählen Sie bitte **Dynamische IP-Adresse**. Ihr Router holt die IP-Parameter dann automatisch vom ISP. Die Seite sieht so aus (Bild 4-12):

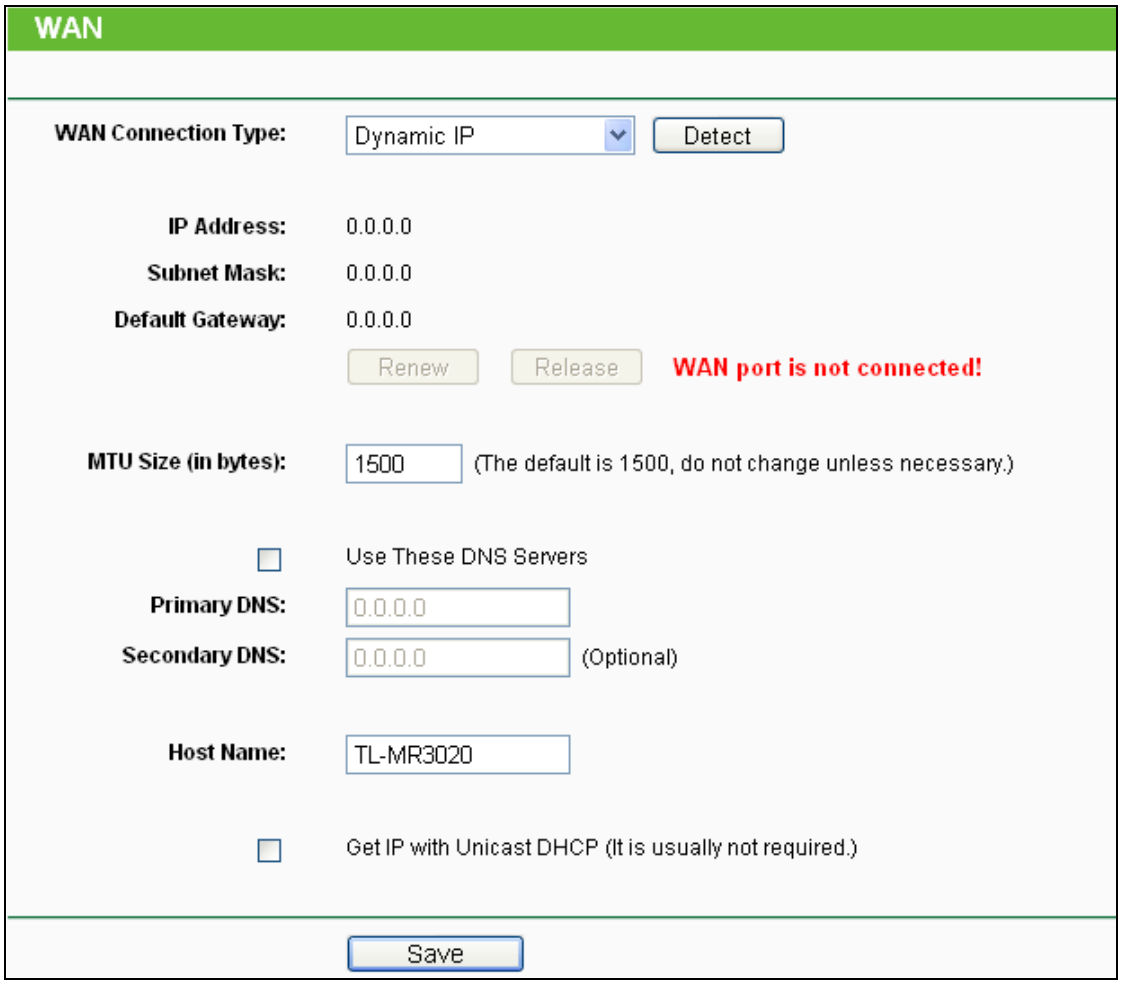


Bild 4-12 WAN - Dynamic IP

Diese Seite zeigt die WAN-IP-Parameter, die durch Ihren ISP dynamisch zugewiesen wurden: IP-Adresse, Subnetzmaske, Standardgateway, etc.. Klicken Sie **Renew**, um die IP-Parameters erneut vom ISP abzurufen. Klicken Sie **Release**, um Ihre IP-Parameter freizugeben.

- **MTU Size -** Die MTU-Größe (**M**aximum **T**ransmission **U**nit) liegt bei den meisten Ethernet-Netzen bei 1500 Byte. Es wird nicht empfohlen, diesen Wert zu ändern, wenn Ihr ISP dies nicht erfordert.
- **Use These DNS Servers -** Hat Ihr ISP Ihnen eine oder zwei DNS-Server-Adressen gegeben, wählen Sie **Use These DNS Servers** und geben Sie die Adressen in diese Felder ein. Ansonsten werden die DNS-Serveradressen dynamisch vom ISP zugewiesen.

Bemerkung:

Sollten Sie nach Eingabe der DNS-Serveradressen keine Webseiten mehr aufrufen können, könnten Ihre DNS-Einstellungen fehlerhaft sein. In diesem Fall kontaktieren Sie Ihren ISP.

- **Host Name -** Hostname des Routers.
- **Get IP with Unicast DHCP -** Einige ISPs betreiben DHCP-Server, die keine Broadcast-Anwendungen beherrschen. Können Sie auf normalem Wege keine IP-Adresse bekommen, können Sie es mit dieser Option versuchen (selten benötigt).

2. Wenn Ihr Anbieter eine statische IP-Adresse verwendet, sollte er Ihnen diese mitgeteilt haben, ebenso Subnetzmaske, Gateway und DNS-Server. Wählen Sie in diesem Fall **Static IP** aus. Bild 4-13 erscheint.

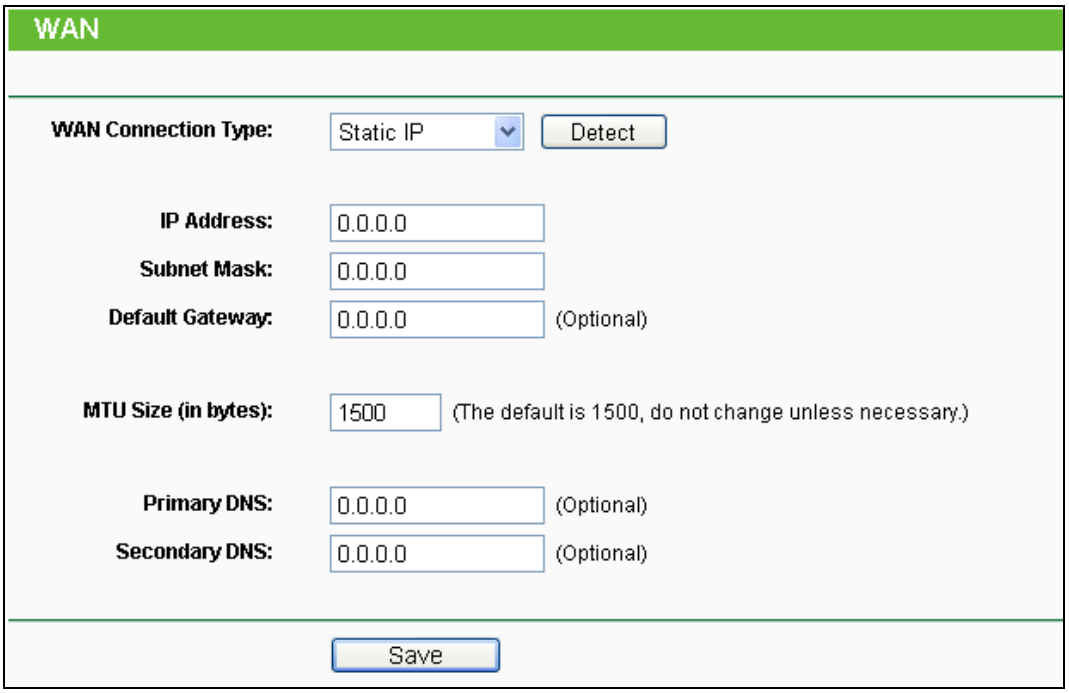


Bild 4-13 WAN - Static IP

- **IP Address -** Die IP-Adresse, die Sie von Ihrem ISP erhalten haben.
- **Subnet Mask -** Die Subnetzmaske, gewöhnlich 255.255.255.0.
- **Default Gateway -** Die IP-Adresse des Gateways Ihres ISPs (optional).
- **MTU Size -** Die Standard-MTU-Größe (**M**aximum **T**ransmission **U**nit) ist in normalen Ethernets 1500 Byte groß. Es wird nicht empfohlen, diese zu ändern, wenn es nicht erforderlich ist.
- **Primary/Secondary DNS -** Geben Sie eine oder zwei DNS-Serveradressen ein (optional).

3. Arbeiten Sie mit einer PPPoE-Verbindung, wählen Sie **PPPoE/Russia PPPoE** aus. Es sind folgende Parameter einzugeben (Bild 4-14):

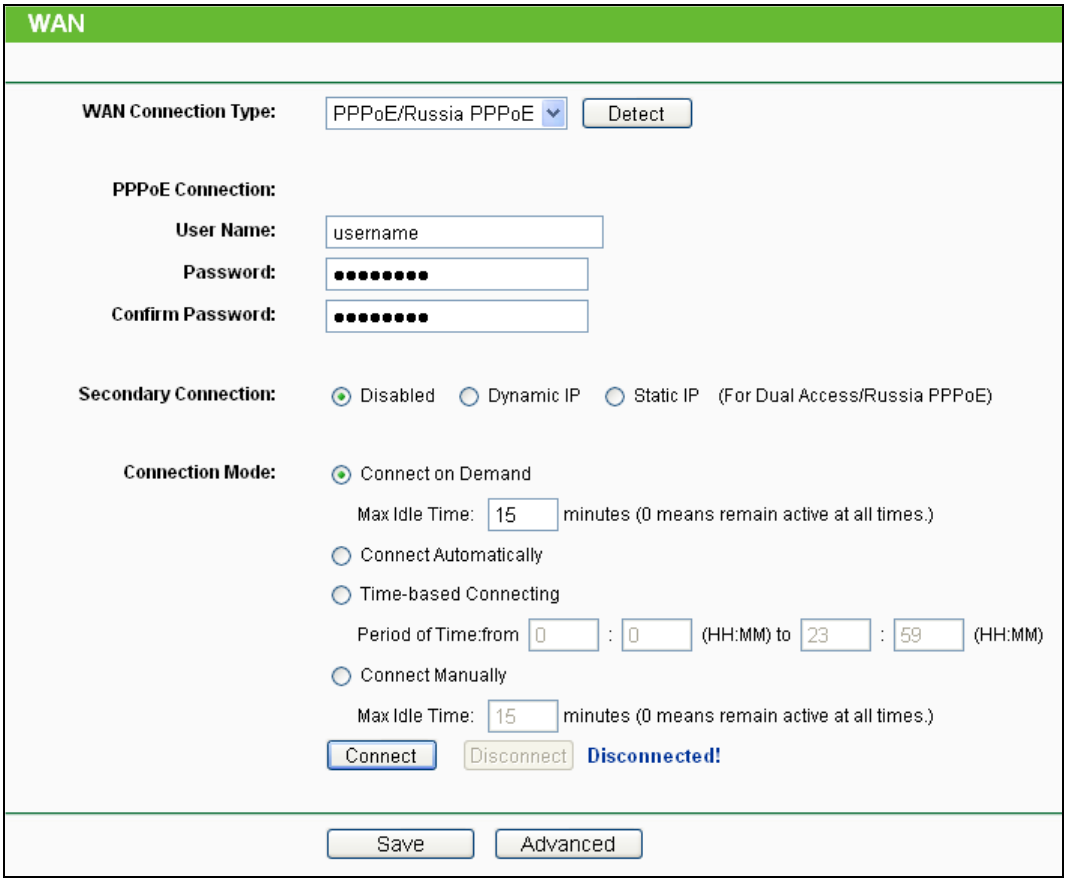


Bild 4-14 WAN - PPPoE

- **User Name/Password -** Geben Sie Benutzernamen und Passwort ein, so wie Sie sie von Ihrem ISP erhalten haben. Hier wird zwischen Groß- und Kleinschreibung unterschieden.
- **Secondary Connection -** Diese Option wird nur bei PPPoE angeboten. Bietet Ihr ISP einen extra Verbindungstyp wie dynamische/statische IP-Adresse für den Zugang zu einem LAN an, können Sie hier die passende Option aktivieren.
  - **Disabled -** Die Zweitverbindung ist deaktiviert (empfohlen).
  - **Dynamic IP -** Aktivieren Sie dies, wenn Sie mit dynamischer IP-Adresse über die Zweitverbindung zum LAN Ihres ISPs Verbindung aufnehmen wollen.
  - **Static IP -** Aktivieren Sie dies, wenn Sie mit statischer IP-Adresse über die Zweitverbindung zum LAN Ihres ISPs Verbindung aufnehmen wollen.
- **Connect on Demand -** In diesem Modus wird die Internetverbindung nach einer konfigurierbaren Dauer der Inaktivität (**Max Idle Time**) getrennt und bei Bedarf erneut hergestellt werden. Soll Ihre Internetverbindung ständig aktiv sein, geben Sie hier 0 als **Max Idle Time** ein. Andernfalls geben Sie die **Max Idle Time** in min an.
- **Connect Automatically -** Neu verbinden, nachdem die Verbindung getrennt wurde.
- **Time-based Connecting -** Die Verbindung wird nur im angegebenen Zeitraum hergestellt. Startzeit und Endzeit sind im Format „hh:mm“ anzugeben.

☞ **Bemerkung:**

Time-based Connecting funktioniert nur, wenn Sie **unter System Tools** -> **Time** Angaben gemacht haben.

- **Connect Manually -** Mit der Schaltfläche **Connect/Disconnect** können Sie die Verbindung augenblicklich von Hand herstellen oder trennen. Auch dieser Modus unterstützt die Funktion der **Max Idle Time**, genau wie **Connect on Demand**.

Vorsicht: Unter Umständen fängt die maximale Leerlaufzeit (**Max Idle Time**) nicht an zu laufen oder wird unterbrochen, nämlich dann, wenn einige Applikationen im Hintergrund noch Datenverkehr erzeugen.

Für weitere Konfigurationsmöglichkeiten klicken Sie **Advanced**. Die Seite in Bild 4-15 erscheint:

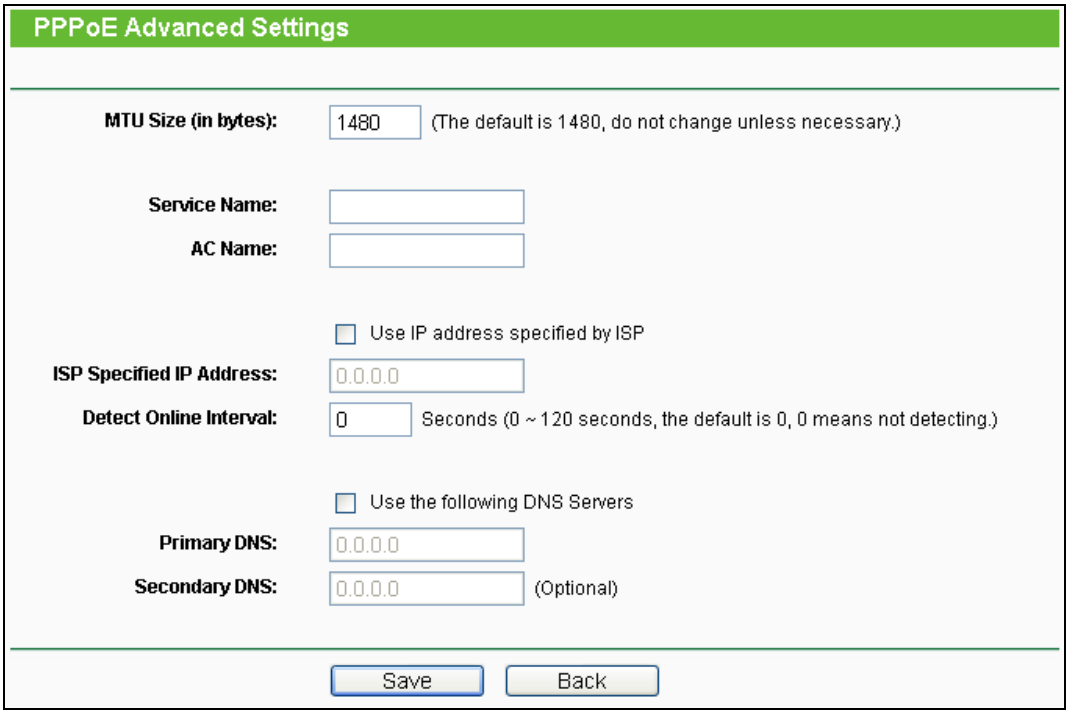


Bild 4-15 Erweiterte PPPoE-Einstellungen

- **MTU Size -** Die Standard-MTU(**M**aximum **T**ransmission **U**nit)-Größe beträgt bei PPPoE 1480 Byte. Bei einigen ISPs muss diese reduziert werden. Da dies allerdings nur selten erforderlich ist, sollten Sie diesen Wert nur ändern, wenn Sie sich sicher sind.

- **Service Name/AC Name -** Der Servicename und der AC(**A**ccess **C**oncentrator)-Name. Sollten nicht geändert werden, außer es ist bei Ihrem ISP notwendig.

- **ISP Specified IP Address -** Wenn Sie wissen, dass Ihr ISP bei der Einwahl die IP-Adresse nicht automatisch überträgt, wählen Sie **Use IP address specified by ISP** und geben Sie die IP-Adresse hier ein.

- **Detect Online Interval -** Dies ist der Zeitabstand in Sekunden, in dem der Router überprüft, ob der Access Concentrator online ist. Zulässige Werte sind von 0 bis 120. Der Standardwert ist 0 (=deaktiviert).
- **Primary/Secondary DNS -** Wenn Sie wissen, dass Ihr ISP bei der Einwahl die DNS-Server-Adresse(n) nicht automatisch überträgt, wählen Sie **Use the following DNS servers** und geben Sie hier die Adresse(n) ein.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

4. Haben Sie einen BigPond-Kabelzugang (oder Heartbeat-Signal), wählen Sie **BigPond Cable** und geben Sie folgende Parameter ein (Bild 4-16):

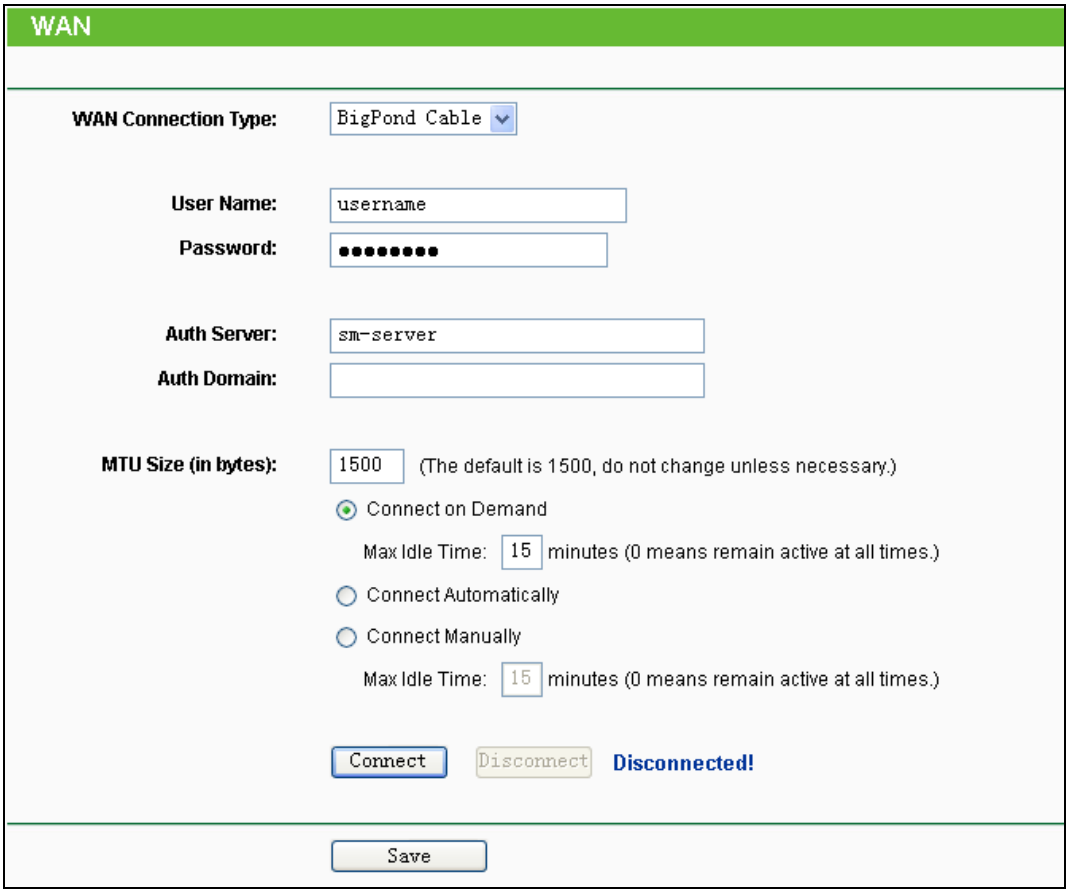


Bild 4-16 WAN – BigPond Cable

- **User Name/Password -** Geben Sie Ihren Benutzernamen und Ihr Passwort ein, so wie Sie sie von Ihrem ISP erhalten haben. Hier wird zwischen Groß- und Kleinschreibung unterschieden.
- **Auth Server -** Geben Sie hier die IP-Adresse oder den Hostnamen des Authentifizierungsservers ein.
- **Auth Domain -** Geben Sie hier den Domänensuffixservernamen basierend auf Ihrem Standort ein, z.B.:

NSW / ACT - **nsw.bigpond.net.au**
VIC / TAS / WA / SA / NT - **vic.bigpond.net.au**
QLD - **qld.bigpond.net.au**

- **MTU Size -** Die MTU-Größe (**M**aximum **T**ransmission **U**nit) liegt bei den meisten Ethernet-Netzen bei 1500 Byte. Es wird nicht empfohlen, diesen Wert zu ändern, wenn Ihr ISP dies nicht erfordert.
- **Connect on Demand -** In diesem Modus wird die Internetverbindung nach einer konfigurierbaren Dauer der Inaktivität (**Max Idle Time**) getrennt und bei Bedarf erneut hergestellt werden. Soll Ihre Internetverbindung ständig aktiv sein, geben Sie hier 0 als **Max Idle Time** ein. Andernfalls geben Sie die maximale Leerlaufzeit in min an.
- **Connect Automatically -** Neu verbinden, nachdem die Verbindung getrennt wurde.
- **Connect Manually -** Mit der Schaltfläche **Connect**/**Disconnect** können Sie die Verbindung augenblicklich von Hand herstellen oder trennen. Auch dieser Modus unterstützt die Funktion der **Max Idle Time**, genau wie **Connect on Demand**.

  Klicken Sie **Connect** um augenblicklich eine Verbindung herzustellen und **Disconnect**, um die Verbindung augenblicklich zu trennen.

Vorsicht: Die Verbindung wird unter Umständen nicht getrennt, nämlich dann, wenn einige Applikationen im Hintergrund Datenverkehr erzeugen.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

5. Benutzen Sie eine L2TP-Verbindung, wählen Sie bitte **L2TP/Russia L2TP** aus. Folgende Parameter sollten nicht fehlen (Bild 4-17):

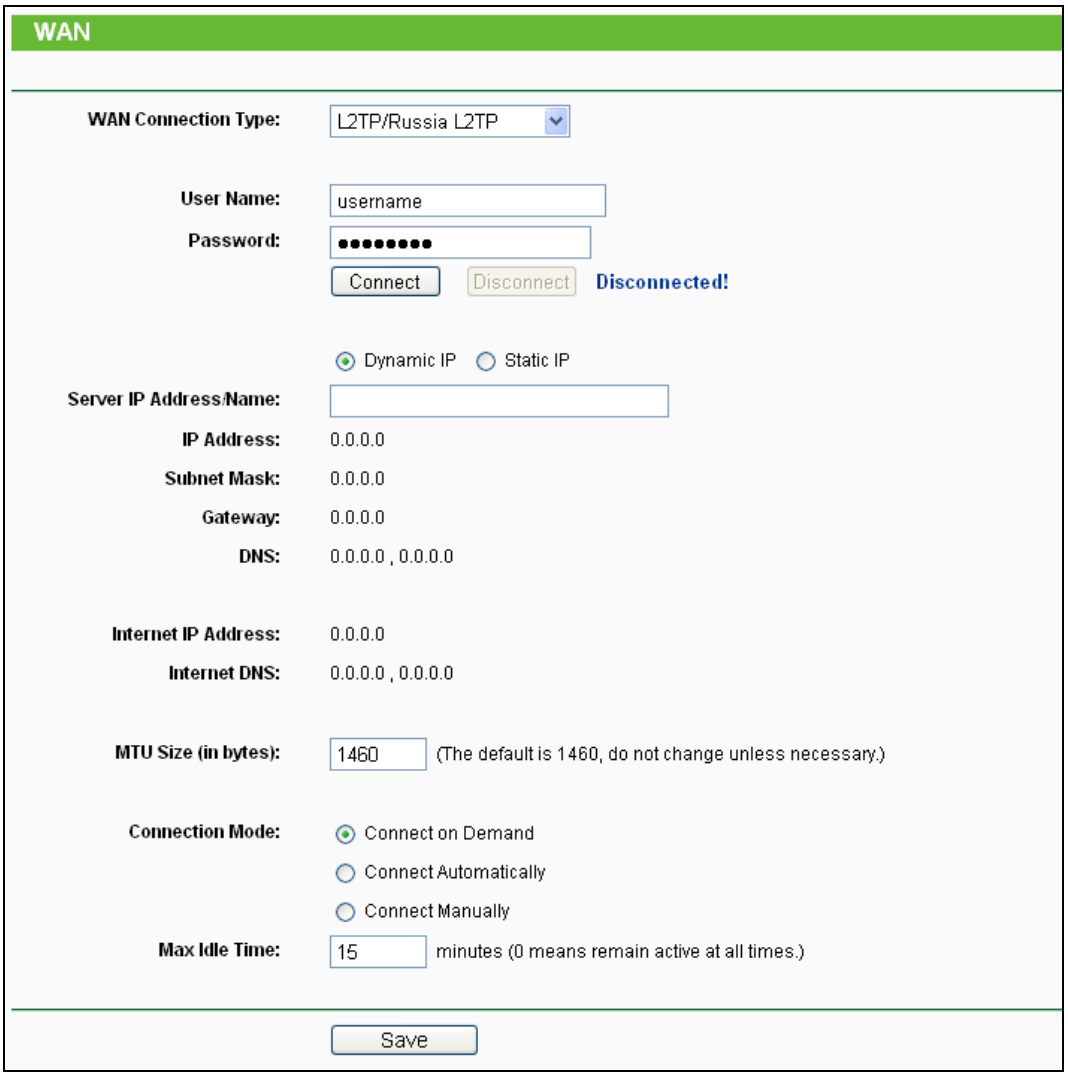


Bild 4-17 L2TP-Einstellungen

- **User Name/Password -** Geben Sie den Benutzernamen und das Passwort ein, so wie Sie sie von Ihrem ISP erhalten haben. Hier wird auf Groß-/Kleinschreibung geachtet.
- **Dynamic IP/Static IP -** Wählen Sie dies anhand der Vorgabe Ihres ISP aus. Klicken Sie **Connect**, um augenblicklich eine Verbindung herzustellen. Klicken Sie **Disconnect**, um die Verbindung augenblicklich zu trennen.
- **Connect on Demand -** Sie können den Router so konfigurieren, dass er nach einer gewissen Zeitspanne der Inaktivität (**Max Idle Time**) die Internetverbindung trennt. **Connect on Demand** erlaubt es dem Router, nach so einer Trennung die Verbindung automatisch wiederherzustellen, sobald Sie erneut versuchen, auf das Internet zuzugreifen. Soll Ihre Internetverbindung dauerhaft aktiv bleiben, geben Sie in das Feld **Max Idle Time** 0 ein. Ansonsten geben Sie die Zeitspanne ein, nach deren Ablauf die Internetverbindung getrennt werden soll.

  Vorsicht: Die Verbindung wird unter Umständen nicht getrennt, nämlich dann, wenn einige Applikationen im Hintergrund Datenverkehr erzeugen
- **Connect Automatically -** Nach Trennung automatisch wiederverbinden.

- **Connect Manually -** Mit dieser Option verbindet der Router sich nur auf manuelle Betätigung hin. Nach der definierten Inaktivitätszeitspanne (**Max Idle Time**) trennt er die Verbindung und stellt sie bis zum nächsten manuellen Verbinden nicht wieder her. Soll die Verbindung dauerhaft bestehen, geben Sie als **Max Idle Time** 0 ein. Ansonsten geben Sie die Zeitspanne ein, nach deren Ablauf die Internetverbindung getrennt werden soll.

Vorsicht: Die Verbindung wird unter Umständen nicht getrennt, nämlich dann, wenn einige Applikationen im Hintergrund Datenverkehr erzeugen.

6. Möchten Sie eine PPTP-Verbindung nutzen, wählen Sie die Option **PPTP/Russia PPTP** aus. Es sollten folgende Parameter eingegeben werden (Bild 4-18):

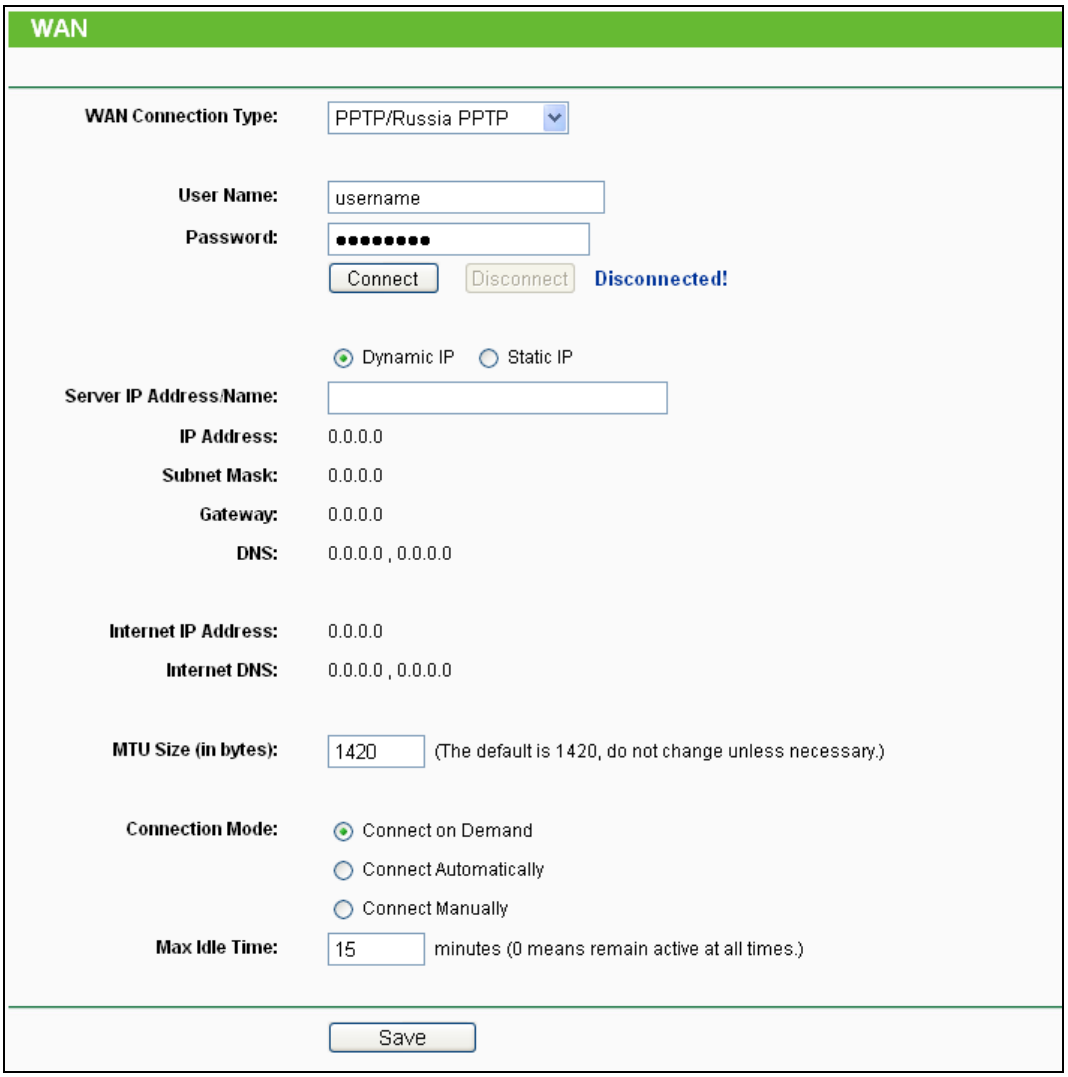


Bild 4-18 PPTP-Einstellungen

- **User Name/Password -** Geben Sie den Benutzernamen und das Passwort ein, so wie Sie sie von Ihrem ISP erhalten haben. Hier wird auf Groß-/Kleinschreibung geachtet.

- **Dynamic IP/Static IP -** Wählen Sie dies anhand der Vorgabe Ihres ISP aus und geben Sie die IP-Adresse oder den Domänennamen Ihres ISPs aus.

Haben Sie **Static IP** gewählt und den Domänennamen eingegeben, sollten Sie auch den

DNS-Server angeben. Klicken Sie am Schluss **Save**.

Klicken Sie **Connect**, um augenblicklich eine Verbindung herzustellen. Klicken Sie **Disconnect**, um die Verbindung augenblicklich zu trennen.

- **Connect on Demand -** Sie können den Router so konfigurieren, dass er nach einer gewissen Zeitspanne der Inaktivität (**Max Idle Time**) die Internetverbindung trennt. **Connect on Demand** erlaubt es dem Router, nach so einer Trennung die Verbindung automatisch wiederherzustellen, sobald Sie erneut versuchen, auf das Internet zuzugreifen. Soll Ihre Internetverbindung dauerhaft aktiv bleiben, geben Sie in das Feld **Max Idle Time** 0 ein. Ansonsten geben Sie die Zeitspanne ein, nach deren Ablauf die Internetverbindung getrennt werden soll.

  Vorsicht: Die Verbindung wird unter Umständen nicht getrennt, nämlich dann, wenn einige Applikationen im Hintergrund Datenverkehr erzeugen

- **Connect Automatically -** Nach Trennung automatisch wiederverbinden.

- **Connect Manually -** Mit dieser Option verbindet der Router sich nur auf manuelle Betätigung hin. Nach der definierten Inaktivitätszeitspanne (**Max Idle Time**) trennt er die Verbindung und stellt sie bis zum nächsten manuellen Verbinden nicht wieder her. Soll die Verbindung dauerhaft bestehen, geben Sie als **Max Idle Time** 0 ein. Ansonsten geben Sie die Zeitspanne ein, nach deren Ablauf die Internetverbindung getrennt werden soll.

  Vorsicht: Die Verbindung wird unter Umständen nicht getrennt, nämlich dann, wenn einige Applikationen im Hintergrund Datenverkehr erzeugen.

Bemerkung:

Wenn Sie nicht wissen, welcher Verbindungstyp auszuwählen ist, klicken Sie **Detect**, damit der Router versucht, ihn automatisch auszuwählen. Um sicherzugehen, dass der automatisch gewählte Verbindungstyp stimmt, setzen Sie sich bitte mit Ihrem ISP in Verbindung. Der Router ist in der Lage, folgende Verbindungstypen zu erkennen:

- **PPPoE -** PPPoE, benötigt Benutzernamen und Passwort.
- **Dynamic IP -** Zuweisung einer IP-Adresse.
- **Static IP -** Statische IP-Adresse.

Der Router kann keine PPTP-, L2TP- oder BigPond-Verbindungen erkennen. Haben Sie eine solche, konfigurieren Sie diese bitte von Hand.

4.5.4 MAC Clone

Im Menü **Network** → **MAC Clone** können Sie die MAC-Adresse des WAN-Ports setzen, Bild 4-19:

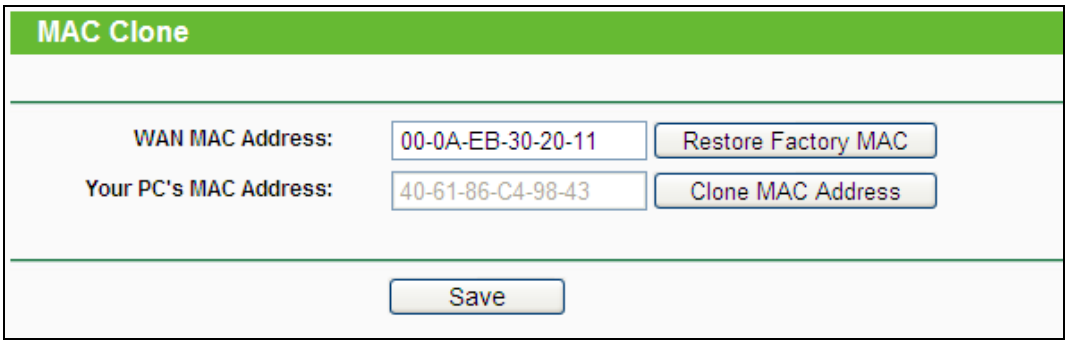


Bild 4-19 MAC-Adresse klonen

Einige ISPs verlangen eine Registrierung Ihrer MAC-Adresse. Dies ist jedoch sehr selten.

- **WAN MAC Address -** Die aktuelle MAC-Adresse des WAN-Ports. Verlangt Ihr ISP eine Registrierung Ihrer MAC-Adresse, geben Sie die registrierte MAC-Adresse hier im Format „XX-XX-XX-XX-XX-XX“ („X“ steht hierbei für eine Hexadezimalziffer) ein.
- **Your PC's MAC Address -** Zeigt die MAC-Adresse des PCs, an dem Sie gerade sitzen. Wird diese MAC-Adresse verlangt, können Sie sie mittels **Clone MAC Address** in das Feld **WAN MAC Address** übertragen.

Klicken Sie **Restore Factory MAC** um die Original-MAC-Adresse des WAN-Ports wiederherzustellen.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

Bemerkung:

Über die MAC-Adress-Klon-Funktionalität kann nur aus dem LAN verfügt werden.

4.5.5 LAN

Wählen Sie **Network** → **LAN**. Dann können Sie die LAN-IP-Parameter wie unten beschrieben konfigurieren.

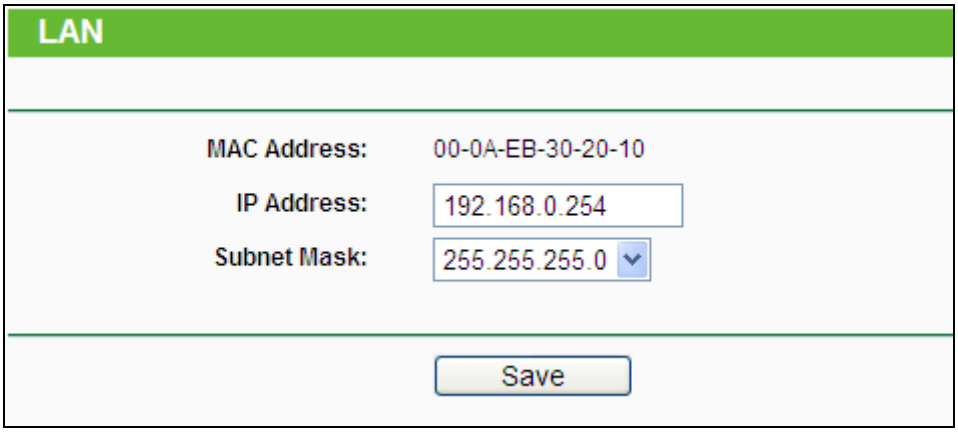


Bild 4-20 LAN

- **MAC Address -** Die physische Adresse des Routers, wie sie vom LAN aus gesehen werden kann. Diese kann nicht geändert werden.

- **IP Address -** Hier können Sie die Router-IP-Adresse festlegen (Standard: 192.168.1.1).
- **Subnet Mask -** Ein Adresscode, der die Größe Ihres Netzes angibt. Normalerweise ist die Subnetzmaske 255.255.255.0.

Bemerkungen:

1) Ändern Sie die LAN-IP-Adresse, muss ab dann die neue IP-Adresse verwendet werden, um den Router zu administrieren.
2) Liegt die neue LAN-IP-Adresse in einem anderen Subnetz als die alte, ändert der Adresspool des DHCP-Servers sich automatisch entsprechend, während die Einstellungen zu Virtuellen Servern und DMZ-Host neu konfiguriert werden müssen.

4.6 Wireless

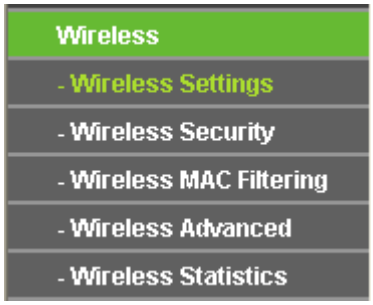


Bild 4-21 Wireless-Menü

Im WLAN-Menü gibt es fünf Untermenüs (Bild 4-21): **Wireless Settings**, **Wireless Security, Wireless MAC Filtering, Wireless Advanced** und **Wireless Statistics**.

4.6.1 Wireless Settings

Im Menü **Wireless** → **Wireless Settings** können Sie die Grundeinstellungen Ihres WLANs tätigen.

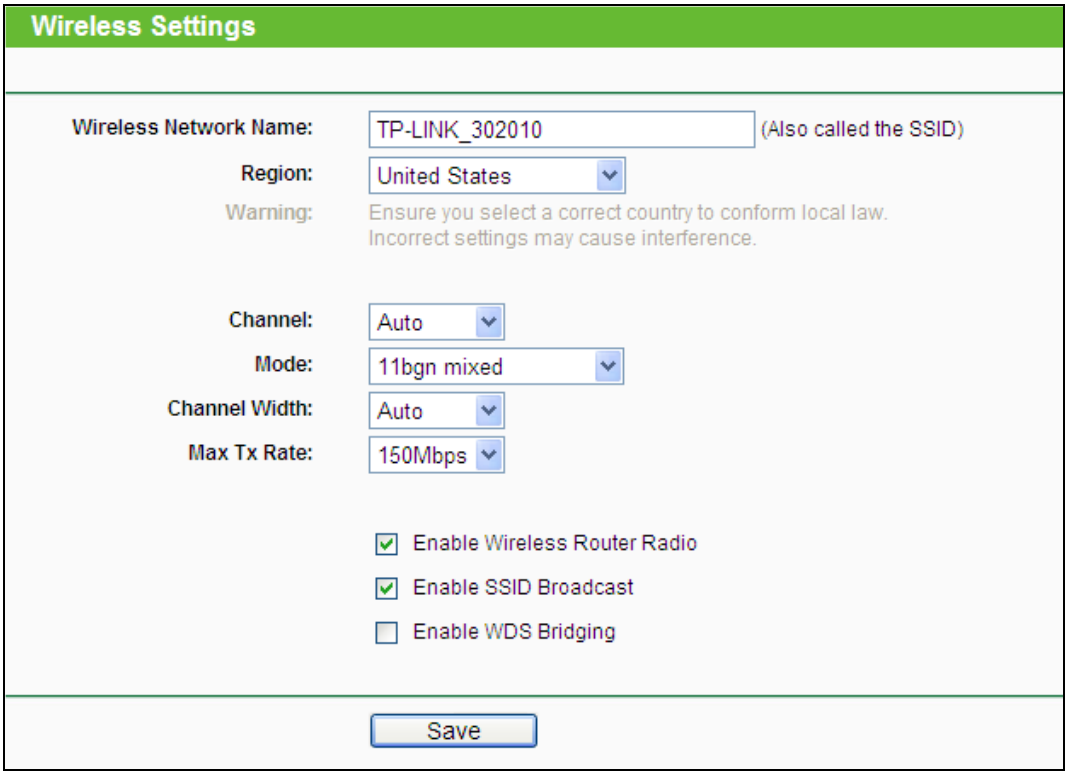
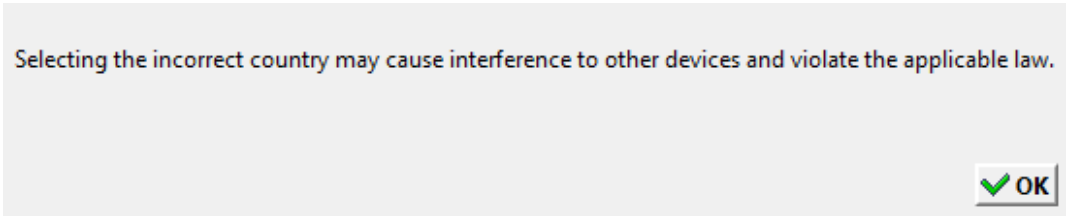


Bild 4-22 Wireless Settings

- **Wireless Network Name -** Geben Sie einen Namen von bis zu 32 Zeichen an (SSID). Dieser muss von allen anderen Geräten in Ihrem WLAN verwendet werden. Standardwert ist TP-LINK, doch sollte dieser geändert werden. Hier wird zwischen Groß- und Kleinschreibung unterschieden, z.B. bezeichnen *TP-LINK* und *tp-link* unterschiedliche Netze.

- **Region -** Wählen Sie hier den Standort des Routers aus. Eine falsche Auswahl könnte gegen geltende Gesetze verstoßen. Ist Ihre Region nicht aufgeführt, wenden Sie sich bitte an die zuständigen Behörden. Standardeinstellung ist **United States**, so dass hier in der Regel eine Anpassung vorgenommen werden muss. In Deutschland setzen Sie bitte **Germany**, in der Schweiz **Switzerland** und in Österreich **Austria** ein.

  Bei einer Änderung dieses Wertes und Klick auf **Save** sehen Sie folgende Meldung, die Sie mit Klick auf **OK** bestätigen müssen.



Dialogfenster

Bemerkung:

Aufgrund gesetzlicher Restriktionen verfügt die Nordamerika-Version des Produktes nicht über diese Option.

.

- **Channel -** Dieses Feld legt die Betriebsfrequenz des Routers fest. In der Standardeinstellung **Auto** wählt der Router automatisch einen Kanal aus. Es ist nicht erforderlich, diese zu ändern, es sei denn, Sie stellen Interferenzen von einem nahen Accesspoint fest.
- **Mode -** Wählen Sie den gewünschten Modus aus. Standardwert: **11bgn mixed**.

  11b only - Wählen Sie dies nur aus, wenn alle Clients in Ihrem WLAN 802.11b-Clients sind.

  11g only - Wählen Sie dies nur aus, wenn alle Clients in Ihrem WLAN 802.11g-Clients sind.

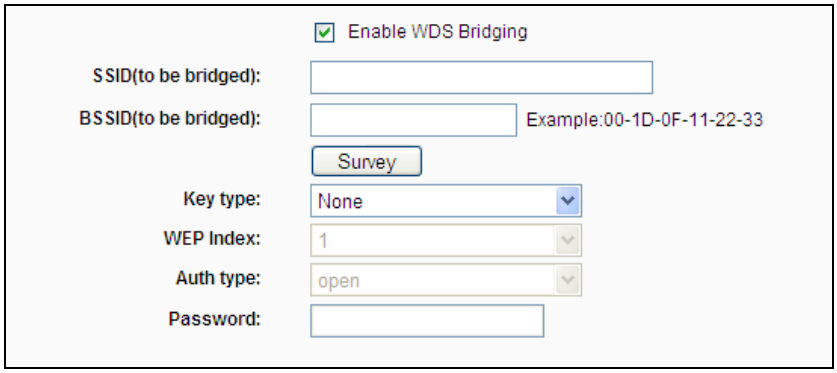
  11n only - Wählen Sie dies nur aus, wenn alle Clients in Ihrem WLAN 802.11n-Clients sind.

  11bg mixed - Diese Option ist die richtige, wenn Sie sowohl 802.11b- als auch 802.11g-Clients in Ihrem Netz betreiben.

  11bgn mixed - Wählen Sie diese Option in allen anderen Fällen (empfohlene Standardeinstellung). Damit können sowohl b- und g- als auch n-Clients Verbindung aufnehmen.
- **Channel width -** Wählen Sie die Kanalbreite aus. Standardeinstellung ist **Automatic**.

  Bemerkung:

  Diese Option kann nicht geändert werden, wenn über **Modus** 802.11n-Clients ausgeschlossen wurden. Der Kanalbreitenwert ist dann auf 20MHz eingestellt.
- **Max Tx Rate -** Die WLAN-Datentransferrate kann hiermit begrenzt werden.
- **Enable Wireless Router Radio -** Die WLAN-Funktion des Routers kann ein- und ausgeschaltet werden, um drahtlosen Zugriff zu ermöglichen oder zu verhindern.
- **Enable SSID Broadcast -** Wird dies ausgewählt, sendet der Router den WLAN-Namen (SSID) aus und Clients können das Netz in ihrer Übersicht anzeigen.
- **Enable WDS Bridging -** Hiermit können Sie die WDS-Brücke aktivieren. Damit kann der Router mittels Bridging mehrere WLANs miteinander verbinden. Ist die Option gewählt, müssen diese Felder ausgefüllt werden:



- **SSID(to be bridged)** - Die SSID des APs, zu dem der Router sich als Client verbinden soll. Sie können die **SSID** mit Hilfe der **Survey**-Funktion eintragen.
- **BSSID(to be bridged)** - Die BSSID des APs, zu dem der Router sich als Client verbinden soll. Sie können die **BSSID** mit Hilfe der **Survey**-Funktion eintragen.
- **Survey** - Klicken Sie hier, um Accesspoints auf dem aktuellen Kanal zu suchen.
- **Key type** - Diese Option wird entsprechend den Sicherheitseinstellungen des APs gesetzt. Es wird empfohlen, die gleichen Einstellungen zu verwenden.
- **WEP Index** - Der Index des verwendeten WEP-Schlüssels.
- **Auth Type** - Der Authentifizierungstyp des Root-Accesspoints.
- **Password** - Benötigt der Root-Accesspoint ein Passwort, muss dieses hier eingetragen werden.

4.6.2 Wireless Security

Im Menü **Wireless** → **Wireless Security** können Sie die Sicherheitseinstellungen ändern.

Der Router verfügt über fünf Möglichkeiten, das WLAN zu verschlüsseln: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), WPA2-PSK (Pre-Shared Key) und WPA-PSK (Pre-Shared Key).

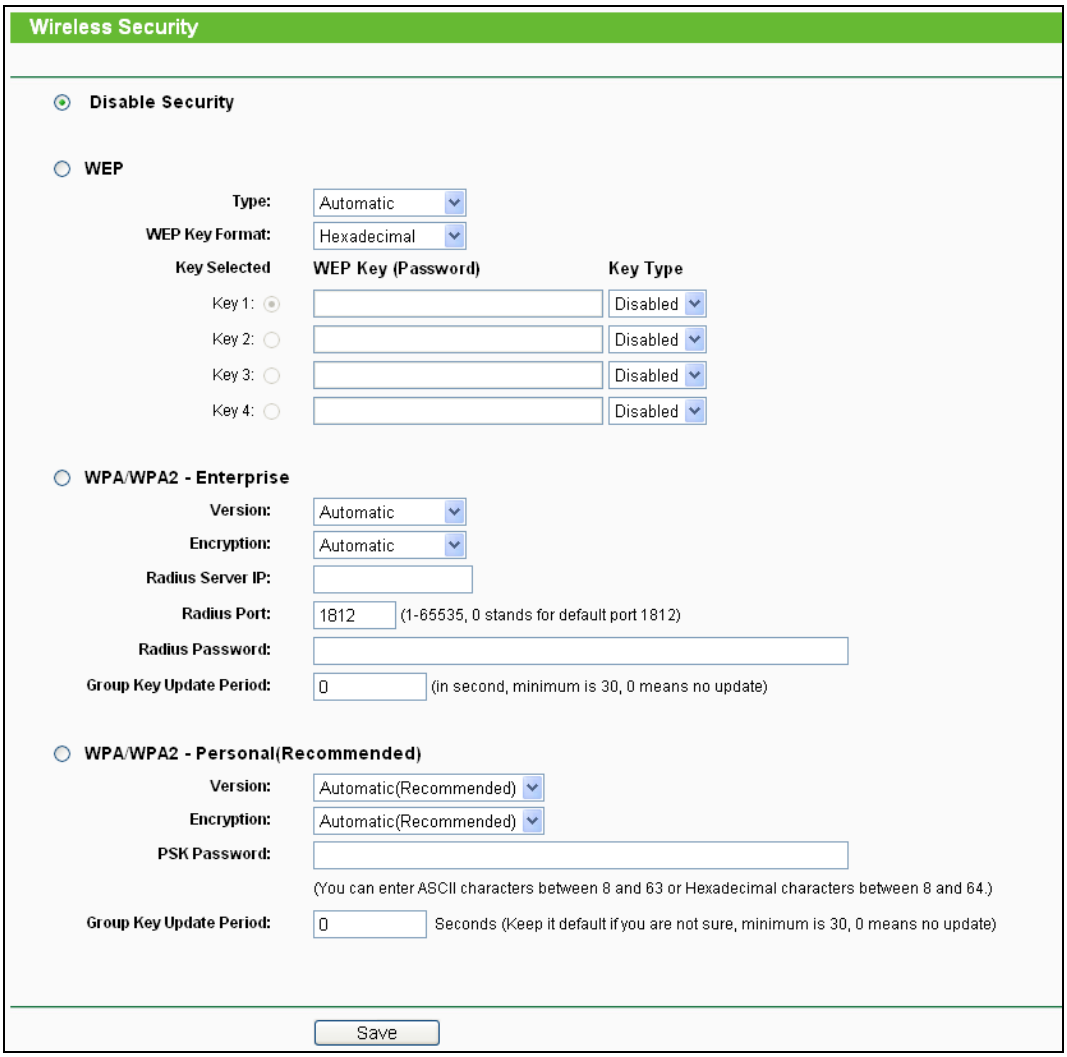


Bild 4-23 Drahtlose Sicherheit

- **Disable Security -** Möchten Sie keine Verschlüsselung einsetzen, wählen Sie diese Option. Es wird aber wärmstens empfohlen, dass Sie Ihr WLAN verschlüsseln.
- **WEP -** WEP basierend auf 802.11-Authentifizierung verwenden. Wählen Sie diese Option aus, wird in Rot die in Bild 4-24 sichtbare Meldung eingeblendet.

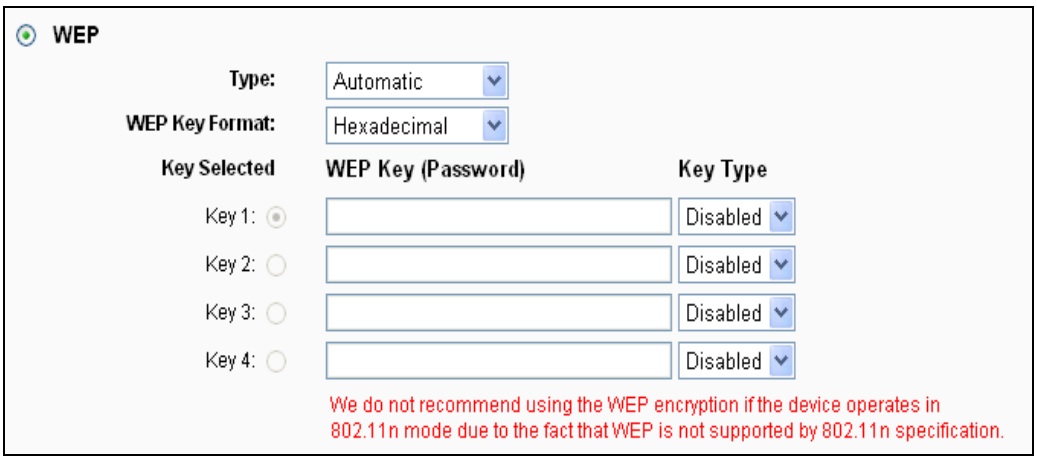


Bild 4-24 WEP mit Wireless-N

- **Type -** Der WEP-Authentifizierungstyp kann auf **Automatic** (Standard), **Open System** oder **Shared Key** eingestellt werden. **Automatic** lässt den Client den Typ auswählen.
- **WEP Key Format -** Es können die Formate **Hexadecimal** und **ASCII** ausgewählt werden. Im Fall von **Hexadecimal** können Sie eine Folge Hexadezimalziffern (0..9, a..f) in der angegebenen Länge eingeben. Bei **ASCII**-Format können Sie alle Zeichen nehmen.
- **WEP Key -** Wählen Sie aus, welcher der vier Schlüssel verwendet werden soll, und geben Sie den passenden WEP-Schlüssel ein. Stellen Sie sicher, dass Sie diese auf allen Geräten in Ihrem WLAN korrekt eingeben.
- **Key Type -** Hier können Sie die WEP-Schlüssellänge (64 Bit, 128 Bit oder 152 Bit) auswählen. **Disabled** sagt aus, dass der eingegebene WEP-Schlüssel ungültig ist.

  Bei **64-Bit**-Verschlüsselung sind 10 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 5 ASCII-Zeichen einzugeben.

  Bei **128-Bit**-Verschlüsselung sind 26 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 13 ASCII-Zeichen einzugeben.

  Bei **152-Bit**-Verschlüsselung sind 32 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 16 ASCII-Zeichen einzugeben.

  ☞ **Bemerkung:**

  Wird hier kein Schlüssel angegeben, wird die WLAN-Sicherheit nicht aktiviert, selbst wenn dies so eingestellt ist.

➢ **WPA /WPA2 - Enterprise -** Basiert auf einem Radius-Server.

- **Version -** Hier können Sie die WPA-Version auswählen. Die Standardeinstellung ist **Automatic**, womit entsprechend der Fähigkeiten/Anforderungen der Clients entweder mit **WPA** (Wi-Fi Protected Access) oder **WPA2** (WPA Version 2) gearbeitet wird.
- **Encryption -** Hier können Sie zwischen **Automatic**, **TKIP** und **AES** wählen**.**
- ☞ **Bemerkung:**
- Wählen Sie hier TKIP-Verschlüsselung aus, wird Folgendes in Rot gemeldet (Bild 4-25).

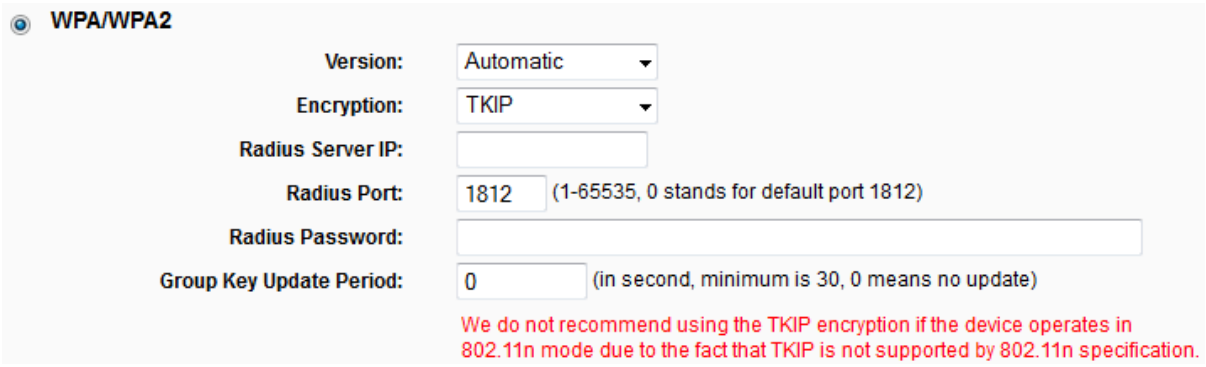


Bild 4-25 TKIP mit Wireless-N

- **Radius Server IP -** IP-Adresse des Radius-Servers.
- **Radius Port -** Port, auf dem der Radius-Dienst läuft.
- **Radius Password -** Das Passwort des Radius-Servers.
- **Group Key Update Period -** Geben Sie die Dauer der Gültigkeit eines einzigen Gruppenschlüssels in Sekunden an. Dieser Wert sollte 0 (=deaktiviert) oder mindestens 30 betragen. Empfohlen sind Werte von 500 oder 600.

➢ **WPA/WPA2 – Personal (Recommended) -** WPA/WPA2-Authentifizierung, basierend auf einem Passwort. Empfohlene Einstellung.

- **Version -** WPA-PSK-Version. Die Standardeinstellung ist **Automatic**, womit entsprechend der Fähigkeiten/Anforderungen der Clients entweder mit **WPA-PSK** (Wi-Fi Protected Access) oder **WPA2-PSK** (WPA Version 2) gearbeitet wird.
- **Encryption -** Hier können Sie zwischen **Automatic**, **TKIP** und **AES** wählen.
- ☞ **Bemerkung:**

  Wählen Sie hier TKIP-Verschlüsselung aus, wird Folgendes in Rot gemeldet (Bild 4-26).

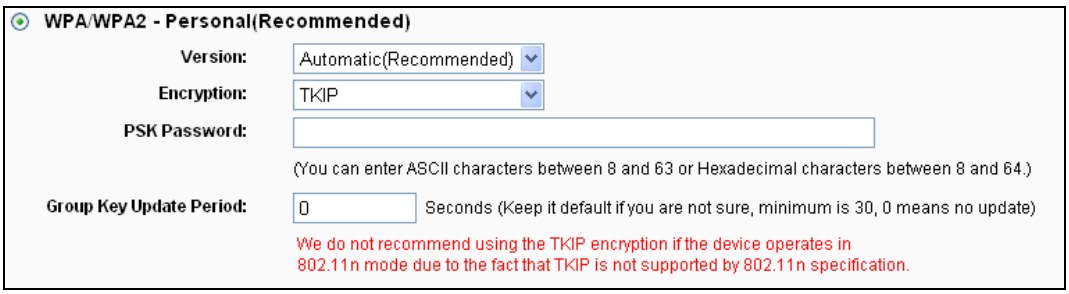


Bild 4-26 TKIP mit Wireless-N

- **PSK Password -** Das Passwort kann 8 bis 63 ASCII- oder 8 bis 64 Hexadezimalzeichen lang sein.
- **Group Key Update Period -** Geben Sie die Dauer der Gültigkeit eines einzigen Gruppenschlüssels in Sekunden an. Dieser Wert sollte 0 (=deaktiviert) oder mindestens 30 betragen. Empfohlen sind Werte von 500 oder 600.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

4.6.3 Wireless MAC Filtering

Auf dieser Seite wird die MAC-Adressfilterung konfiguriert (Bild 4-27).

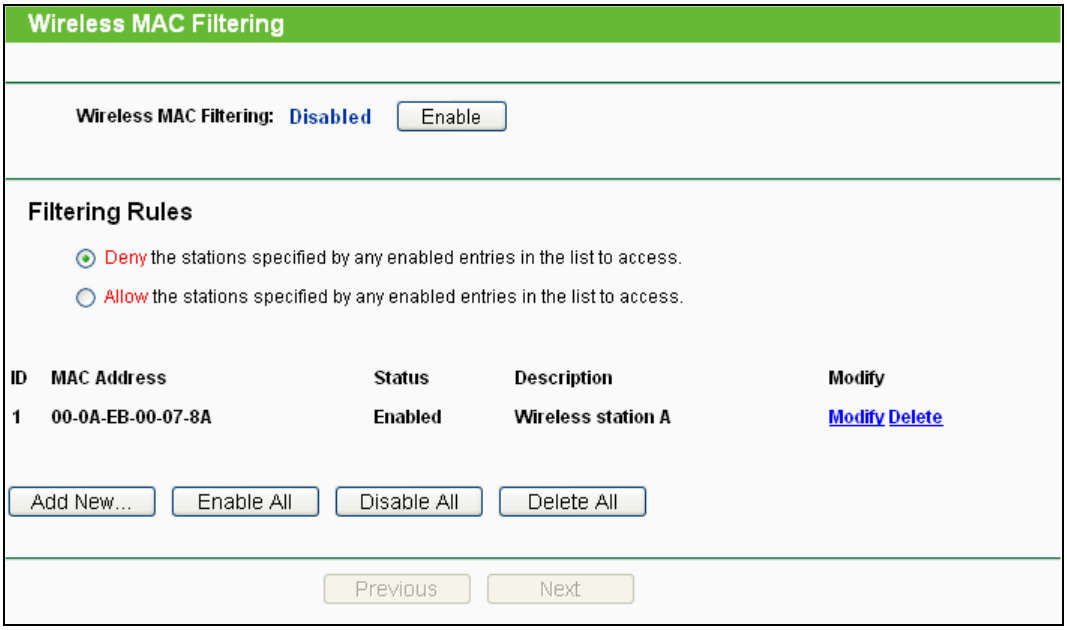


Bild 4-27 MAC-Adressfilterung

Um WLAN-Geräte nach MAC-Adresse zu filtern, klicken Sie **Enable**. Im andern Fall wählen Sie **Disabled** (Standardeinstellung).

- **MAC Address -** Die MAC-Adresse des WLAN-Gerätes, das Sie filtern möchten.
- **Status -** Der Status dieses Eintrags (**Enabled** oder **Disabled**).
- **Description -** Eine einfache Beschreibung der WLAN-Station.

Um einen Eintrag zur MAC-Adressfilterungsliste hinzuzufügen, klicken Sie **Add New…**. Die Seite **Add or Modify Wireless MAC Address Filtering entry** erscheint (Bild 4-28):

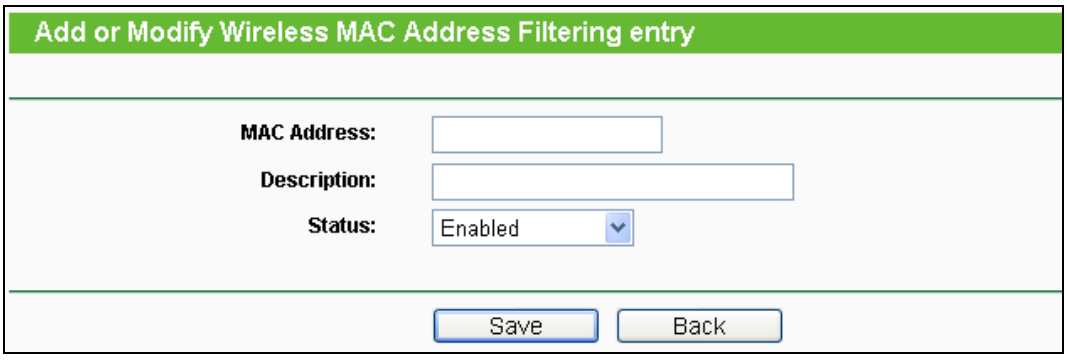


Bild 4-28 Eintrag in der MAC-Adressfilterungsliste erstellen oder bearbeiten

Um einen Eintrag in der MAC-Adressfilterungsliste zu erstellen oder zu bearbeiten:

1. Geben Sie die entsprechende MAC-Adresse in das Feld **MAC Address** im Format „XX-XX-XX-XX-XX-XX“ ein („X“ repräsentiert eine Hexadezimalziffer). Beispiel: „00-0A-EB-B0-00-0B“.
2. Geben Sie eine frei wählbare Beschreibung der WLAN-Station (Bsp.: „Kurts PC“) in das Feld **Description** ein.

3. **Status - Enabled** oder **Disabled** sind auswählbar.

4. Klicken Sie **Save**, um den Eintrag zu speichern.

Um einen Eintrag zu bearbeiten oder zu löschen, tun Sie bitte Folgendes:

1. Klicken Sie für den entsprechenden Eintrag **Modify**, wenn Sie ihn bearbeiten wollen und **Delete**, um ihn zu löschen.

2. Bearbeiten Sie die Informationen, falls erforderlich
3. Klicken Sie **Save**.

Klicken Sie **Enable All**, um alle Einträge zu aktivieren.

Klicken Sie **Disable All**, um alle Einträge zu deaktivieren.

Klicken Sie **Delete All,** um alle Einträge zu löschen.

Klicken Sie **Next**, um zur nächsten Seite zu blättern oder **Previous**, um zur vorigen Seite zurückzukehren.

Beispiel: Sollen nur die beiden PCs mit den MAC-Adressen 00-0A-EB-00-07-8A und 00-0A-EB-00-23-11 auf das WLAN zugreifen können, sollte die Liste **Wireless MAC Filtering** so eingerichtet werden:

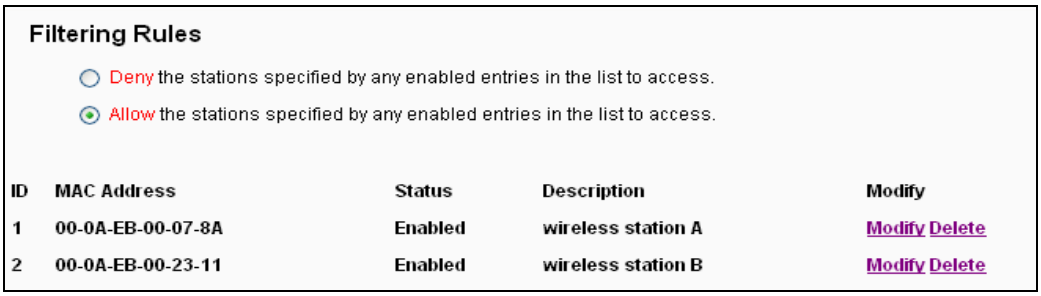
1. Klicken Sie **Enable**, um die MAC-Adressfilterfunktion zu aktivieren.

2. Wählen Sie **Allow the stations specified by any enabled entries in the list to access** aus.

3. Löschen oder deaktivieren Sie alle bereits bestehenden Einträge.

4. Klicken Sie **Add New...** und geben Sie die MAC-Adresse 00-0A-EB-00-07-8A in das Feld **MAC Address** und eine Beschreibung in das Feld **Description** ein. Wählen Sie **Enabled** als **Status**. Klicken Sie **Save**. Wiederholen Sie diesen Schritt für die MAC-Adresse 00-0A-EB-00-23-11.

   Die Filterregelliste sollte nun so aussehen:



4.6.4 Wireless Advanced

Unter **Wireless** → **Wireless Advanced** können Sie die erweiterten WLAN-Einstellungen

tätigen.

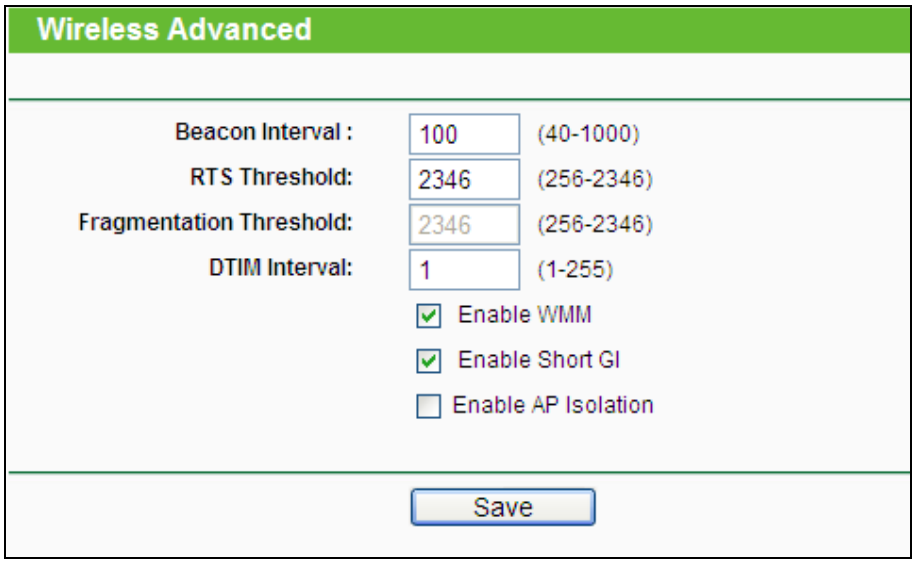


Bild 4-29 Wireless Advanced

- **Beacon Interval -** Geben Sie einen Wert von 20 bis 1000 (Millisek.) ein. Ortungspakete werden vom Router zur Synchronisierung des WLANs ausgesendet. Standardwert ist 100.
- **RTS Threshold -** Hier können Sie den RTS(Request to Send)-Grenzwert angeben. Ist ein Paket größer als dieser Wert, sendet der Router RTS-Frames zu einer bestimmten Empfangsstation, um den Versand eines Datenframes abzustimmen. Standardwert: 2346.
- **Fragmentation Threshold -** Dieser Wert ist die Maximalgröße, ab der Pakete fragmentiert werden. Eine zu niedrige Einstellung dieses Wertes könnte sich negativ auf die Performance auswirken. Standardwert: 2346 (empfohlen).
- **DTIM Interval -** Dieser Wert bezeichnet die Intervalllänge zwischen zwei aufeinanderfolgenden Delivery Traffic Indication Messages (DTIMs). Ein DTIM-Feld ist ein Countdown, der die Clients des nächsten Fensters anweist, auf Broadcasts und Multicasts zu hören. Hat der Router Broadcasts oder Multicasts für verbundene Clients gepuffert, sendet er den nächsten DTIM. Sie können diese Dauer in Ortungsintervallen (1..255) angeben. Standard ist 1, d.h. das DTIM-Intervall ist genauso lang wie ein Ortungsintervall.
- **Enable WMM - WMM** garantiert, dass Nachrichten hoher Priorität bevorzugt übertragen werden. Es wird wärmstens empfohlen, diese Option aktiviert zu lassen.
- **Enable Short GI -** Die Verwendung dieser Funktion wird empfohlen, da sie die Übertragungskapazitäten auf Kosten der Schutzintervallzeit vergrößert.
- **Enabled AP Isolation -** Diese Funktion kann WLAN-Stationen innerhalb Ihres Netzes untereinander unsichtbar machen. Damit können Sie nur mit dem Router, aber nicht miteinander kommunizieren. AP-Isolation ist standardmäßig deaktiviert.

Bemerkung:

Sind Sie mit den Einstellungen dieser Seite nicht vertraut, sollten Sie deren Werte auf den Standardwerten eingestellt lassen. Ansonsten könnte dies sich negativ auf die Performance auswirken.

4.6.5 Wireless Statistics

Im Menü **Wireless** → **Wireless Statistics** können Sie die MAC-Adresse, den aktuellen Status, Empfangene Pakete und gesendete Pakete pro verbundener WLAN-Station einsehen.

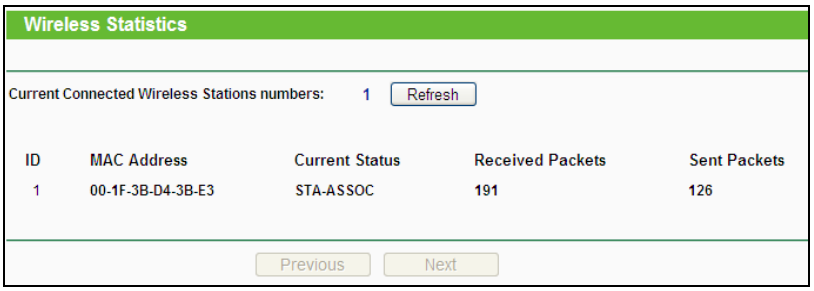


Bild 4-30 Mit dem Router verbundene WLAN-Geräte

- **MAC Address -** Die MAC-Adresse der verbundenen Station
- **Current Status -** Laufzeitstatus der verbundenen Station: **STA-AUTH**, **STA-ASSOC**, **STA-JOINED**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK**, **AP-UP**, **AP-DOWN** oder **Disconnected**
- **Received Packets -** Anzahl der durch die Station empfangenen Pakete
- **Sent Packets -** Anzahl der durch die Station gesendeten Pakete

Die auf dieser Seite angezeigten Werte können nicht geändert werden. Um die Ansicht zu aktualisieren, klicken Sie **Refresh**.

Passt die Liste der verbundenen Stationen nicht auf eine Seite, können Sie mittels **Next** und **Previous** zwischen den Seiten hin- und herblättern.

Bemerkung:

Diese Seite lädt sich alle 5 Sekunden neu.

4.7 DHCP

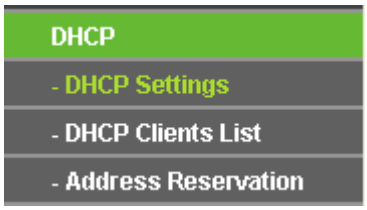


Bild 4-31 Das Menü „DHCP“

Im Menü DHCP gibt es drei Untermenüs (Bild 4-31): **DHCP Settings**, **DHCP Clients List** und

Address Reservation.

4.7.1 DHCP Settings

Im Menü **DHCP** → **DHCP Settings** können Sie den DHCP-Server konfigurieren (Bild 4-32). Der DHCP(Dynamic Host Configuration Protocol)-Server des Routers ist standardmäßig aktiv und stellt DHCP-Clients im LAN ihre TCP/IP-Konfiguration bereit.

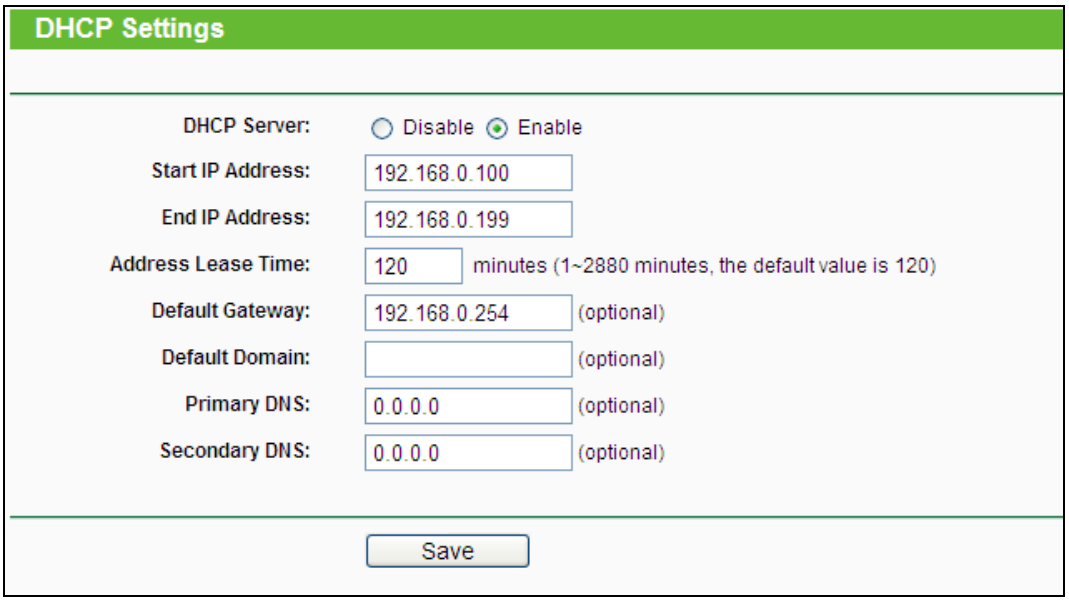


Bild 4-32 DHCP-Einstellungen

- **DHCP Server -** DHCP-Server **aktivieren** oder **deaktivieren**. Deaktivieren Sie den DHCP-Server, benötigen Sie einen anderen in Ihrem LAN oder Sie müssen die IP-Konfiguration jedes Clients in Ihrem Netz von Hand vornehmen.
- **Start IP Address -** Die erste vergebbare IP-Adresse. Standard ist 192.168.1.100.
- **End IP Address -** Die letzte IP-Adresse im Adresspool. Standard: 192.168.1.199.
- **Address Lease Time -** Die Dauer (in min.), für die ein Netzbenutzer seine IP-Konfiguration behalten darf, in Minuten. Gültig sind Werte von 1 bis 2880. Standard: 120.
- **Default Gateway -** (optional) Es wird empfohlen, hier die LAN-IP-Adresse des Routers (Standard: 192.168.1.1) einzugeben.
- **Default Domain -** (optional) Hier sollte der Domänenname Ihres Netzes eingegeben werden.
- **Primary DNS -** (optional) Geben Sie eine von Ihrem ISP erhaltene DNS-Server-IP-Adresse ein. Sollten Sie keine erhalten haben, fragen Sie bitte nach.
- **Secondary DNS -** (optional) Geben Sie hier die eventuell von Ihrem ISP erhaltene zweite DNS-Server-IP-Adresse ein, falls vorhanden.

Bemerkung:

Um den DHCP-Server nutzen zu können, müssen die Clients auf „IP-Adresse automatisch beziehen“ konfiguriert sein.

4.7.2 DHCP Clients List

Unter **DHCP → DHCP Clients List** können Sie Informationen über die gerade verbundenen DHCP-Clients abfragen (Bild 4-33).

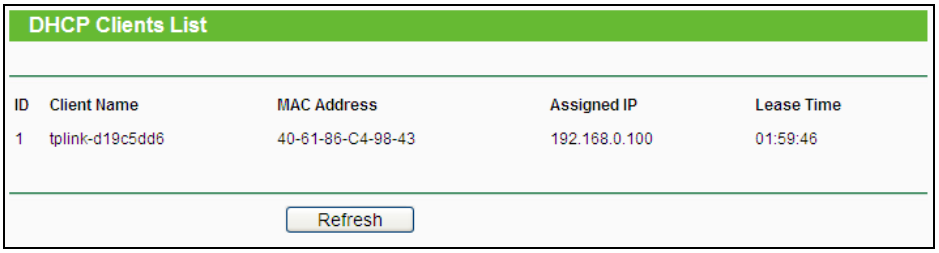


Bild 4-33 DHCP-Clientliste

- **ID -** Eine eindeutige Nummer des DHCP Clients
- **Client Name -** Name des DHCP-Clients
- **MAC Address -** MAC-Adresse des DHCP-Clients
- **Assigned IP -** Die IP-Adresse, die der Router diesem Client gegeben hat.
- **Lease Time -** Die verbleibende Zeit, die der DHCP-Client die aktuelle Konfiguration noch behalten kann. Nach Ablauf dieser Zeit bekommt dieser automatisch eine neue IP-Adresse.

Die auf dieser Seite angezeigten Werte können nicht hier direkt geändert werden. Um die Ansicht zu aktualisieren, klicken Sie **Refresh**.

4.7.3 Address Reservation

Das Menü **DHCP → Address Reservation** befasst sich mit der Reservierung von IP-Adressen für Clients (Bild 4-34). Geben Sie hier eine reservierte IP-Adresse für einen LAN-PC an, wird dieser immer diese Adresse zugeteilt bekommen. Diese Funktionalität ist hilfreich, wenn Sie einen Server im LAN betreiben wollen.

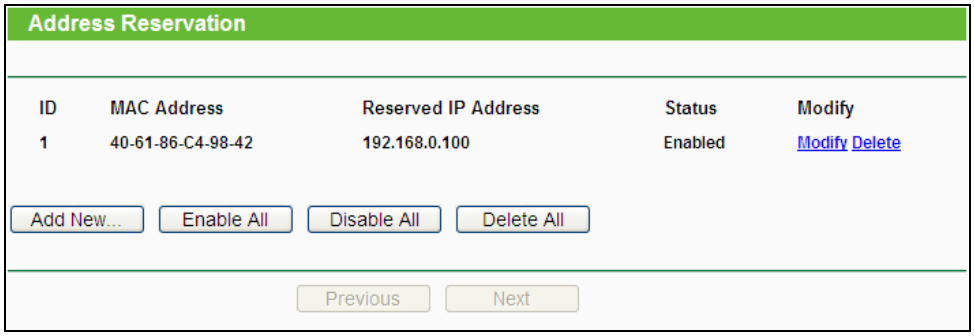


Bild 4-34 Address Reservation

- **MAC Address -** MAC-Adresse des PCs, für den Sie eine IP-Adresse reservieren möchten.
- **Assigned IP Address -** IP-Adresse, die für diesen Host reserviert wurde.
- **Status -** Status dieses Eintrags: **Enabled** (aktiv) oder **Disabled** (inaktiv).

Um IP-Adressen zu reservieren:

1. Klicken Sie **Add New…**. Bild 4-35 erscheint.
2. Geben Sie die MAC-Adresse (Format „XX-XX-XX-XX-XX-XX“) und die IP-Adresse des betreffenden Computers ein.
3. Klicken Sie **Save**, wenn Sie fertig sind.

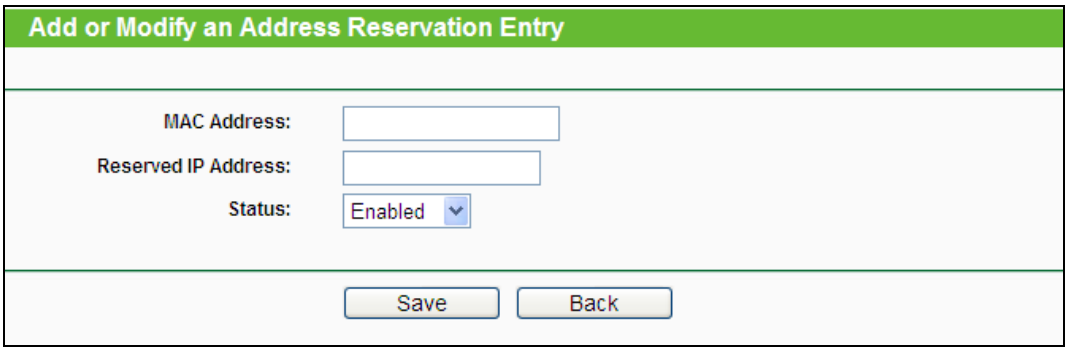


Bild 4-35 Adressreservierungseintrag hinzufügen oder bearbeiten

Um einen Eintrag zu bearbeiten oder zu löschen:

1. Klicken Sie für den zu bearbeitenden Eintrag. Klicken Sie **Delete**, wenn Sie ihn löschen möchten.
2. Bearbeiten Sie die Informationen, wie gewünscht.
3. Klicken Sie **Save**.

Klicken Sie **Enable All/Disable All**, um alle Einträge zu (de)aktivieren.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

Klicken Sie **Next**, um auf die nächste Seite zu blättern oder **Previous**, um auf die vorige Seite zurückzukehren.

4.8 Forwarding

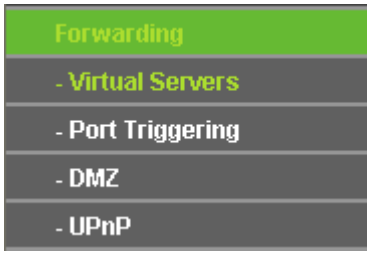


Bild 4-36 Menü **Forwarding**

Im Forwarding-Menü gibt es vier Untermenüs (Bild 4-36): **Virtual Servers**, **Port Triggering**, **DMZ** und **UPnP**.

4.8.1 Virtual Servers

Unter **Forwarding** → **Virtual Servers** können Sie virtuelle Server ansehen und bearbeiten (Bild 4-37). Virtuelle Server erlauben es, Dienste aus Ihrem LAN auch im Internet zur Verfügung zu stellen, z.B. DNS, E-Mail und FTP. Ein virtueller Server wird mittels eines Ports definiert. Alle auf diesem Port von außen ankommenden Anfragen werden auf den angegebenen Computer weitergegeben. Dieser benötigt dafür eine statische oder eine reservierte IP-Adresse, um erreichbar zu bleiben.

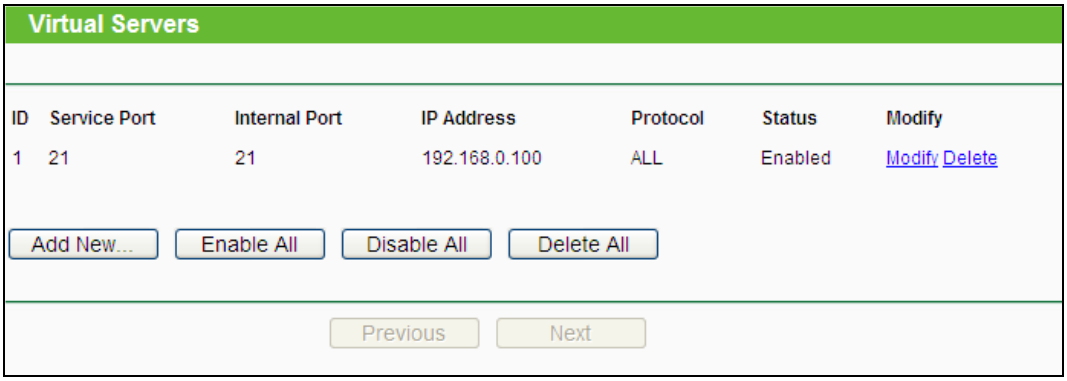


Bild 4-37 Virtual Servers

- **Service Port -** Nummern externer Ports. Hier können einzelne Ports oder Portbereiche (Format „XXX - YYY“, wobei „XXX“ die Nummer des Startports und „YYY“ die Nummer des Endports des entsprechenden Bereiches darstellt) definiert werden.
- **IP Address -** Die IP-Adresse des Servers im LAN.
- **Protocol -** Das Protokoll, das diese Anwendung einsetzt: **TCP**, **UDP** oder **All** (alle Protokolle, die der Router unterstützt).
- **Status -** Status dieses Eintrags: **Enabled** oder **Disabled**.

Um einen neuen Virtuellen Server anzulegen:

1. Klicken Sie **Add New…** (Bild 4-38).
2. Wählen Sie den Dienst, den Sie anbieten möchten, aus der Liste **Common Service Port** aus. Ist Ihr Dienst dort nicht enthalten, geben Sie einfach die Portnummer in das Feld **Service Port** ein.
3. Geben Sie die LAN-IP-Adresse des Servers in das Feld **IP Address** ein.
4. Wählen Sie das Protokoll, das diese Anwendung benutzt: **TCP**, **UDP** oder **All**.
5. Wählen Sie **Enable** aus, um den Virtuellen Server zu aktivieren.
6. Klicken Sie **Save**.

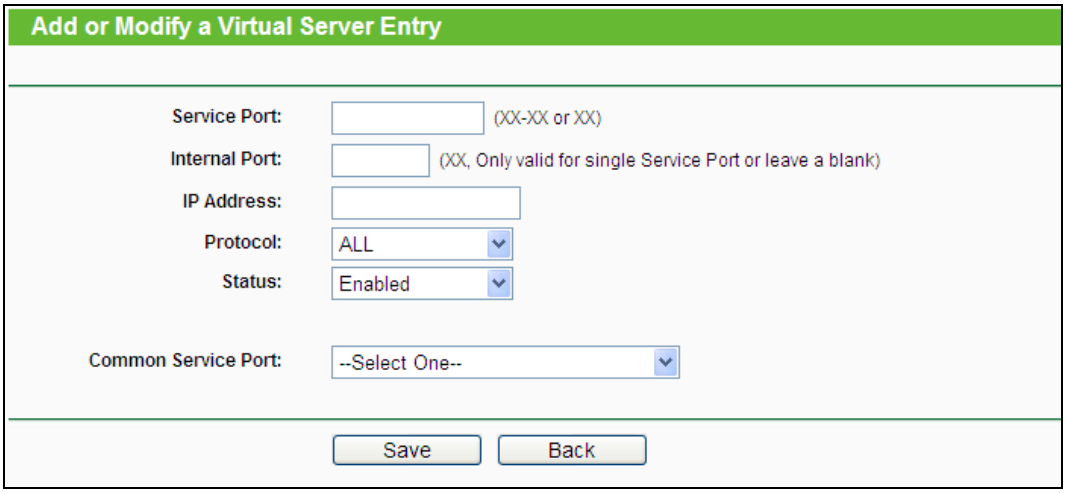


Bild 4-38 Virtuellen Server hinzufügen oder bearbeiten

☞ **Bemerkung:**

Möchten Sie auf einem Computer mehrere Dienste anbieten, legen Sie für diesen einfach mehrere Virtuelle Server an.

Um einen bestehenden Eintrag zu bearbeiten oder zu löschen:

1. Klicken Sie **Modify** für den zu bearbeitenden Eintrag. Möchten Sie ihn löschen, drücken Sie **Delete**.
2. Bearbeiten Sie die Informationen, wie gewünscht.
3. Klicken Sie **Save**.
4. Klicken Sie **Enable All/Disable All**, um alle Einträge zu (de)aktivieren.
5. Klicken Sie **Delete All**, um alle Einträge auf dieser Seite zu entfernen.
6. Klicken Sie **Next**, um auf die nächste Seite zu wechseln oder **Previous**, um auf die vorige Seite zurückzukehren.

☞ **Bemerkung:**

Wird ein Virtueller Server auf Port 80 eingerichtet, muss der Webmanagement-Port unter **Security –> Remote Management** auf einen anderen Wert als 80 gesetzt werden, z.B. 8080. Ansonsten wird es zu Konflikten kommen.

4.8.2 Port Triggering

Wählen Sie das Menü **Forwarding** → **Port Triggering**. Hier können Sie die Einstellungen zum Porttriggering ansehen und anpassen (Bild 4-39). Einige Anwendungen wie z.B. Internetspiele oder Videokonferenzen erfordern Mehrfachverbindungen. Dies ist mit einem einfachen NAT-Router nicht realisierbar. Damit dies mit einem NAT-Router funktioniert, muss auf Porttriggering zurückgegriffen werden.

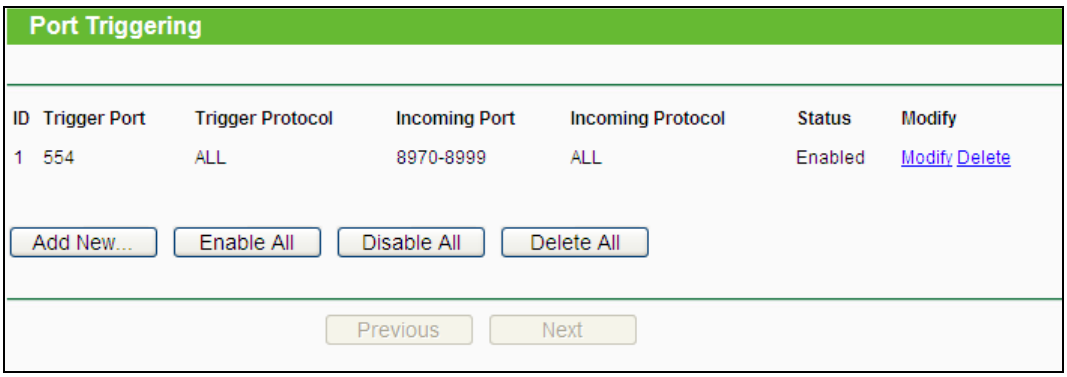


Bild 4-39 Porttriggering

Porttriggering funktioniert so:

1. Ein lokaler PC öffnet eine ausgehende Verbindung auf dem Port, der im Feld **Trigger Port** angegeben ist.
2. Der Router merkt sich diese Verbindung, öffnet die damit assoziierten **Incoming Ports** und leitet auf diesen ankommende Verbindungen an den lokalen PC weiter.
3. Hierüber kann der entfernte Host nun den lokalen PC erreichen.

- **Trigger Port -** Der Port, auf dem eine ausgehende Verbindung diese Regel auslöst.
- **Trigger Protocol -** Das Protokoll, das zur Auslösung verwendet wird: Entweder **TCP**, **UDP** oder **All** (alle Protokolle, die der Router unterstützt).
- **Incoming Port -** Port oder Portbereich, den das entfernte System benutzt, um auf die Triggerverbindung zu reagieren. Verbindungen, die auf diesen Ports ankommen, werden zu dem auslösenden PC weitergeleitet. Es können bis zu 5 durch Kommata getrennte einzelne Ports bzw. Portbereiche angegeben werden, z.B.: 2000-2038, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol -** Das Protokoll für die eingehenden Verbindungen, entweder **TCP**, **UDP** oder **All** (alle Protokolle, die der Router unterstützt).
- **Status -** Der Status dieses Eintrags: **Enabled** oder **Disabled**.

Um eine neue Regel hinzuzufügen, geben Sie auf der Seite **Port Triggering** Folgendes ein**.**

1. Klicken Sie **Add New…**. Bild 4-40 erscheint.
2. Wählen Sie eine gebräuchliche Applikation aus **Common Applications** aus, werden **Trigger Port** und **Incoming Ports** automatisch eingegeben. Ist Ihre Applikation in der Liste **Common Applications** nicht enthalten, geben Sie **Trigger Port** und **Incoming Ports** von Hand an.
3. Wählen Sie das Protokoll (**Trigger Protocol**), das auf dem **Triggerport** verwendet wird, aus: Entweder **TCP**, **UDP** oder **All**.
4. Wählen Sie das Protokoll für die eingehenden Ports (**Incoming Ports**) aus: **TCP**, **UDP** oder **Alle**.
5. Wählen Sie **Enabled** als **Status**.

6. Klicken Sie **Save**, um die neue Regel zu speichern.

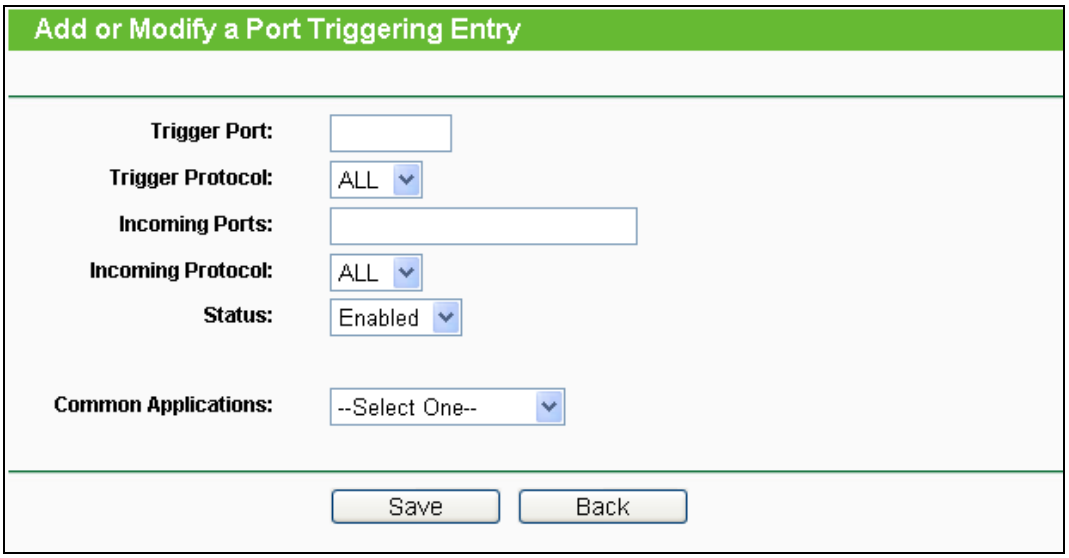


Bild 4-40 Triggereintrag hinzufügen oder bearbeiten

To modify or delete an existing entry:

1. Klicken Sie **Modify** für den zu bearbeitenden Eintrag oder **Delete**, um ihn zu löschen.
2. Bearbeiten Sie die Informationen, wie gewünscht.
3. Klicken Sie **Save**.

Klicken Sie **Enable All**, um alle Einträge zu aktivieren.

Klicken Sie **Disable All**, um alle Einträge zu deaktivieren.

Klicken Sie **Delete All,** um alle Einträge zu löschen.

☞ **Bemerkungen:**

1) Wird die Triggerverbindung geschlossen, schließt der Router auch die für die eingehenden Verbindungen geöffneten Ports.

2) Jede Regel kann nur von einem Computer zugleich verwendet werden. Eine eventuell von einem anderen LAN-Host initiierte Triggerverbindung wird, sofern sie schon in Verwendung ist, verweigert.

3) Portbereiche für eingehende Verbindungen dürfen einander nicht überlappen.

4.8.3 DMZ

Die Funktionalität **DMZ-Host** unter **Forwarding** → **DMZ** (Bild 4-41) erlaubt es, einen lokalen Host für aus dem Internet kommende Verbindungen komplett (d.h. auf allen Ports) freizugeben. Dies ist sinnvoll für z.B. Gaming- oder Videokonferenzserver. Der DMZ-Host darf nicht mit DHCP konfiguriert sein, sondern muss eine statische IP-Adresse haben.

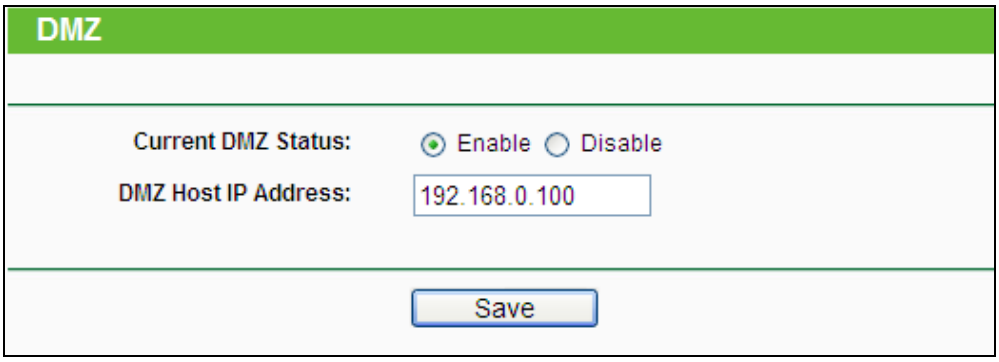


Bild 4-41 DMZ

Um einen Computer/Server als DMZ-Host zu konfigurieren:

1. Klicken Sie **Enable**.
2. Geben Sie die lokale IP-Adresse in das Feld **DMZ Host IP Address** ein.
3. Klicken Sie **Save**.

☞ **Bemerkung:**

Nachdem ein Computer zum DMZ-Host erklärt wurde, funktioniert die Router-Firewall für diesen nicht mehr.

4.8.4 UPnP

UPnP (Universal Plug and Play) ermöglicht es Geräten wie Internetcomputern, auf Ressourcen des lokalen PCs zuzugreifen. UPnP-Geräte können automatisch vom UPnP-Dienst erkannt werden. Sie können UPnP auf dieser Seite konfigurieren (Bild 4-42).

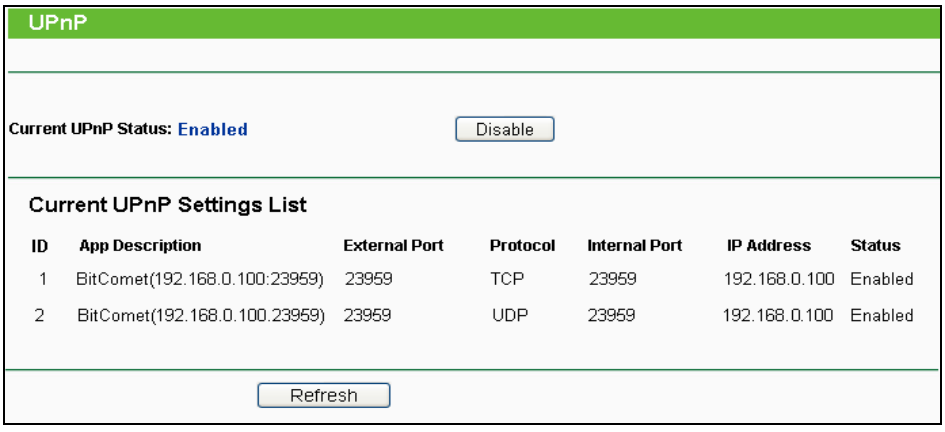


Bild 4-42 UPnP-Einstellungen

- **Current UPnP Status -** UPnP kann aktiviert oder deaktiviert werden. Da UPnP ein Sicherheitsrisiko darstellen kann, sollte es bei Nichtbenutzung deaktiviert werden.
- **Current UPnP Settings List -** In dieser Tabelle finden Sie die aktuell gültigen UPnP-Informationen.
  - **App Description -** Beschreibung der Applikation, die die UPnP-Anfrage gestellt hat.

- **External Port -** Externer Port, den der Router dieser Applikation geöffnet hat.
- **Protocol -** Zeigt das benutzte Protokoll an.
- **Internal Port -** Interner Port, den der Router für den lokalen Host geöffnet hat.
- **IP Address -** Das gerade auf den Router zugreifende UPnP-Gerät.
- **Status -** Entweder **Enabled** oder **Disabled**. **Enabled** bedeutet, dass der Port noch aktiv ist, ansonsten ist der Port inaktiv.

Klicken Sie **Refresh**, um die Ansicht der UPnP-Einstellungen zu aktualisieren.

4.9 Security

Bild 4-43 Das Menü **Security**

Im Menü **Security** gibt es vier Untermenüs (Bild 4-43): **Basic Security**, **Advanced Security**, **Local Management** und **Remote Management**.

4.9.1 Basic Security

Im Menü **Security** → **Basic Security** können Sie, wie in Bild 4-44 gezeigt, die Basissicherheit einstellen.

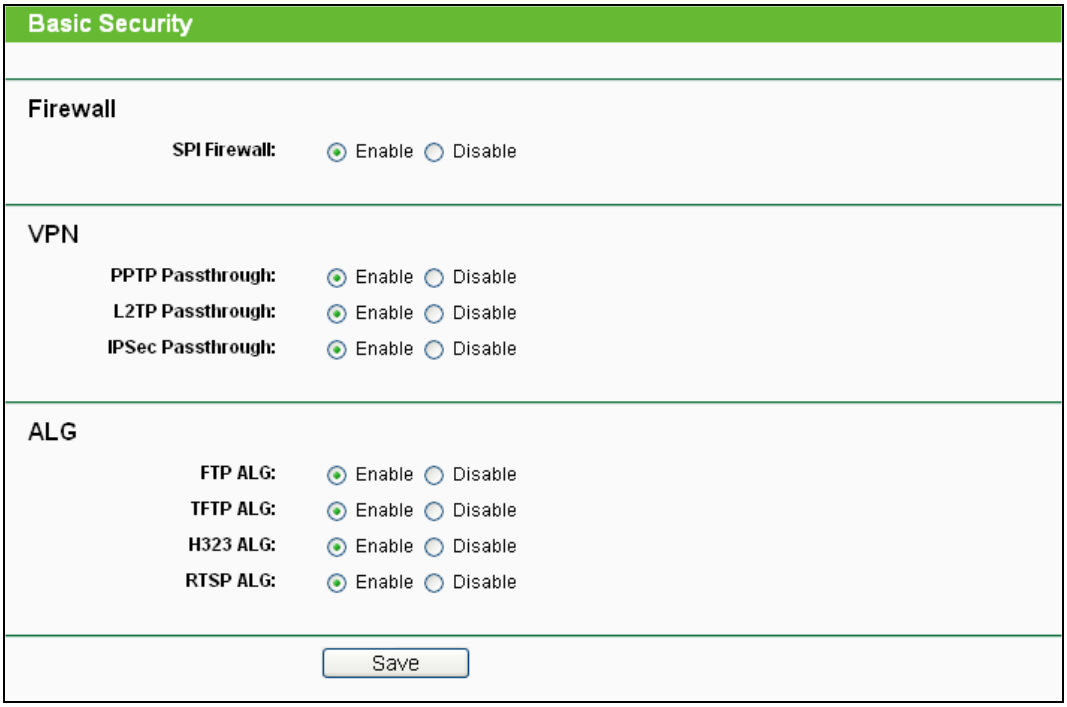


Bild 4-44 Basissicherheit

- **Firewall -** Eine Firewall schützt Ihr Netz vor Angriffen von außen. Hiermit können Sie die einzelnen Firewallfunktionen ein- und ausschalten.

- **SPI Firewall -** SPI (Stateful Packet Inspection, auch bekannt als dynamische Paketfilterung) hilft durch Paketinspektion dabei, Angriffe von außen zu vereiteln. Hierbei untersucht es, ob der Datenverkehr zu dem verwendeten Protokoll passt. Die SPI-Firewall ist standardmäßig eingeschaltet. Sollen die PCs in Ihrem LAN nicht dadurch geschützt werden, können Sie diese Funktion abschalten.

➢ **VPN -** VPN-Passthrough muss aktiv sein, wenn Sie mittels VPN-Tunneln über IPSec, PPTP oder L2TP durch den Router passieren möchten.

- **PPTP Passthrough -** Das „Point-to-Point Tunneling Protocol“ (PPTP) ermöglicht die Tunnelung des Point-to-Point-Protokolls (PPP) durch ein IP-Netz.
- **L2TP Passthrough -** „Layer 2 Tunneling Protocol“ (L2TP) wird verwendet, um Punkt-zu-Punkt-Sitzungen über das Internet auf Layer-2-Ebene zu öffnen.
- **IPSec Passthrough -** „Internet Protocol Security“ (IPSec) ist eine Protokollsuite zur Ermöglichung privater, sicherer Kommunikation über Internetprotokoll (IP) mit Hilfe von Verschlüsselung.

➢ **ALG -** Es wird empfohlen, Application Layer Gateway (ALG) zu aktivieren, da dies benutzerspezifisches NAT für bestimmte Kontroll- und Datenprotokolle wie z.B. FTP, TFTP und H232 erlaubt.

- **FTP ALG -** Um FTP-Clients und -Server Daten durch den NAT-Router übertragen zu lassen, lassen Sie die Standardeinstellung **Enabled**.
- **TFTP ALG -** Um TFTP-Clients und -Server Daten durch den NAT-Router übertragen zu lassen, lassen Sie die Standardeinstellung **Enabled**.
- **H323 ALG -** Um Microsoft-NetMeeting-Clients Daten durch den NAT-Router übertragen zu lassen, lassen Sie die Standardeinstellung **Enabled**.
- **RTSP ALG -** Um RTSP-Streaming durch den NAT-Router zuzulassen, lassen Sie die Standardeinstellung **Enabled**.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

4.9.2 Advanced Security

Mittels der Seite **Security** → **Advanced Security** (Bild 4-45) können Sie den Router vor TCP-SYN-Flood-, UDP-Flood- und ICMP-Flood-Angriffen schützen.

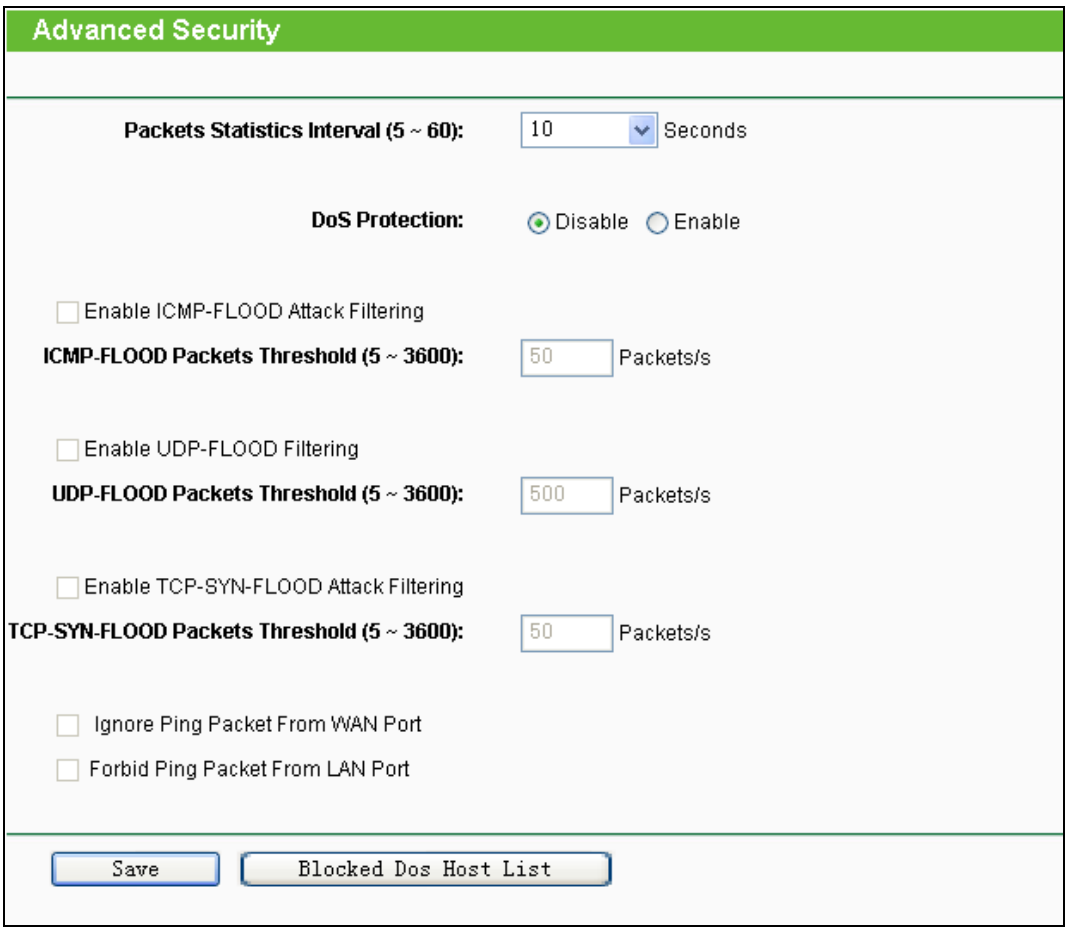


Bild 4-45 Erweiterte Sicherheitseinstellungen

- **Packets Statistics Interval (5~60) -** Der Wert **Packets Statistics Interval** bezeichnet die Dauer, die eine einzelne Paketstatistik umfasst. Das Ergebnis dieser Statistik wird für Analysen der Funktionen **SYN-Flood**, **UDP-Flood** und **ICMP-Flood** verwendet. Gültige Werte sind von 5 bis 60, Einheit ist Sekunden. Standardwert ist 10.
- **DoS Protection - DoS-Schutz** aktivieren oder deaktivieren. Nur, wenn er aktiviert ist, funktionieren die Floodfiltermechanismen.
- **Enable ICMP-FLOOD Attack Filtering - ICMP-FLOOD-Schutz** aktivieren oder deaktivieren.
- **ICMP-FLOOD Packets Threshold (5~3600) -** Überschreitet die aktuelle Zahl der **ICMP-FLOOD**-Pakete diesen Wert, blockiert der Router alle weiteren sofort. Standardwert ist 50. Gültige Werte sind von 5..3600.
- **Enable UDP-FLOOD Filtering - UDP-FLOOD-Schutz** aktivieren oder deaktivieren.
- **UDP-FLOOD Packets Threshold (5~3600) -** Überschreitet die aktuelle Zahl der **UDP-FLOOD**-Pakete diesen Wert, blockiert der Router alle weiteren sofort. Standardwert ist 50. Gültige Werte sind von 5..3600.
- **Enable TCP-SYN-FLOOD Attack Filtering - TCP-SYN-FLOOD-Schutz** aktivieren oder deaktivieren.

- **TCP-SYN-FLOOD Packets Threshold (5~3600) -** Überschreitet die aktuelle Zahl der **TCP-SYN-FLOOD**-Pakete diesen Wert, blockiert der Router alle weiteren sofort. Standardwert ist 50. Gültige Werte sind von 5..3600.
- **Ignore Ping Packet From WAN Port -** Ping-Pakete vom WAN-Port ignorieren oder nicht. Standardmäßig deaktiviert. Ist die Funktion aktiv, können Pingpakete aus dem Internet nicht verarbeitet werden.
- **Forbid Ping Packet From LAN Port -** Ping-Pakete vom LAN-Port ignorieren oder nicht Standardmäßig deaktiviert. Ist die Funktion aktiv, können Pingpakete aus dem LAN nicht verarbeitet werden (stört die Funktion einiger Viren).

Klicken Sie **Save**, um diese Einstellungen zu speichern.

Klicken Sie **Blocked DoS Host List**, um die Liste der blockierten DoS-Hosts anzusehen.

4.9.3 Local Management

Im Menü **Security** → **Local Management** können Sie die Verwaltungsregeln wie in Bild 4-46 erkennbar bearbeiten. Damit können Sie einzelnen LAN-PCs die Berechtigung, auf den Router zuzugreifen, erteilen oder entziehen.

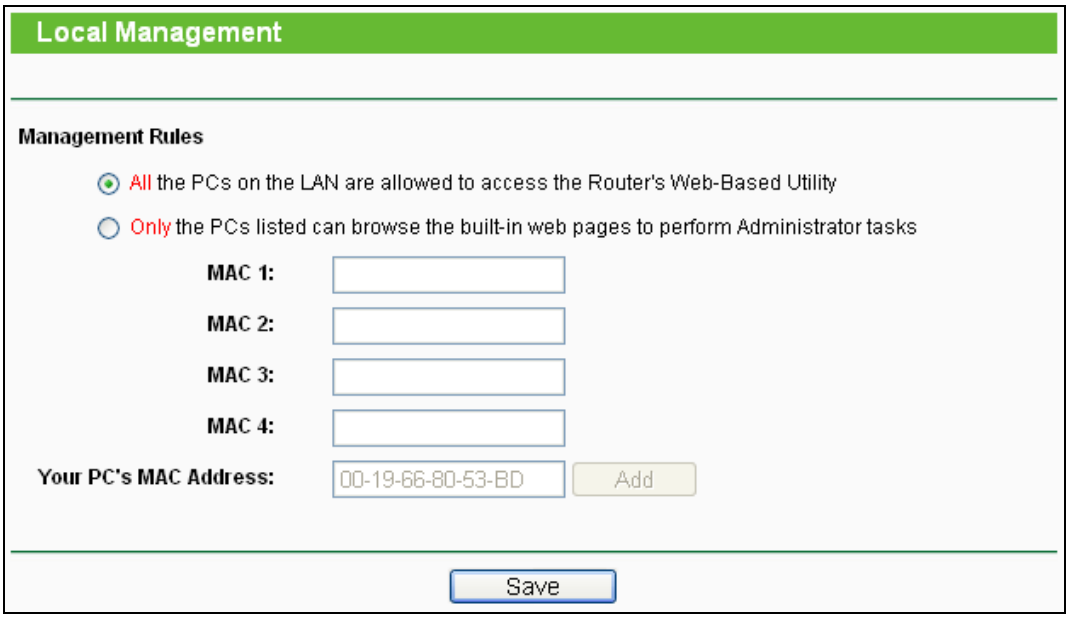


Bild 4-46 Lokale Verwaltung

Standardmäßig gilt die Option **All the PCs on the LAN are allowed to access the Router's Web-Based Utility** Möchten Sie diesen Zugriff nur ein paar PCs gewähren, können Sie die zugehörigen MAC-Adressen auf dieser Seite eintragen (Format: „XX-XX-XX-XX-XX-XX“, wobei jedes „X“ für eine Hexadezimalziffer steht) und **Only the PCs listed can browse the built-in web pages to perform Administrator tasks** aktivieren. Dann können nur noch diese PCs auf das Webinterface des Routers zugreifen.

Nach Klick auf **Add** wird die MAC-Adresse Ihres PCs in die Liste aufgenommen.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

☞ **Bemerkung:**

Haben Sie sich mittels dieses Features aus dem Router ausgesperrt und kein anderer PC kann die Sperrung aufheben, müssen Sie den Router mittels der **Reset-Taste** (Rückseite des Routers) zurücksetzen. Drücken Sie mit einem spitzen Gegenstand mindestens 5 Sekunden darauf. Danach muss der Router komplett neu konfiguriert werden.

4.9.4 Remote Management

Im Menü **Security** → **Remote Management** können Sie die Fernwartungsfunktion aktivieren (Bild 4-47). Damit kann der Router aus der Ferne über das Internet konfiguriert werden.

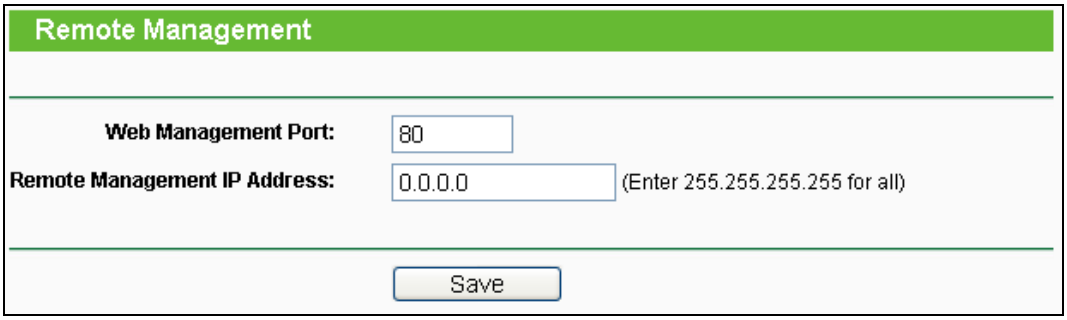


Bild 4-47 Konfiguration der Fernwartung

- **Web Management Port -** Die Nummer des Ports, über den aus dem Internet auf den Router zugegriffen werden kann. Standardwert ist 80. Um die Sicherheit zu erhöhen, wird empfohlen, diese Nummer zu ändern. Nehmen Sie vorzugsweise einen Wert von 1024 bis 65534, jedoch keinen Port, der zu gebräuchlich ist.
- **Remote Management IP Address -** Von dieser IP-Adresse aus können Sie über das Internet auf Ihren Router zugreifen. Standard ist 0.0.0.0, was bedeutet, dass die Fernwartungsfunktion deaktiviert ist. Ändern Sie diesen Wert, um die Funktion zu aktivieren. Setzen Sie den Wert auf 255.255.255.255, kann von allen Internethosts auf Ihren Router zugegriffen werden.

☞ **Bemerkungen:**

1. Um auf den Router zuzugreifen, geben Sie die WAN-IP-Adresse des Routers in die Adresszeile Ihres Browsers ein, gefolgt von einem Doppelpunkt und der Portnummer. Beispiel: Die WAN-Adresse lautet 202.96.12.8 und die Portnummer 8888. In diesem Fall ist http://202.96.12.8:8888 einzugeben. Bei erfolgreicher Verbindung werden Sie hierauf nach dem Passwort des Routers gefragt.
2. Bitte verwenden Sie für die Fernwartung ein besonders sicheres Passwort.

4.10 Parental Control

Im Menü **Parental Control** können Sie die Zugriffskontrolle nach Bild 4-48 einrichten. Mit dieser Funktion können Sie die Internetaktivitäten Ihrer Kinder/Angestellten auf bestimmte Websites und/oder Zeiträume einschränken.

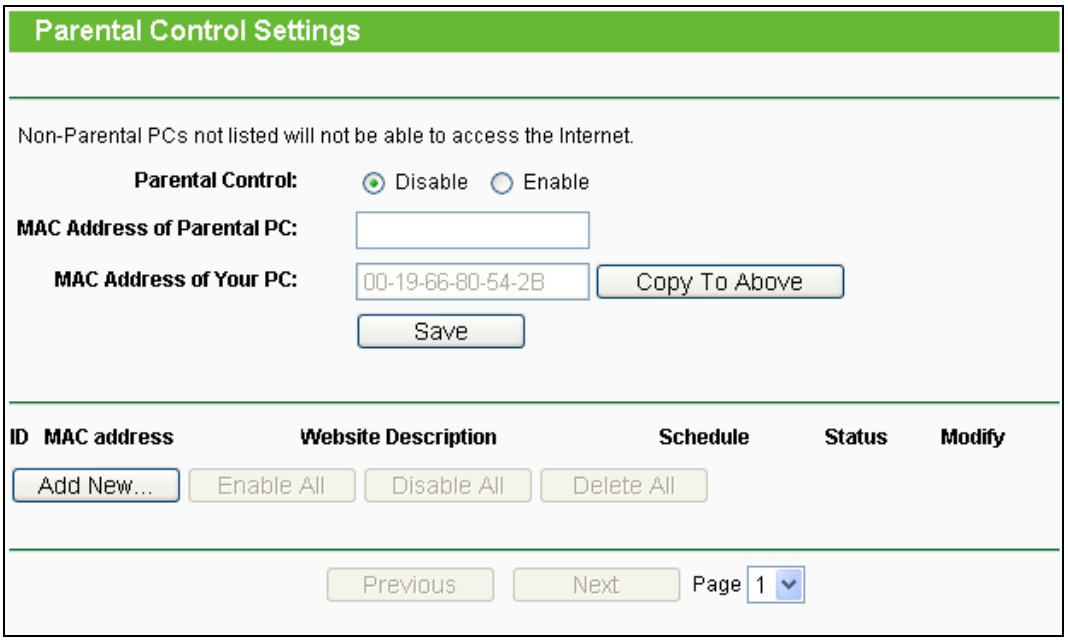


Bild 4-48 Parental Control

- **Parental Control - Enable** (Aktivieren) oder **Disable** (Deaktivieren) der Funktion.
- **MAC Address of Parental PC -** Geben Sie hier die MAC-Adresse des kontrollierten PCs ein oder benutzen Sie die Funktion **Copy To Above**, um Ihre Adresse einzusetzen.
- **MAC Address of Your PC -** Dieses Feld zeigt die MAC-Adresse des gerade verbundenen PCs an. Diese können Sie mit einem Klick in das darüberliegende Feld kopieren.
- **Website Description -** Beschreibung der eingetragenen Website.
- **Schedule -** Der Zeitraum, in dem der PC auf das Internet zugreifen darf. Für weitere Einzelheiten gegen Sie bitte in den Abschnitt **Access Control → Schedule**.
- **Modify -** Hiermit können Sie einen Eintrag bearbeiten oder löschen.

Um einen neuen Eintrag hinzuzufügen, folgen Sie bitte diesen Schritten.

1. Klicken Sie **Add New…**. Das nächste Bild erscheint (Bild 4-49).
2. Geben Sie die MAC-Adresse des zu kontrollierenden PCs (z.B. 00-11-22-33-44-AA) ein oder suchen Sie eine aus der **Liste All Address in Current LAN** aus.
3. Geben Sie in das Feld **Website Description** eine Webseitenbeschreibung (z.B. „Google zulassen“) ein.
4. Geben Sie den Domänennamen der zugelassenen Webseite oder Schlüsselwörter (z.B. kinder) ein. Jeder Domänenname, der die Schlüsselwörter enthält (www.kinderseite.com, www.kinderspielplatz.de), ist zugänglich.
5. Wählen Sie den gewünschten Wirksamkeitszeitraum aus der Drop-Down-Liste aus (z.B. Samstagabend). Ist kein passender dabei, können Sie durch Klick auf **Schedule** (unten in rot) auf die Planungsseite gelangen und dort einen anlegen.
6. Im Feld **Status** können Sie den Eintrag aktivieren oder deaktivieren.
7. Klicken Sie **Save**.

Klicken Sie **Enable All**, um alle Regeln zu aktivieren.

Klicken Sie **Disable All**, um alle Regeln zu aktivieren.

Klicken Sie **Delete All**, um alle Regeln zu löschen.

Klicken Sie **Next**, um zur nächsten Seite zu blättern oder **Previous**, um zur vorigen Seite zurückzukehren.

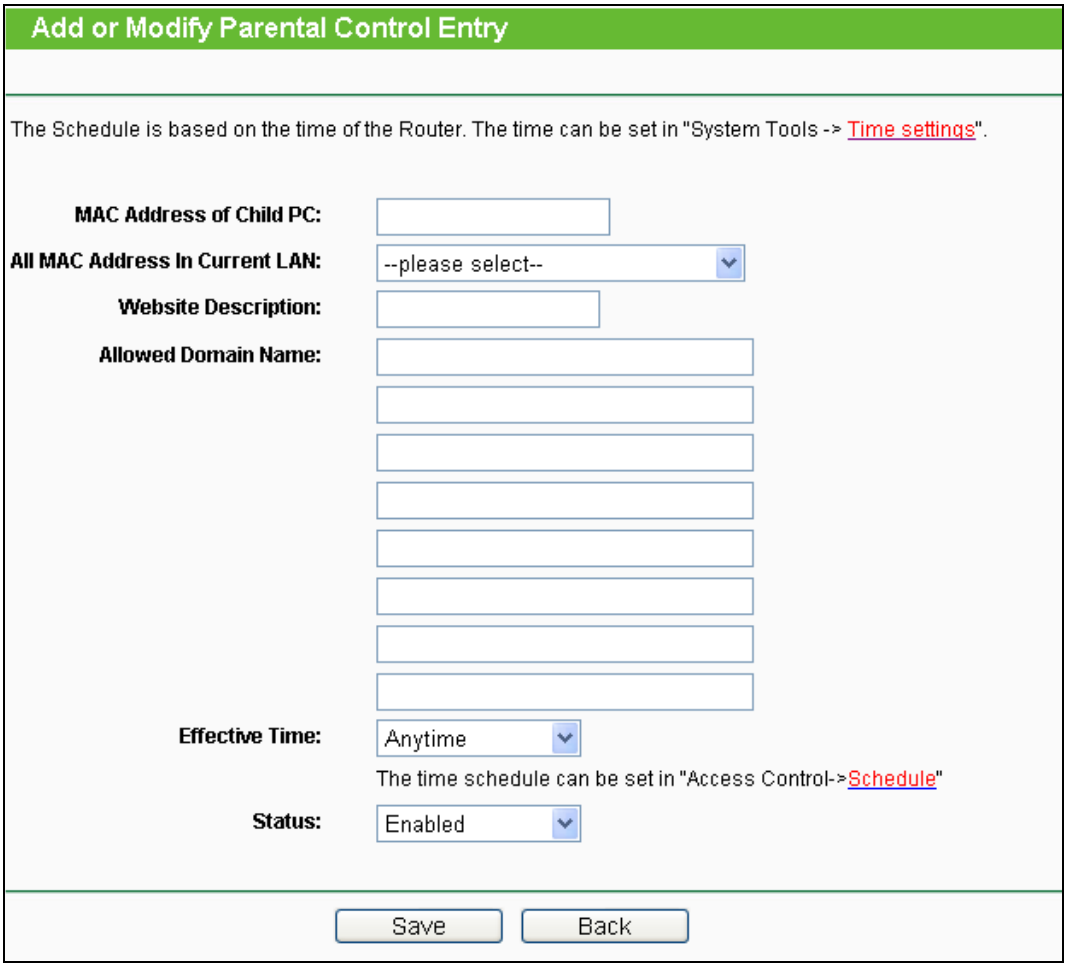


Bild 4-49 Zugriffskontrolleintrag anlegen oder verändern

Beispiel: Soll der PC mit der MAC-Adresse 00-11-22-33-44-AA nur samstags und nur Kinderseiten erreichen können, während der PC mit der MAC-Adresse 00-11-22-33-44-BB keinen Zugangseinschränkungen unterliegen soll, sollte Folgendes konfiguriert werden.

1. Klicken Sie auf **Parental Control**. Aktivieren (**Enable**) Sie die Funktion und geben Sie 00-11-22-33-44-BB in das Feld **MAC Address of Parental PC** ein.
2. Klicken Sie **Access Control** → **Schedule**, um auf die Planungsseite zu gelangen. Klicken Sie **Add New...**, um eine neue Planung anzulegen. **Schedule Description** könnte „Samstag“ lauten, **Day** ist „Sat“ und **Time all day-24 hours**.
3. Gehen Sie zurück zu **Parental Control** und legen Sie folgendermaßen einen Eintrag an:
   - Klicken Sie **Add New...**.
   - Geben Sie „00-11-22-33-44-AA“ in das Feld **MAC Address of Child PC** ein.

- Geben Sie „Kinderseiten” als **Website Description** ein.
- Geben Sie „kinder” unter **Allowed Domain Name** ein.
- Wählen Sie die gerade erstellte Planung „Sat” als **Effective Time** aus.
- Als **Status** nehmen Sie **Enable**.

4. Klicken Sie **Save**, um den Eintrag zu speichern.

Damit kommen Sie auf die Übersichtsseite zurück und sehen Bild 4-50.

Bild 4-50 PC-Kontrollseite

4.11 Access Control

Bild 4-51 Menü **Access Control**

Im Menü **Access Control** gibt es vier Untermenüs (Bild 4-51): **Rule**, **Host**, **Target** und **Schedule**.

4.11.1 Rule

Im Menü **Access Control** → **Rule** können Sie Zugangskontrollregeln setzen, wie in Bild 5-47 zu sehen ist.

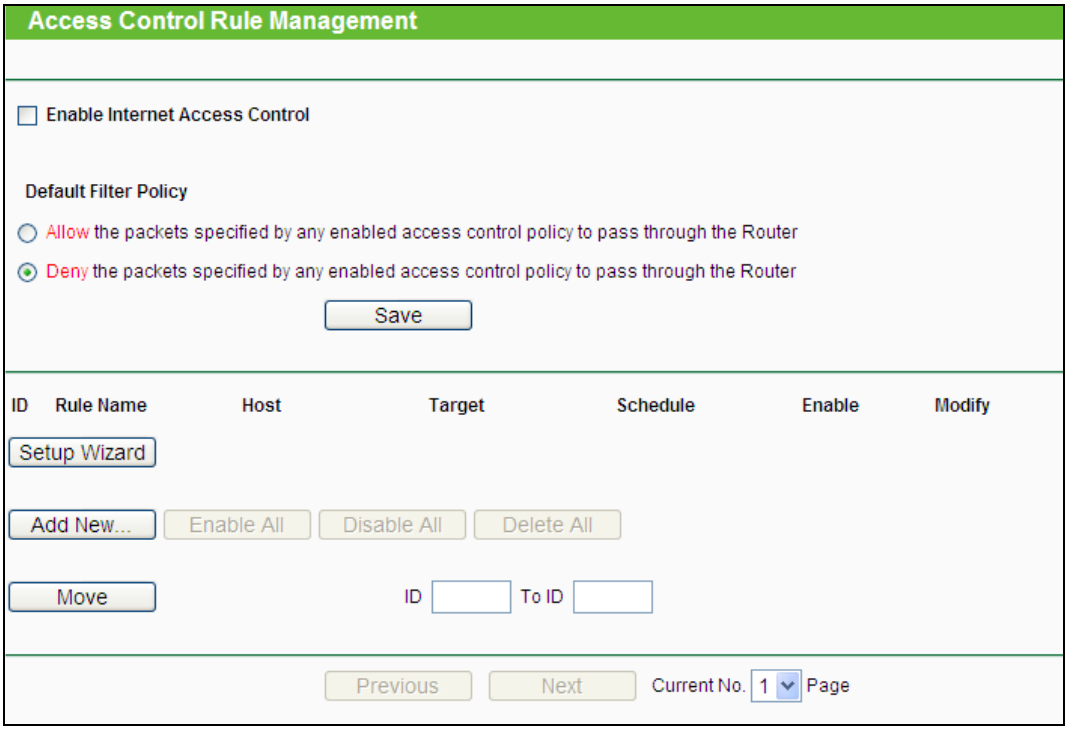


Bild 4-52 Zugriffskontrollregelverwaltung

- **Enable Internet Access Control -** Wählen Sie dies an, damit die Internetzugriffskontrolle aktiv wird.
- **Rule Name -** Hier sehen Sie den eindeutigen Namen der Regel.
- **Host -** Dies ist der Name des von der Regel betroffenen Hosts.
- **Target -** Dies ist das Ziel, auf das die Regel Anwendung findet.
- **Schedule -** Die mit der Regel assoziierte Planung.
- **Status -** Status dieser Regel: **Enabled** oder **Disabled**.
- **Modify -** Hier kann die Regel bearbeitet oder gelöscht werden.
- **Setup Wizard -** Hiermit können Sie ganz einfach Regeln erstellen.
- **Add New... -** Klicken Sie **Add New...**, um eine neue Regel hinzuzufügen.
- Klicken Sie **Enable all**, um alle Regeln zu aktivieren.
- Klicken Sie **Disable all**, um alle Regeln zu deaktivieren.
- Klicken Sie **Delete all**, um alle Regeln zu löschen.
- **Move -** Sie können die Reihenfolge der Regeln nach Belieben ändern. Dies beeinflusst ihre Priorität. Frühere Regeln sind stärker als spätere. Geben Sie in das erste Feld die ID des zu verschiebenden Eintrags ein und in das zweite Feld die Stelle, an die verschoben werden soll. Klicken Sie dann **Move**, um die Reihenfolge zu ändern.
- Klicken Sie **Previous**, um zur letzten Seite zurückzukehren oder **Next**, um die nächste Seite anzusehen.

Es existieren zwei Methoden, um neue Regeln hinzuzufügen.

Methode 1:

1. Klicken Sie auf **Setup Wizard**. Es erscheint Bild 4-53.

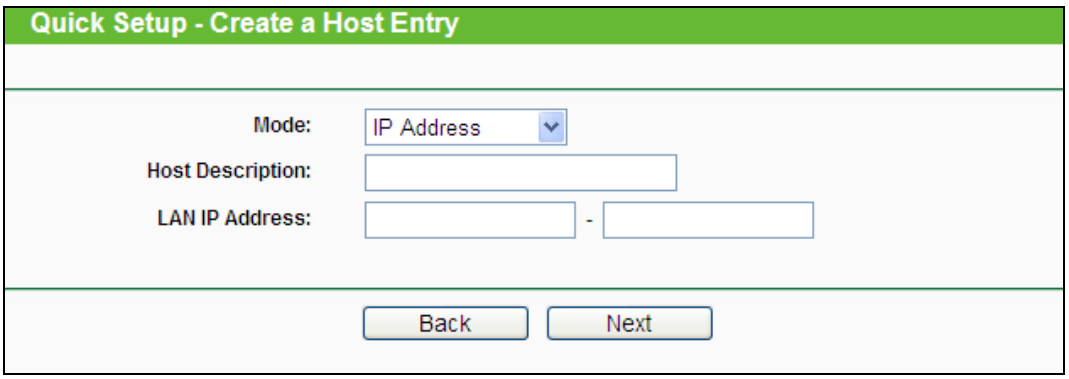


Bild 4-53 Regelassistent – Hosteintrag anlegen

- **Host Description** - Hier können Sie eine eindeutige Hostbeschreibung angeben (z.B. Pauls PC).
- **Mode** - Hier können Sie auswählen, ob der Host anhand seiner **IP-** oder seiner **MAC-Adresse** identifiziert werden soll.

Wurde **IP Address** ausgewählt, erscheint folgendes Feld:

LAN IP Address - Geben Sie hier die IP-Adresse oder den IP-Adressenbereich des zu spezifizierenden Hosts an, z.B. **192.168.0.23**

Wurde **MAC-Adresse** ausgewählt, erscheint folgendes Feld:

- **MAC Address** - Geben Sie hier die MAC-Adresse des zu spezifizierenden Hosts an. Format: XX-XX-XX-XX-XX-XX. Beispiel: **00-11-22-33-44-AA**.

2. Klicken Sie **Next**. Es erscheint Bild 4-54.

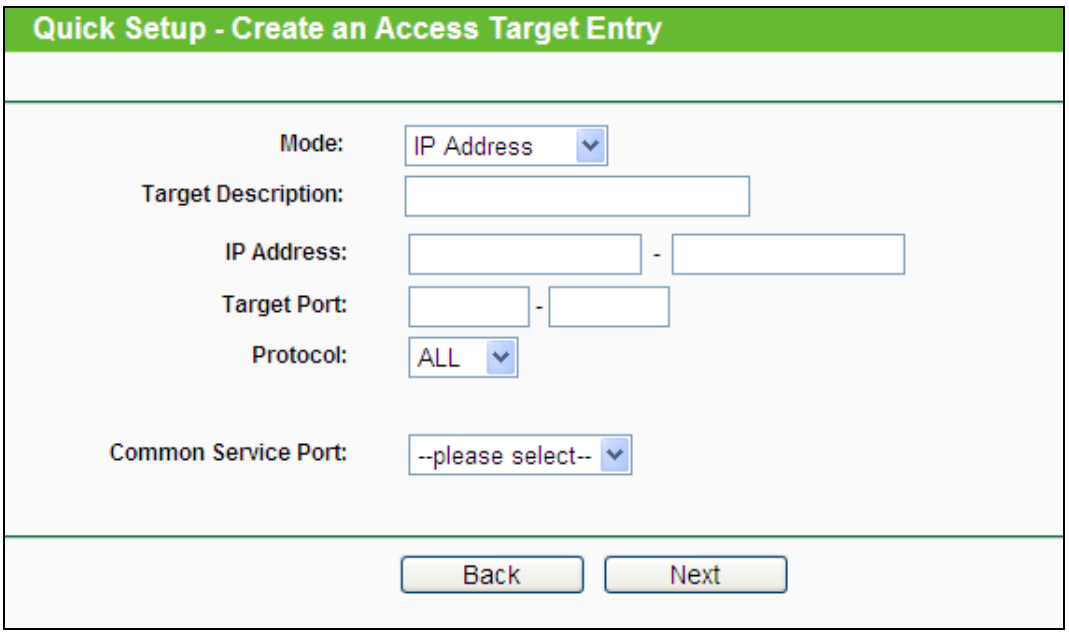


Bild 4-54 Regelassistent – Anlegen eines Eintrags für ein Zugriffsziel

- **Target Description** - Geben Sie hier eine eindeutige Bezeichnung für das Ziel ein, z.B. „google“.
- **Mode** - Hier können Sie auswählen, ob das Ziel anhand seiner **IP-Adresse** oder seines **Domänennamens** identifiziert werden soll.

Wurde **IP Address** gewählt, erscheinen folgende Felder:

- **IP Address** - Geben Sie hier die IP-Adresse (oder den IP-Adressbereich) des Ziels/der Ziele ein. Beispiel: **217.72.195.48**.
- **Target Port** - Der Port(bereich), der für das Ziel gelten soll. Für den Fall, dass Sie gebräuchliche Dienste verwenden wollen, könnte der Port unter **Common Service Port**s gelistet sein.
- **Protocol** - Hier haben Sie vier Optionen: **All**, **TCP**, **UDP** und **ICMP**.
- **Common Service Port** - Eine Liste einiger bekannter Dienste mit ihren zugehörigen Portnummern. Wenn Sie hier einen Dienst auswählen, wird die Standard-Portnummer eingetragen. Beispiel: Wählen Sie **FTP** aus, wird als Port automatisch die Nummer **21** gesetzt.

Wurde **Domain Name** ausgewählt, sehen Sie nur eine Eingabemöglichkeit:

- **Domain Name** - Hier können Sie bis zu 4 Domänennamen eingeben, entweder volle Namen oder Schlüsselwörter, z.B. „kinder“. In diesem Fall würde die Regel auf alle Domänennamen, die das Schlüsselwort enthalten (wie „kinderseite.de“, „kinderspielplatz.net“), zutreffen.

3. Klicken Sie **Next**, wenn Sie Ihre Einstellungen vorgenommen haben. Es erscheint Bild 4-55.

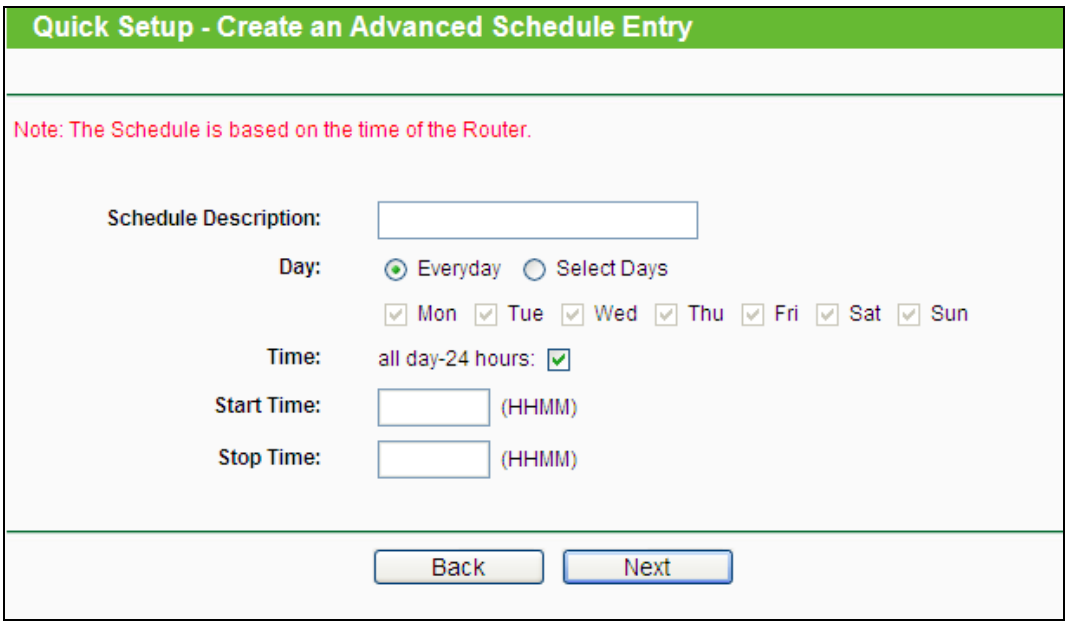


Bild 4-55 Regelassistent – Anlegen eines erweiterten Planungseintrags

- **Schedule Description** - Hier können Sie eine Beschreibung für die anzulegende Planung vergeben. Diese sollte eindeutig sein.
- **Day** - Wählen Sie den/die Wochentag(e) oder **Everyday** (täglich) aus.
- **Time** - Wählen Sie **24 hours** (ständig) oder geben Sie Start- und Endzeit an.
- **Start Time** - Die Uhrzeit, ab der die Regel gelten soll (Format: HHMM. Beispiel: „0800“ bedeutet 8 Uhr morgens).
- **Stop Time** - Die Uhrzeit, bis zu der die Regel gelten soll (Format: HHMM. Beispiel: „2100“ bedeutet 9 Uhr abends).

4. Klicken Sie **Next**. Es erscheint Bild 4-56.

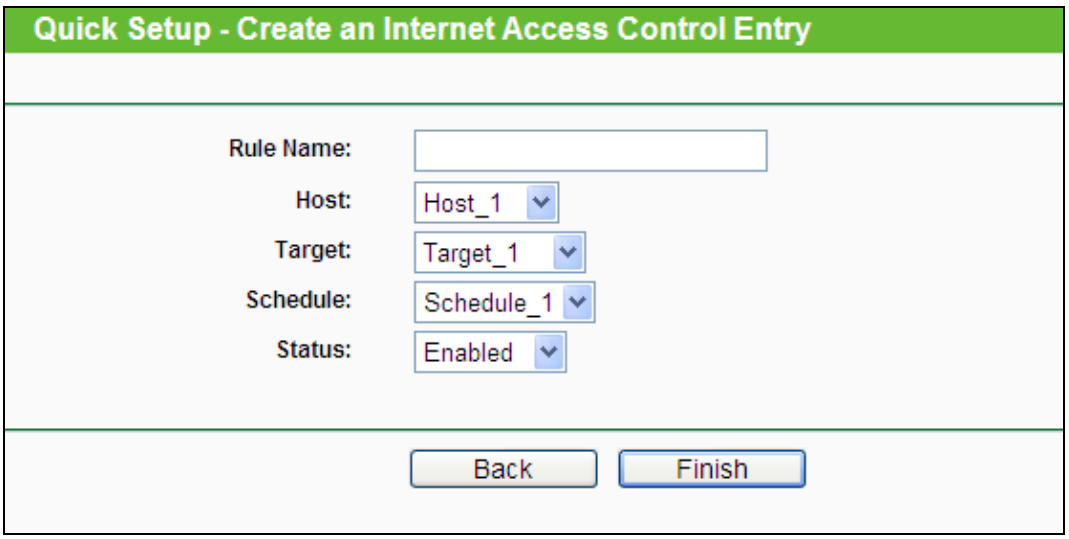


Bild 4-56 Regelassistent - Internetzugriffskontrollregel anlegen

- **Host** - Hier wählen Sie einen zuvor definierten Host aus, auf den die Regel zutreffen soll. Sie sehen in der Liste die zuvor gesetzte **Host Description**.

- **Target** - Hier wählen Sie ein zuvor definiertes Ziel aus, auf das die Regel zutreffen soll. Sie sehen in der Liste die zuvor gesetzte **Target Description**.
- **Schedule** - Hier wählen Sie eine zuvor definierte Planung aus, auf die die Regel zutreffen soll. Sie sehen in der Liste die zuvor gesetzte **Schedule Description**.
- **Status** - Aktivieren (**Enable**) oder Deaktivieren (**Disable**) der Regel.

5. Klicken Sie **Finish**, um die neue Regel zu speichern.

Methode 2:

1. Klicken Sie **Add New…**. Bild 5-52 erscheint.
2. Vergeben Sie unter **Rule Name** einen Namen für die Regel (z.B. „adult_verbieten“).
3. Wählen Sie einen Host aus der Liste **Host** aus oder wählen Sie **Click Here To Add New Host List**.
4. Suchen Sie ein Ziel aus der Liste **Target** aus oder wählen Sie **Click Here To Add New Target List**.
5. Entscheiden Sie sich für eine Planung aus der Liste **Schedule** oder wählen Sie **Click Here To Add New Schedule**.
6. Im Feld **Status** wählen Sie zwischen **Enabled** (aktiviert) und **Disabled** (deaktiviert).
7. Klicken Sie **Save**.

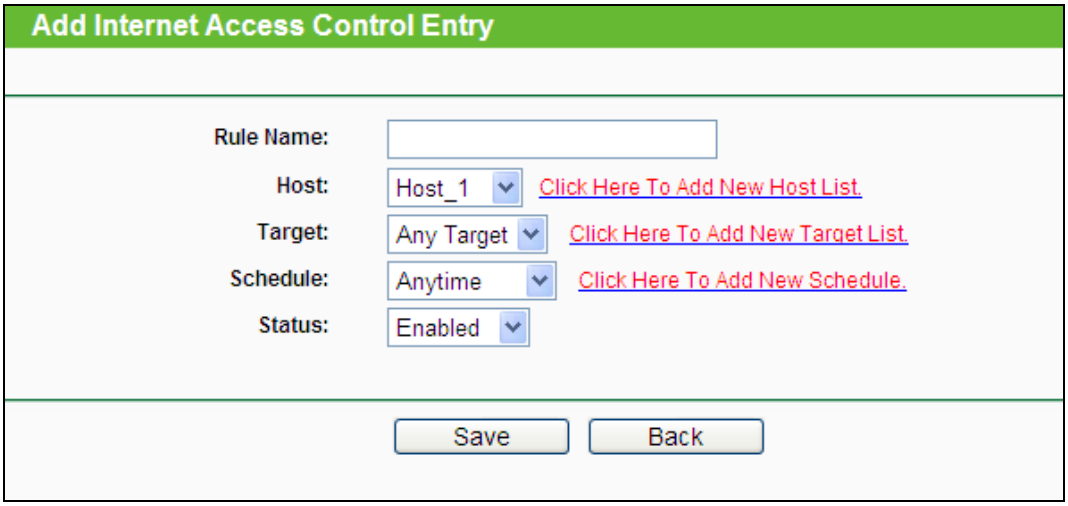


Bild 4-57 Internetzugangskontrolleintrag anlegen

Beispiel: Soll der Host mit der MAC-Adresse 00-11-22-33-44-AA nur **www.google.com** und diese Adresse auch nur **samstags und sonntags von 18 bis 20 Uhr** erreichen können, müssen folgende Einstellungen getätigt werden:

1. Gehen Sie in das Untermenü **Rule of Access Control** und aktivieren Sie die Internetzugriffskontrolle (**Enable Internet Access Control**). Wählen Sie **Allow the packets specified by any enabled access control policy to pass through the Router**.
2. Es ist empfohlen, den **Setup Wizard** zu verwenden, um die folgenden Einstellungen zu tätigen.

3. Öffnen Sie das Untermenü **Host of Access Control**. Legen Sie einen neuen Host an und vergeben Sie eine Beschreibung. Die **MAC-Adresse** ist mit 00-11-22-33-44-AA anzugeben.
4. Öffnen Sie das Untermenü **Target of Access Control**. Legen Sie ein neues Ziel (Domänenname) an und geben Sie ihm eine Beschreibung (z.B. Google). Der **Domänenname** ist www.google.com.
5. Öffnen Sie das Untermenü **Schedule of Access Control**. Legen Sie eine Planung mit einem eindeutigen Bezeichner (z.B. „SaSo1820“) an und wählen Sie die Wochentage Samstag und Sonntag aus. Startzeit ist 1800 und Endzeit 2000.
6. Öffnen Sie das Untermenü **Rule of Access Control**. Klicken Sie **Add New...** und legen Sie eine Regel mit den folgenden Parametern an:
   - Als **Rule Name** vergeben Sie einen eindeutigen Namen, z.B. **SaSo1820Google**.
   - Als **Host** wählen Sie den oben definierten Host aus.
   - Als **Target** wählen Sie **Google**.
   - Im Feld **Schedule** wählen Sie **SaSo1820** aus.
   - Der Status ist **Enable**.
   - Klicken Sie **Save**, um Ihre neuen Einstellungen zu speichern.

Sie landen nun auf der Seite der Zugriffskontrollregelverwaltung und sehen dies.

4.11.2 Host

Im Menü **Access Control** → **Host** können Sie eine Liste der zu kontrollierenden Hosts verwalten (Bild 4-58). Diese wird für die Zugriffskontrolle benötigt.

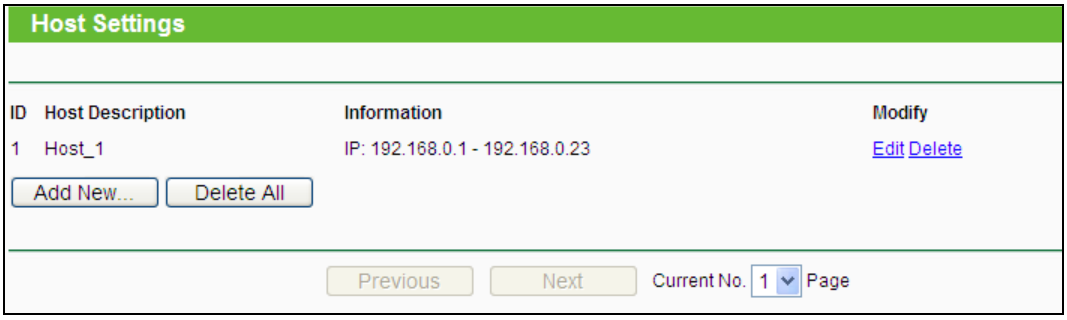


Bild 4-58 Host Settings

- **Host Description -** Eine eindeutige Beschreibung des Hosts.
- **Information -** Informationen über diesen Host: IP- oder MAC-Adresse.
- **Modify -** Bearbeiten oder Löschen eines bestehenden Eintrags.

Um einen neuen Eintrag anzulegen, tun Sie bitte Folgendes**.**

1. Click the **Add New…** button.

2. Als **Mode** wählen Sie **IP Address** oder **MAC Address**.
   - Haben Sie „IP-Adresse“ gewählt, erscheint Bild 4-59.
     1) Im Feld **Host Description** hinterlegen Sie eine eindeutige Beschreibung, z.B. „Meikes Computer“.
     2) Im Feld **LAN IP Address** geben Sie die IP-Adresse oder den IP-Adressbereich ein.
   - Haben Sie „MAC-Adresse“ gewählt, erscheint Bild 4-60.
     1) Im Feld **Host Description** hinterlegen Sie eine eindeutige Beschreibung, z.B. „Meikes Computer“).
     2) Im Feld **MAC Address** geben Sie die IP-Adresse ein.
3. Klicken Sie **Save**, um den Eintrag zu übernehmen.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

Klicken Sie **Previous**, um zur vorigen Seite zurückzukehren oder **Next**, um die nächste Seite anzusehen.

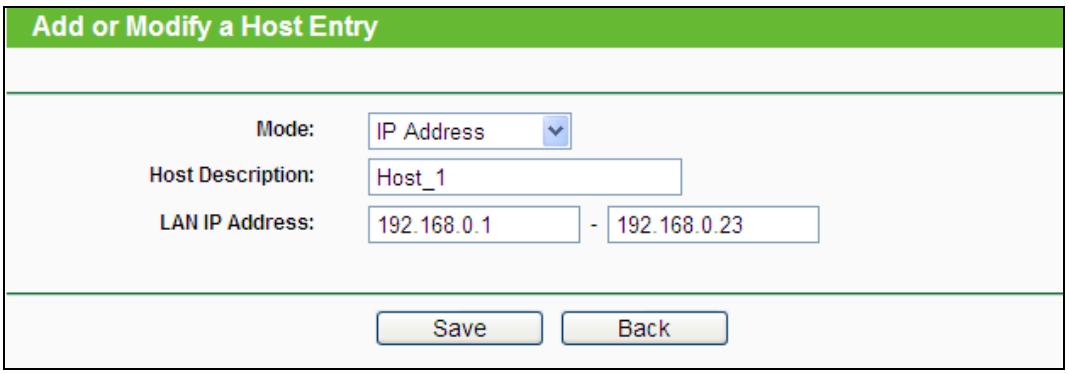


Bild 4-59 Hosteintrag anlegen oder bearbeiten

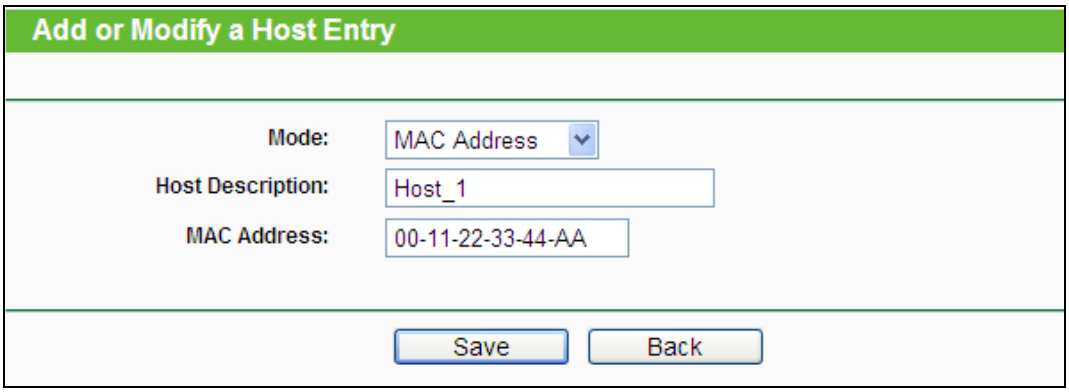


Bild 4-60 Hosteintrag anlegen oder bearbeiten

Beispiel: Möchten Sie die Internetaktivitäten des Hosts mit der MAC-Adresse 00-11-22-33-44-AA einschränken, sollten Sie so vorgehen:

1. Klicken Sie auf Bild 4-58 **Add New...**.
2. Als **Mode** geben Sie **MAC Address** an.
3. Als **Host Description** vergeben Sie eine eindeutige Hostbeschreibung (z.B. Jans PC).

4. In das Feld **MAC Address** geben Sie 00-11-22-33-44-AA ein.
5. Klicken Sie **Save**.

Sie werden dann auf die Hosteinstellungsseite zurückgebracht und sehen folgende Tabelle.

ID	Host Description	Information	Modify
1	Host_1	MAC: 00-11-22-33-44-AA	Edit Delete

4.11.3 Target

Gehen Sie zum Menü **Access Control** → **Target**. Hier können Sie eine Zielliste wie in Bild 4-61 zu sehen erstellen. Diese ist erforderlich für Zugriffskontrollregeln.

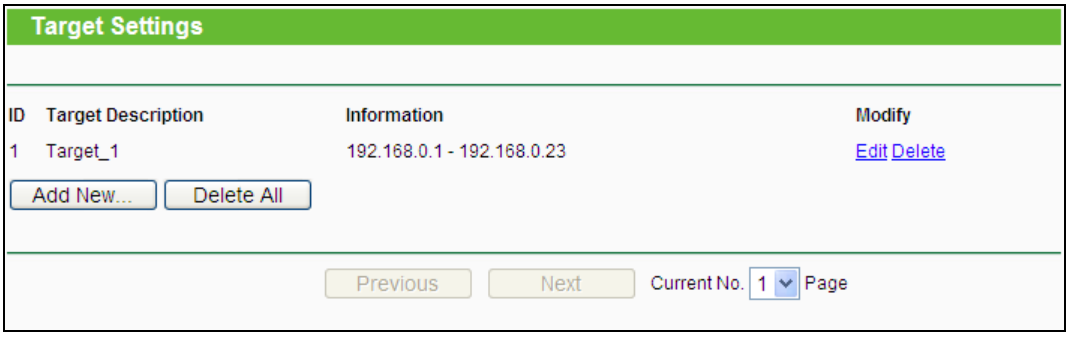


Bild 4-61 Target Settings

- **Target Description -** Hier steht eine eindeutige Beschreibung des Ziels.
- **Information -** Als Ziel können entweder IP-Adressen, Ports oder Domänennamen stehen.
- **Modify -** Um einen Eintrag zu bearbeiten/löschen, klicken Sie den entsprechenden Link.

Um einen neuen Eintrag anzulegen, gehen Sie bitte wie folgt vor**.**

- Klicken Sie **Add New…**.
- Als **Mode** wählen Sie **IP Address** oder **Domain Name** aus.
  - Haben Sie **IP Address** gewählt, erscheint Bild 4-62.
    1) Im Feld **Target Description** erstellen Sie eine eindeutige Beschreibung des Ziels
    2) Als **IP Address** geben Sie die Ziel-IP-Adresse an.
    3) Wählen Sie einen Dienst aus der Liste **Common Service Port** aus, damit der **Target Port** automatisch eingetragen wird. Ist Ihre Anwendung in der Liste nicht enthalten, geben Sie die Portnummer(n) von Hand in das Feld **Target Port** ein.
    4) Als **Protocol** wählen Sie nach Bedarf **TCP**, **UDP**, **ICMP** oder **All**.
  - Haben Sie **Domain Name** gewählt, erscheint Bild 4-63.
    1) Im Feld **Target Description** erstellen Sie eine eindeutige Beschreibung des Ziels.
    2) Als **Domain Name** geben Sie entweder den vollen Domänennamen oder Schlüsselwörter (z.B. google) ein. Damit wird jeder Domänenname, der diese Schlüsselwörter enthält, betroffen sein, z.B. www.google.com, www.googleanalytics.com). Es können maximal vier Begriffe angegeben werden.

2. Klicken Sie **Save**.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

Klicken Sie **Next**, um auf die nächste Seite zu blättern oder **Previous**, um auf die vorige Seite zurückzukehren.

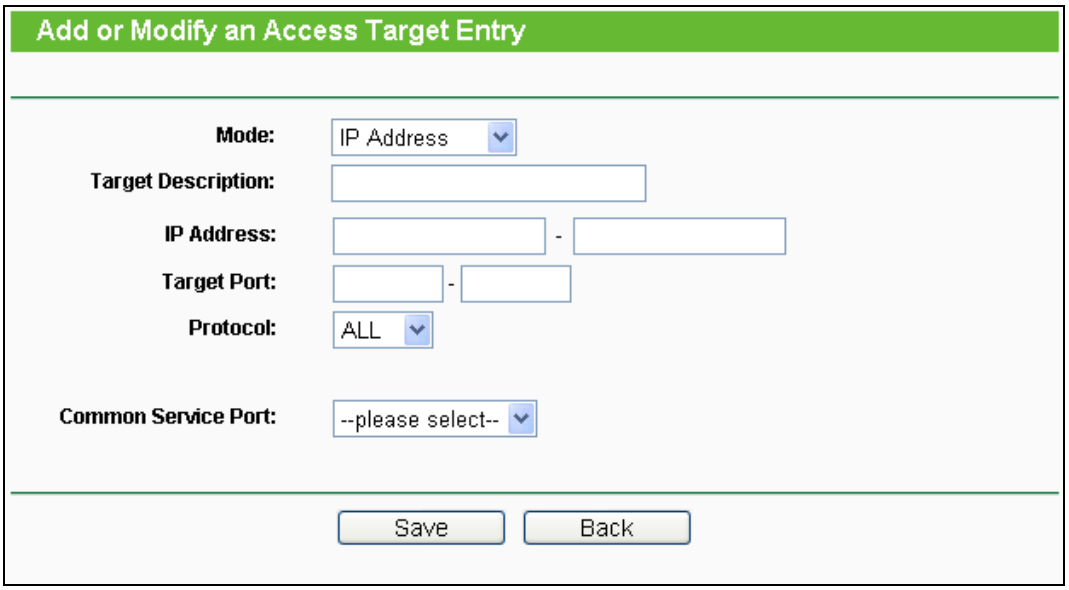


Bild 4-62 Zugriffszieleintrag anlegen oder bearbeiten

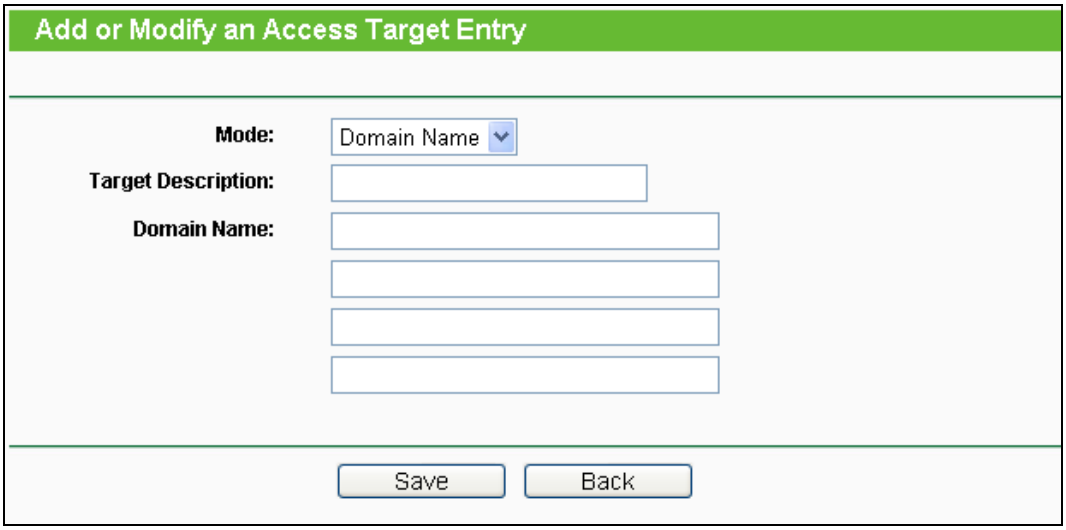


Bild 4-63 Zugriffszieleintrag anlegen oder bearbeiten

Beispiel: Möchten Sie die Internetaktivitäten des Hosts mit der MAC-Adresse 00-11-22-33-44-AA auf **www.google.com** beschränken, sollten Sie diesen Anweisungen Folge leisten:

1. Klicken Sie **Add New…** Bild 4-61, um den entsprechenden Dialog zu öffnen.
2. Als **Mode** wählen Sie „Domänenname“ aus.
3. Im Feld **Target Description** setzen Sie eine eindeutige Beschreibung für das Ziel, z.B. „Google“.
4. In das Feld **Domain Name** geben Sie „www.google.com“ ein.
5. Klicken Sie **Save**, um die Einstellungen zu übernehmen.

Sie werden auf die Zieleinstellungsseite zurückgeleitet, wo Sie die folgende Liste sehen.

ID	Target Description	Information	Modify
1	Target_1	www.google.com	Edit Delete

4.11.4 Schedule

Gehen Sie in das Menü **Access Control** → **Schedule**. Hier können Sie eine Planungsliste anlegen (Bild 4-64). Diese Liste wird von den Zugriffskontrollregeln benötigt.

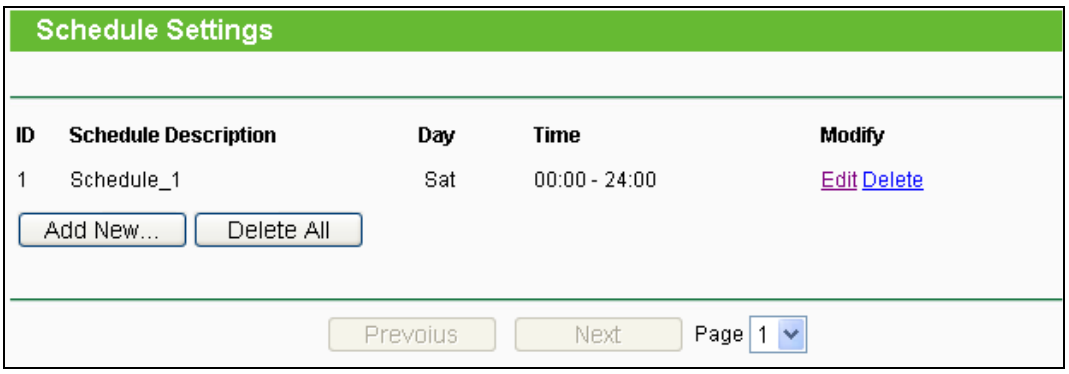


Bild 4-64 Planungseinstellungen

- **Schedule Description** - Die Beschreibung der Planung. Muss eindeutig sein.
- **Day** - Der Tag/die Tage, für den/die diese Planung zutrifft.
- **Time** - Der Zeitraum, zu dem diese Planung gilt.
- **Modify** - Hier können Sie Planungseinträge bearbeiten oder löschen.

Um eine neue Planung anzulegen, folgen Sie diesen Schritten**.**

1. Klicken Sie **Add New...** (Bild 4-64). Bild 4-65 erscheint.
2. Als **Schedule Description** geben Sie eine eindeutige Beschreibung (e.g. Planung_1).
3. Bei **Day** wählen Sie die Tage aus, die Sie wünschen.
4. Als **Time** können Sie den ganzen Tag auswählen (Option **all day-24 hours**) oder einen selbstgewählten Zeitabschnitt angeben.
5. Klicken Sie **Save**, um die Planungseinstellungen zu übernehmen.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

Klicken Sie **Next**, um auf die nächste Seite zu blättern oder **Previous**, um auf die vorige Seite zurückzukehren.

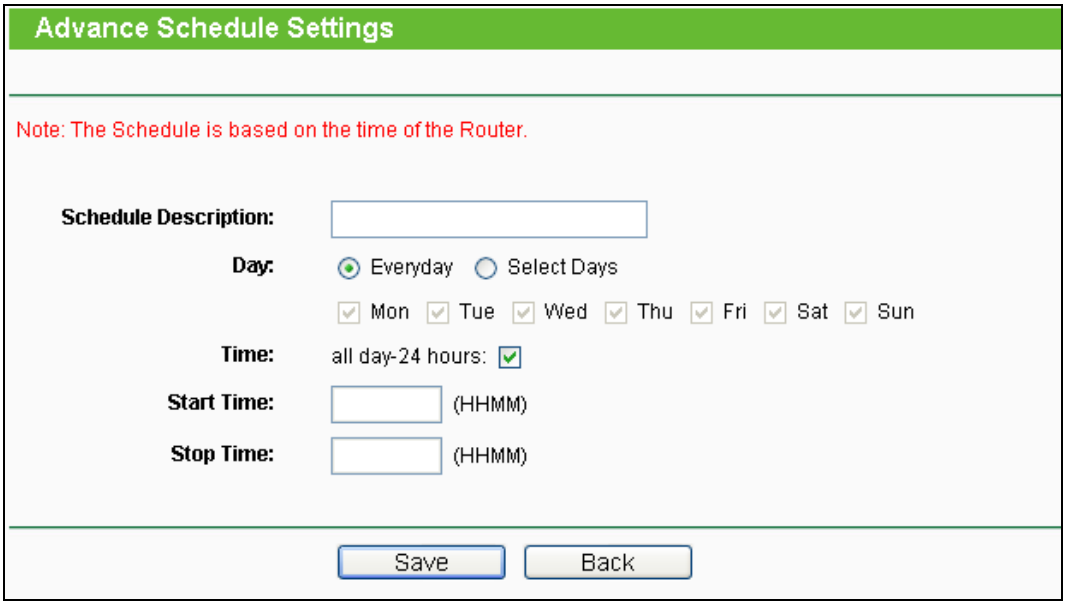


Bild 4-65 Erweiterte Planungseinstellungen

Beispiel: Sie möchten die Internetaktivitäten des Hosts mit der MAC-Adresse 00-11-22-33-44-AA auf www.google.com einschränken und dies auch nur samstags und sonntags von 18 bis 20 Uhr erlauben. Gehen Sie dazu wie folgt vor:

1. Klicken Sie **Add New...** (Bild 4-64) um auf die Seite **Advanced Schedule Settings** zu kommen.
2. In das Feld **Schedule Description** setzen Sie eine eindeutige Beschreibung, z.B. Schedule_1.
3. Unter **Day** wählen Sie „Sat“ und „Sun“ aus.
4. Aus **Start Time** geben Sie „1800“ und als **Stop Time** „2000“ ein.
5. Klicken Sie **Save**.

Sie kommen zurück auf die Planungseinstellungsseite und sehen diese Übersicht.

ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Sat Sun	18:00 - 20:00	Edit Delete

4.12 Advanced Routing

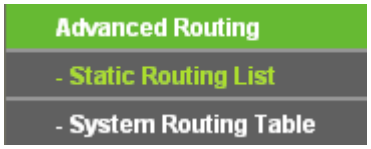


Bild 4-66 Advanced Routing

Im Menü **Advanced Routing** können Sie, wie in Bild 4-66 erkennbar, erweiterte Routingfunktionen konfigurieren.

4.12.1 Static Routing List

Im Menü **Advanced Routing** → **Static Routing List** können Sie statische Routen definieren (Bild 4-67). Eine Statische Route ist ein vorbestimmter Pfad, den ein Paket gehen muss, um einen bestimmten Host oder ein bestimmtes Netz zu erreichen.

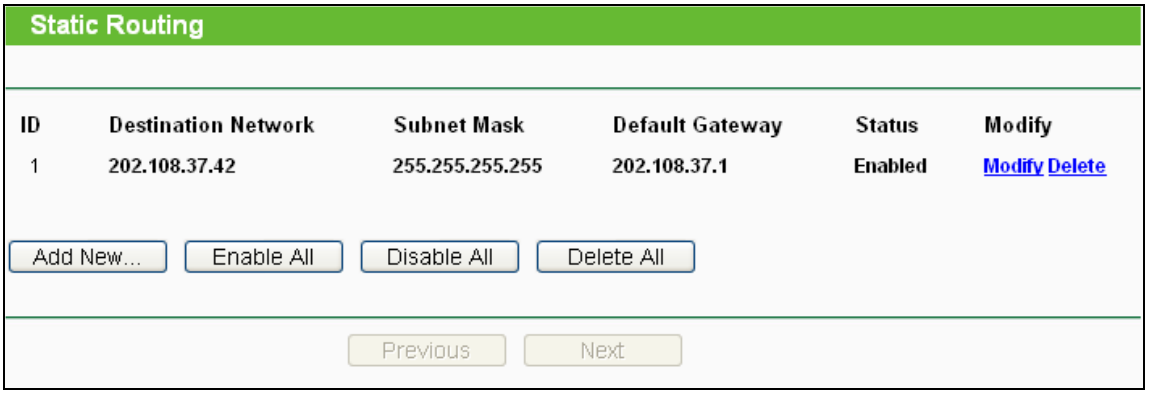


Bild 4-67 Statische Routen

Um Einträge für das Statische Routing zu erstellen:

1. Klicken Sie **Add New…** (Bild 4-67). Sie sehen Folgendes.

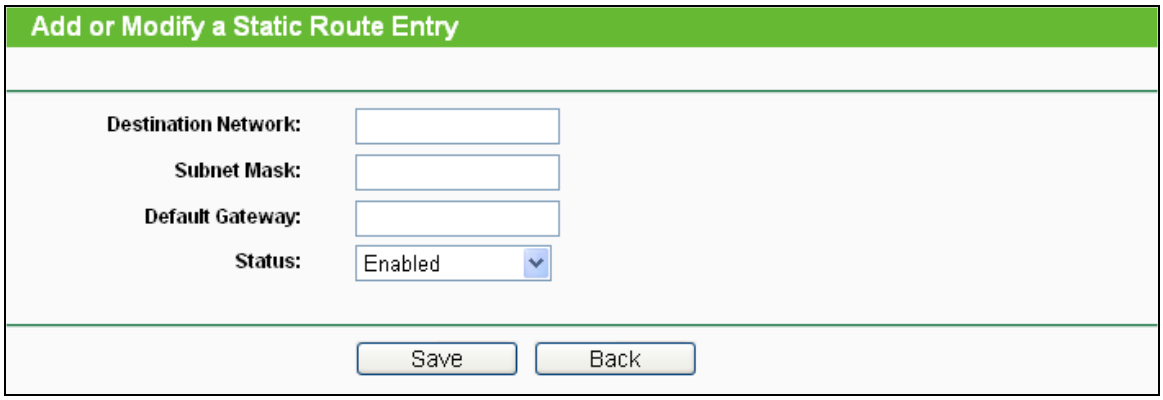


Bild 4-68 Statische Route hinzufügen oder bearbeiten

2. Geben Sie Folgendes ein:

   - **Destination Network** - Die Adresse des Zielnetzes/-hosts der statischen Route.
   - **Subnet Mask -** Die Subnetzmaske bestimmt, welcher Teil der IP-Adresse das Netz und welcher den Host bezeichnet.
   - **Default Gateway** - Die IP-Adresse des Gateways, der den Netzübergang zwischen dem Router und dem Zielnetz/-host darstellt.

3. Wählen Sie wunschgemäß **Enabled** (Aktiviert) or **Disabled** (Deaktiviert) als **Status** für diesen Eintrag aus.

4. Klicken Sie **Save**.

Weitere Optionen:

Klicken Sie **Delete**, um diesen Eintrag zu löschen.

Klicken Sie **Enable All**, um alle Einträge zu aktivieren.

Klicken Sie **Disable All**, um alle Einträge zu deaktivieren.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

Klicken Sie **Next**, um auf die nächste Seite zu blättern oder **Previous**, um auf die vorige Seite zurückzukehren.

4.12.2 System Routing Table

Über das Menü **Advanced Routing** → **System Routing Table** sehen Sie das im Bild 4-69 Gezeigte. Die Tabelle zeigt die aktuell verwendeten Statischen Routen mit **Destination Network** (Zielnetz), **Subnet Mask** (Subnetzmaske), **Gateway** und **Interface** (Schnittstelle).

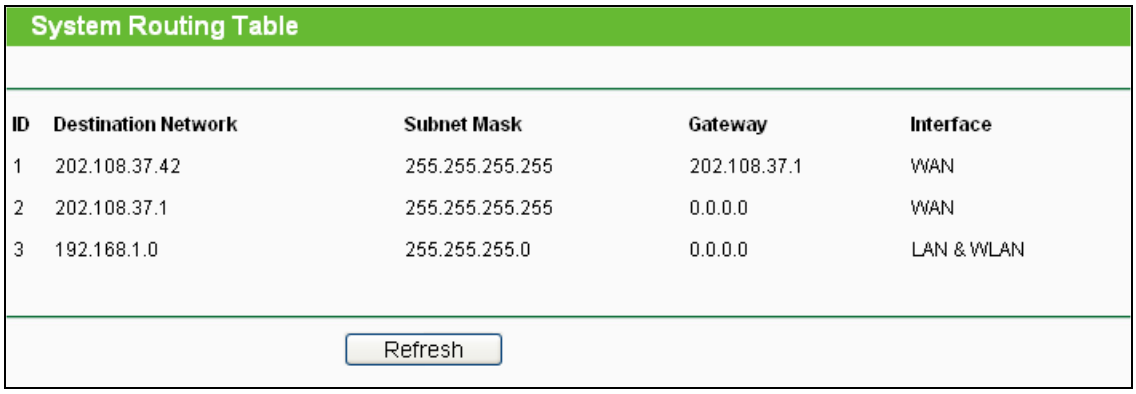


Bild 4-69 Systemroutingtabelle

- **Destination Network** - Die Adresse des Netzes, das das Ziel der Statischen Route darstellt.
- **Subnet Mask** - Die Subnetzmaske bestimmt, welcher Teil der IP-Adresse das Netz und welcher den Host definiert.
- **Gateway** - Die IP-Adresse des Gateways, der den Weg zum Ziel zur Verfügung stellt.
- **Interface** - Zeigt an, ob das Ziel über die **WAN**- (Internet) oder die lokale Seite (**LAN & WLAN**) erreichbar ist.

4.13 Bandwidth Control

Bild 4-70 Bandwidth Control

Das Menü **Bandwidth Control** erlaubt die Konfiguration der Upload- und der Download-Datenrate (Bild 4-70).

4.13.1 Control Settings

Das Menü **Bandwidth Control → Control Settings** ermöglicht die Konfiguration der Upload- und der Download-Datenrate. Zugelassen sind Werte von bis zu 100000kbps. Zur optimalen Kontrolle der Bandbreite wählen Sie bitte den richtigen Leitungstyp aus und fragen Sie bei Ihrem ISP bezüglich der jeweiligen Maximalbandbreite nach.

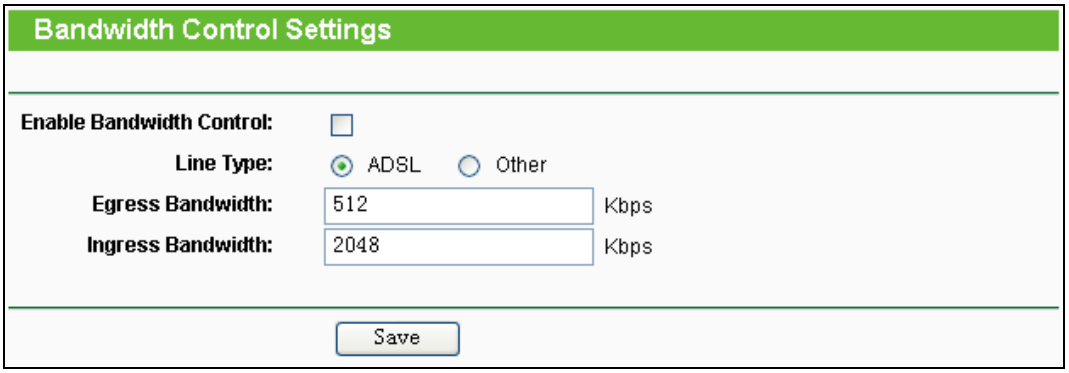


Bild 4-71 Datenratenkontrolleinstellungen

- **Enable Bandwidth Control -** Funktion aktivieren oder deaktivieren.
- **Line Type -** Wählen Sie hier Ihre Zugangsart aus. Sind Sie diesbezüglich unsicher, fragen Sie bitte bei Ihrem Internetdiensteanbieter nach.
- **Egress Bandwidth -** Uploadgeschwindigkeit des WAN-Ports.
- **Ingress Bandwidth -** Downloadgeschwindigkeit des WAN-Ports.

4.13.2 Rules List

Im Menü **Bandwidth Control → Rules List** können Sie die QoS-Regeln ansehen und bearbeiten (siehe folgende Abbildung).

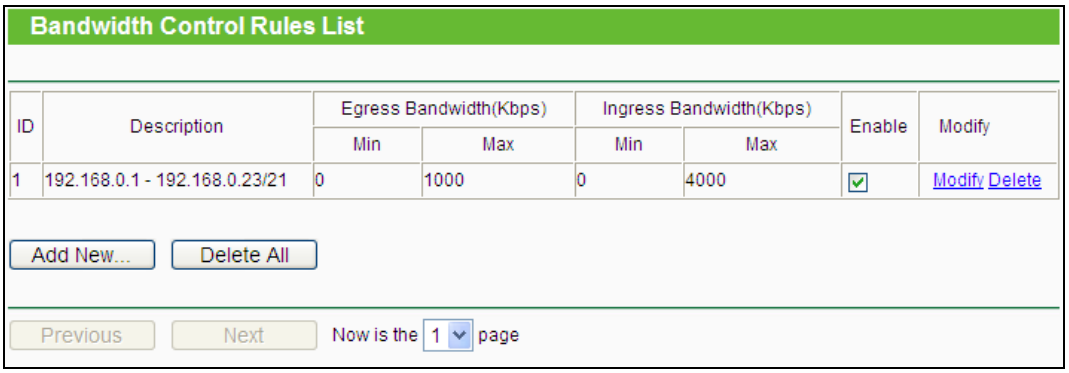


Bild 4-72 Regelliste der Datenratenkontrolle

- **Description -** Eine einfache Regelbeschreibung, z,B. der Adressbereich.
- **Egress bandwidth -** Maximale und minimale Uploadgeschwindigkeit am WAN-Port. Standard ist 0.

- **Ingress bandwidth -** Maximale und minimale Downloadgeschwindigkeit am WAN-Port. Standard ist 0.
- **Enable -** Zeigt an, ob die Regel aktiv ist.
- **Modify -** Klicken Sie **Modify** zum Bearbeiten der Regel oder **Delete**, um sie zu löschen.

Um eine Bandbreitenkontrollregel anzulegen.

Schritt 1: Klicken Sie **Add New…** (Bild 4-72). Sie sehen Bild 4-73.

Schritt 2: Geben Sie die im Folgenden gezeigten Informationen ein.

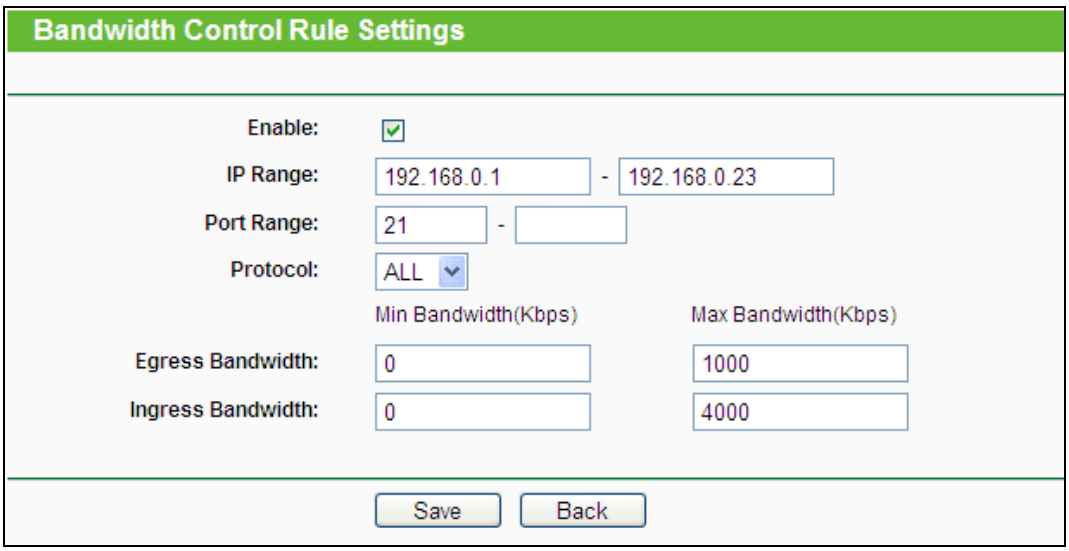


Bild 4-73 Datenratenkontrolleinstellungen

Schritt 3: Klicken Sie **Save**.

4.14 IP & MAC Binding

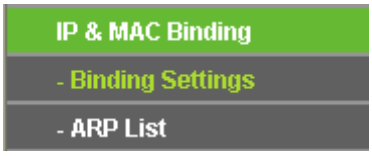


Bild 4-74 Bindungsmenü

Unter dem Bindungsmenü gibt es zwei Untermenüs (Bild 4-74): **Binding Setting** und **ARP List**.

4.14.1 Binding Settings

Diese Seite zeigt Ihnen die IP- und MAC-Adressbindungstabelle (Bild 4-75).

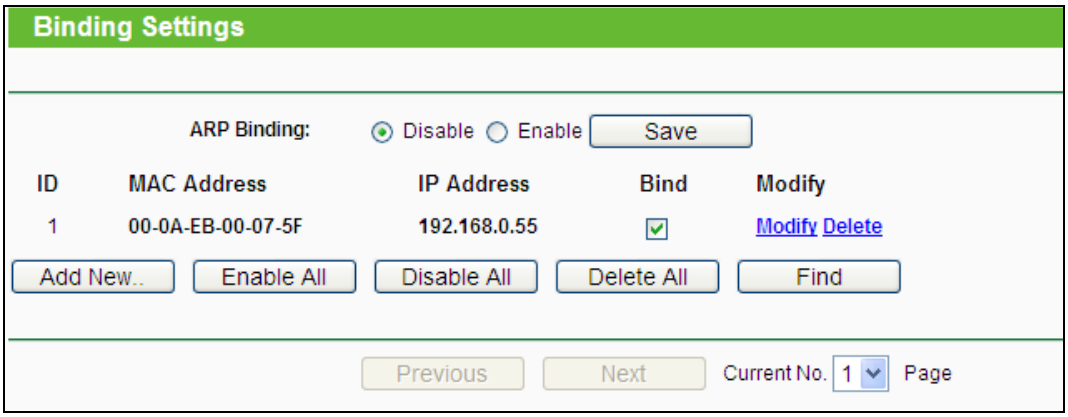


Bild 4-75 Bindungseinstellungen

- **MAC Address -** Die MAC-Adresse des kontrollierten LAN-Computers.
- **IP Address -** Die IP-Adresse des kontrollierten LAN-Computers.
- **Bind -** Wählen Sie dies an, um die ARP-Bindung für dieses Gerät zu aktivieren.
- **Modify -** Eintrag bearbeiten oder löschen.

Möchten Sie einen IP-/MAC-Adressbindungseintrag hinzufügen oder bearbeiten, können Sie **Add New** oder **Modify** klicken. Sie werden dann auf die nächste Seite weitergeleitet (Bild 4-76).

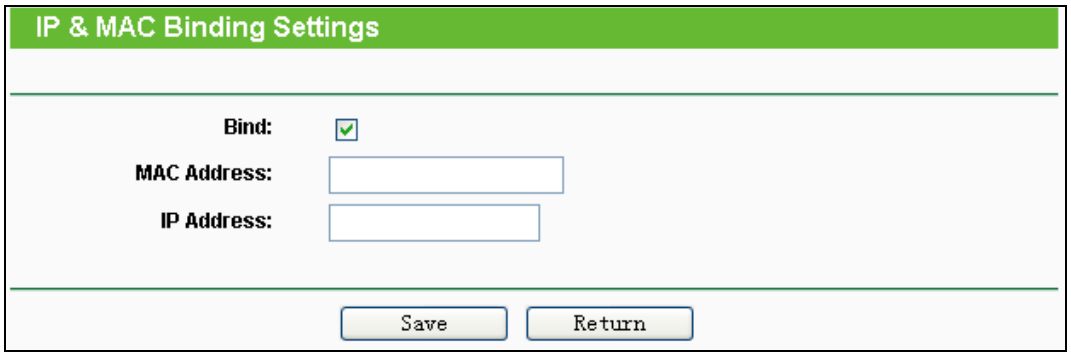


Bild 4-76 IP-/MAC-Adressbindungseinstellungen hinzufügen/bearbeiten

Um Einträge zur IP-/MAC-Adressbindung hinzuzufügen.

1. Klicken Sie **Add New...** Bild 4-75.
2. Geben Sie MAC- und IP-Adresse ein.
3. Wählen Sie **Bind** an.
4. Klicken Sie **Save**.

Um einen bestehenden Eintrag zu bearbeiten oder löschen, klicken Sie einfach in der entsprechenden Zeile auf **Modify** oder **Delete** in der Spalte **Modify**.

Um eine Suche nach einem Eintrag durchzuführen.

1. Klicken Sie **Find** (Bild 4-75).
2. Geben Sie die MAC-Adresse oder die IP-Adresse ein.

3. Klicken Sie **Find**, wie auf Bild 4-77 gezeigt.

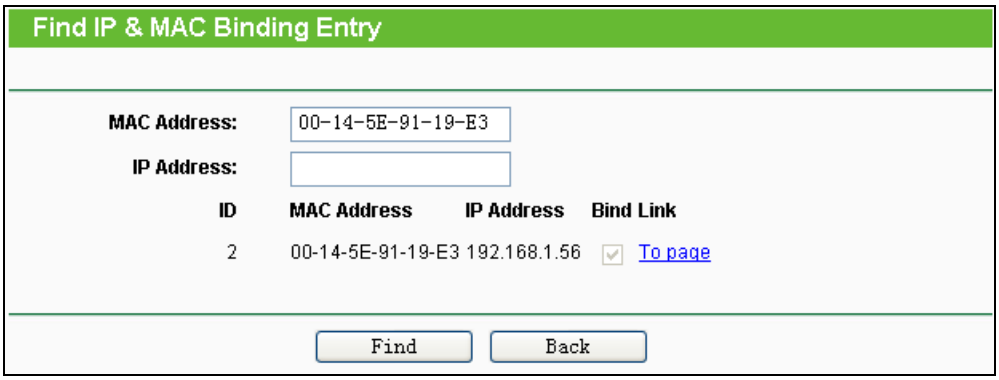


Bild 4-77 IP-/MAC-Adressbindungseintrag finden

Klicken Sie **Enable All**, um alle Einträge zu aktivieren.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

4.14.2 ARP List

Zur Computerverwaltung können Sie die Zusammenhänge zwischen MAC- und IP-Adresse auf der ARP-Liste überwachen und die Einträge in der ARP-Liste bearbeiten. Diese Seite zeigt die ARP-Liste mit allen existierenden IP- und MAC-Adressbindungseinträgen (Bild 4-78).

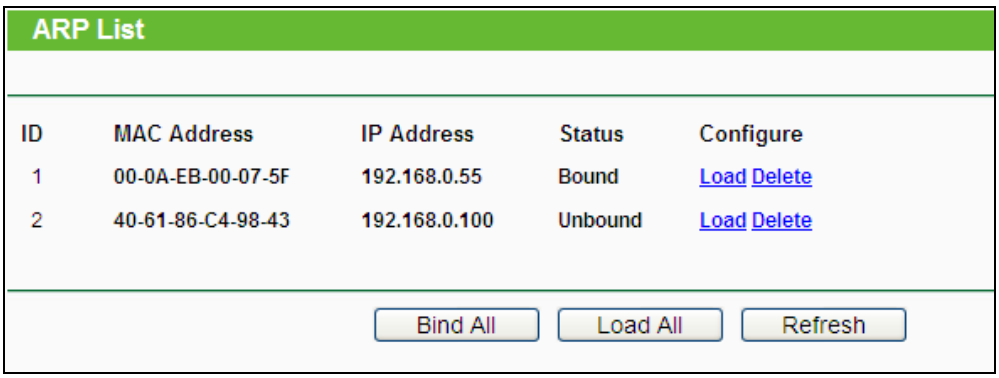


Bild 4-78 ARP-Liste

- **MAC Address -** Die MAC-Adresse des kontrollierten LAN-Computers.
- **IP Address -** Die zugewiesene IP-Adresse des kontrollierten LAN-Computers.
- **Status - Bound** oder **Unbound** (Status der Bindung).
- **Configure -** Eintrag laden (**Load**) oder löschen (**Delete)**.
  - **Load -** Element in die IP-/MAC-Adressbindungsliste aufnehmen.
  - **Delete -** Element aus der Liste entfernen.

Klicken Sie **Bind All**, um alle aktuellen Einträge zu binden. Diese Funktion ist nur für aktive Einträge verfügbar.

Klicken Sie **Load All**, um alle Einträge in die Bindungsliste zu laden.

Klicken Sie **Refresh**, um die Ansicht zu aktualisieren.

☞ **Bemerkung:**

Ein Eintrag könnte unter Umständen nicht in die Bindungsliste geladen werden, wenn dessen IP-Adresse schon geladen ist. In diesem Fall informiert Sie eine Warnung. Entsprechend lädt der Befehl **Alle laden** nur die konfliktfreien Elemente in die Bindungsliste.

4.15 Dynamic DNS

Im Menü **Dynamic DNS** können Sie die Funktionalität des Dynamischen DNS einstellen.

Der Router verfügt über die DDNS(Dynamic Domain Name System)-Funktionalität. Mit DDNS können Sie Ihrer dynamisch zugeteilten Internet-IP-Adresse einen festen Host-/Domänennamen zuordnen. Dies ist sehr nützlich, wenn Sie Ihre Website selbst hosten oder Serverdienste wie z.B. FTP hinter dem Router laufen lassen wollen. Bevor Sie diese Funktionalität nutzen können, müssen Sie sich bei einem DDNS-Dienst wie z.B. dyndns.org, comexe.cn oder no-ip.com anmelden. Der Anbieter gibt Ihnen dann ein Passwort oder einen Schlüssel.

4.15.1 Comexe

Haben Sie als DDNS-Anbieter comexe.cn gewählt, erscheint folgende Seite (Bild 4-79).

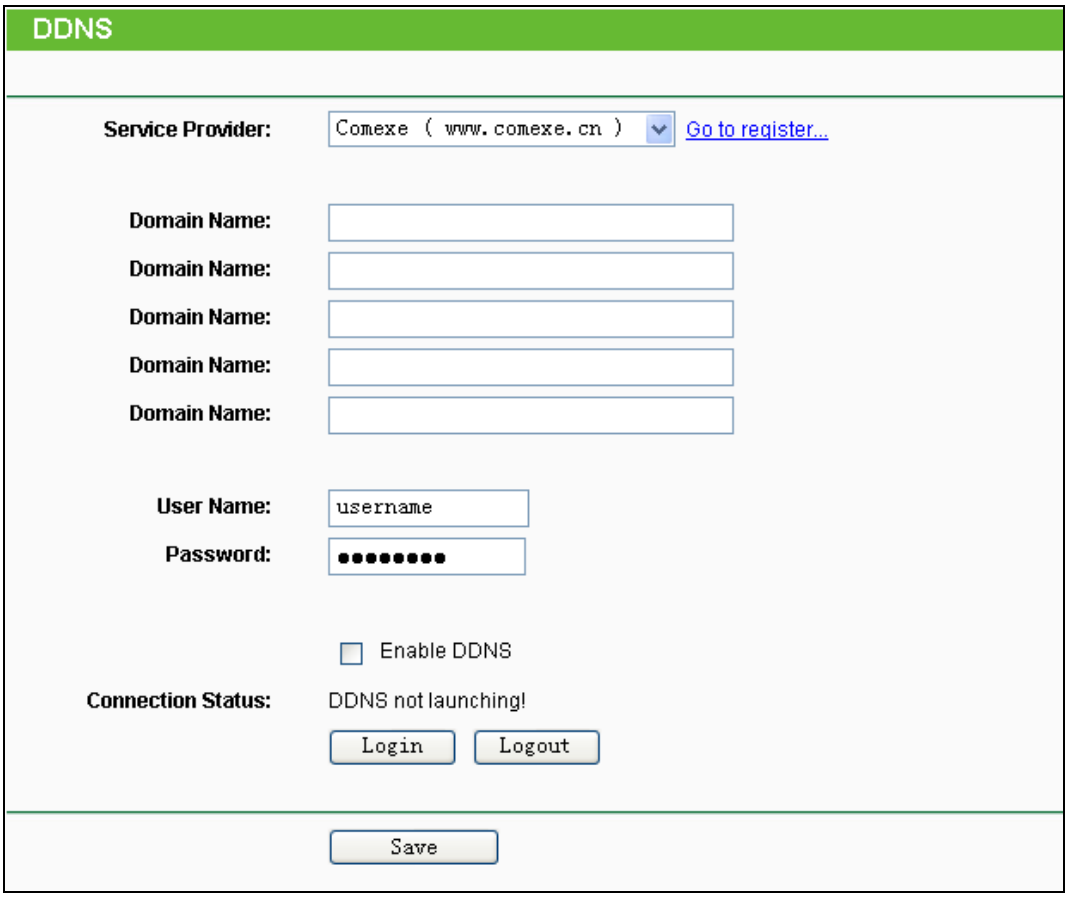


Bild 4-79 DDNS mit comexe.cn

Um DDNS einzurichten, tun Sie Folgendes:

1. Geben Sie den Domänennamen unter **Domain Name** ein.
2. Geben Sie unter **User Name** den Benutzernamen Ihres DDNS-Accounts ein.
3. Geben Sie unter **Password** das Passwort Ihres DDNS-Accounts ein.
4. Klicken Sie **Login,** um sich in den DDNS-Dienst einzuloggen.

Connection Status - Der Verbindungsstatus des DDNS-Dienstes.

Klicken Sie **Logout**, um sich aus dem DDNS-Dienst auszuloggen.

4.15.2 DynDNS

Haben Sie als DDNS-Anbieter dyndns.org ausgewählt, erscheint folgende Seite (Bild 4-80).

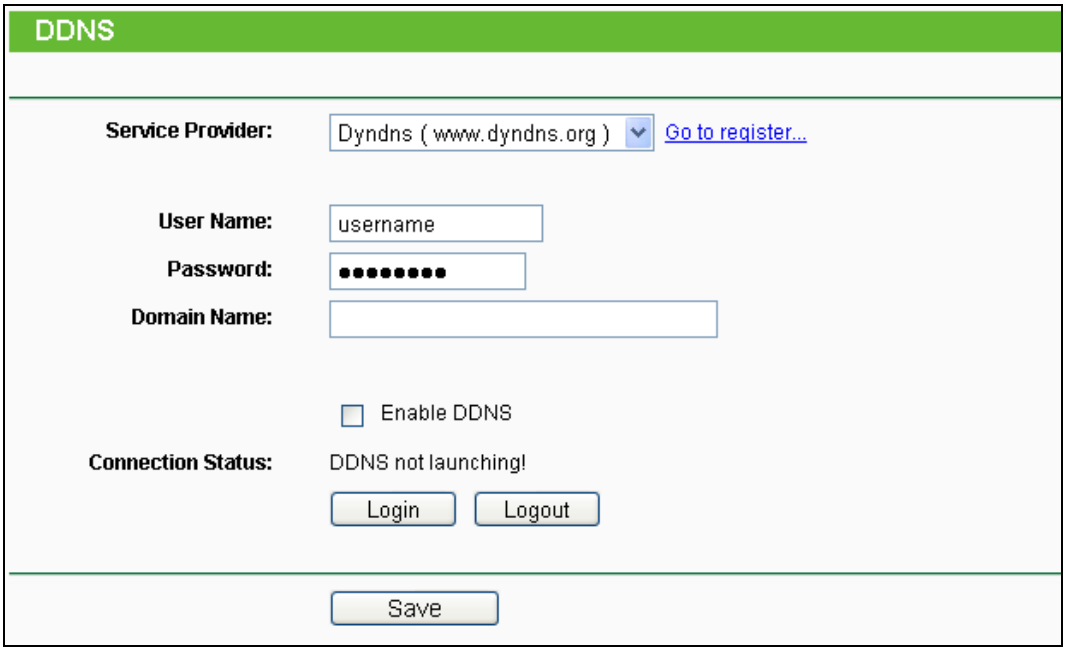


Bild 4-80 DDNS mit dyndns.org

Um DDNS einzurichten, tun Sie Folgendes:

1. Geben Sie unter **User Name** den Benutzernamen Ihres DDNS-Accounts ein.
2. Geben Sie unter **Password** das Passwort Ihres DDNS-Accounts ein.
3. Geben Sie den Domänennamen unter **Domain Name** ein.
4. Klicken Sie **Login,** um sich in den DDNS-Dienst einzuloggen.

Connection Status - Der Verbindungsstatus des DDNS-Dienstes.

Klicken Sie **Logout**, um sich aus dem DDNS-Dienst auszuloggen.

4.15.3 No-IP

Haben Sie als DDNS-Anbieter no-ip.com ausgewählt, erscheint folgende Seite (Bild 4-81).

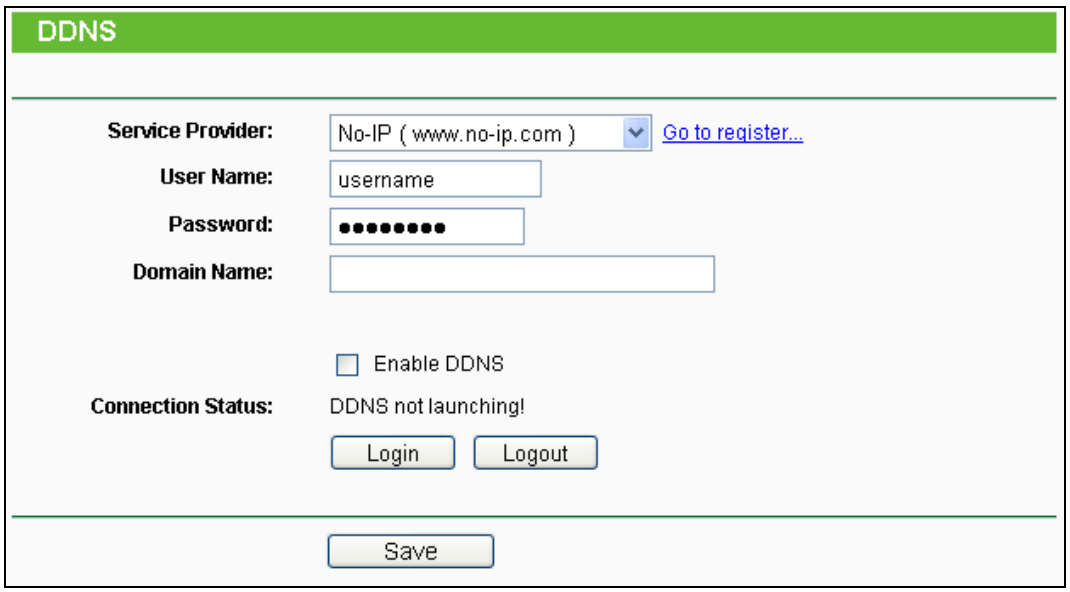


Bild 4-81 DDNS mit no-ip.com

Um DDNS einzurichten, tun Sie Folgendes:

1. Geben Sie unter **User Name** den Benutzernamen Ihres DDNS-Accounts ein.
2. Geben Sie unter **Password** das Passwort Ihres DDNS-Accounts ein.
3. Geben Sie den Domänennamen unter **Domain Name** ein.
4. Klicken Sie **Login,** um sich in den DDNS-Dienst einzuloggen.
5. Klicken Sie **Logout**, um sich aus dem DDNS-Dienst auszuloggen.

4.16 System Tools

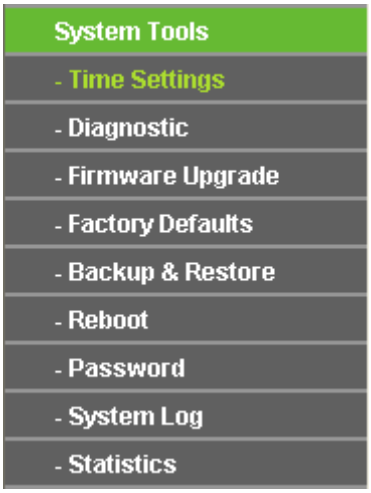


Bild 4-82 Das Menü **System Tools**

Das Menü **System Tools** bietet Ihnen folgende Untermenüs: **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults, Backup & Restore, Reboot, Password, System Log** und **Statistics**.

4.16.1 Time Settings

Im Menü **System Tools** → **Time Settings** können Sie die Echtzeituhr des Routers von Hand oder mittels der aus dem Internet abgefragten GMT einstellen.

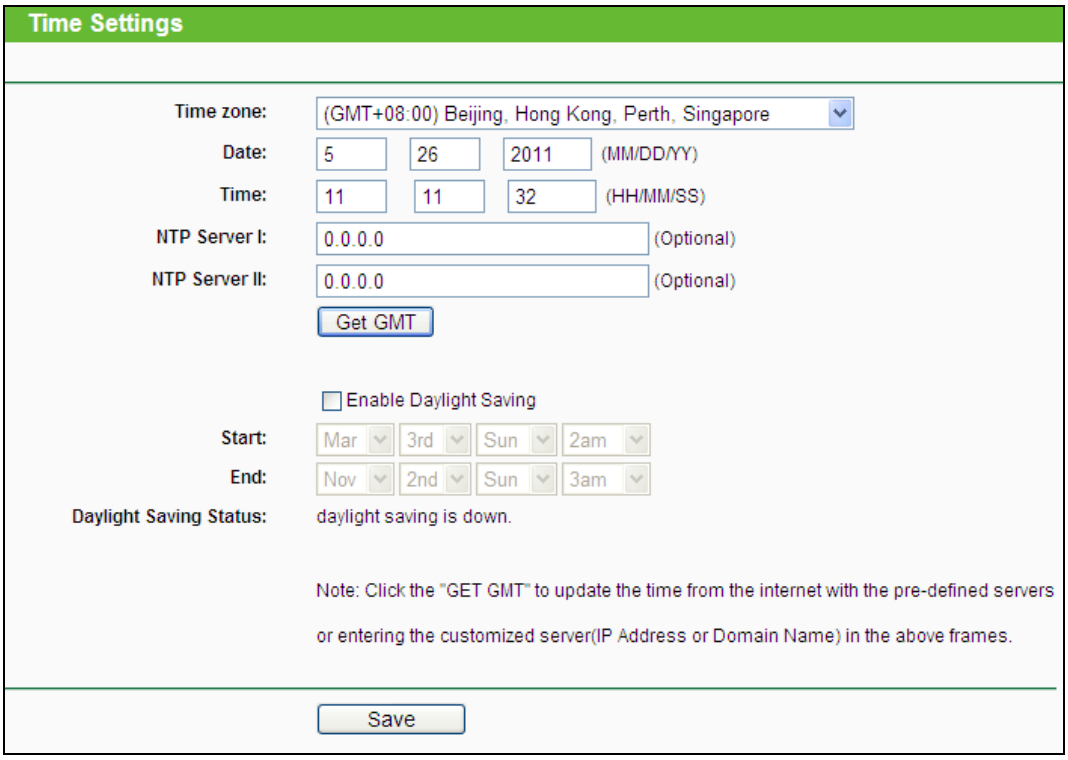


Bild 4-83 Zeiteinstellungen

- **Time Zone -** Wählen Sie hier die Zeitzone aus, in der der Router steht.
- **Date -** Geben Sie das aktuelle Datum im Format „MM/TT/JJJJ“ ein.
- **Time -** Geben Sie die aktuelle Uhrzeit im Format „hh/mm/ss“ ein.
- **NTP Server I, NTP Server II -** Geben Sie hier die Adresse eines NTP-Servers oder zweier NTP-Server ein, wird der Router von diesem die Uhrzeit abfragen, sobald er eine Internetverbindung hergestellt hat. Zusätzlich zu diesem konfigurierbaren sind einige weitere NTP-Server in der Routersoftware hart kodiert, so dass er auch von diesen die Uhrzeit automatisch abfragen kann.
- **Enable Daylight Saving -** Hiermit beachtet der Router die weiter unten definierte Sommerzeitregelung.
- **Start -** Beginn der Sommerzeit. Wählen Sie nacheinander Monat, Woche, Tag und Stunde.
- **End -** Ende der Sommerzeit. Wählen Sie nacheinander Monat, Woche, Tag und Stunde.
- **Daylight Saving Status -** Zeigt an, ob die Sommerzeit gerade aktiv ist.

Die Zeit können Sie auch von Hand mit folgenden Schritten einstellen:

1. Wählen Sie die zutreffende Zeitzone aus.

2. Geben Sie das Datum (als **Date**) im Format „MM/TT/JJJJ“ und die aktuelle Uhrzeit (als **Time**) im Format „HH/MM/SS“ ein.
3. Klicken Sie **Save**.

Zur automatischen Zeiteinstellung konfigurieren Sie Ihren Router bitte so:

1. Wählen Sie die zutreffende Zeitzone aus.
2. Geben Sie unter **NTP Server I** oder **NTP Server II** eine oder zwei NTP-Server-Adressen ein.
3. Klicken Sie **Get GMT**, um die GMT bei bestehender Internetverbindung abzurufen.

Zur automatischen Umstellung zwischen Sommer- und Winterzeit tun Sie dies:

1. Aktivieren Sie Sommerzeit (**Enable Daylight Saving**).
2. Wählen Sie den **Start**- und den **End**zeitpunkt der Sommerzeit aus.
3. Klicken Sie **Save**.

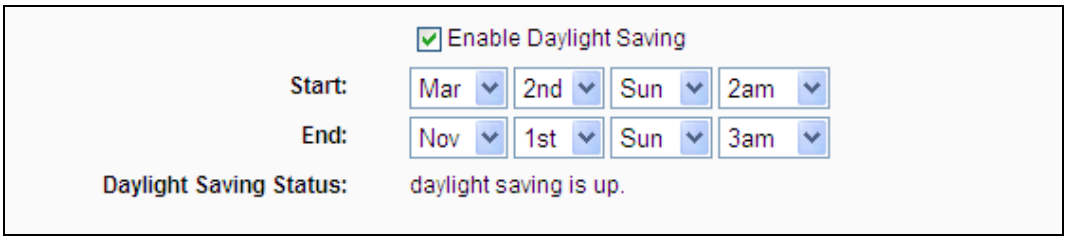


Bild 4-84 Sommerzeiteinstellungen

Bemerkungen:

1) Diese Einstellung beeinflusst einige zeitbasierende Funktionen wie z.B. die Firewall. Hierfür müssen die Uhrzeit und die Zeitzone zwingend gesetzt werden.
2) Die Uhrzeit geht verloren, wenn die Spannungsversorgung getrennt wird.
3) Der Router setzt die Systemzeit automatisch, wenn er eine Internetverbindung bekommt und entsprechend konfiguriert ist.
4) Es dauert nach dem Speichern ca. eine Minute, bis die Sommerzeiteinstellung wirksam wird.

4.16.2 Diagnostic

Das Menü **System Tools** → **Diagnostic** erlaubt die Ausführung von Ping- und Traceroute-Befehlen zur Überprüfung der Konnektivität.

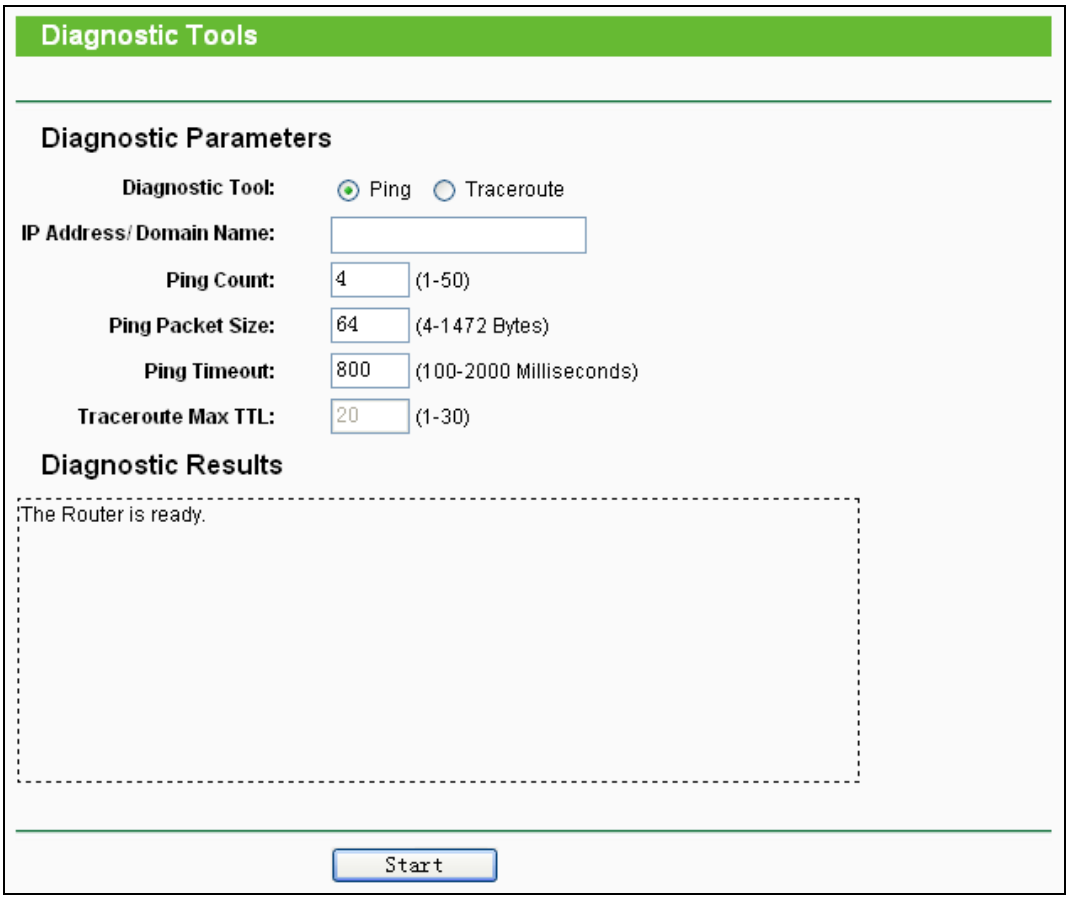


Bild 4-85 Diagnosetools

- **Diagnostic Tool -** Wählen Sie zwischen Ping und Traceroute.
  - **Ping -** Hiermit können Sie die Konnektivität, die Erreichbarkeit und die Namensauflösung für einen gegebenen Host testen.
  - **Traceroute -** Dieses Tool ist in der Lage, die Verbindungsperformance zu testen.

  Bemerkung:

  Ping und Traceroute akzeptieren sowohl IP-Adressen als auch Domänennamen. Können Sie eines der Tools für eine IP-Adresse erfolgreich laufen lassen, für einen Domänennamen aber nicht, deutet dies darauf hin, dass die Namensauflösung nicht funktioniert.

IP Address/Domain Name - Geben Sie das Ziel als IP-Adresse (z.B. 202.108.22.5) oder als Domänenname (z.B. www.tp-link.com) an.

- **Pings Count -** Die Anzahl der zu sendenden Ping-Pakete.
- **Ping Packet Size -** Die Größe eines Pingpakets.
- **Ping Timeout -** Setzen Sie hier die Wartezeit für ein Pingpaket. Kommt innerhalb dieser Zeit keine Antwort, gilt der Ping als fehlgeschlagen.
- **Traceroute Max TTL -** Die maximale Knotenanzahl für eine Traceroute-Verbindung.

Klicken Sie **Start**, um die Konnektivität zu testen.

Der Abschnitt **Diagnostic Results** zeigt die Ergebnisse der Diagnose an. Bei einem Ergebnis ähnlich wie diesem ist die Internetkonnektivität gut.

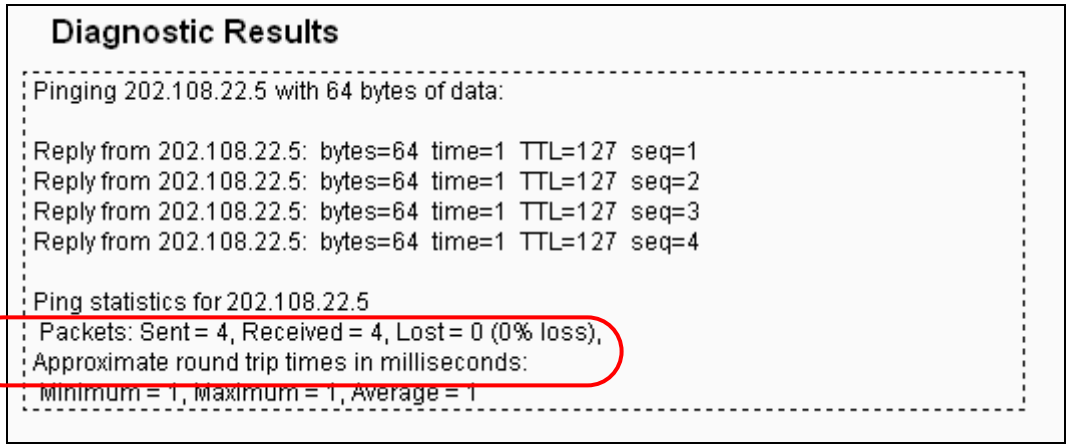


Bild 4-86 Diagnoseergebnisse

Bemerkung:

Diese Tools können nur von einem Computer aus zur gleichen Zeit gestartet werden. Die Optionen **Ping Count**, **Ping Packet Size** und **Ping Timeout** werden von der **Ping**-Funktion verwendet, während **Traceroute Max TTL** von der **Traceroute**-Funktion genutzt wird.

4.16.3 Firmware Upgrade

Die Seite **System Tools** → **Firmware Upgrade** erlaubt Firmwareupgrades, um Ihren Router aktuell zu halten.

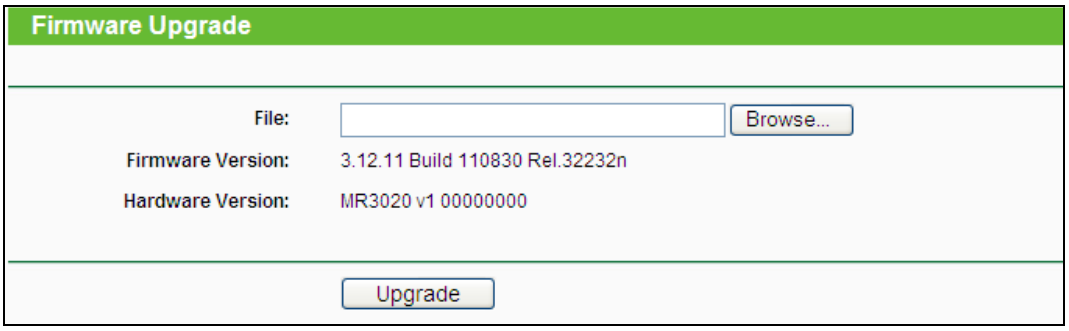


Bild 4-87 Firmwareupgrade

- **Firmware Version -** Zeigt Ihnen die aktuell installierte Firmwareversion.
- **Hardware Version -** Zeigt Ihnen die aktuelle Hardwareversion. Diese muss unbedingt mit der Hardwareversion der Update-Datei übereinstimmen.

Um die Firmware zu aktualisieren, gehen Sie so vor:

1. Laden Sie sich die neueste Firmwaredatei für Ihr Modell von der TP-LINK-Webseite www.tp-link.com herunter und entpacken Sie sie.
2. Verbinden Sie sich mit dem Router über eine Kabelverbindung, nicht über WLAN. Klicken Sie im Webinterface **Durchsuchen…**, um die heruntergeladene und entpackte Datei auszuwählen.
3. Klicken Sie **Upgrade**.

☞ **Bemerkungen:**

1) Neue Firmware ist auf **www.tp-link.com** zu finden und kann kostenlos heruntergeladen werden. Haben Sie mit dem Router keine Probleme und bietet die neue Firmware keine unbedingt benötigten neuen Funktionalitäten, brauchen Sie die Firmware nicht zwingend zu aktualisieren.
2) Beim Firmwareupgrade kann Ihre aktuelle Konfiguration verloren gehen. Stellen Sie also sicher, dass Sie sie in einer Datei gespeichert haben, bevor Sie mit dem Upgrade beginnen.
3) Während des Firmwareupgrades darf der Router keinesfalls von der Versorgungsspannung getrennt oder mittels der Reset-Taste zurückgesetzt werden.
4) Nach erfolgreichem Upgrade startet der Router automatisch neu.
5) Führen Sie das Upgrade nie über eine WLAN-Verbindung durch, sondern nur über Kabel.

4.16.4 Factory Defaults

Die Seite **System Tools** → **Factory Defaults** ermöglicht das Wiederherstellen der Standardeinstellungen des Routers.

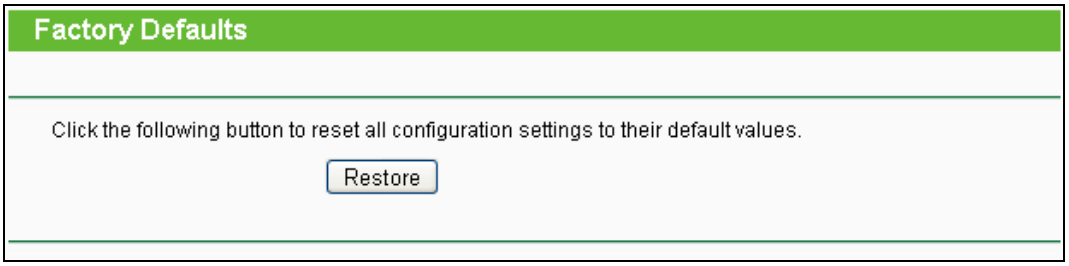


Bild 4-88 Standardeinstellungen wiederherstellen

Klicken Sie **Restore**, um alle Einstellungen zurückzusetzen. Danach gelten.

- **Benutzername**: admin
- **Passwort**: admin
- **IP-Adresse**: 192.168.0.254
- **Subnetzmaske**: 255.255.255.0

☞ **Bemerkung:**

Hierbei gehen prinzipbedingt alle im Router gespeicherten Einstellungen verloren.

4.16.5 Backup & Restore

Unter **System Tools** → **Backup & Restore** können Sie die Routerkonfiguration lokal speichern sowie eine zuvor gespeicherte Konfiguration wiederherstellen (Bild 4-89).

Bild 4-89 Konfiguration sichern und wiederherstellen

- Klicken Sie **Backup**, um die aktuelle Konfiguration herunterzuladen und lokal zu speichern.
- Um eine alte Konfiguration wiederherzustellen, tun Sie Folgendes.
  - Klicken Sie **Durchsuchen**, um die Backup-Datei auszuwählen.
  - Klicken Sie **Restore**.

Bemerkung:

Beim Wiederherstellungsprozess geht die aktuell im Router befindliche Konfiguration verloren. Der Prozess dauert ca. 20 Sekunden. Anschließend startet der Router neu. Bitte lassen Sie den Router während der Wiederherstellung eingeschaltet, um Schäden zu vermeiden.

4.16.6 Reboot

Unter **System Tools** → **Reboot** können Sie durch Klick auf **Reboot** den Router neustarten.

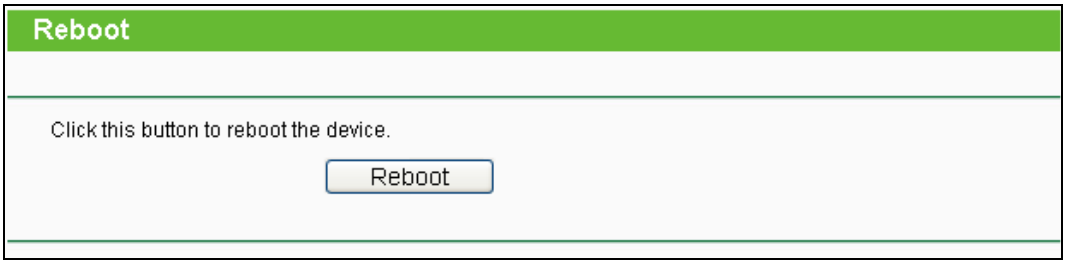


Bild 4-90 Routerneustart

Einige Einstellungen des Routers können nur durch einen Neustart übernommen werden:

- Ändern der LAN-IP-Adresse (der Router startet automatisch neu).
- DHCP-Konfigurationsänderungen.
- Änderungen an der Drahtloskonfiguration.
- Ändern des Ports für die Fernwartung.
- Firmwareupgrade (der Router startet automatisch neu).
- Zurücksetzen der Routereinstellungen (der Router startet automatisch neu).
- Wiederherstellen einer alten Konfiguration mittels Dateiupload (der Router startet automatisch neu).

4.16.7 Password

Auf **System Tools** → **Password** können Sie die Router-Zugangsdaten ändern (Bild 4-91).

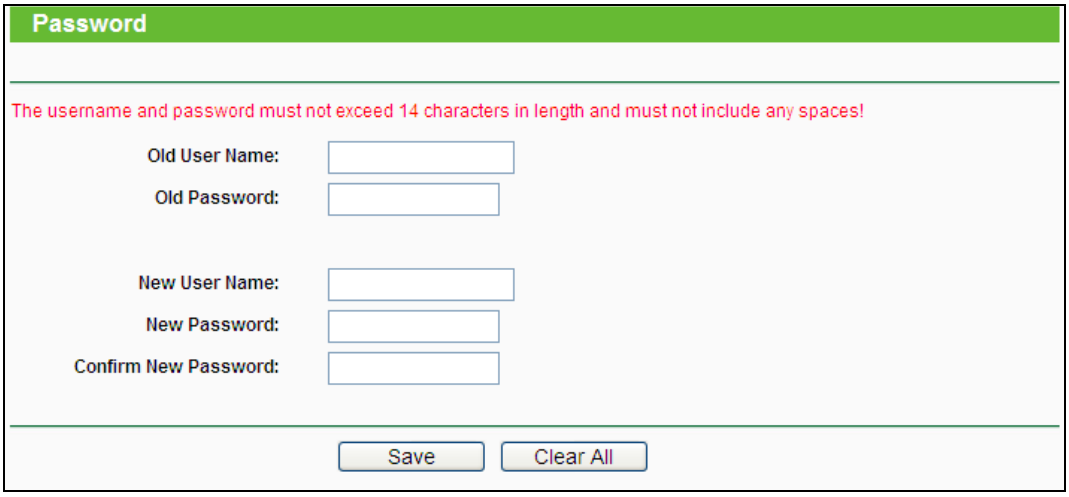


Bild 4-91 Benutzernamen und Passwort ändern

Es wird empfohlen, die Zugangsdaten abzuändern. Diese werden von allen Benutzern abgefragt, die versuchen, auf das webbasierende Konfigurationstool zuzugreifen.

Bemerkung:

Benutzername und Passwort dürfen nicht länger als jeweils 14 Zeichen sein und keine Leerzeichen enthalten. Um Tippfehler auszuschließen, muss das Passwort zweimal eingegeben werden.

Klicken Sie **Save**, wenn Sie die Daten eingegeben haben.

Klicken Sie **Clear All,** um die Feldinhalte zu löschen.

4.16.8 System Log

Über die Seite **System Tools** → **System Log** können Sie die Routerprotokolle abfragen.

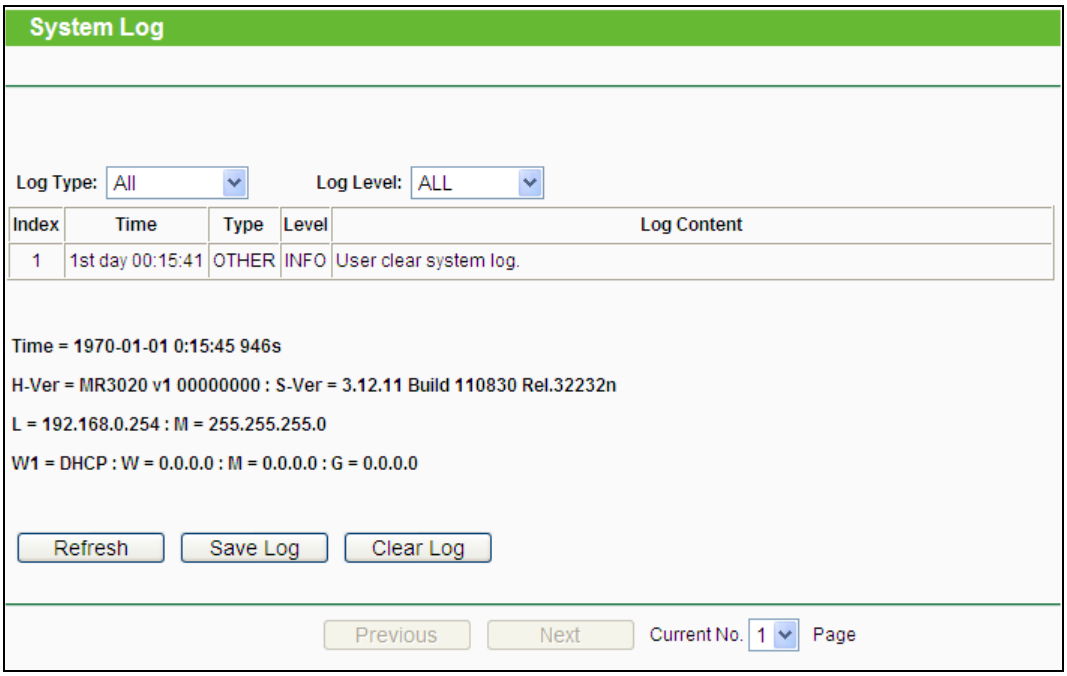


Bild 4-92 Systemprotokoll

4.16.9 Statistics

Unter **System Tools** → **Statistics** können Sie die Routerstatistiken einsehen. Diese umfassen: Gesamtdatenverkehr und Datenverkehr während des letzten „Packet Statistics Interval“.

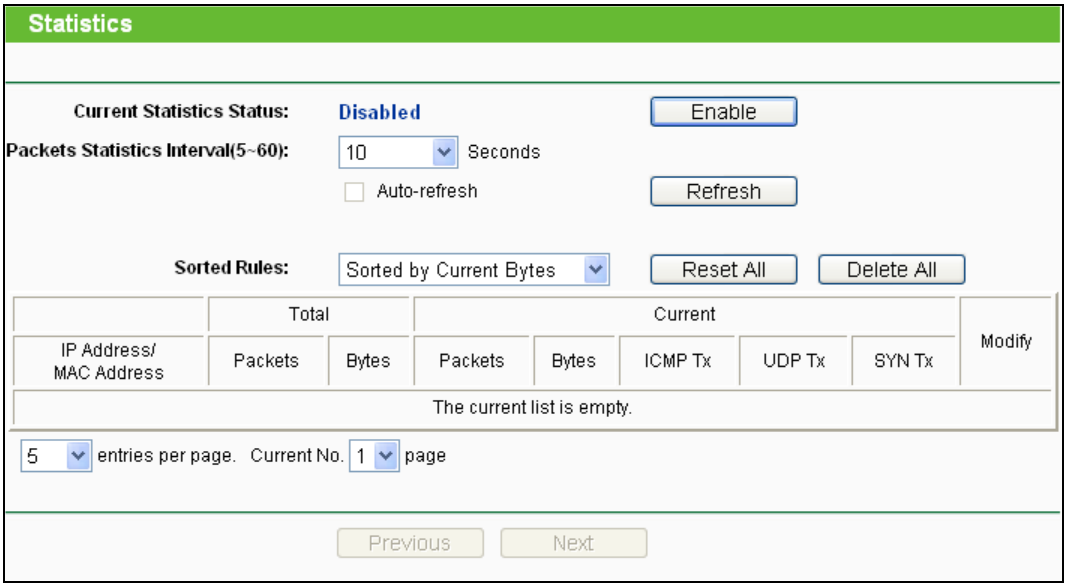


Bild 4-94 Statistiken

- **Current Statistics Status -** Kann hier aktiviert oder deaktiviert werden.
- **Packets Statistics Interval(5-60) -** Die Dauer eines Zeitabschnittes, den eine Paketstatistik geführt wird, in Sekunden. Standardwert ist 10. Gültige Werte: 5 bis 60.
- **Sorted Rules -** Hiermit können Sie die Regeln nach Ihren Vorstellungen ordnen.

Aktivieren Sie **Auto-refresh**, um die Ansicht periodisch neu zu laden.

Klicken Sie **Refresh**, um die Ansicht sofort zu aktualisieren.

Klicken Sie **Reset All**, um alle Werte auf null zu setzen.

Klicken Sie **Delete All,** um alle Einträge aus der Tabelle zu entfernen.

Statistiktabelle:

IP/MAC Address		Die IP-/MAC-Adresse, zu der diese Statistiken gehören.
Total	**Packets**	Gesamtanzahl der vom Router übertragenen Pakete.
	Bytes	Vom Router übertragene Gesamtdatenmenge.
Current	**Packets**	Anzahl übertragener Pakete während des letzten Paketstatistikintervalls.
	Bytes	Während des letzten Paketstatistikintervalls übertragene Datenmenge.
	ICMP Tx	Anzahl zum WAN-Port gesendeter ICMP-Pakete während des letzten Paketstatistikintervalls.
	UDP Tx	Anzahl zum WAN-Port gesendeter UDP-Pakete während des letzten Paketstatistikintervalls.
	TCP SYN Tx	Anzahl zum WAN-Port gesendeter TCP-SYN-Pakete während des letzten Paketstatistikintervalls.
Modify	**Reset**	Wert des Eintrags auf Null zurücksetzen.
	Delete	Diesen Eintrag aus der Tabelle löschen.

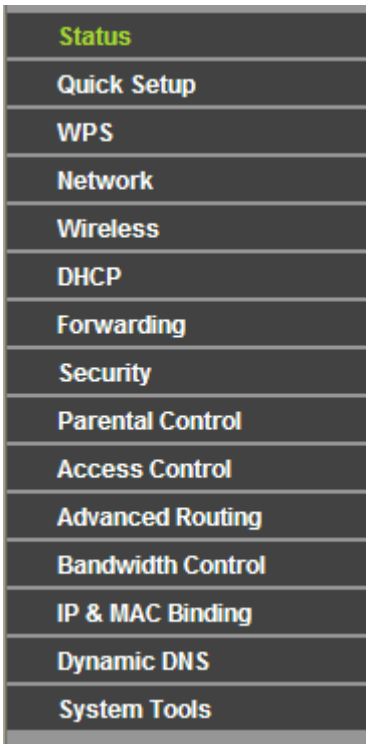
Standardmäßig sind 5 Einträge pro Seite zu sehen. Klicken Sie **Next**, um zur nächsten Seite zu blättern oder **Previous**, um zur vorigen Seite zurückzukehren.

Kapitel 5. WISP-Modus

Dieses Kapitel zeigt Ihnen die Schlüsselfunktionalitäten und Konfigurationsmöglichkeiten jedes Menüs.

5.1 Login

Nachdem Sie sich erfolgreich eingeloggt haben, sehen Sie die fünfzehn Hauptmenüs auf der linken Bildschirmseite. Im rechten HTML-Frame ist der Hilfetext zu sehen.



Im Folgenden werden diese Hauptmenüs detailliert behandelt.

5.2 Status

Die Seite **Status** zeigt Statusinformationen zum Router. Diese Informationen können hier nicht geändert werden.

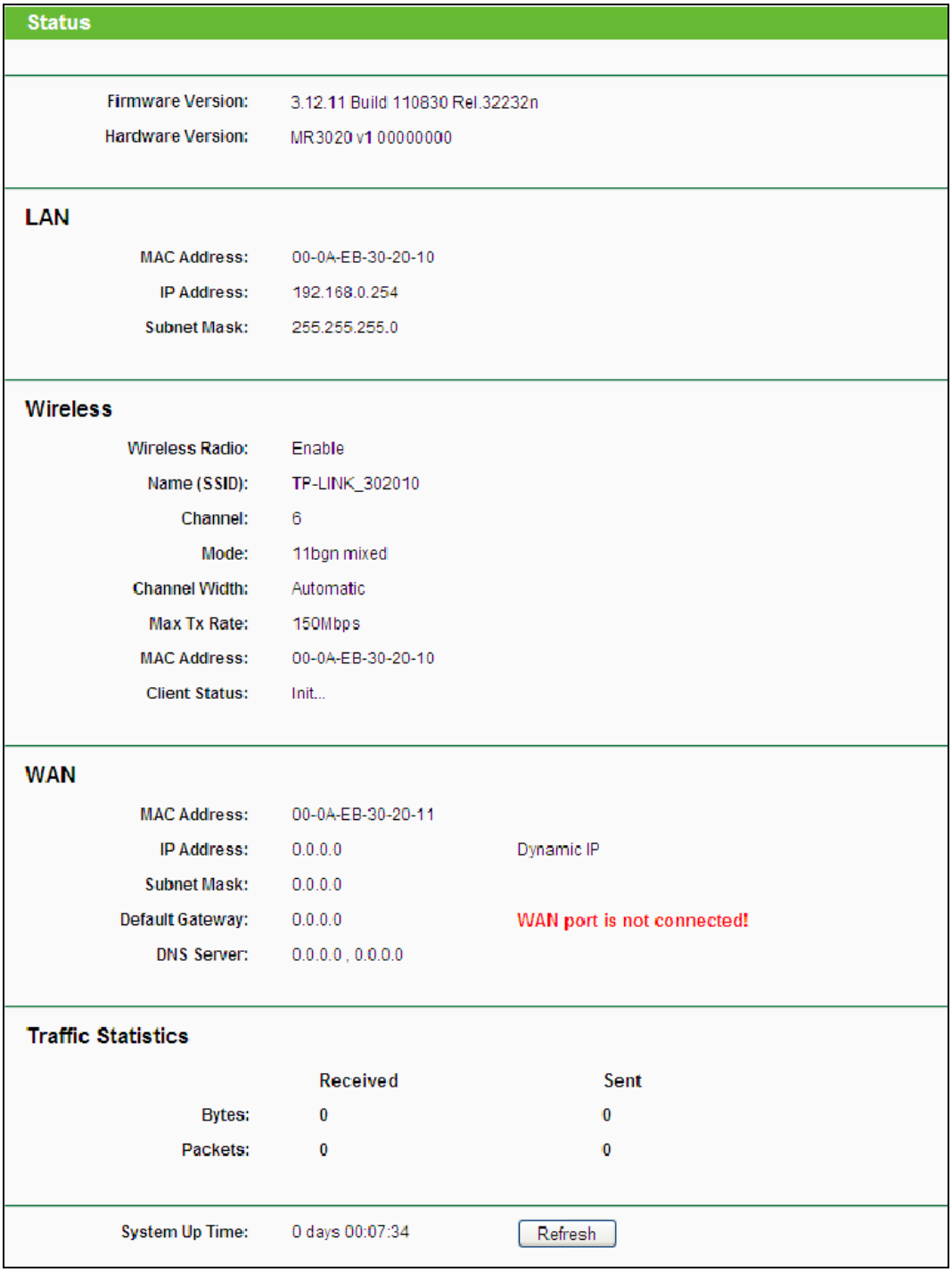


Bild 5-1 Routerstatusseite

5.3 Schnellinstallation

Bitte schauen Sie für die Schnellinstallation im Kapitel 3.2 nach.

5.4 WPS

WPS (Wi-Fi Protected Setup) ermöglicht es Ihnen, ohne viel Arbeit ein weiteres drahtloses Gerät Ihrem verschlüsselten WLAN hinzuzufügen.

a). Gehen Sie in das Menü **WPS**. Sie sehen Folgendes (Bild 5-2).

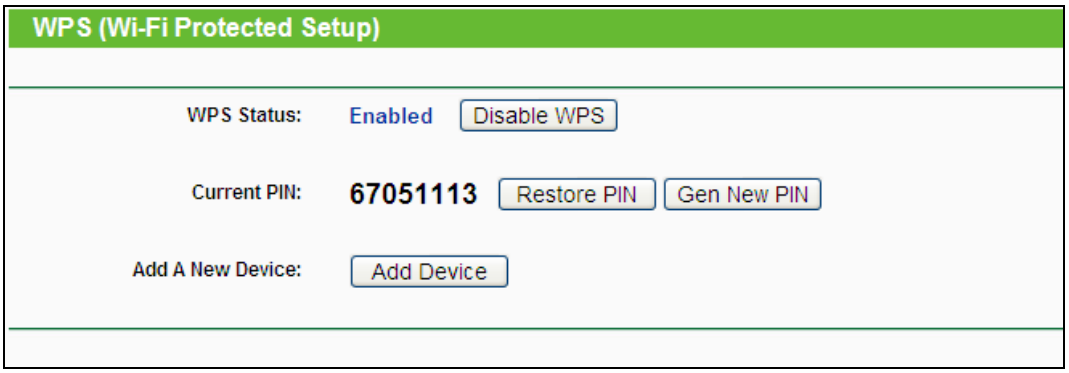


Bild 5-2 WPS

- **WPS Status -** WPS QSS aktivieren oder deaktivieren.
- **Current PIN -** Aktuelle Router-PIN. Die Standard-PIN kann auf dem Etikett auf der Geräteunterseite oder auf dem Handbuch gefunden werden.
- **Restore PIN -** Standard-PIN des Routers wiederherstellen.
- **Gen New PIN -** Neue PIN per Zufallsgenerator erstellen. Damit können Sie die Sicherheit wiederherstellen, wenn die alte PIN Unbefugten bekannt wurde.
- **Add device -** Mit dieser Schaltfläche können Sie neue Geräte von Hand einbinden.

b). Um ein neues Gerät hinzuzufügen:

Unterstützt der Drahtlosadapter WPS (Wi-Fi Protected Setup), können Sie die Verbindung entweder mit der Tastendruckmethode (PBC) oder der PIN-Methode herstellen.

☞ **Bemerkung:**

Um mittels WPS erfolgreich eine Verbindung herzustellen, sollten Sie zeitgleich die entsprechende WPS-Konfiguration des Adapters durchführen.

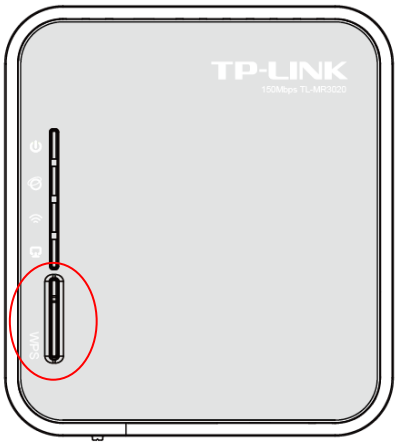
Als Beispiel dient im Folgenden ein QSS-fähiger TP-LINK-Adapter.

I. Mittels PBC

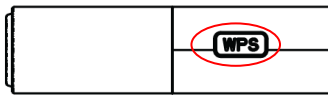
Unterstützt der drahtlose Adapter Wi-Fi Protected Setup und die Tastendruck-Konfigurationsmethode (PBC), können Sie diesen auf folgenden beiden Wegen in das WLAN einbinden.

Methode 1:

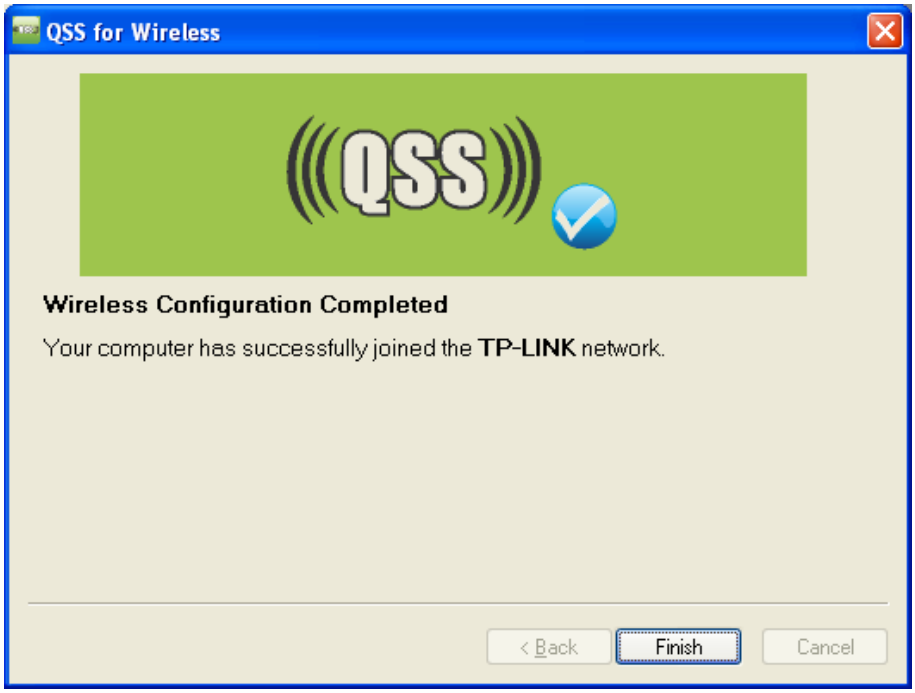
Schritt 1: Drücken Sie die WPS-Taste auf der Vorderseite des Routers.



Schritt 2: Drücken Sie die WPS-Taste des Adapters und halten Sie sie für 2 oder 3 Sekunden.



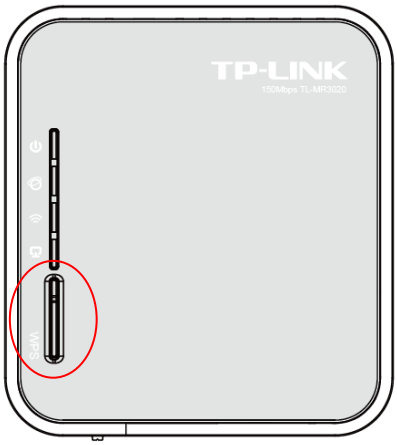
Schritt 3: Warten Sie, bis auf dem Bildschirm Folgendes erscheint. Klicken Sie **Finish**.



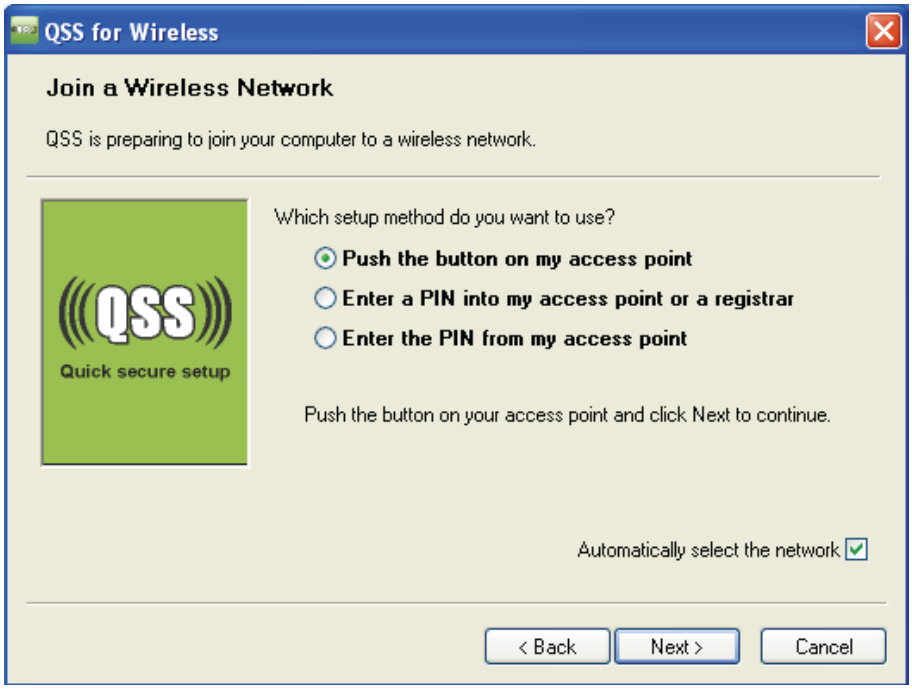
Die WPS/QSS-Konfigurationssoftware des WLAN-Adapters

Methode 2:

Schritt 1: Drücken Sie die WPS-Taste auf der Vorderseite des Routers.

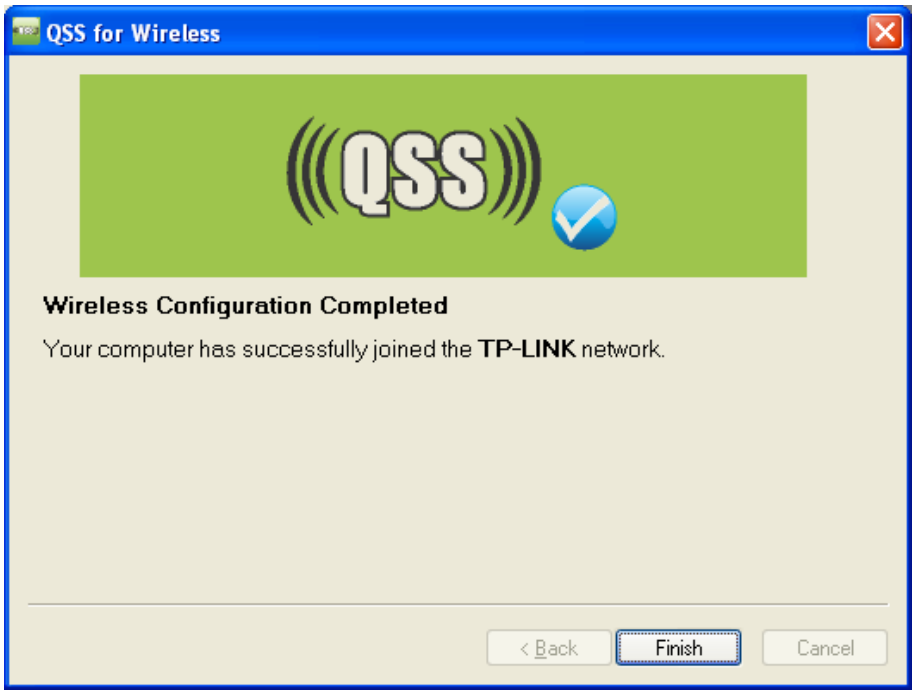


Schritt 2: Zur Konfiguration des Adapters wählen Sie in der QSS-Software bitte **Push the button on my access point** und klicken Sie **Weiter**.



QSS-Konfigurationssoftware des Adapters

Schritt 3: Warten Sie, bis Sie auf dem Bildschirm Folgendes sehen. Klicken Sie **Finish**.



QSS-Konfigurationssoftware des Adapters

Methode 3:

Schritt 1: Stellen Sie sicher, dass WPS aktiviert ist und klicken Sie **Gerät hinzufügen**, wie in Bild 5-2. Folgendes Bild erscheint.

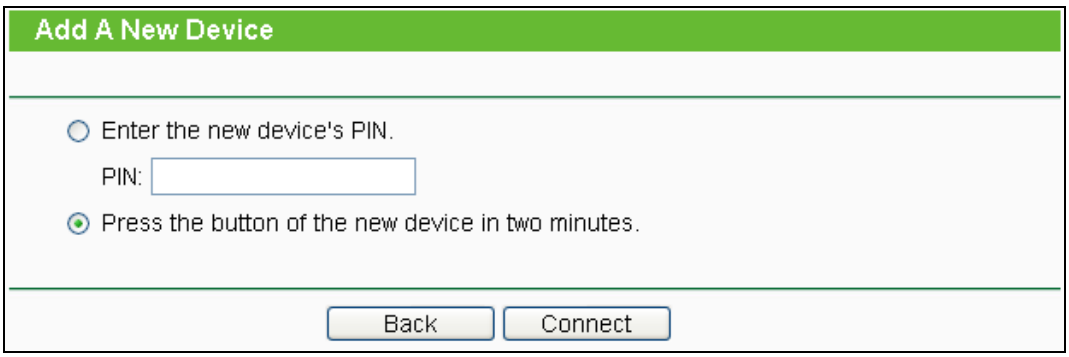
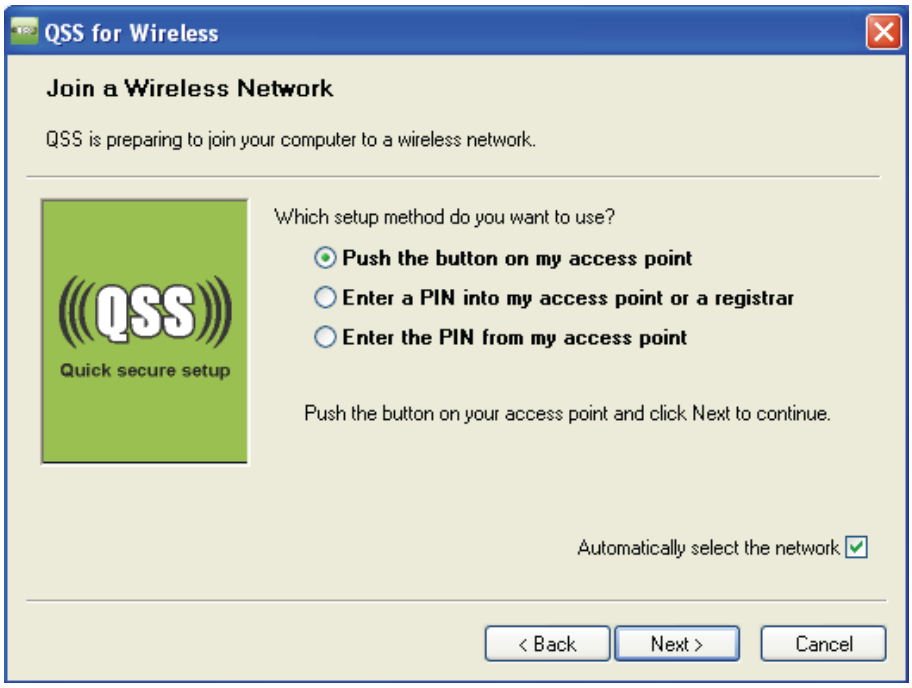


Bild 5-3 Hinzufügen eines neuen Geräts

Schritt 2: Wählen Sie **Press the button of the new device in two minutes** und klicken Sie **Connect**.

Schritt 3: Zur Konfiguration des drahtlosen Adapters wählen Sie bitte im QSS-Konfigurationstool **Push the button on my access point** und klicken Sie **Next**.



QSS-Konfigurationssoftware des Adapters

Schritt 4: Warten Sie, bis folgendes Fenster erscheint. Klicken Sie **Finish**, um die QSS-Konfiguration abzuschließen.

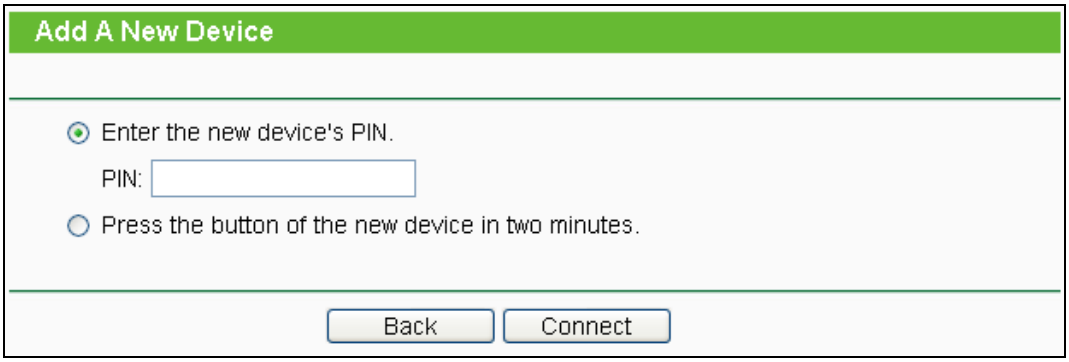
QSS-Konfigurationssoftware des Adapters

I. Mittels PIN

Unterstützt das neue Gerät WPS (Wi-Fi Protected Setup) und die PIN-Methode, können Sie es mittels der folgenden beiden Methoden durch PIN-Eingabe in das WLAN integrieren.

Methode 1: Enter the PIN into my Router

Schritt 1: Belassen Sie den Standard-WPS-Status (**Enabled**) und klicken Sie **Add device** (Bild 5-2). Folgendes Bild erscheint.

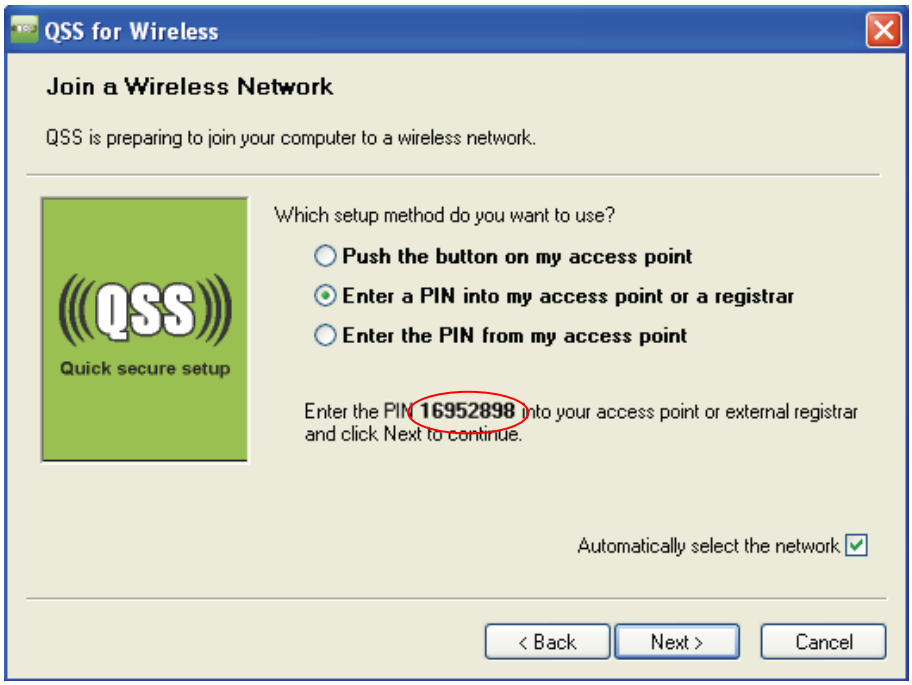


Schritt 2: Wählen Sie **Enter the new device's PIN** und geben Sie die PIN des Adapters in das Feld **PIN** ein. Klicken Sie **Connect**.

☞ **Bemerkung:**

Die PIN des Adapters wird im QSS-Konfigurationsprogramm angezeigt

Schritt 3: Zur Konfiguration des Adapters wählen Sie bitte **Enter a PIN into my access point or a registrar** aus und klicken Sie **Next**.



QSS-Konfigurationssoftware des Adapters

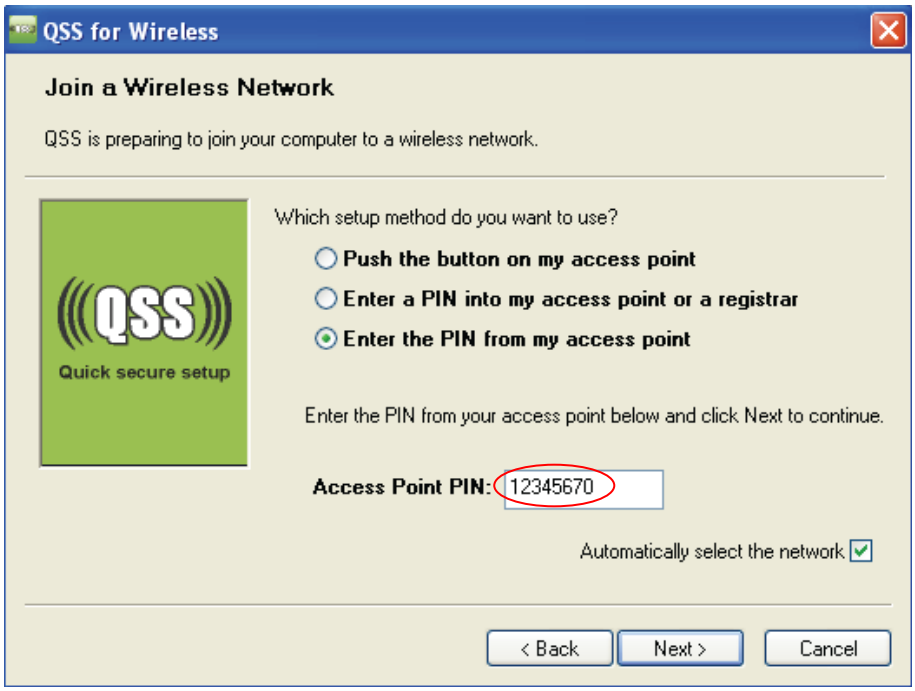
☞ **Bemerkung:**

Die PIN des Adapters lautet in diesem Beispiel 16952898, wie oben ersichtlich.

Methode 2: PIN des Routers eingeben

Schritt 1: Lesen Sie die aktuelle Router-PIN in Bild 5-2 Jeder Router hat eine andere PIN. In diesem Beispiel lautet sie 12345670.

Schritt 2: Zur Konfiguration des Adapters wählen Sie im QSS-Konfigurationsprogramm **PIN meines Accesspoints eingeben** und geben Sie sie bei **Accesspoint-PIN** ein. Klicken Sie **Weiter**.

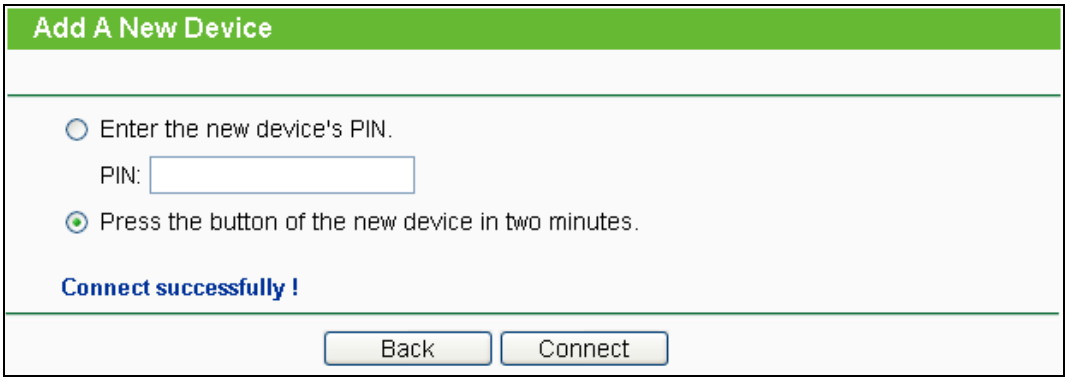


QSS-Konfigurationssoftware des Adapters

Bemerkung:

Die Standard-PIN des Routers kann auf einem Aufkleber auf der Geräterückseite oder im Webinterface wie in Bild 5-2 abgelesen werden.

Schritt 3: Haben Sie ein Gerät erfolgreich in das Netz gebracht, sehen Sie folgende Meldung.



Bemerkungen:

1) Die Router-LED **WPS** leuchtet für einige Minuten grün, nachdem das Gerät erfolgreich dem Netz hinzugefügt wurde.
1) Die WPS-Funktionalität steht nicht zur Verfügung, wenn die WLAN-Schnittstelle des Routers deaktiviert ist. Bitte stellen Sie sicher, dass diese aktiv ist, bevor Sie WPS verwenden.

5.5 Network

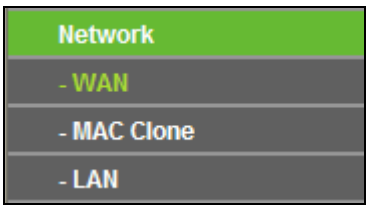


Bild 5-4 Das Menü **Network**

Das Menü **Network** (Bild 5-4) enthält die Untermenüs **WAN**, **MAC Clone** und **LAN**.

5.5.1 WAN

Wählen Sie im Menü **Network** → **WAN** können Sie die WAN-IP-Parameter einstellen.

1. Bietet Ihr ISP einen DHCP-Dienst, wählen Sie bitte **Dynamische IP-Adresse**. Ihr Router holt die IP-Parameter dann automatisch vom ISP. Die Seite sieht so aus (Bild 5-5):

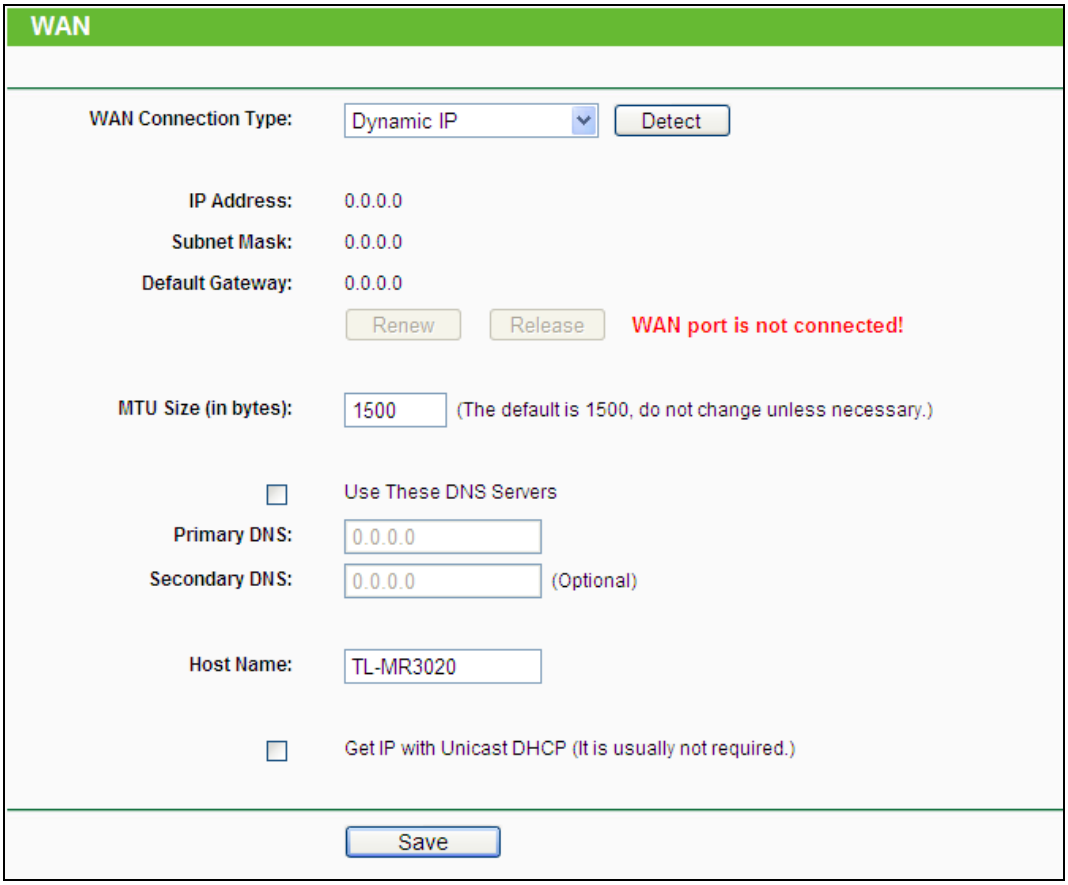


Bild 5-5 WAN - Dynamic IP

Diese Seite zeigt die WAN-IP-Parameter, die durch Ihren ISP dynamisch zugewiesen wurden: IP-Adresse, Subnetzmaske, Standardgateway, etc.. Klicken Sie **Renew**, um die IP-Parameters erneut vom ISP abzurufen. Klicken Sie **Release**, um Ihre IP-Parameter freizugeben.

- **MTU Size -** Die MTU-Größe (**M**aximum **T**ransmission **U**nit) liegt bei den meisten Ethernet-Netzen bei 1500 Byte. Es wird nicht empfohlen, diesen Wert zu ändern, wenn Ihr ISP dies nicht erfordert.

- **Use These DNS Servers -** Hat Ihr ISP Ihnen eine oder zwei DNS-Server-Adressen gegeben, wählen Sie **Use These DNS Servers** und geben Sie die Adressen in diese Felder ein. Ansonsten werden die DNS-Serveradressen dynamisch vom ISP zugewiesen.

Bemerkung:

Sollten Sie nach Eingabe der DNS-Serveradressen keine Webseiten mehr aufrufen können, könnten Ihre DNS-Einstellungen fehlerhaft sein. In diesem Fall kontaktieren Sie Ihren ISP.

- **Get IP with Unicast DHCP -** Einige ISPs betreiben DHCP-Server, die keine Broadcast-Anwendungen beherrschen. Können Sie auf normalem Wege keine IP-Adresse bekommen, können Sie es mit dieser Option versuchen (selten benötigt)

2. Wenn Ihr Anbieter eine statische IP-Adresse verwendet, sollte er Ihnen diese mitgeteilt haben, ebenso Subnetzmaske, Gateway und DNS-Server. Wählen Sie in diesem Fall **Static IP** aus Bild 5-6 erscheint.

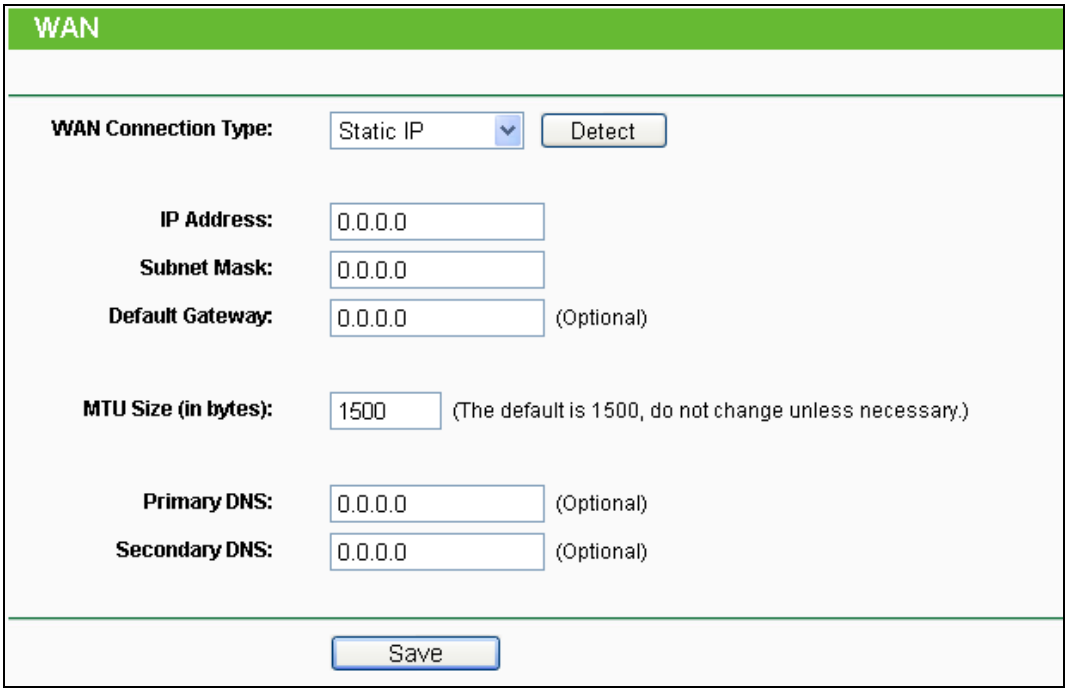


Bild 5-6 WAN - Static IP

- **IP Address -** Die IP-Adresse, die Sie von Ihrem ISP erhalten haben.
- **Subnet Mask -** Die Subnetzmaske, gewöhnlich 255.255.255.0.
- **Default Gateway -** Die IP-Adresse des Gateways Ihres ISPs (optional).
- **MTU Size -** Die Standard-MTU-Größe (**M**aximum **T**ransmission **U**nit) ist in normalen Ethernets 1500 Byte groß. Es wird nicht empfohlen, diese zu ändern, wenn es nicht erforderlich ist.
- **Primary/Secondary DNS -** Geben Sie eine oder zwei DNS-Serveradressen ein (optional).

3. Arbeiten Sie mit einer PPPoE-Verbindung, wählen Sie **PPPoE/Russia PPPoE** aus. Es sind folgende Parameter einzugeben (Bild 5-7):

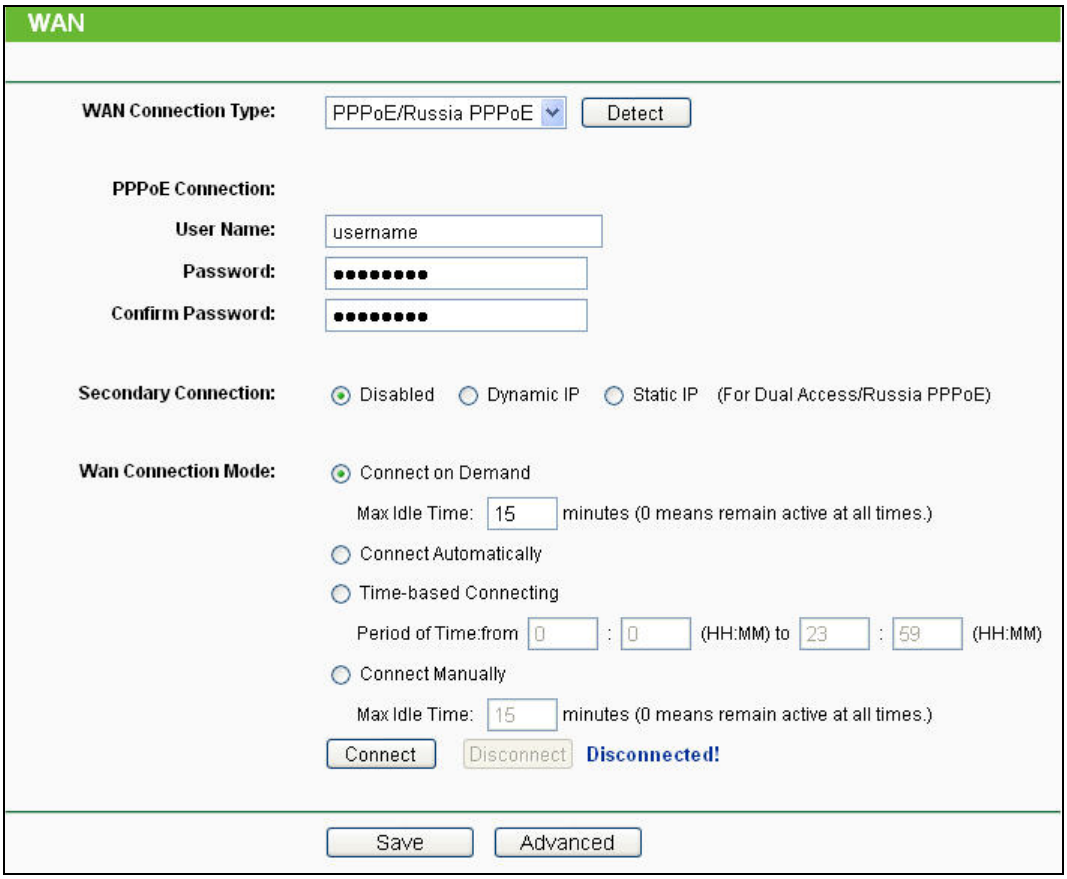


Bild 5-7 WAN - PPPoE

- **User Name/Password -** Geben Sie Benutzernamen und Passwort ein, so wie Sie sie von Ihrem ISP erhalten haben. Hier wird zwischen Groß- und Kleinschreibung unterschieden.
- **Confirm Password -** Geben Sie Ihr Passwort hier erneut ein, um sicherzugehen, dass Sie es korrekt eingegeben haben.
- **Secondary Connection -** Diese Option wird nur bei PPPoE angeboten. Bietet Ihr ISP einen extra Verbindungstyp wie dynamische/statische IP-Adresse für den Zugang zu einem LAN an, können Sie hier die passende Option aktivieren.
  - **Disabled -** Die Zweitverbindung ist deaktiviert (empfohlen).
  - **Dynamic IP -** Aktivieren Sie dies, wenn Sie mit dynamischer IP-Adresse über die Zweitverbindung zum LAN Ihres ISPs Verbindung aufnehmen wollen.
  - **Static IP -** Aktivieren Sie dies, wenn Sie mit statischer IP-Adresse über die Zweitverbindung zum LAN Ihres ISPs Verbindung aufnehmen wollen.
- **Connect on Demand -** In diesem Modus wird die Internetverbindung nach einer konfigurierbaren Dauer der Inaktivität (**Max Idle Time**) getrennt und bei Bedarf erneut hergestellt werden. Soll Ihre Internetverbindung ständig aktiv sein, geben Sie hier 0 als **Max Idle Time** ein. Andernfalls geben Sie die **Max Idle Time** in min an.
- **Connect Automatically -** Neu verbinden, nachdem die Verbindung getrennt wurde.
- **Time-based Connecting -** Die Verbindung wird nur im angegebenen Zeitraum hergestellt.

Startzeit und Endzeit sind im Format „hh:mm“ anzugeben.

Bemerkung:

Time-based Connecting funktioniert nur, wenn Sie **unter System Tools** -> **Time** Angaben gemacht haben.

- **Connect Manually -** Mit der Schaltfläche **Connect/Disconnect** können Sie die Verbindung augenblicklich von Hand herstellen oder trennen. Auch dieser Modus unterstützt die Funktion der **Max Idle Time**, genau wie **Connect on Demand**.

Vorsicht: Unter Umständen fängt die maximale Leerlaufzeit **Max Idle Time** nicht an zu laufen oder wird unterbrochen, nämlich dann, wenn einige Applikationen im Hintergrund noch Datenverkehr erzeugen.

Für weitere Konfigurationsmöglichkeiten klicken Sie **Advanced**. Die Seite in Bild 5-8 erscheint erscheint:

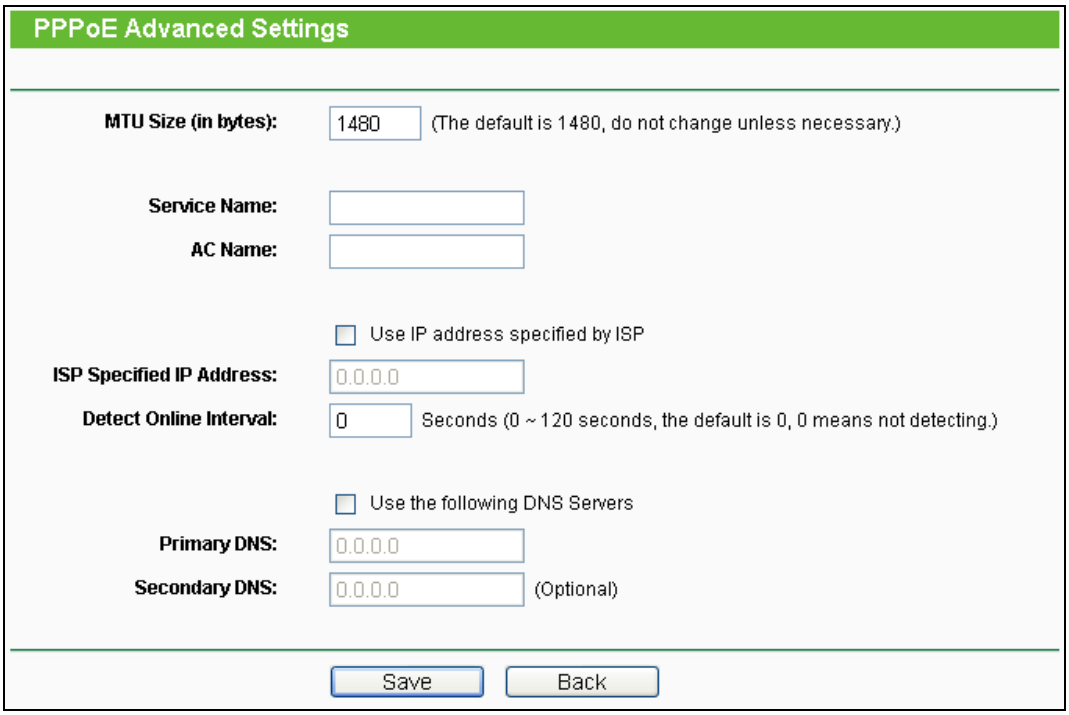


Bild 5-8 Erweiterte PPPoE-Einstellungen

- **MTU Size -** Die Standard-MTU(**M**aximum **T**ransmission **U**nit)-Größe beträgt bei PPPoE 1480 Byte. Bei einigen ISPs muss diese reduziert werden. Da dies allerdings nur selten erforderlich ist, sollten Sie diesen Wert nur ändern, wenn Sie sich sicher sind.
- **Service Name/AC Name -** Der Servicename und der AC(**A**ccess **C**oncentrator)-Name. Sollten nicht geändert werden, außer es ist bei Ihrem ISP notwendig.
- **ISP Specified IP Address -** Wenn Sie wissen, dass Ihr ISP bei der Einwahl die IP-Adresse nicht automatisch überträgt, wählen Sie **Use IP address specified by ISP** und geben Sie die IP-Adresse hier ein.
- **Detect Online Interval -** Dies ist der Zeitabstand in Sekunden, in dem der Router überprüft,

ob der Access Concentrator online ist. Zulässige Werte sind von 0 bis 120. Der Standardwert ist 0 (=deaktiviert).

- **Primary/Secondary DNS -** Wenn Sie wissen, dass Ihr ISP bei der Einwahl die DNS-Server-Adresse(n) nicht automatisch überträgt, wählen Sie **Use the following DNS servers** und geben Sie hier die Adresse(n) ein.

Click the **Save** button to save your settings.

4. Haben Sie einen BigPond-Kabelzugang (oder Heartbeat-Signal), wählen Sie **BigPond Cable** und geben Sie folgende Parameter ein (Bild 5-9):

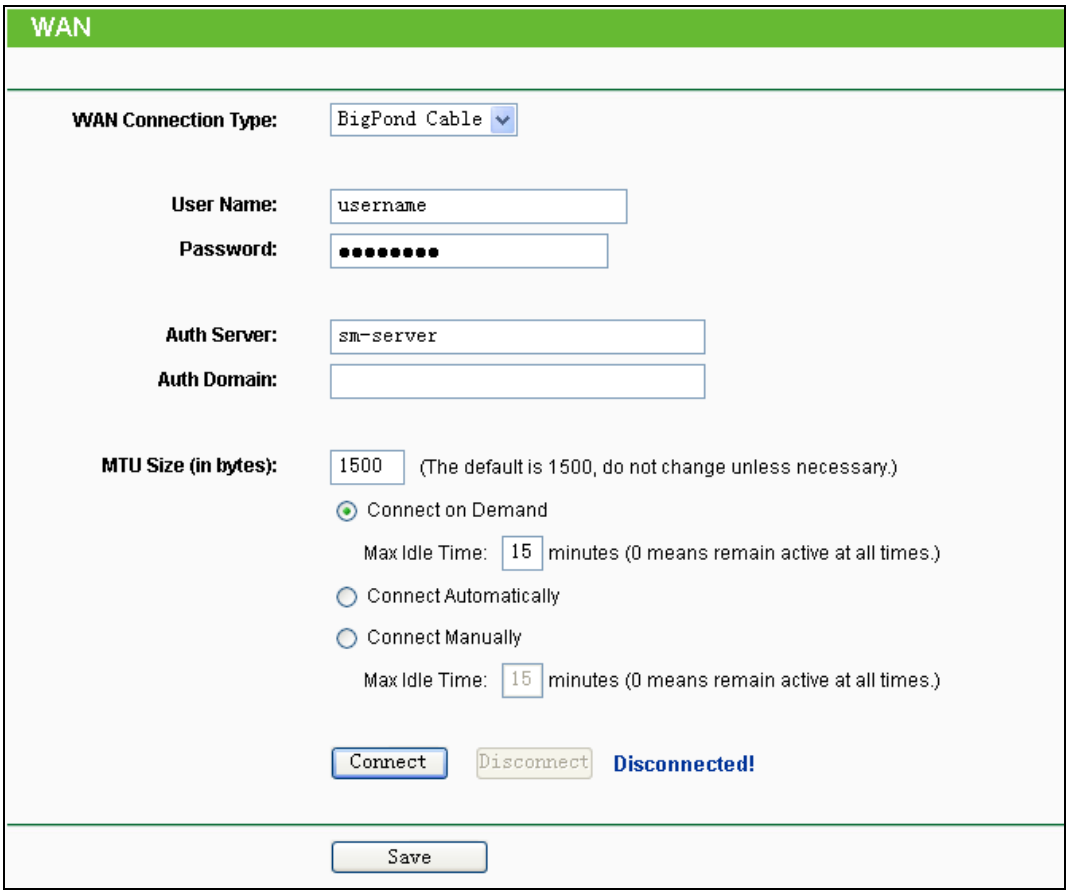


Bild 5-9 WAN – BigPond Cable

- **User Name/Password -** Geben Sie Ihren Benutzernamen und Ihr Passwort ein, so wie Sie sie von Ihrem ISP erhalten haben. Hier wird zwischen Groß- und Kleinschreibung unterschieden.

- **Auth Server -** Geben Sie hier die IP-Adresse oder den Hostnamen des Authentifizierungsservers ein.

- **Auth Domain -** Geben Sie hier den Domänensuffixservernamen basierend auf Ihrem Standort ein, z.B.:

NSW / ACT - **nsw.bigpond.net.au**
VIC / TAS / WA / SA / NT - **vic.bigpond.net.au**

QLD - **qld.bigpond.net.au**

- **MTU Size -** Die MTU-Größe (**M**aximum **T**ransmission **U**nit) liegt bei den meisten Ethernet-Netzen bei 1500 Byte. Es wird nicht empfohlen, diesen Wert zu ändern, wenn Ihr ISP dies nicht erfordert.
- **Connect on Demand -** In diesem Modus wird die Internetverbindung nach einer konfigurierbaren Dauer der Inaktivität (**Max Idle Time**) getrennt und bei Bedarf erneut hergestellt werden. Soll Ihre Internetverbindung ständig aktiv sein, geben Sie hier 0 als **Max Idle Time** ein. Andernfalls geben Sie die maximale Leerlaufzeit in min an.
- **Connect Automatically -** Neu verbinden, nachdem die Verbindung getrennt wurde.
- **Connect Manually -** Mit der Schaltfläche **Connect**/**Disconnect** können Sie die Verbindung augenblicklich von Hand herstellen oder trennen. Auch dieser Modus unterstützt die Funktion der **Max Idle Time**, genau wie **Connect on Demand**.

  Klicken Sie **Connect** um augenblicklich eine Verbindung herzustellen und **Disconnect**, um die Verbindung augenblicklich zu trennen.

Vorsicht: Die Verbindung wird unter Umständen nicht getrennt, nämlich dann, wenn einige Applikationen im Hintergrund Datenverkehr erzeugen.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

5. Benutzen Sie eine L2TP-Verbindung, wählen Sie bitte **L2TP/Russia L2TP** aus. Folgende Parameter sollten nicht fehlen (Bild 5-10):

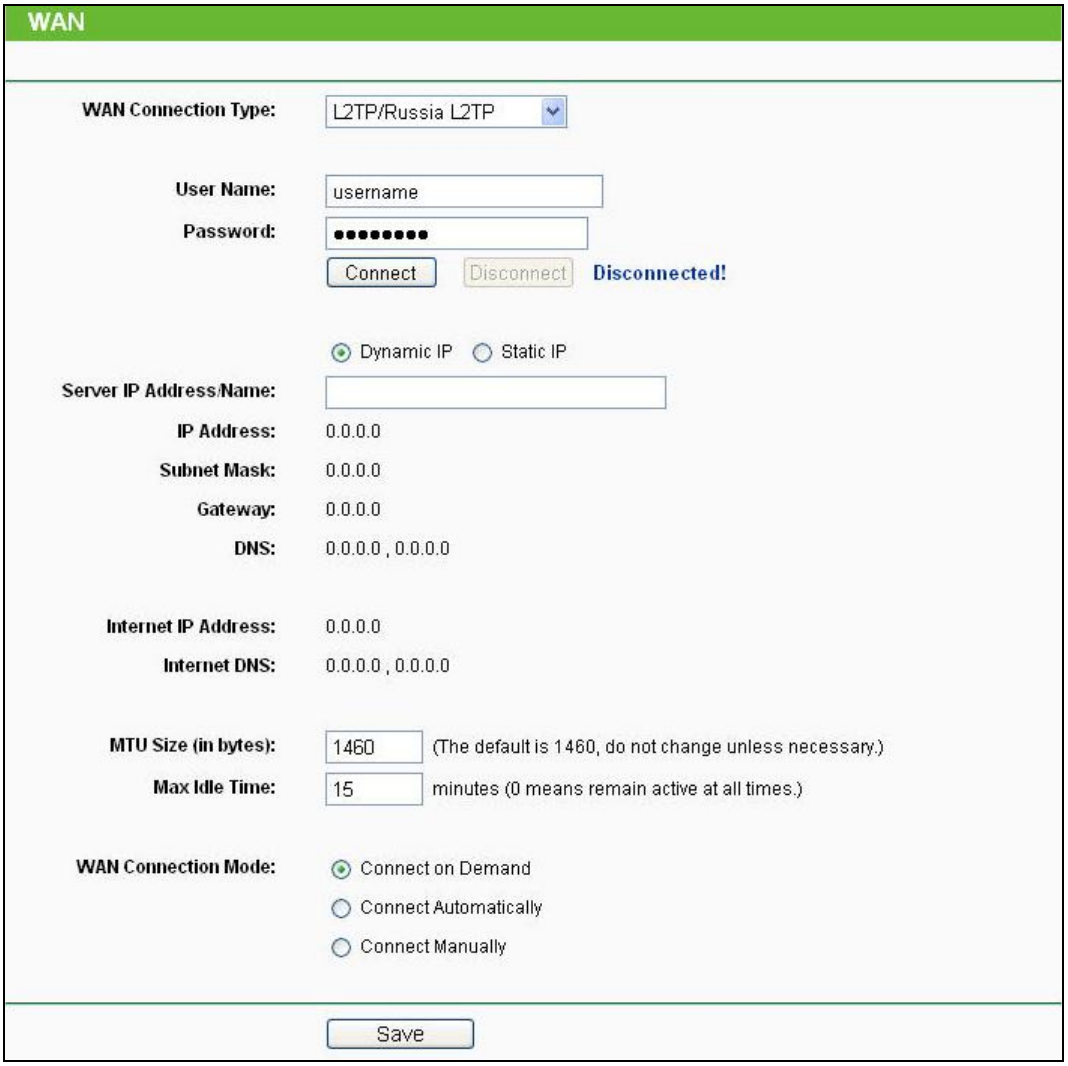


Bild 5-10 WAN – L2TP-Einstellungen

- **User Name/Password -** Geben Sie den Benutzernamen und das Passwort ein, so wie Sie sie von Ihrem ISP erhalten haben. Hier wird auf Gro-/Kleinschreibung geachtet.
- **Dynamic IP/Static IP -** Wählen Sie dies anhand der Vorgabe Ihres ISP aus. Klicken Sie **Connect**, um augenblicklich eine Verbindung herzustellen. Klicken Sie **Disconnect**, um die Verbindung augenblicklich zu trennen.
- **Connect on Demand -** Sie können den Router so konfigurieren, dass er nach einer gewissen Zeitspanne der Inaktivität (**Max Idle Time**) die Internetverbindung trennt. **Connect on Demand** erlaubt es dem Router, nach so einer Trennung die Verbindung automatisch wiederherzustellen, sobald Sie erneut versuchen, auf das Internet zuzugreifen. Soll Ihre Internetverbindung dauerhaft aktiv bleiben, geben Sie in das Feld **Max Idle Time** 0 ein. Ansonsten geben Sie die Zeitspanne ein, nach deren Ablauf die Internetverbindung getrennt werden soll

  Vorsicht: Die Verbindung wird unter Umständen nicht getrennt, nämlich dann, wenn einige Applikationen im Hintergrund Datenverkehr erzeugen.
- **Connect Automatically -** Nach Trennung automatisch wiederverbinden.

- **Connect Manually -** Mit dieser Option verbindet der Router sich nur auf manuelle Betätigung hin. Nach der definierten Inaktivitätszeitspanne (**Max Idle Time**) trennt er die Verbindung und stellt sie bis zum nächsten manuellen Verbinden nicht wieder her. Soll die Verbindung dauerhaft bestehen, geben Sie als **Max Idle Time** 0 ein. Ansonsten geben Sie die Zeitspanne ein, nach deren Ablauf die Internetverbindung getrennt werden soll.
  Vorsicht: Die Verbindung wird unter Umständen nicht getrennt, nämlich dann, wenn einige Applikationen im Hintergrund Datenverkehr erzeugen.

6. Möchten Sie eine PPTP-Verbindung nutzen, wählen Sie die Option **PPTP/Russia PPTP** aus. Es sollten folgende Parameter eingegeben werden (Bild 5-11):

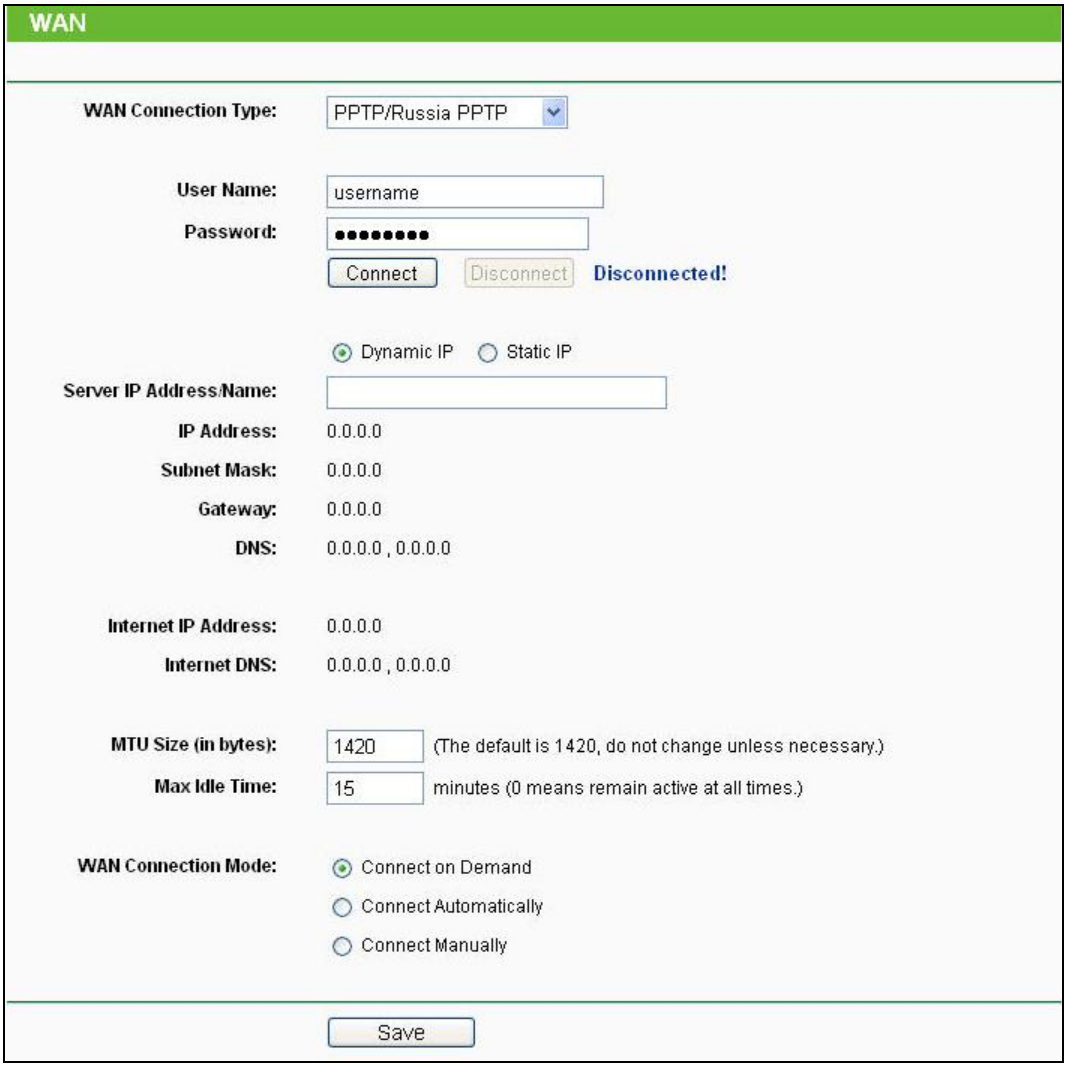


Bild 5-11 WAN – PPTP-Einstellungen

- **User Name/Password -** Geben Sie den Benutzernamen und das Passwort ein, so wie Sie sie von Ihrem ISP erhalten haben. Hier wird auf Groß-/Kleinschreibung geachtet.

- **Dynamic IP/ Static IP -** Wählen Sie dies anhand der Vorgabe Ihres ISP aus und geben Sie die IP-Adresse oder den Domänennamen Ihres ISPs aus.

  Haben Sie **Static IP** gewählt und den Domänennamen eingegeben, sollten Sie auch den

DNS-Server angeben. Klicken Sie am Schluss **Save**.

Klicken Sie **Connect**, um augenblicklich eine Verbindung herzustellen. Klicken Sie **Disconnect**, um die Verbindung augenblicklich zu trennen.

- **Connect on Demand -** Sie können den Router so konfigurieren, dass er nach einer gewissen Zeitspanne der Inaktivität (**Max Idle Time**) die Internetverbindung trennt. **Connect on Demand** erlaubt es dem Router, nach so einer Trennung die Verbindung automatisch wiederherzustellen, sobald Sie erneut versuchen, auf das Internet zuzugreifen. Soll Ihre Internetverbindung dauerhaft aktiv bleiben, geben Sie in das Feld **Max Idle Time** 0 ein. Ansonsten geben Sie die Zeitspanne ein, nach deren Ablauf die Internetverbindung getrennt werden soll.
  Vorsicht: Die Verbindung wird unter Umständen nicht getrennt, nämlich dann, wenn einige Applikationen im Hintergrund Datenverkehr erzeugen.

- **Connect Automatically -** Nach Trennung automatisch wiederverbinden.

Connect Manually - Mit dieser Option verbindet der Router sich nur auf manuelle Betätigung hin. Nach der definierten Inaktivitätszeitspanne (**Max Idle Time**) trennt er die Verbindung und stellt sie bis zum nächsten manuellen Verbinden nicht wieder her. Soll die Verbindung dauerhaft bestehen, geben Sie als **Max Idle Time** 0 ein. Ansonsten geben Sie die Zeitspanne ein, nach deren Ablauf die Internetverbindung getrennt werden soll.
Vorsicht: Die Verbindung wird unter Umständen nicht getrennt, nämlich dann, wenn einige Applikationen im Hintergrund Datenverkehr erzeugen.

☞ **Bemerkung:**

Wenn Sie nicht wissen, welcher Verbindungstyp auszuwählen ist, klicken Sie **Detect**, damit der Router versucht, ihn automatisch auszuwählen. Um sicherzugehen, dass der automatisch gewählte Verbindungstyp stimmt, setzen Sie sich bitte mit Ihrem ISP in Verbindung. Der Router ist in der Lage, folgende Verbindungstypen zu erkennen:

- **PPPoE -** PPPoE, benötigt Benutzernamen und Passwort.
- **Dynamic IP -** Zuweisung einer IP-Adresse.
- **Static IP -** Statische IP-Adresse.

Der Router kann keine PPTP-, L2TP- oder BigPond-Verbindungen erkennen. Haben Sie eine solche, konfigurieren Sie diese bitte von Hand.

5.5.2 MAC Clone

Im Menü **Network** → **MAC Clone** können Sie die MAC-Adresse des WAN-Ports setzen, siehe Bild 5-12:

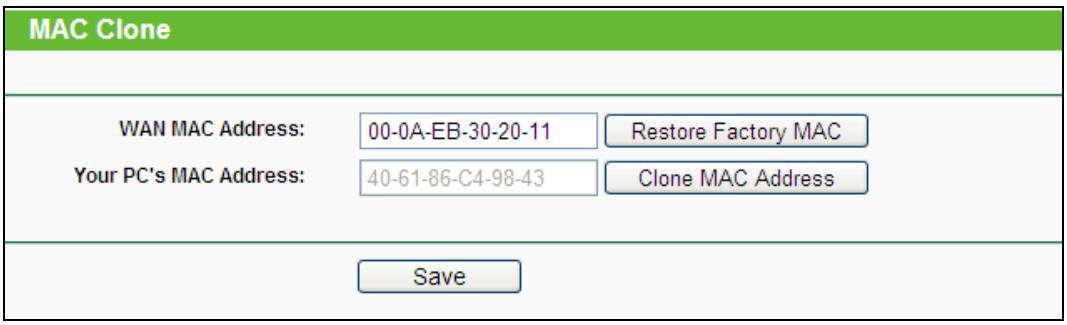


Bild 5-12 MAC-Adresse klonen

Einige ISPs verlangen eine Registrierung Ihrer MAC-Adresse. Dies ist jedoch sehr selten.

- **WAN MAC Address -** Die aktuelle MAC-Adresse des WAN-Ports. Verlangt Ihr ISP eine Registrierung Ihrer MAC-Adresse, geben Sie die registrierte MAC-Adresse hier im Format „XX-XX-XX-XX-XX-XX“ („X“ steht hierbei für eine Hexadezimalziffer) ein.
- **Your PC's MAC Address -** Zeigt die MAC-Adresse des PCs, an dem Sie gerade sitzen. Wird diese MAC-Adresse verlangt, können Sie sie mittels **Clone MAC Address** in das Feld **WAN MAC Address** übertragen.

  Klicken Sie **Restore Factory MAC** um die Original-MAC-Adresse des WAN-Ports wiederherzustellen.

  Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

Bemerkung:

Über die MAC-Adress-Klon-Funktionalität kann nur aus dem LAN verfügt werden.

5.5.3 LAN

Wählen Sie **Network** → **LAN**. Dann können Sie die LAN-IP-Parameter wie unten beschrieben konfigurieren.

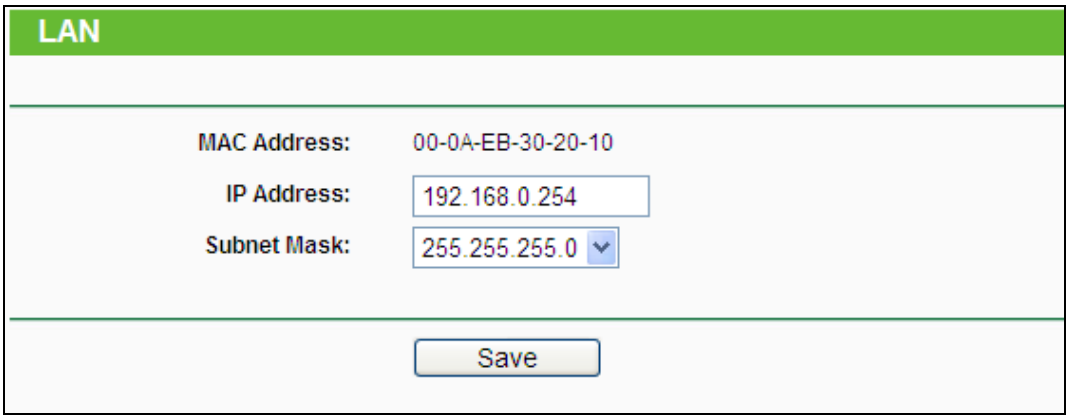


Bild 5-13 LAN

- **MAC Address -** Die physische Adresse des Routers, wie sie vom LAN aus gesehen werden kann. Diese kann nicht geändert werden.
- **IP Address -** Hier können Sie die Router-IP-Adresse festlegen (Standard: 192.168.1.1).

- **Subnet Mask -** Ein Adresscode, der die Größe Ihres Netzes angibt. Normalerweise ist die Subnetzmaske 255.255.255.0.

☞ **Bemerkungen:**

Ändern Sie die LAN-IP-Adresse, muss ab dann die neue IP-Adresse verwendet werden, um den Router zu administrieren.

Liegt die neue LAN-IP-Adresse in einem anderen Subnetz als die alte, ändert der Adresspool des DHCP-Servers sich automatisch entsprechend, während die Einstellungen zu Virtuellen Servern und DMZ-Host neu konfiguriert werden müssen.

5.6 Wireless

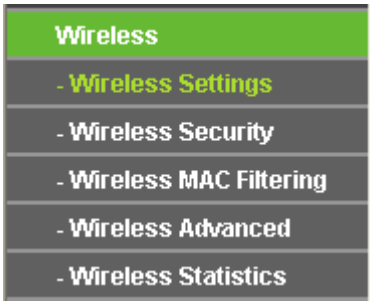


Bild 5-14 Wireless-Menü

Im WLAN-Menü gibt es fünf Untermenüs (Bild 5-14): **Wireless Settings**, **Wireless Security, Wireless MAC Filtering, Wireless Advanced** und **Wireless Statistics**.

5.6.1 Wireless Settings

Im Menü **Wireless** → **Wireless Settings** können Sie die Grundeinstellungen Ihres WLANs tätigen.

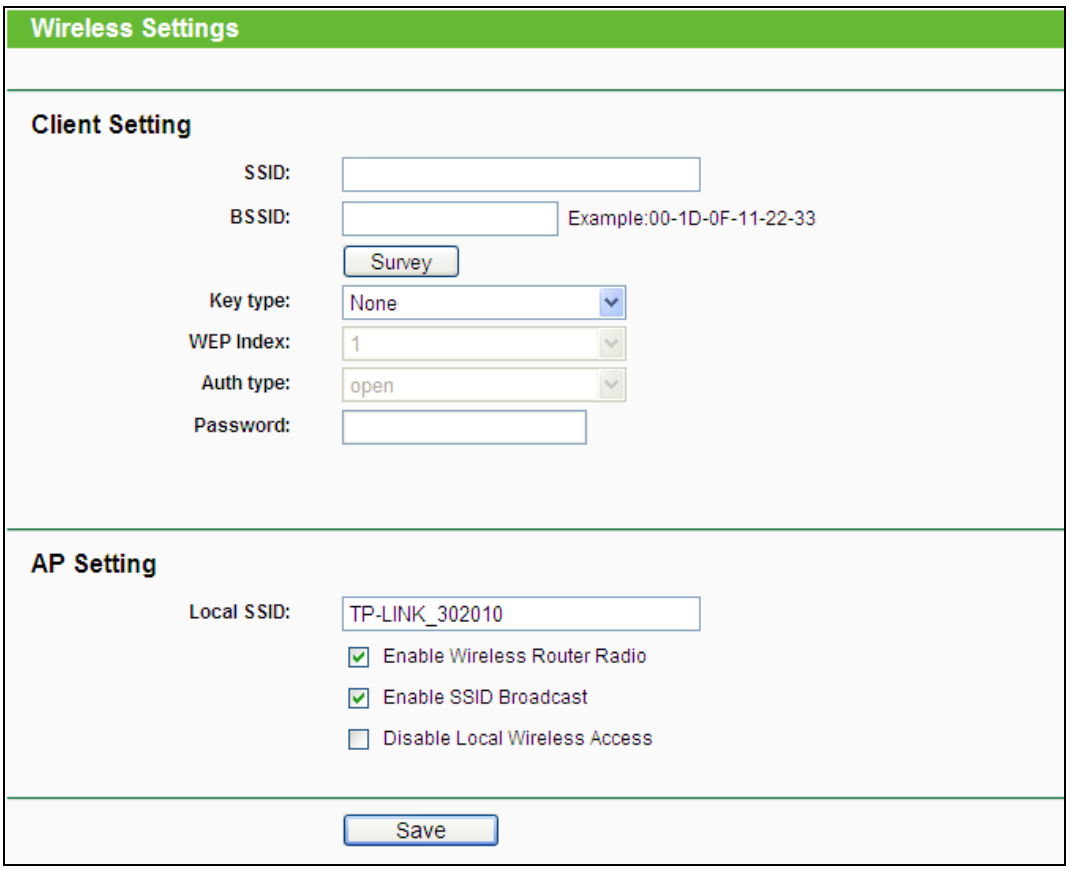


Bild 5-15 Wireless Settings

- **SSID -** Die SSID des APs, zu dem der Router sich als Client verbinden soll. Sie können die **SSID** mit Hilfe der **Survey**-Funktion eintragen.
- **BSSID -** Die BSSID des APs, zu dem der Router sich als Client verbinden soll. Sie können die **BSSID** mit Hilfe der **Survey**-Funktion eintragen.
- **Survey -** Klicken Sie hier, um Accesspoints auf dem aktuellen Kanal zu suchen.
- **Key type -** Diese Option wird entsprechend den Sicherheitseinstellungen des APs gesetzt. Es wird empfohlen, die gleichen Einstellungen zu verwenden.
- **WEP Index -** Der Index des verwendeten WEP-Schlüssels.
- **Auth type -** Der Authentifizierungstyp des Root-Accesspoints.
- **Password -** Benötigt der Root-Accesspoint ein Passwort, muss dieses hier eingetragen werden.
- **Local SSID -** Geben Sie einen Namen von bis zu 32 Zeichen an (SSID). Dieser muss von allen anderen Geräten in Ihrem WLAN verwendet werden. Standardwert ist TP-LINK, doch sollte dieser geändert werden. Hier wird zwischen Groß- und Kleinschreibung unterschieden, z.B. bezeichnen *TP-LINK* und *tp-link* unterschiedliche Netze.
- **Enable Wireless Router Radio -** Die WLAN-Funktion des Routers kann ein- und ausgeschaltet werden, um drahtlosen Zugriff zu ermöglichen oder zu verhindern.

- **Enable SSID Broadcast -** Wird dies ausgewählt, sendet der Router den WLAN-Namen (SSID) aus und Clients können das Netz in ihrer Übersicht anzeigen.
- **Disable Local Wireless Access -** Wenn Sie **Disable Local Wireless Access** wählen wird das locale WLAN abgeschalten und kein weiteres Gerät kan sich am Router per WLAN verbinden.

5.6.2 Wireless Security

Im Menü **Wireless** → **Wireless Security** können Sie die Sicherheitseinstellungen ändern.

Der Router verfügt über fünf Möglichkeiten, das WLAN zu verschlüsseln: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), WPA2-PSK (Pre-Shared Key) und WPA-PSK (Pre-Shared Key).

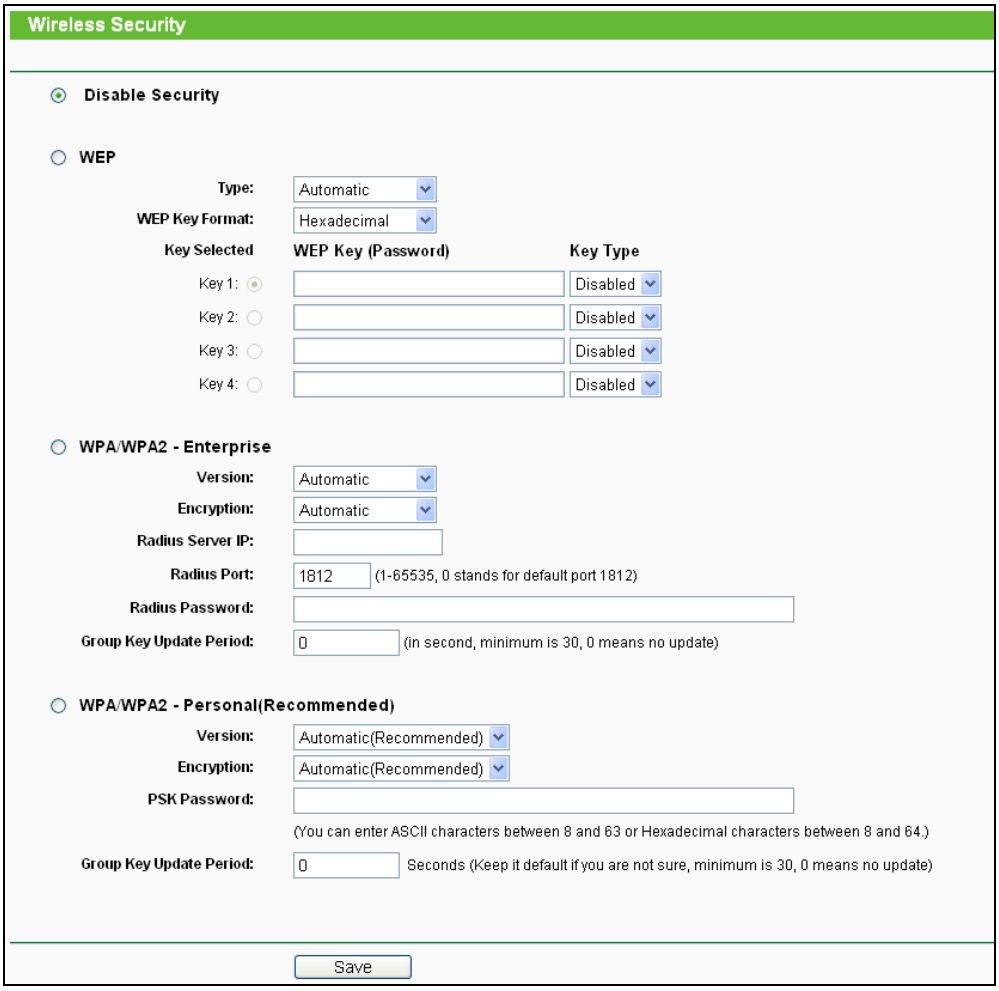


Bild 5-18 Drahtlose Sicherheit

- **Disable Security -** Möchten Sie keine Verschlüsselung einsetzen, wählen Sie diese Option. Es wird aber wärmstens empfohlen, dass Sie Ihr WLAN verschlüsseln.
- **WEP -** WEP, basierend auf 802.11-Authentifizierung verwenden. Wählen Sie diese Option aus, wird in Rot die in Bild 5-19 sichtbare Meldung eingeblendet.

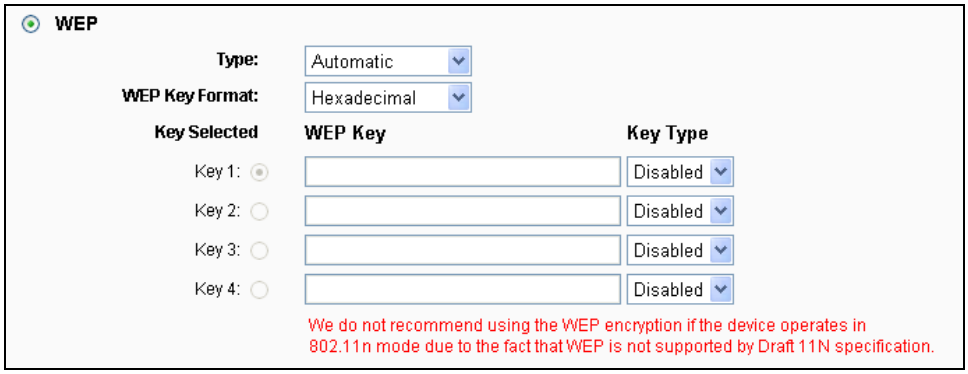


Bild 5-19 WEP mit Wireless-N

- **Type -** Der WEP-Authentifizierungstyp kann auf **Automatic** (Standard), **Open System** oder **Shared Key** eingestellt werden. **Automatic** lässt den Client den Typ auswählen.
- **WEP Key Format -** Es können die Formate **Hexadecimal** und **ASCII** ausgewählt werden. Im Fall von **Hexadecimal** können Sie eine Folge Hexadezimalziffern (0..9, a..f) in der angegebenen Länge eingeben. Bei **ASCII**-Format können Sie alle Zeichen nehmen.
- **WEP Key -** Wählen Sie aus, welcher der vier Schlüssel verwendet werden soll, und geben Sie den passenden WEP-Schlüssel ein. Stellen Sie sicher, dass Sie diese auf allen Geräten in Ihrem WLAN korrekt eingeben.
- **Key Type -** Hier können Sie die WEP-Schlüssellänge (64 Bit, 128 Bit oder 152 Bit) auswählen. **Disabled** sagt aus, dass der eingegebene WEP-Schlüssel ungültig ist.
- Bei **64-Bit**-Verschlüsselung sind 10 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 5 ASCII-Zeichen einzugeben.
- Bei **128-Bit**-Verschlüsselung sind 26 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 13 ASCII-Zeichen einzugeben.
- Bei **152-Bit**-Verschlüsselung sind 32 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 16 ASCII-Zeichen einzugeben.

Bemerkung:
Wird hier kein Schlüssel angegeben, wird die WLAN-Sicherheit nicht aktiviert, selbst wenn dies so eingestellt ist.

➢ **WPA/WPA2-Enterprise -** Basiert auf einem Radius-Server.

- **Version -** Hier können Sie die WPA-Version auswählen. Die Standardeinstellung ist **Automatic**, womit entsprechend der Fähigkeiten/Anforderungen der Clients entweder mit **WPA** (Wi-Fi Protected Access) oder **WPA2** (WPA Version 2) gearbeitet wird.
- **Encryption -** Hier können Sie zwischen **Automatic**, **TKIP** und **AES** wählen**.**

Bemerkung:
Wählen Sie hier TKIP-Verschlüsselung aus, wird Folgendes in Rot gemeldet Bild 5-20.

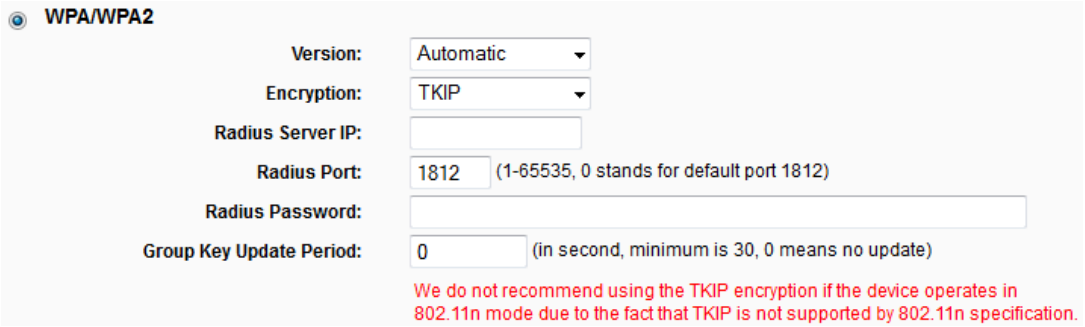


Bild 5-20 TKIP mit Wireless-N

- **Radius Server IP -** IP-Adresse des Radius-Servers.
- **Radius Port -** Port, auf dem der Radius-Dienst läuft.
- **Radius Password -** Das Passwort des Radius-Servers.
- **Group Key Update Period -** Geben Sie die Dauer der Gültigkeit eines einzigen Gruppenschlüssels in Sekunden an. Dieser Wert sollte 0 (=deaktiviert) oder mindestens 30 betragen. Empfohlen sind Werte von 500 oder 600.

➢ **WPA-PSK/WPA2- Personal (Recommended) -** WPA/WPA2-Authentifizierung, basierend auf einem Passwort. Empfohlene Einstellung.

- **Version -** WPA-PSK-Version. Die Standardeinstellung ist **Automatic**, womit entsprechend der Fähigkeiten/Anforderungen der Clients entweder mit **WPA-PSK** (Wi-Fi Protected Access) oder **WPA2-PSK** (WPA Version 2) gearbeitet wird.
- **Encryption -** Hier können Sie zwischen **Automatic**, **TKIP** und **AES** wählen.

Bemerkung:

Wählen Sie hier TKIP-Verschlüsselung aus, wird Folgendes in Rot gemeldet Bild 5-21.

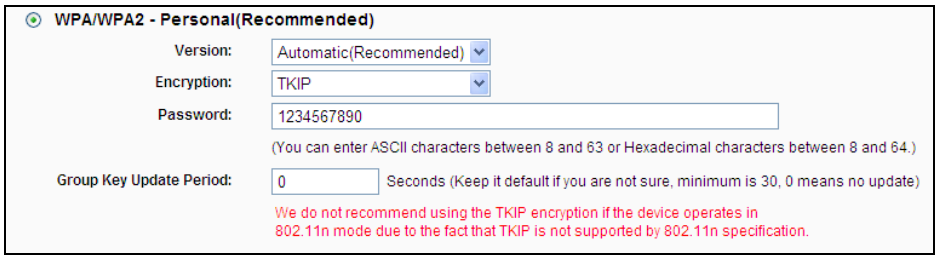


Bild 5-21 TKIP mit Wireless-N

- **PSK Password -** Das Passwort kann 8 bis 63 ASCII- oder 8 bis 64 Hexadezimalzeichen lang sein.
- **Group Key Update Period -** Geben Sie die Dauer der Gültigkeit eines einzigen Gruppenschlüssels in Sekunden an. Dieser Wert sollte 0 (=deaktiviert) oder mindestens 30 betragen. Empfohlen sind Werte von 500 oder 600.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

5.6.3 Wireless MAC Filtering

Auf dieser Seite wird die MAC-Adressfilterung konfiguriert Bild 5-22.

Bild 5-22 MAC-Adressfilterung

Um WLAN-Geräte nach MAC-Adresse zu filtern, klicken Sie **Enable**. Im andern Fall wählen Sie **Disabled** (Standardeinstellung).

- **MAC Address -** Die MAC-Adresse des WLAN-Gerätes, das Sie filtern möchten.
- **Status -** Der Status dieses Eintrags (**Enabled** oder **Disabled**).
- **Description -** Eine einfache Beschreibung der WLAN-Station.

Um einen Eintrag zur MAC-Adressfilterungsliste hinzuzufügen, klicken Sie **Add New…**. Die Seite **Add or Modify Wireless MAC Address Filtering entry** erscheint (Bild 5-23):

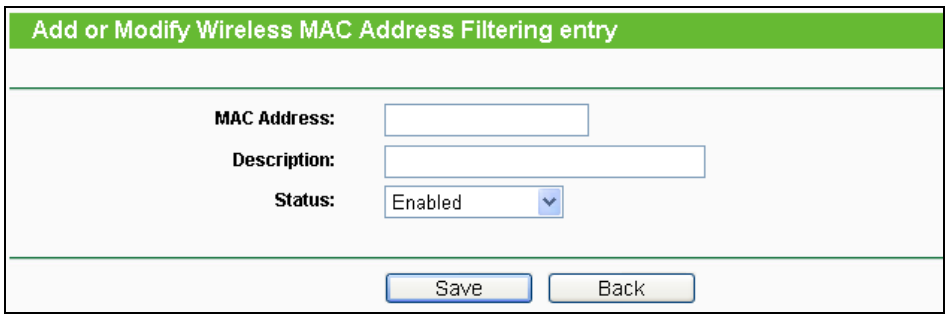


Bild 5-23 Eintrag in der MAC-Adressfilterungsliste erstellen oder bearbeiten

Um einen Eintrag in der MAC-Adressfilterungsliste zu erstellen oder zu bearbeiten:

1. Geben Sie die entsprechende MAC-Adresse in das Feld **MAC Address** im Format „XX-XX-XX-XX-XX-XX“ ein („X“ repräsentiert eine Hexadezimalziffer). Beispiel: „00-0A-EB-B0-00-0B“.
2. Geben Sie eine frei wählbare Beschreibung der WLAN-Station (Bsp.: „Kurts PC“) in das Feld **Description** ein.

3. **Status - Enabled** oder **Disabled** sind auswählbar.

4. Klicken Sie **Save**, um den Eintrag zu speichern.

Um einen Eintrag zu bearbeiten oder zu löschen, tun Sie bitte Folgendes:

1. Klicken Sie für den entsprechenden Eintrag **Modify**, wenn Sie ihn bearbeiten wollen und **Delete, um ihn zu löschen.**
2. Bearbeiten Sie die Informationen, falls erforderlich.
3. Klicken Sie **Save**.

Klicken Sie **Enable All**, um alle Einträge zu aktivieren.

Klicken Sie **Disable All**, um alle Einträge zu deaktivieren.

Klicken Sie **Delete All,** um alle Einträge zu löschen.

Klicken Sie **Next**, um zur nächsten Seite zu blättern oder **Previous**, um zur vorigen Seite zurückzukehren.

Beispiel: Sollen nur die beiden PCs mit den MAC-Adressen 00-0A-EB-00-07-8A und 00-0A-EB-00-23-11 auf das WLAN zugreifen können, sollte die Liste **Wireless MAC Filtering** so eingerichtet werden:

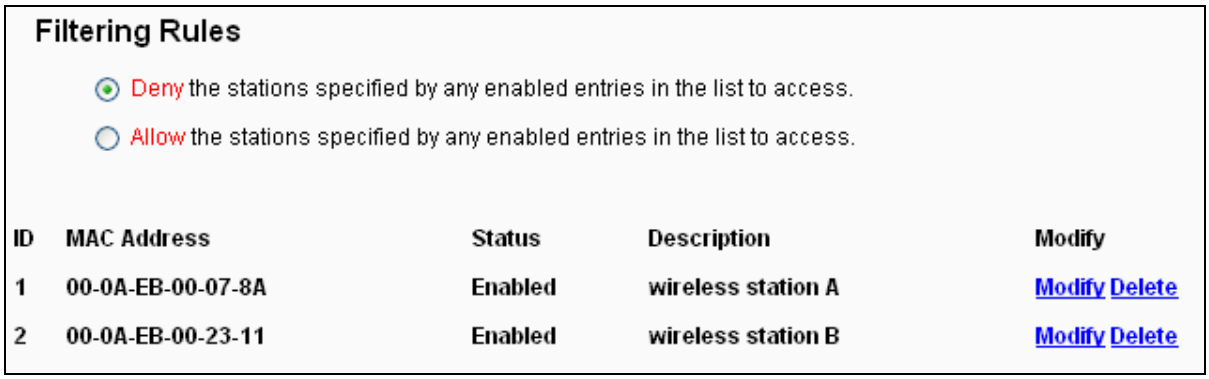
1. Klicken Sie **Enable**, um die MAC-Adressfilterfunktion zu aktivieren.

2. Wählen Sie: **Allow the stations specified by any enabled entries in the list to access** aus.

3. Löschen oder deaktivieren Sie alle bereits bestehenden Einträge.

4. Klicken Sie **Add New...** und geben Sie die MAC-Adresse 00-0A-EB-00-07-8A in das Feld **MAC Address** und eine Beschreibung in das Feld **Description** ein. Wählen Sie **Enabled** als **Status**. Klicken Sie **Save**. Wiederholen Sie diesen Schritt für die MAC-Adresse 00-0A-EB-00-23-11.

   Die Filterregelliste sollte nun so aussehen:



5.6.4 Wireless Advanced

Unter **Wireless** → **Wireless Advanced** können Sie die erweiterten WLAN-Einstellungen tätigen.

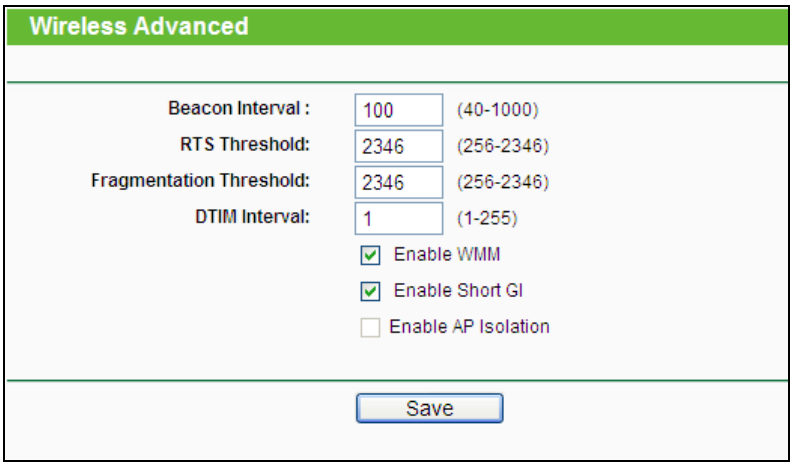


Bild 5-24 Wireless Advanced

- **Beacon Interval -** Geben Sie einen Wert von 20 bis 1000 (Millisek.) ein. Ortungspakete werden vom Router zur Synchronisierung des WLANs ausgesendet. Standardwert ist 100.
- **RTS Threshold -** Hier können Sie den RTS(Request to Send)-Grenzwert angeben. Ist ein Paket größer als dieser Wert, sendet der Router RTS-Frames zu einer bestimmten Empfangsstation, um den Versand eines Datenframes abzustimmen. Standardwert: 2346.
- **Fragmentation Threshold -** Dieser Wert ist die Maximalgröße, ab der Pakete fragmentiert werden. Eine zu niedrige Einstellung dieses Wertes könnte sich negativ auf die Performance auswirken. Standardwert: 2346 (empfohlen).
- **DTIM Interval -** Dieser Wert bezeichnet die Intervalllänge zwischen zwei aufeinanderfolgenden Delivery Traffic Indication Messages (DTIMs). Ein DTIM-Feld ist ein Countdown, der die Clients des nächsten Fensters anweist, auf Broadcasts und Multicasts zu hören. Hat der Router Broadcasts oder Multicasts für verbundene Clients gepuffert, sendet er den nächsten DTIM. Sie können diese Dauer in Ortungsintervallen (1..255) angeben. Standard ist 1, d.h. das DTIM-Intervall ist genauso lang wie ein Ortungsintervall.
- **Enable WMM - WMM** garantiert, dass Nachrichten hoher Priorität bevorzugt übertragen werden. Es wird wärmstens empfohlen, diese Option aktiviert zu lassen.
- **Enable Short GI -** Die Verwendung dieser Funktion wird empfohlen, da sie die Übertragungskapazitäten auf Kosten der Schutzintervallzeit vergrößert.

- **Enabled AP Isolation -** Diese Funktion kann WLAN-Stationen innerhalb Ihres Netzes untereinander unsichtbar machen. Damit können Sie nur mit dem Router, aber nicht miteinander kommunizieren. AP-Isolation ist standardmäßig deaktiviert.

Bemerkung:

Sind Sie mit den Einstellungen dieser Seite nicht vertraut, sollten Sie deren Werte auf den Standardwerten eingestellt lassen. Ansonsten könnte dies sich negativ auf die Performance auswirken.

5.6.5 Wireless Statistics

Im Menü **Wireless** → **Wireless Statistics** können Sie die MAC-Adresse, den aktuellen Status, Empfangene Pakete und gesendete Pakete pro verbundener WLAN-Station einsehen.

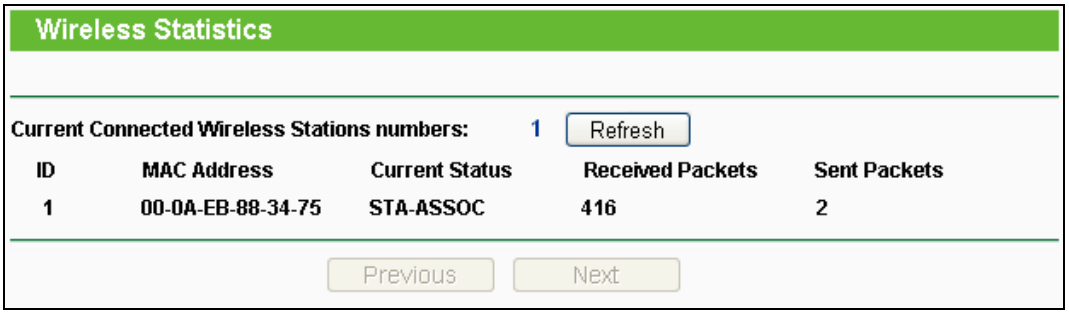


Bild 5-25 Mit dem Router verbundene WLAN-Geräte

- **MAC Address -** Die MAC-Adresse der verbundenen Station
- **Current Status -** Laufzeitstatus der verbundenen Station: **STA-AUTH**, **STA-ASSOC**, **STA-JOINED**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK**, **AP-UP**, **AP-DOWN** oder **Disconnected**.
- **Received Packets -** Anzahl der durch die Station empfangenen Pakete
- **Sent Packets -** Anzahl der durch die Station gesendeten Pakete

Die auf dieser Seite angezeigten Werte können nicht geändert werden. Um die Ansicht zu aktualisieren, klicken Sie **Refresh**.

Passt die Liste der verbundenen Stationen nicht auf eine Seite, können Sie mittels **Next** und **Previous** zwischen den Seiten hin- und herblättern.

Bemerkung:

Diese Seite lädt sich alle 5 Sekunden neu.

5.7 DHCP

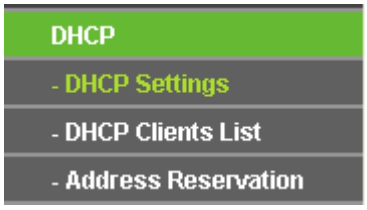


Bild 5-26 Das Menü **DHCP**

Im DHCP-Menü (Bild 5-26) existieren die folgenden drei Untermenüs: **DHCP Settings**, **DHCP Clients List** und **Address Reservation**.

5.7.1 DHCP Settings

Im Menü **DHCP** → **DHCP Settings** können Sie den DHCP-Server konfigurieren (Bild 5-27). Der DHCP(Dynamic Host Configuration Protocol)-Server des Routers ist standardmäßig aktiv und stellt DHCP-Clients im LAN ihre TCP/IP-Konfiguration bereit.

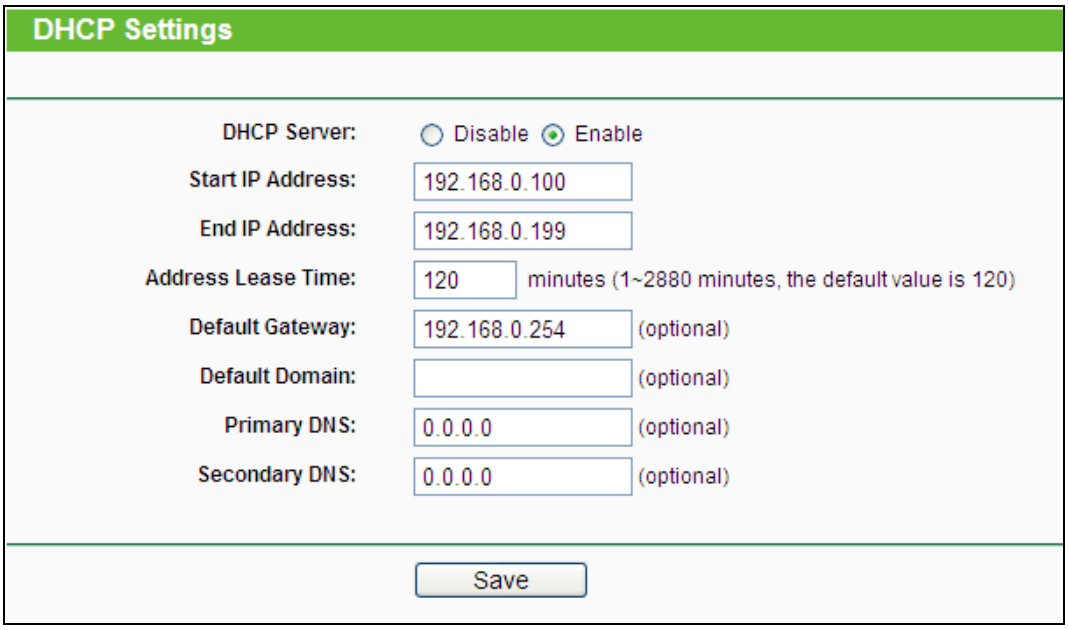


Bild 5-27 DHCP-Einstellungen

- **DHCP Server -** DHCP-Server **aktivieren** oder **deaktivieren**. Deaktivieren Sie den DHCP-Server, benötigen Sie einen anderen in Ihrem LAN oder Sie müssen die IP-Konfiguration jedes Clients in Ihrem Netz von Hand vornehmen.
- **Start IP Address -** Die erste vergebbare IP-Adresse. Standard ist 192.168.1.100.
- **End IP Address -** Die letzte IP-Adresse im Adresspool. Standard: 192.168.1.199.
- **Address Lease Time -** Die Dauer (in min.), für die ein Netzbenutzer seine IP-Konfiguration behalten darf, in Minuten. Gültig sind Werte von 1 bis 2880. Standard: 120.

- **Default Gateway -** (optional) Es wird empfohlen, hier die LAN-IP-Adresse des Routers (Standard: 192.168.1.1) einzugeben.
- **Default Domain -** (optional) Hier sollte der Domänenname Ihres Netzes eingegeben werden.
- **Primary DNS -** (optional) Geben Sie eine von Ihrem ISP erhaltene DNS-Server-IP-Adresse ein. Sollten Sie keine erhalten haben, fragen Sie bitte nach.
- **Secondary DNS -** (optional) Geben Sie hier die eventuell von Ihrem ISP erhaltene zweite DNS-Server-IP-Adresse ein, falls vorhanden.

Bemerkung:

Um den DHCP-Server nutzen zu können, müssen die Clients auf „IP-Adresse automatisch beziehen“ konfiguriert sein.

5.7.2 DHCP Clients List

Unter **DHCP → DHCP Clients List** können Sie Informationen über die gerade verbundenen DHCP-Clients abfragen (Bild 5-28).

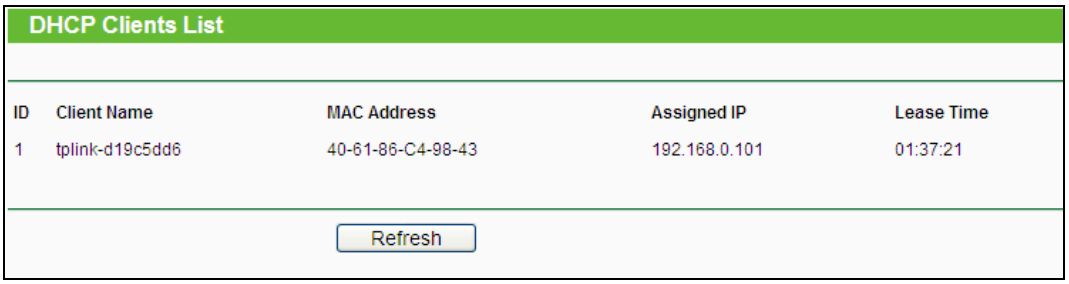


Bild 5-28 DHCP-Clientliste

- **ID -** Eine eindeutige Nummer des DHCP-Clients
- **Client Name -** Name des DHCP-Clients
- **MAC Address -** MAC-Adresse des DHCP-Clients
- **Assigned IP -** Die IP-Adresse, die der Router diesem Client gegeben hat.
- **Lease Time -** Die verbleibende Zeit, die der DHCP-Client die aktuelle Konfiguration noch behalten kann. Nach Ablauf dieser Zeit bekommt dieser automatisch eine neue IP-Adresse.

Die auf dieser Seite angezeigten Werte können nicht hier direkt geändert werden. Um die Ansicht zu aktualisieren, klicken Sie **Refresh**.

5.7.3 Address Reservation

Das Menü **DHCP → Address Reservation** befasst sich mit der Reservierung von IP-Adressen für Clients (Bild 5-29). Geben Sie hier eine reservierte IP-Adresse für einen LAN-PC an, wird dieser immer diese Adresse zugeteilt bekommen. Diese Funktionalität ist hilfreich, wenn Sie einen Server im LAN betreiben wollen.

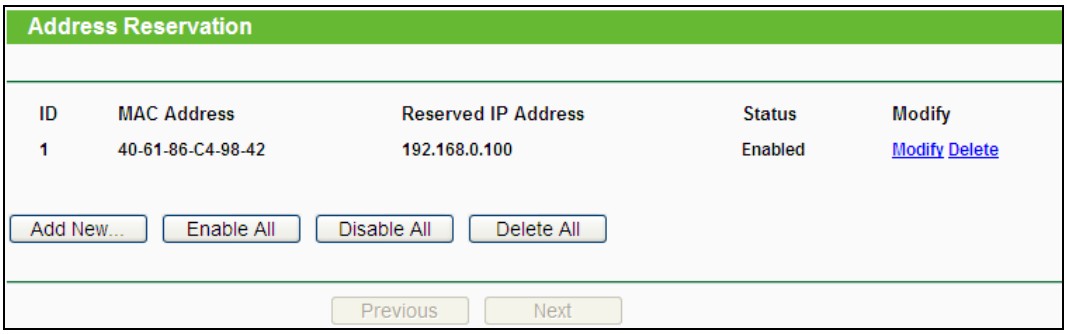


Bild 5-29 Address Reservation

- **MAC Address -** MAC-Adresse des PCs, für den Sie eine IP-Adresse reservieren möchten.
- **Assigned IP Address -** IP-Adresse, die für diesen Host reserviert wurde.
- **Status -** Status dieses Eintrags: **Enabled** (aktiv) oder **Disabled** (inaktiv).

Um IP-Adressen zu reservieren:

1. Klicken Sie **Add New…** Bild 5-30 erscheint.
2. Geben Sie die MAC-Adresse (Format „XX-XX-XX-XX-XX-XX“) und die IP-Adresse des betreffenden Computers ein.
3. Klicken Sie **Save**, wenn Sie fertig sind.

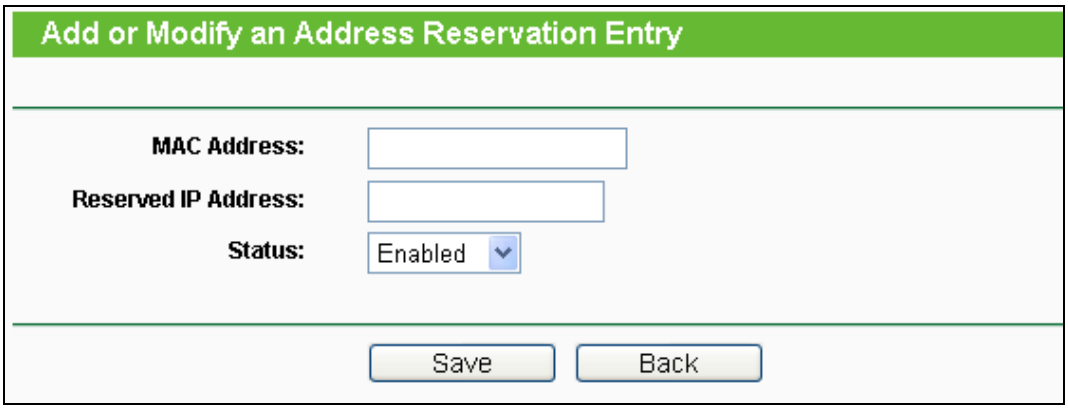


Bild 5-30 Adressreservierungseintrag hinzufügen oder bearbeiten

Um einen Eintrag zu bearbeiten oder zu löschen:

1. Klicken Sie für den zu bearbeitenden Eintrag. Klicken Sie **Delete**, wenn Sie ihn löschen möchten.
2. Bearbeiten Sie die Informationen, wie gewünscht.
3. Klicken Sie **Save**.

Klicken Sie **Enable All/Disable All**, um alle Einträge zu (de)aktivieren.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

Klicken Sie **Next**, um auf die nächste Seite zu blättern oder **Previous**, um auf die vorige Seite zurückzukehren.

5.8 Forwarding

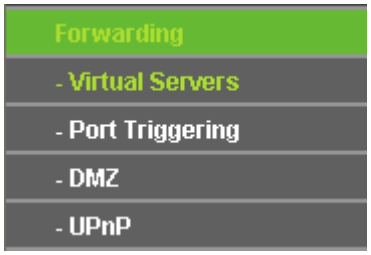


Bild 5-31 Menü **Forwarding**

Im Forwarding-Menü gibt es vier Untermenüs (Bild 5-31): **Virtual Servers**, **Port Triggering**, **DMZ** und **UPnP**.

5.8.1 Virtual Servers

Unter **Forwarding** → **Virtual Servers** können Sie virtuelle Server ansehen und bearbeiten (Bild 5-32). Virtuelle Server erlauben es, Dienste aus Ihrem LAN auch im Internet zur Verfügung zu stellen, z.B. DNS, E-Mail und FTP. Ein virtueller Server wird mittels eines Ports definiert. Alle auf diesem Port von außen ankommenden Anfragen werden auf den angegebenen Computer weitergegeben. Dieser benötigt dafür eine statische oder eine reservierte IP-Adresse, um erreichbar zu bleiben.

Bild 5-32 Virtuelle Server

- **Service Port -** Nummern externer Ports. Hier können einzelne Ports oder Portbereiche (Format „XXX - YYY“, wobei „XXX“ die Nummer des Startports und „YYY“ die Nummer des Endports des entsprechenden Bereiches darstellt) definiert werden.
- **Internal Port** - Die Portnummer, die Ihr Dienst benutzt. Ist diese mit dem o.a. **Service Port** identisch, kann das Feld freigelassen werden.
- **IP Address** - Die IP-Adresse des Servers im LAN.
- **Protocol** - Das Protokoll, das diese Anwendung einsetzt: **TCP**, **UDP** oder **All** (alle Protokolle, die der Router unterstützt).

- **Status** - Status dieses Eintrags: **Enabled** oder **Disabled**.
- **Common Service Port** - Hier sind einige häufig verwendete Dienste mit ihren Portnummern hinterlegt.
- **Modify** - Ändern oder Löschen eines bestehenden Eintrages.

Um einen neuen Virtuellen Server anzulegen:

1. Klicken Sie **Add New…** (Bild 5-33).
2. Wählen Sie den Dienst, den Sie anbieten möchten, aus der Liste **Common Service Port** aus. Ist Ihr Dienst dort nicht enthalten, geben Sie einfach die Portnummer in das Feld **Service Port** ein.
3. Geben Sie die LAN-IP-Adresse des Servers in das Feld **IP Address** ein.
4. Wählen Sie das Protokoll, das diese Anwendung benutzt: **TCP**, **UDP** oder **All**.
5. Wählen Sie **Enable** aus, um den Virtuellen Server zu aktivieren.
6. Klicken Sie **Save**.

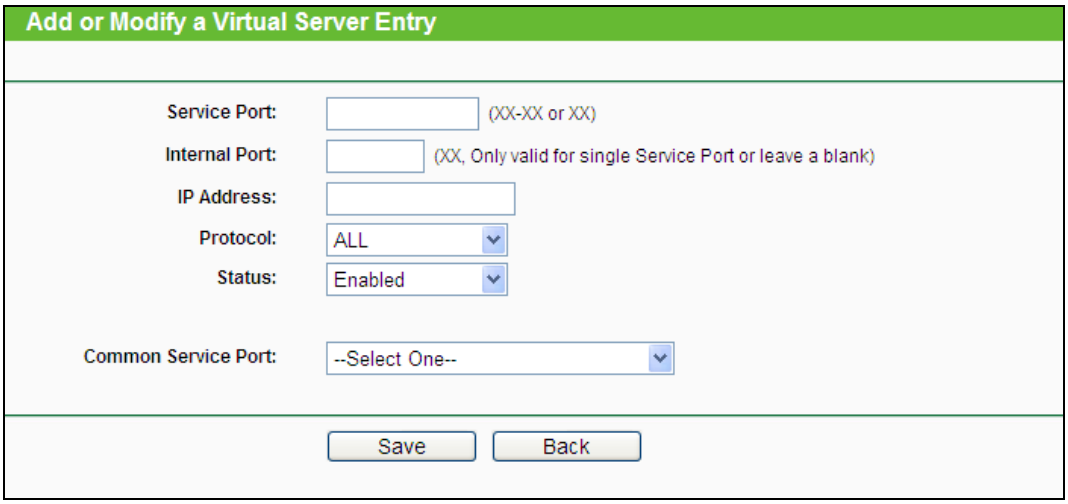


Bild 5-33 Virtuellen Server hinzufügen oder bearbeiten

Bemerkung:

Möchten Sie auf einem Computer mehrere Dienste anbieten, legen Sie für diesen einfach mehrere Virtuelle Server an.

Um einen bestehenden Eintrag zu bearbeiten oder zu löschen:

1. Klicken Sie **Modify** für den zu bearbeitenden Eintrag. Möchten Sie ihn löschen, drücken Sie **Delete**.
2. Bearbeiten Sie die Informationen, wie gewünscht.
3. Klicken Sie **Save**.

Klicken Sie **Enable All/Disable All**, um alle Einträge zu (de)aktivieren.

Klicken Sie **Delete All**, um alle Einträge auf dieser Seite zu entfernen.

Klicken Sie **Next**, um auf die nächste Seite zu wechseln oder **Previous**, um auf die vorige Seite zurückzukehren.

Bemerkung:

Wird ein Virtueller Server auf Port 80 eingerichtet, muss der Webmanagement-Port unter **Security** –> **Remote Management** auf einen anderen Wert als 80 gesetzt werden, z.B. 8080. Ansonsten wird es zu Konflikten kommen.

5.8.2 Port Triggering

Wählen Sie das Menü **Forwarding** → **Port Triggering**. Hier können Sie die Einstellungen zum Porttriggering ansehen und anpassen (Bild 5-34). Einige Anwendungen wie z.B. Internetspiele oder Videokonferenzen erfordern Mehrfachverbindungen. Dies ist mit einem einfachen NAT-Router nicht realisierbar. Damit dies mit einem NAT-Router funktioniert, muss auf Porttriggering zurückgegriffen werden.

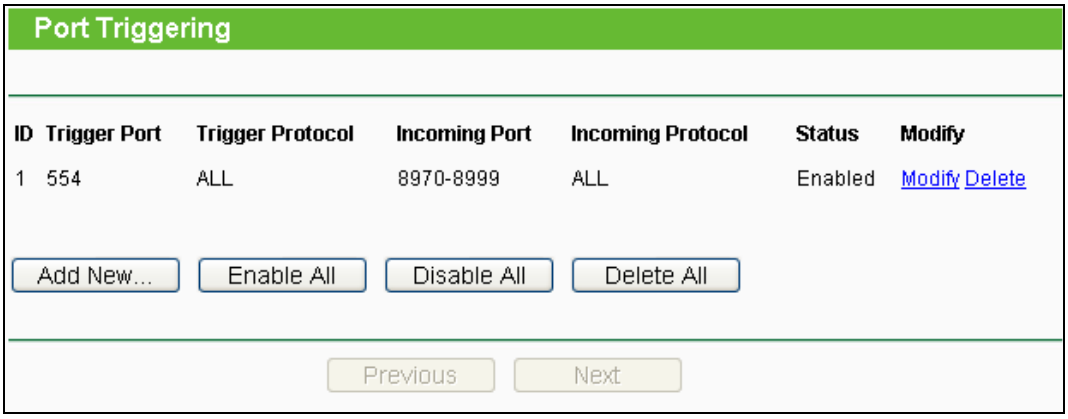


Bild 5-34 Porttriggering

Porttriggering funktioniert so:

1. Ein lokaler PC öffnet eine ausgehende Verbindung auf dem Port, der im Feld **Trigger Port** angegeben ist.
2. Der Router merkt sich diese Verbindung, öffnet die damit assoziierten **Incoming Ports** und leitet auf diesen ankommende Verbindungen an den lokalen PC weiter.
3. Hierüber kann der entfernte Host nun den lokalen PC erreichen

- **Trigger Port -** Der Port, auf dem eine ausgehende Verbindung diese Regel auslöst.
- **Trigger Protocol -** Das Protokoll, das zur Auslösung verwendet wird: Entweder **TCP**, **UDP** oder **All** (alle Protokolle, die der Router unterstützt).
- **Incoming Port -** Port oder Portbereich, den das entfernte System benutzt, um auf die Triggerverbindung zu reagieren. Verbindungen, die auf diesen Ports ankommen, werden zu dem auslösenden PC weitergeleitet. Es können bis zu 5 durch Kommata getrennte einzelne Ports bzw. Portbereiche angegeben werden, z.B.: 2000-2038, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol -** Das Protokoll für die eingehenden Verbindungen, entweder **TCP**, **UDP** oder **All** (alle Protokolle, die der Router unterstützt).
- **Status -** Der Status dieses Eintrags: **Enabled** oder **Disabled**

Um eine neue Regel hinzuzufügen, geben Sie auf der Seite **Port Triggering** Folgendes ein

1. Klicken Sie **Add New…**. Bild 5-35 erscheint.
2. Wählen Sie eine gebräuchliche Applikation aus **Common Applications** aus, werden **Trigger Port** und **Incoming Ports** automatisch eingegeben. Ist Ihre Applikation in der Liste **Common Applications** nicht enthalten, geben Sie **Trigger Port** und **Incoming Ports** von Hand an.
3. Wählen Sie das Protokoll (**Trigger Protocol**), das auf dem **Triggerport** verwendet wird, aus: Entweder **TCP**, **UDP** oder **All**.
4. Wählen Sie das Protokoll für die eingehenden Ports (**Incoming Ports**) aus: **TCP**, **UDP** oder **Alle**.
5. Wählen Sie **Enabled** als **Status**.
6. Klicken Sie **Save**, um die neue Regel zu speichern.

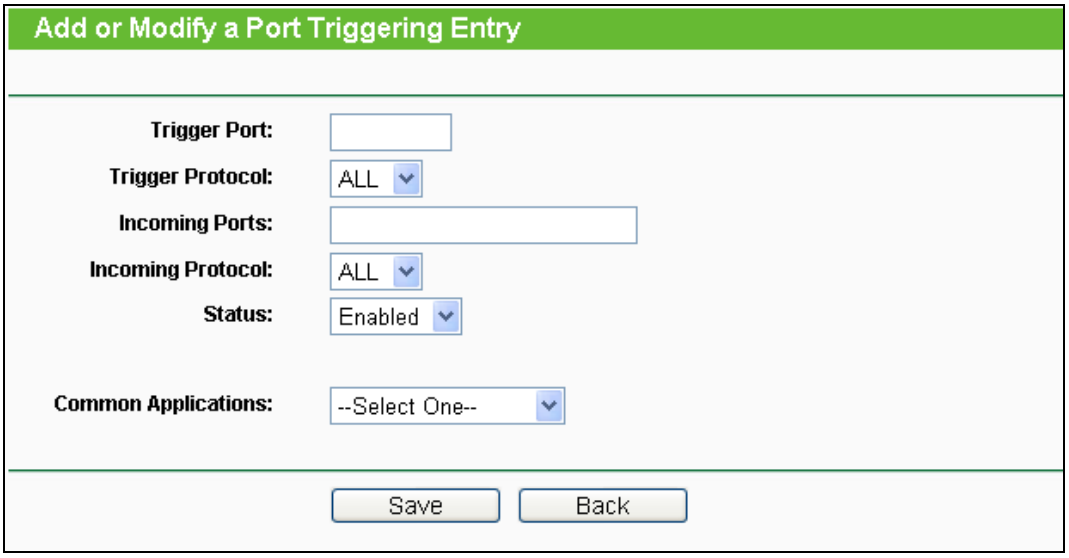


Bild 5-35 Triggereintrag hinzufügen oder bearbeiten.

Um einen bestehenden Eintrag zu bearbeiten oder zu löschen:

1. Klicken Sie **Modify** für den zu bearbeitenden Eintrag oder **Delete**, um ihn zu löschen.
2. Bearbeiten Sie die Informationen, wie gewünscht.
3. Klicken Sie **Save**.

Klicken Sie **Enable All**, um alle Einträge zu aktivieren.

Klicken Sie **Disable All**, um alle Einträge zu deaktivieren.

Klicken Sie **Delete All,** um alle Einträge zu löschen.

Bemerkungen:

1) Wird die Triggerverbindung geschlossen, schließt der Router auch die für die eingehenden Verbindungen geöffneten Ports.

2) Jede Regel kann nur von einem Computer zugleich verwendet werden. Eine eventuell von einem anderen LAN-Host initiierte Triggerverbindung wird, sofern sie schon in Verwendung ist, verweigert.

3) Portbereiche für eingehende Verbindungen dürfen einander nicht überlappen.

5.8.3 DMZ

Die Funktionalität **DMZ-Host** unter **Forwarding** → **DMZ** (Bild 5-36) erlaubt es, einen lokalen Host für aus dem Internet kommende Verbindungen komplett (d.h. auf allen Ports) freizugeben. Dies ist sinnvoll für z.B. Gaming- oder Videokonferenzserver. Der DMZ-Host darf nicht mit DHCP konfiguriert sein, sondern muss eine statische IP-Adresse haben.

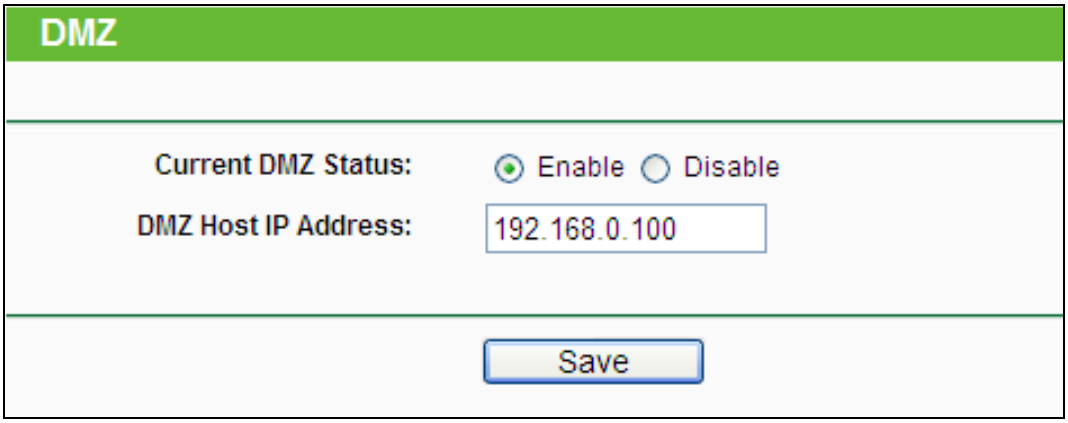


Bild 5-36 DMZ

Um einen Computer/Server als DMZ-Host zu konfigurieren:

1. Klicken Sie **Enable**.
2. Geben Sie die lokale IP-Adresse in das Feld **DMZ Host IP Address** ein.
3. Klicken Sie **Save**.

☞ **Bemerkung:**

Nachdem ein Computer zum DMZ-Host erklärt wurde, funktioniert die Router-Firewall für diesen nicht mehr

5.8.4 UPnP

UPnP (Universal Plug and Play) ermöglicht es Geräten wie Internetcomputern, auf Ressourcen des lokalen PCs zuzugreifen. UPnP-Geräte können automatisch vom UPnP-Dienst erkannt werden. Sie können UPnP auf dieser Seite konfigurieren (Bild 5-37).

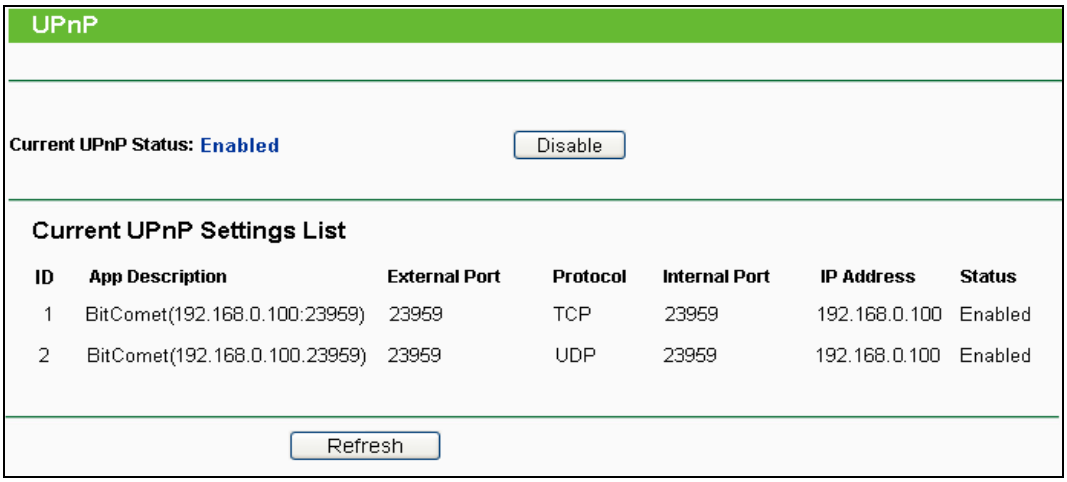


Bild 5-37 UPnP-Einstellungen

- **Current UPnP Status -** UPnP kann aktiviert oder deaktiviert werden. Da UPnP ein Sicherheitsrisiko darstellen kann, sollte es bei Nichtbenutzung deaktiviert werden.
- **Current UPnP Settings List -** In dieser Tabelle finden Sie die aktuell gültigen UPnP-Informationen.
  - **App Description -** Beschreibung der Applikation, die die UPnP-Anfrage gestellt hat.
  - **External Port -** Externer Port, den der Router dieser Applikation geöffnet hat.
  - **Protocol -** Zeigt das benutzte Protokoll an.
  - **Internal Port -** Interner Port, den der Router für den lokalen Host geöffnet hat.
  - **IP Address -** Das gerade auf den Router zugreifende UPnP-Gerät.
  - **Status -** Entweder **Enabled** oder **Disabled**. **Enabled** bedeutet, dass der Port noch aktiv ist, ansonsten ist der Port inaktiv.

Klicken Sie **Enable** bzw. **Disable**, um den UPnP-Status umzuschalten.

Klicken Sie **Refresh**, um die Ansicht der UPnP-Einstellungen zu aktualisieren.

5.9 Security

Bild 5-38 Das Menü **Security**

Im Menü **Security** gibt es vier Untermenüs (Bild 5-38): **Basic Security**, **Advanced Security**, **Local Management** und **Remote Management**.

5.9.1 Basic Security

Im Menü **Security** → **Basic Security** können Sie, wie in Bild 5-39 gezeigt, die Basissicherheit einstellen.

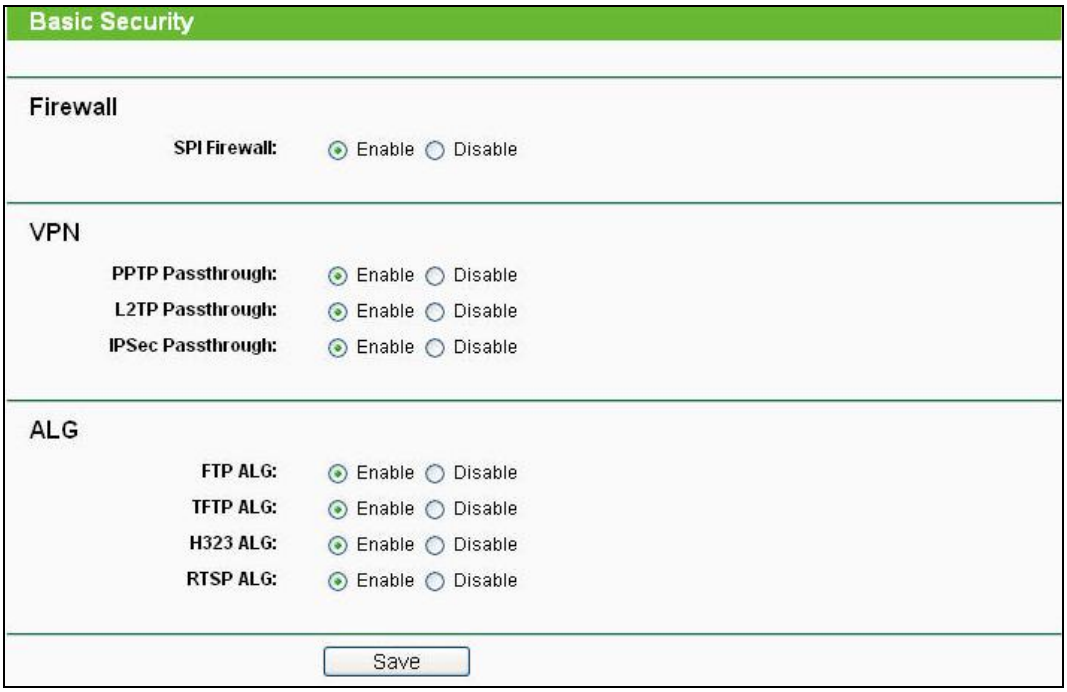


Bild 5-39 Basissicherheit

- **Firewall -** Eine Firewall schützt Ihr Netz vor Angriffen von außen. Hiermit können Sie die einzelnen Firewallfunktionen ein- und ausschalten.

  - **SPI Firewall** - SPI (Stateful Packet Inspection, auch bekannt als dynamische Paketfilterung) hilft durch Paketinspektion dabei, Angriffe von außen zu vereiteln. Hierbei untersucht es, ob der Datenverkehr zu dem verwendeten Protokoll passt. Die SPI-Firewall ist standardmäßig eingeschaltet. Sollen die PCs in Ihrem LAN nicht dadurch geschützt werden, können Sie diese Funktion abschalten.

- **VPN -** VPN-Passthrough muss aktiv sein, wenn Sie mittels VPN-Tunneln über IPSec, PPTP oder L2TP durch den Router passieren möchten.

  - **PPTP Passthrough** - Das „Point-to-Point Tunneling Protocol“ (PPTP) ermöglicht die Tunnelung des Point-to-Point-Protokolls (PPP) durch ein IP-Netz.
  - **L2TP Passthrough** - „Layer 2 Tunneling Protocol“ (L2TP) wird verwendet, um Punkt-zu-Punkt-Sitzungen über das Internet auf Layer-2-Ebene zu öffnen.
  - **IPSec Passthrough** - „Internet Protocol Security“ (IPSec) ist eine Protokollsuite zur Ermöglichung privater, sicherer Kommunikation über Internetprotokoll (IP) mit Hilfe von Verschlüsselung.

- **ALG -** Es wird empfohlen, Application Layer Gateway (ALG) zu aktivieren, da dies benutzerspezifisches NAT für bestimmte Kontroll- und Datenprotokolle wie z.B. FTP, TFTP

und H232 erlaubt.

- **FTP ALG** - Um FTP-Clients und -Server Daten durch den NAT-Router übertragen zu lassen, lassen Sie die Standardeinstellung **Enabled**.
- **TFTP ALG** - Um TFTP-Clients und -Server Daten durch den NAT-Router übertragen zu lassen, lassen Sie die Standardeinstellung **Enabled**.
- **H323 ALG** - Um Microsoft-NetMeeting-Clients Daten durch den NAT-Router übertragen zu lassen, lassen Sie die Standardeinstellung **Enabled**.
- **RTSP ALG** - Um einigen Medienplayern die Kommunikation mit Streamingservern durch den NAT-Router zu ermöglichen, lassen Sie die Standardeinstellung **Enabled**.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

5.9.2 Advanced Security

Mittels der Seite **Security** → **Advanced Security** (Bild 5-40) können Sie den Router vor TCP-SYN-Flood-, UDP-Flood- und ICMP-Flood-Angriffen schützen.

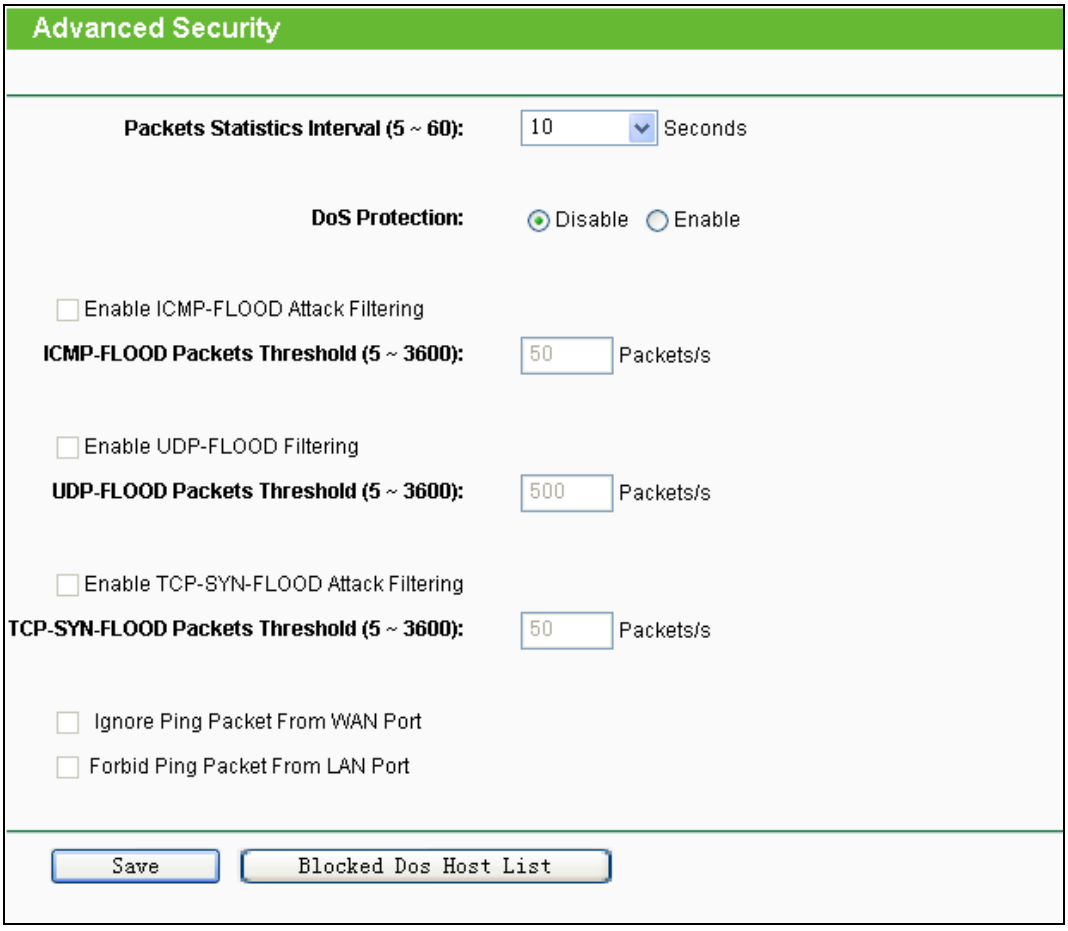


Bild 5-40 Erweiterte Sicherheitseinstellungen

- **Packets Statistics Interval (5~60) -** Der Wert **Packets Statistics Interval** bezeichnet die Dauer, die eine einzelne Paketstatistik umfasst. Das Ergebnis dieser Statistik wird für Analysen der Funktionen **TCP-SYN-Flood**, **UDP-Flood** und **ICMP-Flood** verwendet. Gültige Werte sind von 5 bis 60, Einheit ist Sekunden. Standardwert ist 10.

- **DoS Protection -** DoS-Schutz aktivieren oder deaktivieren. Nur, wenn er **enabled** ist, funktionieren die Floodfiltermechanismen.

  Bemerkung:

  Der DoS-Schutz wird nur wirksam, wenn die **Traffic Statistics** unter **System Tools → Traffic Statistics** aktiv sind.

- **Enable ICMP-FLOOD Attack Filtering -** ICMP-FLOOD-Schutz aktivieren oder deaktivieren.
- **ICMP-FLOOD Packets Threshold (5~3600) -** Überschreitet die aktuelle Zahl der ICMP-FLOOD-Pakete diesen Wert, blockiert der Router alle weiteren sofort. Standardwert ist 50. Gültige Werte sind von 5..3600.
- **Enable UDP-FLOOD Filtering -** UDP-FLOOD-Schutz aktivieren oder deaktivieren.
- **UDP-FLOOD Packets Threshold (5~3600) -** Überschreitet die aktuelle Zahl der UDP-FLOOD-Pakete diesen Wert, blockiert der Router alle weiteren sofort. Standardwert ist 50. Gültige Werte sind von 5..3600.
- **Enable TCP-SYN-FLOOD Attack Filtering -** TCP-SYN-FLOOD-Schutz aktivieren oder deaktivieren.
- **TCP-SYN-FLOOD Packets Threshold (5~3600) -** Überschreitet die aktuelle Zahl der TCP-SYN-FLOOD-Pakete diesen Wert, blockiert der Router alle weiteren sofort. Standardwert ist 50. Gültige Werte sind von 5..3600.
- **Ignore Ping Packet From WAN Port -** Ping-Pakete vom WAN-Port ignorieren oder nicht. Standardmäßig deaktiviert. Ist die Funktion aktiv, können Pingpakete aus dem Internet nicht verarbeitet werden.
- **Forbid Ping Packet From LAN Port -** Ping-Pakete vom LAN-Port ignorieren oder nicht Standardmäßig deaktiviert. Ist die Funktion aktiv, können Pingpakete aus dem LAN nicht verarbeitet werden (stört die Funktion einiger Viren).

Klicken Sie **Save**, um diese Einstellungen zu speichern.

Klicken Sie auf **Blocked DoS Host List**, um die Liste der blockierten DoS-Hosts anzusehen.

5.9.3 Local Management

Im Menü **Security → Local Management** können Sie die Verwaltungsregeln wie in Bild 5-41 erkennbar bearbeiten. Damit können Sie einzelnen LAN-PCs die Berechtigung, auf den Router zuzugreifen, erteilen oder entziehen.

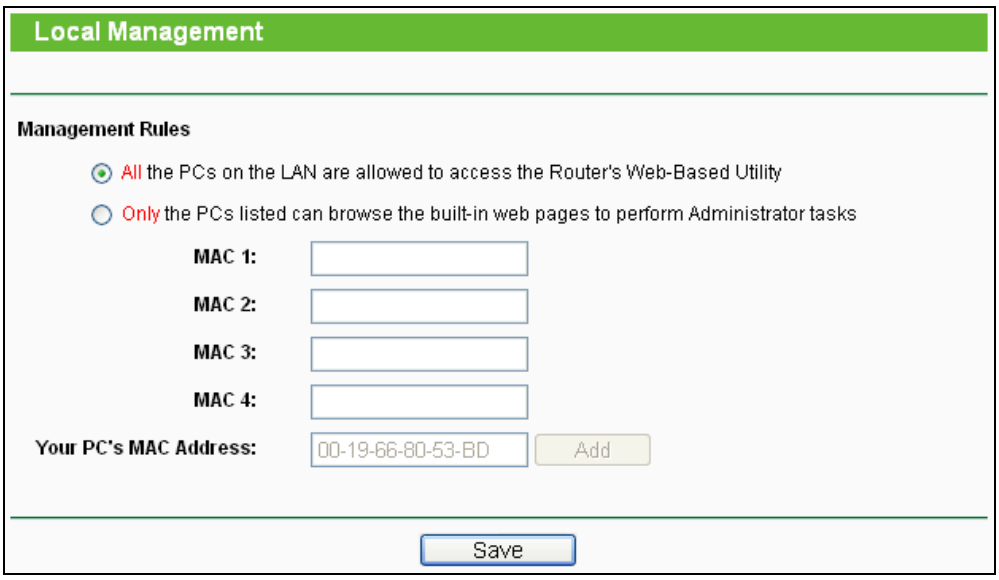


Bild 5-41 Lokale Verwaltung

Standardmäßig gilt die Option **All the PCs on the LAN are allowed to access the Router's Web-Based Utility**. Möchten Sie diesen Zugriff nur ein paar PCs gewähren, können Sie die zugehörigen MAC-Adressen auf dieser Seite eintragen (Format: „XX-XX-XX-XX-XX-XX“, wobei jedes „X“ für eine Hexadezimalziffer steht) und **Only the PCs listed can browse the built-in web pages to perform Administrator tasks** aktivieren. Dann können nur noch diese PCs auf das Webinterface des Routers zugreifen.

Nach Klick auf **Add** wird die MAC-Adresse Ihres PCs in die Liste aufgenommen.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

Bemerkung:

Haben Sie sich mittels dieses Features aus dem Router ausgesperrt und kein anderer PC kann die Sperrung aufheben, müssen Sie den Router mittels der **Reset-Taste** (in einem Loch auf der Rückseite des Routers) zurücksetzen. Drücken Sie mit einem spitzen Gegenstand mindestens 5 Sekunden darauf. Danach muss der Router komplett neu konfiguriert werden.

5.9.4 Remote Management

Im Menü **Security** → **Remote Management** können Sie die Fernwartungsfunktion aktivieren (siehe Bild 5-42). Damit kann der Router aus der Ferne über das Internet konfiguriert werden.

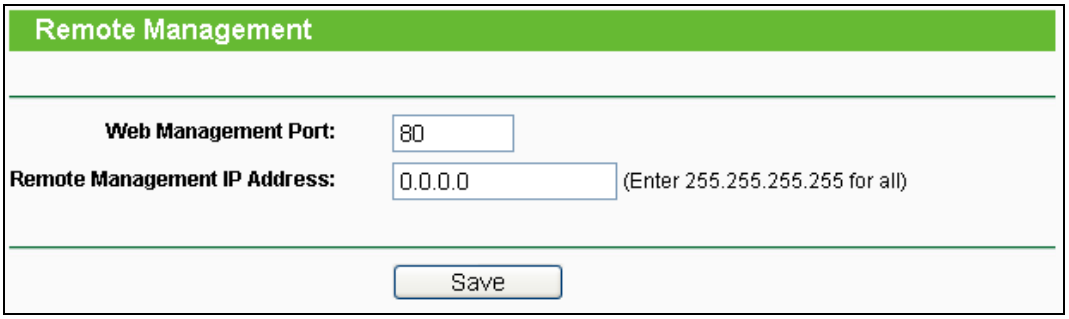


Bild 5-42 Fernwartungseinstellungen

- **Web Management Port -** Die Nummer des Ports, über den aus dem Internet auf den Router zugegriffen werden kann. Standardwert ist 80. Um die Sicherheit zu erhöhen, wird empfohlen, diese Nummer zu ändern. Nehmen Sie vorzugsweise einen Wert von 1024 bis 65534, jedoch keinen Port, der zu gebräuchlich ist.
- **Remote Management IP Address -** Von dieser IP-Adresse aus können Sie über das Internet auf Ihren Router zugreifen. Standard ist 0.0.0.0, was bedeutet, dass die Fernwartungsfunktion deaktiviert ist. Ändern Sie diesen Wert, um die Funktion zu aktivieren. Setzen Sie den Wert auf 255.255.255.255, kann von alle Internethosts auf Ihren Router zugegriffen werden.

Bemerkung:

1. Um auf den Router zuzugreifen, geben Sie die WAN-IP-Adresse des Routers in die Adresszeile Ihres Browsers ein, gefolgt von einem Doppelpunkt und der Portnummer. Beispiel: Die WAN-Adresse lautet 202.96.12.8 und die Portnummer 8888. In diesem Fall ist http://202.96.12.8:8888 einzugeben. Bei erfolgreicher Verbindung werden Sie hierauf nach dem Passwort des Routers gefragt.
2. Bitte verwenden Sie für die Fernwartung ein besonders sicheres Passwort.

5.10 Parental Control

Im Menü **Parental Control** können Sie die Zugangskontrolle nach Bild 5-43 einrichten. Mit dieser Funktion können Sie die Internetaktivitäten Ihrer Kinder/Angestellten auf bestimmte Websites und/oder Zeiträume einschränken.

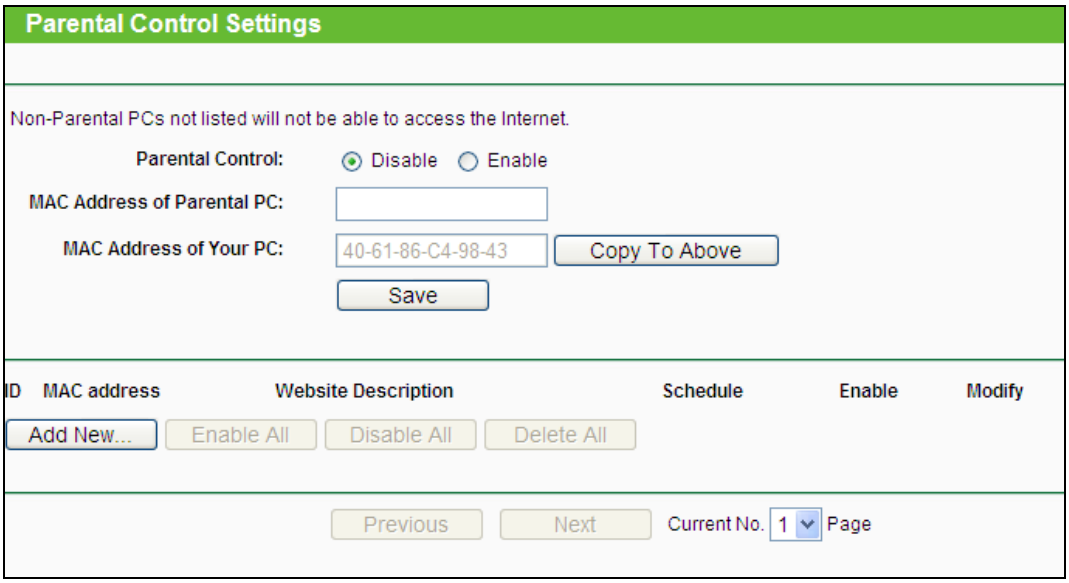


Bild 5-43 Zugangskontrolle

Um einen neuen Eintrag hinzuzufügen, folgen Sie bitte diesen Schritten.

1. Klicken Sie **Hinzufügen…**. Das nächste Bild erscheint (Bild 5-44).

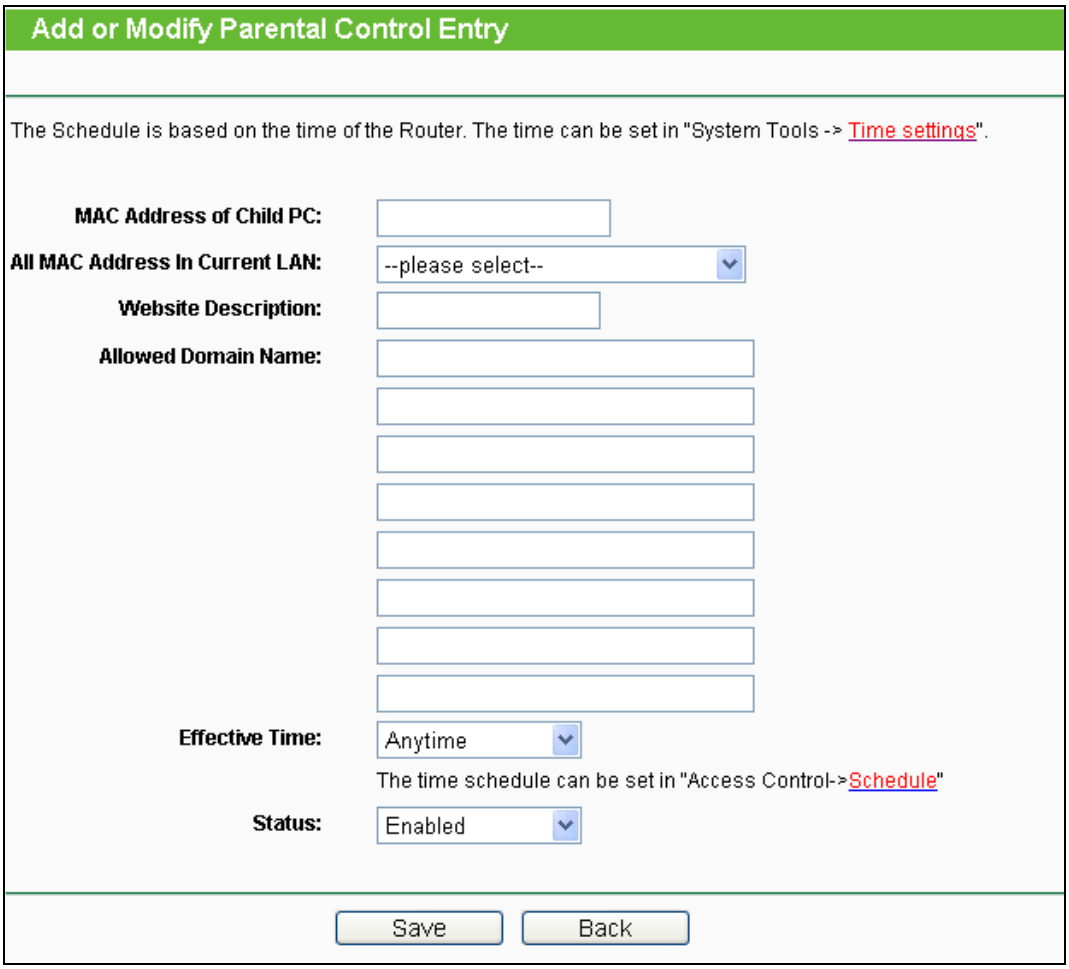


Bild 5-44 Zugriffskontrolleintrag anlegen oder verändern

- **Parental Control -** Aktivieren (**Enable**) oder Deaktivieren (**Disable**) der Funktion.
- **MAC Address of Parental PC -** Geben Sie hier die MAC-Adresse des kontrollierenden PCs ein oder benutzen Sie die Funktion **Copy To Above**, um Ihre Adresse einzusetzen.
- **MAC Address of Your PC -** Dieses Feld zeigt die MAC-Adresse des gerade verbundenen PCs an. Diese können Sie mit einem Klick in das darüberliegende Feld kopieren.
- **Website Description -** Beschreibung der eingetragenen Website.
- **Schedule -** Der Zeitraum, in dem der PC auf das Internet zugreifen darf. Für weitere Einzelheiten gegen Sie bitte in den Abschnitt **Access Control → Schedule**.
- **Enable -** Aktivieren des Eintrages.
- **Modify -** Hiermit können Sie einen Eintrag bearbeiten oder löschen.

2. Geben Sie die MAC-Adresse des zu kontrollierenden PCs (z.B. 00-11-22-33-44-AA) in das Feld **MAC Address of Child PC** ein oder suchen Sie eine aus der Liste **All MAC Address in Current LAN** aus.
3. Geben Sie eine Webseitenbeschreibung als **Website Description** ein.

4. Geben Sie unter **Allowed Domain Name** den Domänennamen der zugelassenen Webseite oder Schlüsselwörter (z.B. kinder) ein. Jeder Domänenname, der die Schlüsselwörter enthält (www.kinderseite.com, www.kinderspielplatz.de), ist zugänglich.
5. Wählen Sie den gewünschten Wirksamkeitszeitraum aus der Drop-Down-Liste aus (z.B. Samstagabend). Ist kein passender dabei, können Sie durch Klick auf **Schedule** (unten in rot) auf die Planungsseite gelangen und dort einen anlegen.
6. Im Feld **Status** können Sie den Eintrag aktivieren oder deaktivieren.
7. Klicken Sie **Save**.

Klicken Sie **Enable All**, um alle Regeln zu aktivieren.

Klicken Sie **Disable All**, um alle Regeln zu aktivieren.

Klicken Sie **Delete All**, um alle Regeln zu löschen.

Klicken Sie **Next**, um zur nächsten Seite zu blättern oder **Previous**, um zur vorigen Seite zurückzukehren.

Beispiel: Soll der PC mit der MAC-Adresse 00-11-22-33-44-AA nur samstags und nur www.google.com erreichen können, während der PC mit der MAC-Adresse 00-11-22-33-44-BB keinen Zugangseinschränkungen unterliegen soll, sollte Folgendes konfiguriert werden.

1. Klicken Sie auf das Menü **Parental Control**, aktivieren Sie die Funktion und geben Sie 00-11-22-33-44-BB in das Feld **MAC Address of Parental PC** ein.
2. Klicken Sie **Access Control** → **Schedule**, um auf die Planungsseite zu gelangen. Klicken Sie **Add New…**, um eine neue Planung anzulegen. **Schedule Description** könnte „Samstag“ lauten, **Day** wäre „Sat“ und **Time all day-24 hours**.
3. Gehen Sie zurück zu **PC-Kontrolle** und legen Sie folgendermaßen einen Eintrag an:
   1) Klicken Sie **Add New...**.
   2) Geben Sie „00-11-22-33-44-AA“ in das Feld **MAC Address of Child PC** ein.
   3) Geben Sie „Google” als **Website Description** an.
   4) Geben Sie „www.google.com” unter **Allowed Domain Name** ein.
   5) Wählen Sie die gerade erstellte Planung „Samstag” als **Effective Time** aus.
   6) Setzen Sie **Status** auf **Enable**.
4. Klicken Sie **Save**, um den Eintrag zu speichern.

   Damit kommen Sie auf die Übersichtsseite zurück und sehen Bild 5-45.

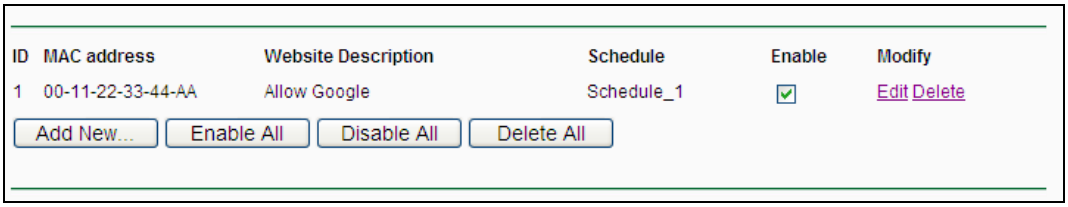


Bild 5-45 PC-Kontrollseite

5.11 Access Control

Bild 5-46 Access Control

Im Menü **Access Control** gibt es vier Untermenüs (Bild 5-46): **Rule**, **Host**, **Target** und **Schedule**.

5.11.1 Rule

Im Menü **Access Control** → **Rule** können Sie Zugangskontrollregeln setzen, wie in Bild 5-47 zu sehen ist.

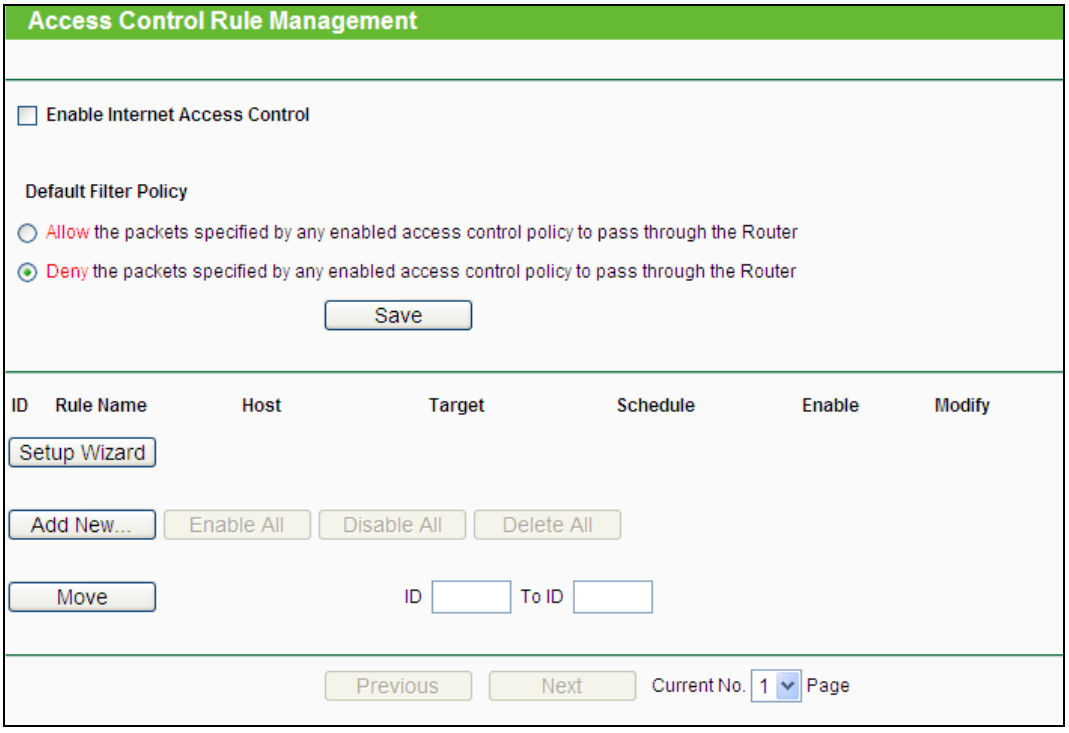


Bild 5-47 Zugriffskontrollregel-Verwaltung

- **Enable Internet Access Control -** Wählen Sie dies an, damit die Internetzugriffskontrolle aktiv wird.
- **Rule Name -** Hier sehen Sie den eindeutigen Namen der Regel.
- **Host -** Dies ist der Name des von der Regel betroffenen Hosts.
- **Target -** Dies ist das Ziel, auf das die Regel Anwendung findet.
- **Schedule -** Die mit der Regel assoziierte Planung.
- **Status -** Status dieser Regel: **Enabled** oder **Disabled**.

- **Modify -** Hier kann die Regel bearbeitet oder gelöscht werden.
- **Setup Wizard -** Hiermit können Sie ganz einfach Regeln erstellen.
- **Add New... -** Klicken Sie **Add New...**, um eine neue Regel hinzuzufügen.
- Klicken Sie **Enable all**, um alle Regeln zu aktivieren.
- Klicken Sie **Disable all**, um alle Regeln zu deaktivieren.
- Klicken Sie **Delete all**, um alle Regeln zu löschen.
- **Move -** Sie können die Reihenfolge der Regeln nach Belieben ändern. Dies beeinflusst ihre Priorität. Frühere Regeln sind stärker als spätere. Geben Sie in das erste Feld die ID des zu verschiebenden Eintrags ein und in das zweite Feld die Stelle, an die verschoben werden soll. Klicken Sie dann **Move**, um die Reihenfolge zu ändern.
- Klicken Sie **Previous**, um zur letzten Seite zurückzukehren oder **Next**, um die nächste Seite anzusehen.

Es existieren zwei Methoden, um neue Regeln hinzuzufügen.

Methode 1:

1. Klicken Sie auf **Setup Wizard**. Es erscheint Bild 5-48.

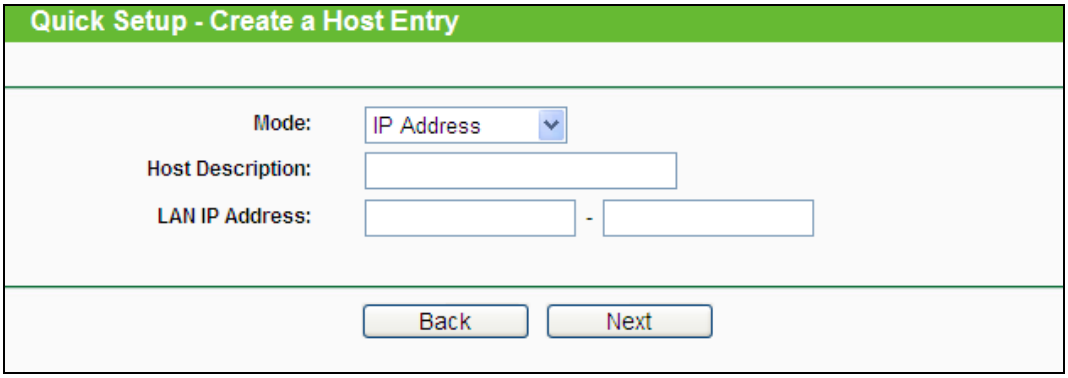


Bild 5-48 Regelassistent – Hosteintrag anlegen

- **Host Description** - Hier können Sie eine eindeutige Hostbeschreibung angeben (z.B. Pauls PC).
- **Mode** - Hier können Sie auswählen, ob der Host anhand seiner **IP-** oder seiner **MAC-Adresse** identifiziert werden soll.

Wurde **IP Address** ausgewählt, erscheint folgendes Feld:

- **LAN IP Address** - Geben Sie hier die IP-Adresse oder den IP-Adressenbereich des zu spezifizierenden Hosts an, z.B. **192.168.0.23**.

Wurde **MAC-Adresse** ausgewählt, erscheint folgendes Feld:

- **MAC Address** - Geben Sie hier die MAC-Adresse des zu spezifizierenden Hosts an. Format: XX-XX-XX-XX-XX-XX. Beispiel: **00-11-22-33-44-AA**.

2. Klicken Sie **Next**. Es erscheint Bild 5-49.

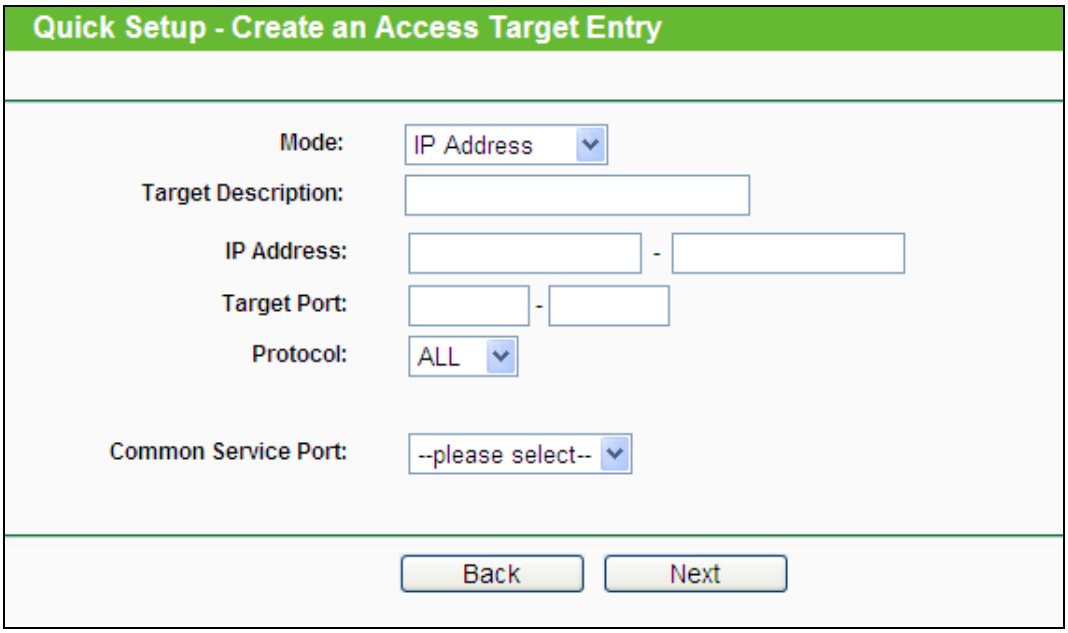


Bild 5-49 Regelassistent – Anlegen eines Eintrags für ein Zugriffsziel

- **Target Description** - Geben Sie hier eine eindeutige Bezeichnung für das Ziel ein, z.B. „google“.
- **Mode** - Hier können Sie auswählen, ob das Ziel anhand seiner **IP-Adresse** oder seines **Domänennamens** identifiziert werden soll.

Wurde **IP Address** gewählt, erscheinen folgende Felder:

- **IP Address** - Geben Sie hier die IP-Adresse (oder den IP-Adressbereich) des Ziels/der Ziele ein. Beispiel: **217.72.195.48**.
- **Target Port** - Der Port(bereich), der für das Ziel gelten soll. Für den Fall, dass Sie gebräuchliche Dienste verwenden wollen, könnte der Port unter **Common Service Port** gelistet sein.
- **Protocol** - Hier haben Sie vier Optionen: **All**, **TCP**, **UDP** und **ICMP**.
- **Common Service Port** - Eine Liste einiger bekannter Dienste mit ihren zugehörigen Portnummern. Wenn Sie hier einen Dienst auswählen, wird die Standard-Portnummer eingetragen. Beispiel: Wählen Sie **FTP** aus, wird als Port automatisch die Nummer **21** gesetzt.

Wurde **Domain Name** ausgewählt, sehen Sie nur eine Eingabemöglichkeit:

- **Domain Name** - Hier können Sie bis zu 4 Domänennamen eingeben, entweder volle Namen oder Schlüsselwörter, z.B. „kinder“. In diesem Fall würde die Regel auf alle Domänennamen, die das Schlüsselwort enthalten (wie „kinderseite.de“, „kinderspielplatz.net“), zutreffen.

3. Klicken Sie **Next**, wenn Sie Ihre Einstellungen vorgenommen haben. Es erscheint Bild 4-50.

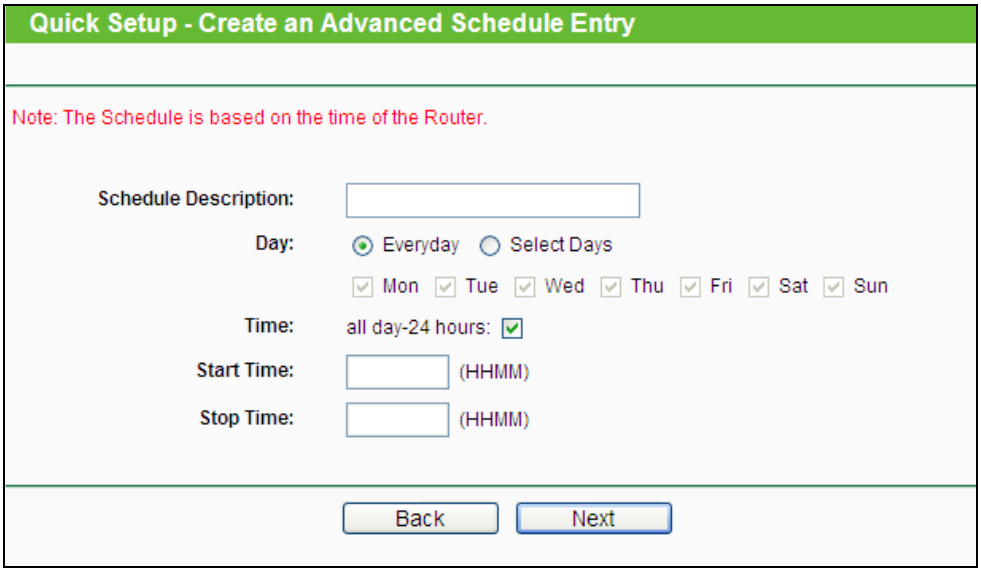


Bild 5-50 Regelassistent – Anlegen eines erweiterten Planungseintrags

- **Schedule Description** - Hier können Sie eine Beschreibung für die anzulegende Planung vergeben. Diese sollte eindeutig sein.
- **Day** - Wählen Sie den/die Wochentag(e) oder **Everyday** (täglich) aus.
- **Time** - Wählen Sie **24 hours** (ständig) oder geben Sie Start- und Endzeit an.
- **Start Time** - Die Uhrzeit, ab der die Regel gelten soll (Format: HHMM. Beispiel: „0800“ bedeutet 8 Uhr morgens).
- **Stop Time** - Die Uhrzeit, bis zu der die Regel gelten soll (Format: HHMM. Beispiel: „2100“ bedeutet 9 Uhr abends).

4. Klicken Sie **Next**. Es erscheint Bild 4-51.

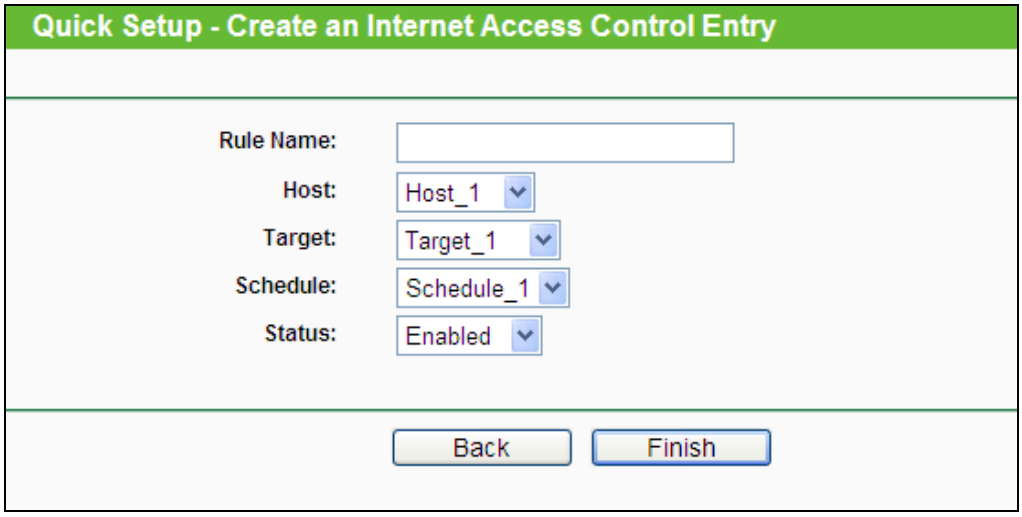


Bild 5-51 Regelassistent - Internetzugriffskontrollregel anlegen

- **Rule** - Denken Sie sich einen eindeutigen Regelnamen aus und tragen Sie ihn hier ein.
- **Host** - Hier wählen Sie einen zuvor definierten Host aus, auf den die Regel zutreffen soll. Sie sehen in der Liste die zuvor gesetzte **Host Description**.
- **Target** - Hier wählen Sie ein zuvor definiertes Ziel aus, auf das die Regel zutreffen soll. Sie sehen in der Liste die zuvor gesetzte **Target Description**.
- **Schedule** - Hier wählen Sie eine zuvor definierte Planung aus, auf die die Regel zutreffen soll. Sie sehen in der Liste die zuvor gesetzte **Schedule Description**.
- **Status** - Aktivieren (**Enable**) oder Deaktivieren (**Disable**) der Regel.

5. Klicken Sie **Finish**, um die neue Regel zu speichern.

Methode 2:

1. Klicken Sie **Add New…** Bild 5-52 erscheint.
2. Vergeben Sie unter **Rule Name** einen Namen für die Regel (z.B. „adult_verbieten“).
3. Wählen Sie einen Host aus der Liste **Host** aus oder wählen Sie **Click Here To Add New Host List**.
4. Suchen Sie ein Ziel aus der Liste **Target** aus oder wählen Sie **Click Here To Add New Target List**.
5. Entscheiden Sie sich für eine Planung aus der Liste **Schedule** oder wählen Sie **Click Here To Add New Schedule**.
6. Im Feld **Status** wählen Sie zwischen **Enabled** (aktiviert) und **Disabled** (deaktiviert).
7. Klicken Sie **Save**.

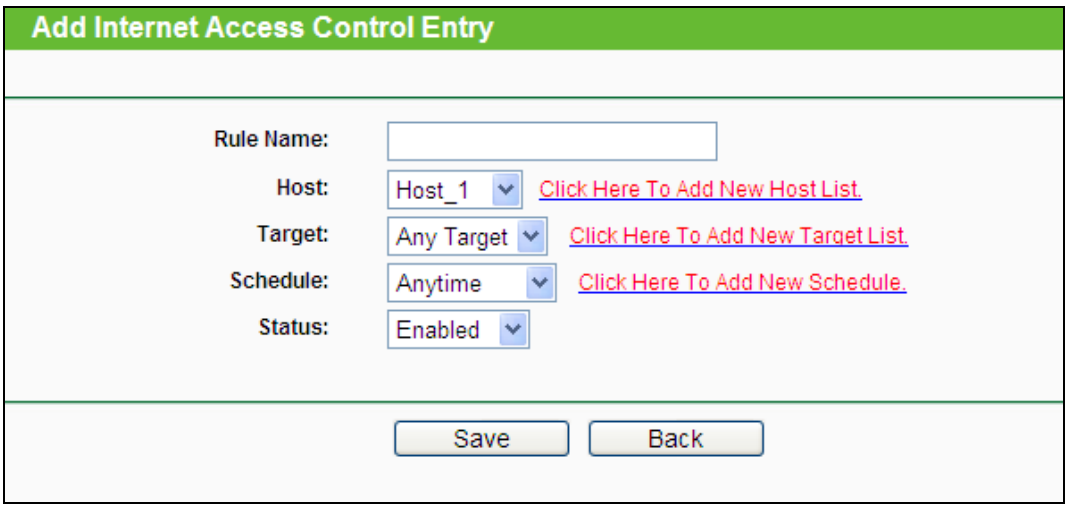


Bild 5-52 Internetzugangskontrolleintrag anlegen

Beispiel: Soll der Host mit der MAC-Adresse 00-11-22-33-44-AA nur **www.google.com** und diese Adresse auch nur **samstags und sonntags von 18 bis 20 Uhr** erreichen können, müssen folgende Einstellungen getätigt werden:

1. Gehen Sie in das Untermenü **Rule of Access Control** und aktivieren Sie die Internetzugriffskontrolle (**Enable Internet Access Control**). Wählen Sie **Allow the packets specified by any enabled access control policy to pass through the Router**.
2. Es ist empfohlen, den **Setup Wizard** zu verwenden, um die folgenden Einstellungen zu tätigen.
3. Öffnen Sie das Untermenü **Host of Access Control**. Legen Sie einen neuen Host an und vergeben Sie eine Beschreibung. Die **MAC-Adresse** ist mit 00-11-22-33-44-AA anzugeben.
4. Öffnen Sie das Untermenü **Target of Access Control**. Legen Sie ein neues Ziel (Domänenname) an und geben Sie ihm eine Beschreibung (z.B. Google). Der **Domänenname** ist www.google.com.
5. Öffnen Sie das Untermenü **Schedule of Access Control**. Legen Sie eine Planung mit einem eindeutigen Bezeichner (z.B. „SaSo1820“) an und wählen Sie die Wochentage Samstag und Sonntag aus. Startzeit ist 1800 und Endzeit 2000.
6. Öffnen Sie das Untermenü **Rule of Access Control**. Klicken Sie **Add New...** und legen Sie eine Regel mit den folgenden Parametern an:
   - Als **Rule Name** vergeben Sie einen eindeutigen Namen, z.B. **SaSo1820Google**.
   - Als **Host** wählen Sie den oben definierten Host aus.
   - Als **Target** wählen Sie **Google**.
   - Im Feld **Schedule** wählen Sie **SaSo1820** aus.
   - Der Status ist **Enable**.
   - Klicken Sie **Save**, um Ihre neuen Einstellungen zu speichern.

Sie landen nun auf der Seite der Zugriffskontrollregelverwaltung und sehen dies.

5.11.2 Host

Im Menü **Access Control** → **Host** können Sie eine Liste der zu kontrollierenden Hosts verwalten (Bild 5-53). Diese wird für die Zugriffskontrolle benötigt.

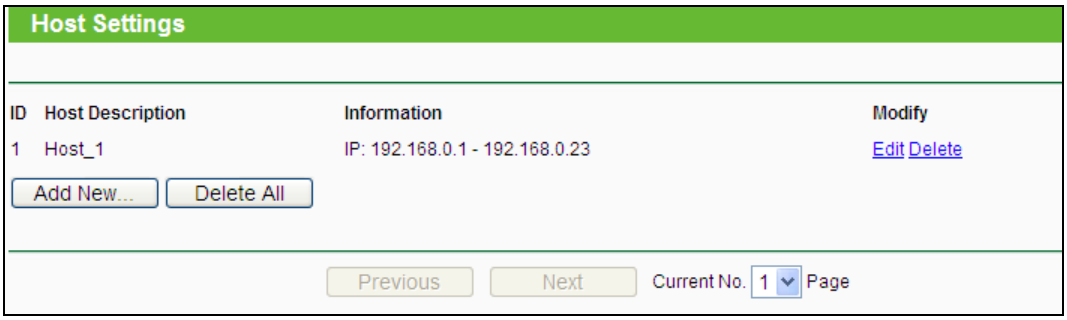


Bild 5-53 Host Settings

➢ **Host Description -** Eine eindeutige Beschreibung des Hosts.

- **Information -** Informationen über diesen Host: IP- oder MAC-Adresse.
- **Modify -** Bearbeiten oder Löschen eines bestehenden Eintrags.

Um einen neuen Eintrag anzulegen, tun Sie bitte Folgendes**.**

1. Klicken Sie **Add New…**.
2. Als **Mode** wählen Sie **IP Address** oder **MAC Address**.
   - Haben Sie „IP-Adresse“ gewählt, erscheint Bild 5-54.
     1) Im Feld **Host Description** hinterlegen Sie eine eindeutige Beschreibung, z.B. „Meikes Computer“.
     2) Im Feld **LAN IP Address** geben Sie die IP-Adresse oder den IP-Adressbereich ein.
   - Haben Sie „MAC-Adresse“ gewählt, erscheint Bild 5-55.
     1) Im Feld **Host Description** hinterlegen Sie eine eindeutige Beschreibung, z.B. „Meikes Computer“).
     2) Im Feld **MAC Address** geben Sie die IP-Adresse ein.
3. Klicken Sie **Save**, um den Eintrag zu übernehmen.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

Klicken Sie **Previous**, um zur vorigen Seite zurückzukehren oder **Next**, um die nächste Seite anzusehen.

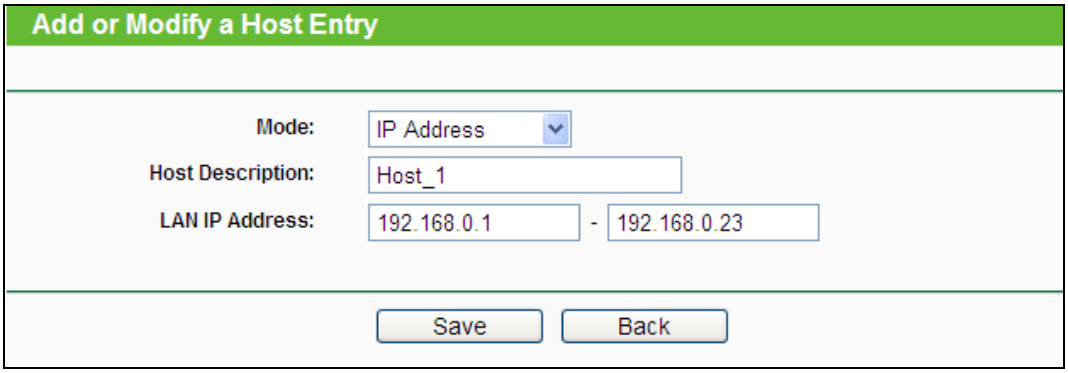


Bild 5-54 Hosteintrag anlegen oder bearbeiten

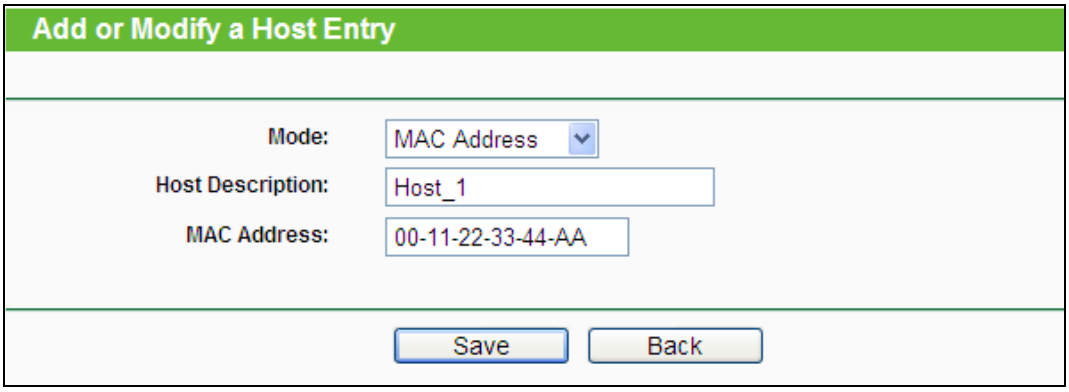


Bild 5-55 Hosteintrag anlegen oder bearbeiten

Beispiel: Möchten Sie die Internetaktivitäten des Hosts mit der MAC-Adresse 00-11-22-33-44-AA einschränken, sollten Sie so vorgehen:

1. Klicken Sie auf Bild 5-53 **Add New...**.
2. Als **Mode** geben Sie **MAC Address** an.
3. Als **Host Description** vergeben Sie eine eindeutige Hostbeschreibung (z.B. Jans PC).
4. In das Feld **MAC Address** geben Sie 00-11-22-33-44-AA ein.
5. Klicken Sie **Save**.

Sie werden dann auf die Hosteinstellungsseite zurückgebracht und sehen folgende Tabelle.

ID	Host Description	Information	Modify
1	Host_1	MAC: 00-11-22-33-44-AA	Edit Delete

5.11.3 Target

Gehen Sie zum Menü **Access Control** → **Target**. Hier können Sie eine Zielliste wie in Bild 5-56. zu sehen erstellen. Diese ist erforderlich für Zugriffskontrollregeln.

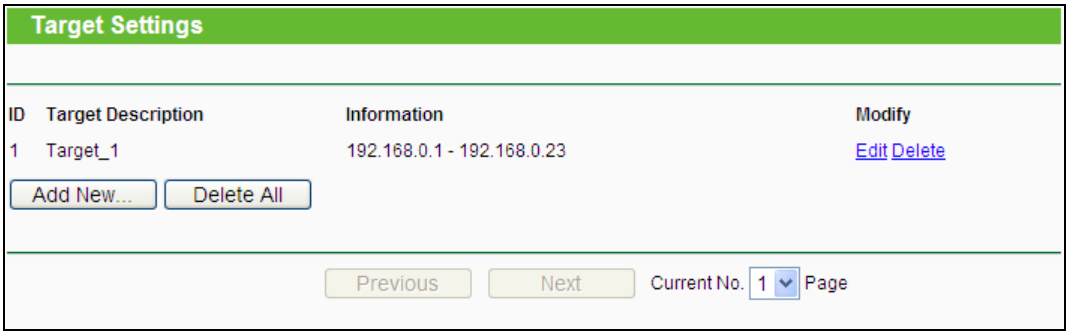


Bild 5-56 Target Settings

- **Target Description -** Hier steht eine eindeutige Beschreibung des Ziels.
- **Information -** Als Ziel können entweder IP-Adressen, Ports oder Domänennamen stehen.
- **Modify -** Um einen Eintrag zu bearbeiten/löschen, klicken Sie den entsprechenden Link.

Um einen neuen Eintrag anzulegen, gehen Sie bitte wie folgt vor:

- Klicken Sie **Add New…**.
- Als **Mode** wählen Sie **IP Address** oder **Domain Name** aus.
  - Haben Sie **Domain Name** gewählt, erscheint Bild 5-57.
    1) Im Feld **Target Description** erstellen Sie eine eindeutige Beschreibung des Ziels.
    2) Als **IP Address** geben Sie die Ziel-IP-Adresse an.
    3) Wählen Sie einen Dienst aus der Liste **Common Service Port** aus, damit der **Target Port** automatisch eingetragen wird. Ist Ihre Anwendung in der Liste nicht enthalten, geben Sie die Portnummer(n) von Hand in das Feld **Target Port** ein.
    4) Als **Protocol** wählen Sie nach Bedarf **TCP**, **UDP**, **ICMP** oder **All**.
  - Haben Sie **Domain Name** gewählt, erscheint Bild 5-58.
    1) Im Feld **Target Description** erstellen Sie eine eindeutige Beschreibung des Ziels.

2) Als **Domain Name** geben Sie entweder den vollen Domänennamen oder Schlüsselwörter (z.B. google) ein. Damit wird jeder Domänenname, der diese Schlüsselwörter enthält, betroffen sein, z.B. www.google.com, www.googleanalytics.com). Es können maximal vier Begriffe angegeben werden.

1) Klicken Sie **Save**.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

Klicken Sie **Next**, um auf die nächste Seite zu blättern oder **Previous**, um auf die vorige Seite zurückzukehren.

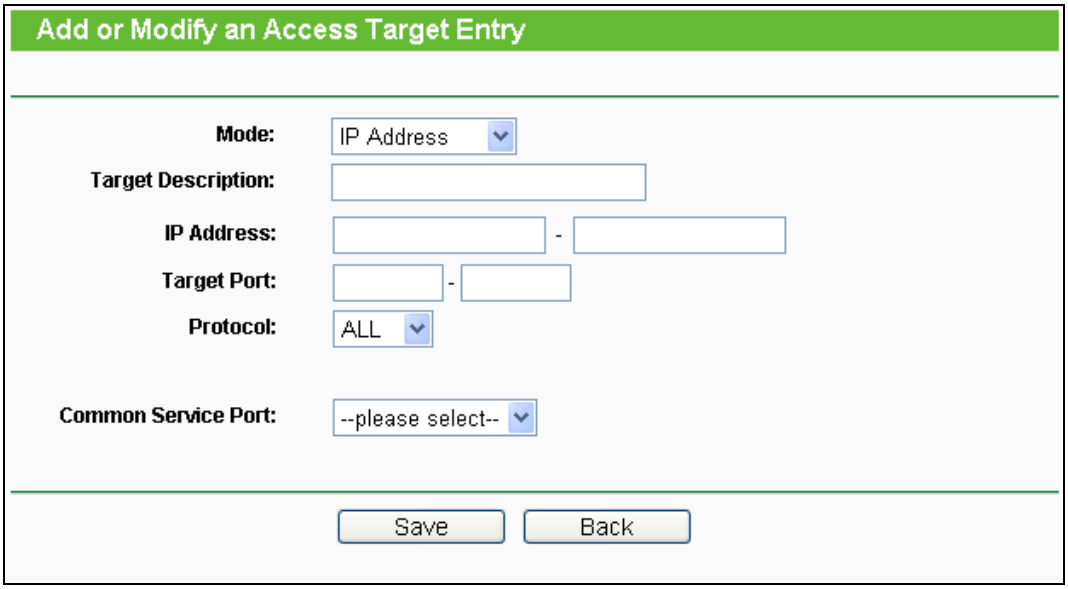


Bild 5-57 Zugriffszieleintrag anlegen oder bearbeiten

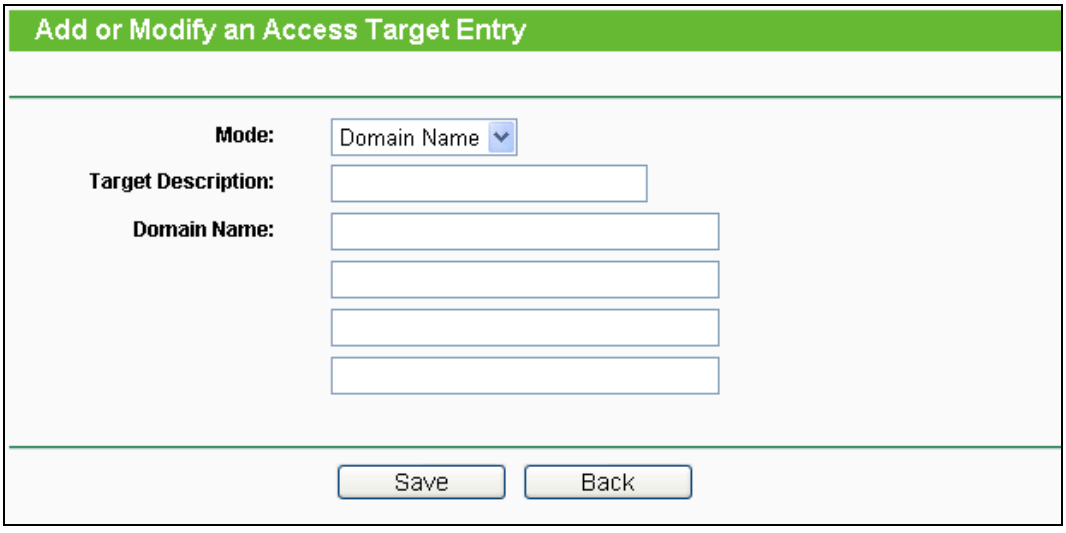


Bild 5-58 Zugriffszieleintrag anlegen oder bearbeiten

Beispiel: Möchten Sie die Internetaktivitäten des Hosts mit der MAC-Adresse 00-11-22-33-44-AA auf **www.google.com** beschränken, sollten Sie diesen Anweisungen Folge leisten:

1. Klicken Sie **Add New…** (Bild 5-56), um den entsprechenden Dialog zu öffnen.
2. Als **Mode** wählen Sie „Domänenname“ aus.

3. Im Feld **Target Description** setzen Sie eine eindeutige Beschreibung für das Ziel, z.B. „Google“.
4. In das Feld **Domain Name** geben Sie „www.google.com“ ein.
5. Klicken Sie **Save**, um die Einstellungen zu übernehmen.

Sie werden auf die Zieleinstellungsseite zurückgeleitet, wo Sie die folgende Liste sehen.

ID	Target Description	Information	Modify
1	Target_1	www.google.com	Edit Delete

5.11.4 Schedule

Gehen Sie in das Menü **Access Control** → **Schedule**. Hier können Sie eine Planungsliste anlegen (Bild 5-59). Diese Liste wird von den Zugriffskontrollregeln benötigt.

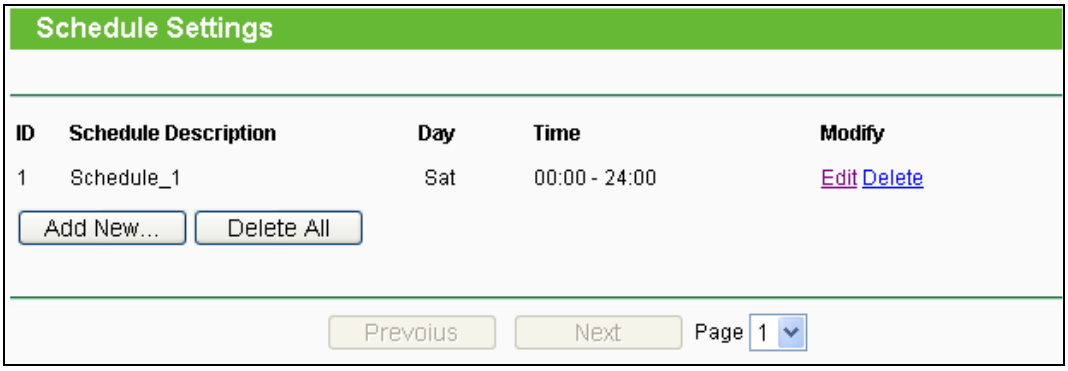


Bild 5-59 Planungseinstellungen

- **Schedule Description** - Die Beschreibung der Planung. Muss eindeutig sein.
- **Day** - Der Tag/die Tage, für den/die diese Planung zutrifft.
- **Time** - Der Zeitraum, zu dem diese Planung gilt.
- **Modify** - Hier können Sie Planungseinträge bearbeiten oder löschen.

Um eine neue Planung anzulegen, folgen Sie diesen Schritten**.**

1. Klicken Sie **Add New...** (Bild 5-59). Bild 5-60 erscheint.
2. Als **Schedule Description** geben Sie eine eindeutige Beschreibung (e.g. Planung_1).
3. Bei **Day** wählen Sie die Tage aus, die Sie wünschen.
4. Als **Time** können Sie den ganzen Tag auswählen (Option **all day-24 hours**) oder einen selbstgewählten Zeitabschnitt angeben.
5. Klicken Sie **Save**, um die Planungseinstellungen zu übernehmen.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

Klicken Sie **Next**, um auf die nächste Seite zu blättern oder **Previous**, um auf die vorige Seite zurückzukehren.

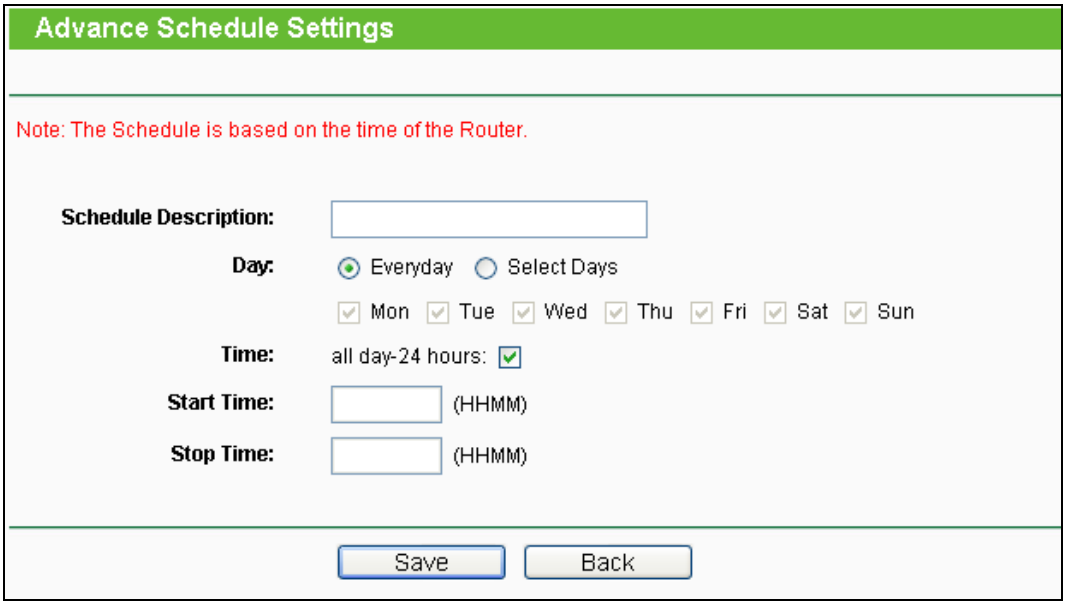


Bild 5-60 Erweiterte Planungseinstellungen

Beispiel: Sie möchten die Internetaktivitäten des Hosts mit der MAC-Adresse 00-11-22-33-44-AA auf www.google.com einschränken und dies auch nur samstags und sonntags von 18 bis 20 Uhr erlauben. Gehen Sie dazu wie folgt vor:

1. Klicken Sie **Add New...** (Bild 5-59), um auf die Seite **Advanced Schedule Settings** zu kommen.
2. In das Feld **Schedule Description** setzen Sie eine eindeutige Beschreibung, z.B. Schedule_1.
3. Unter **Day** wählen Sie „Sat“ und „Sun“ aus.
4. Aus **Start Time** geben Sie „1800“ und als **Stop Time** „2000“ ein.
5. Klicken Sie **Save**.

Sie kommen zurück auf die Planungseinstellungsseite und sehen diese Übersicht.

ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Sat Sun	18:00 - 20:00	Edit Delete

5.12 Advanced Routing

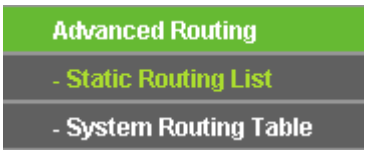


Bild 5-61 Advanced Routing

Im Menü **Advanced Routing** können Sie, wie in Bild 5-61 erkennbar, erweiterte Routingfunktionen konfigurieren.

5.12.1 Static Routing List

Im Menü **Advanced Routing** → **Static Routing List** können Sie statische Routen definieren (siehe Bild 5-62). Eine Statische Route ist ein vorbestimmter Pfad, den ein Paket gehen muss, um einen bestimmten Host oder ein bestimmtes Netz zu erreichen.

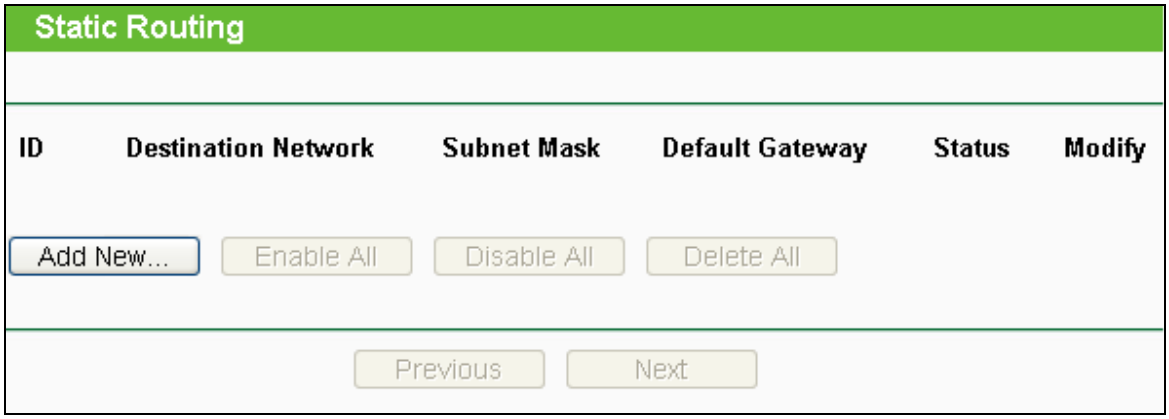


Bild 5-62 Static Routing

Um Einträge für das Statische Routing zu erstellen:

1. Klicken Sie **Add New…** (Bild 5-63). Sie sehen Folgendes:

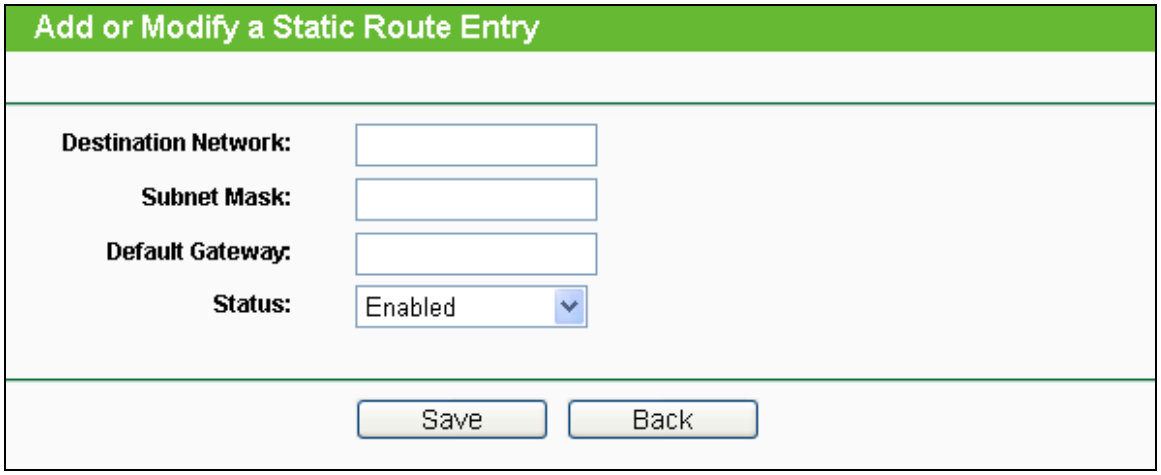


Bild 5-63 Hinzufügen/Ändern einer Statischen Route

2. Geben Sie Folgendes ein:

   - **Destination Network** - Die Adresse des Zielnetzes/-hosts der statischen Route.
   - **Subnet Mask -** Die Subnetzmaske bestimmt, welcher Teil der IP-Adresse das Netz und welcher den Host bezeichnet.
   - **Default Gateway** - Die IP-Adresse des Gateways, der den Netzübergang zwischen dem Router und dem Zielnetz/-host darstellt.

3. Wählen Sie wunschgemäß **Enabled** (Aktiviert) or **Disabled** (Deaktiviert) als **Status** für diesen Eintrag aus.

4. Klicken Sie **Save**.

Weitere Optionen:

Klicken Sie **Delete**, um diesen Eintrag zu löschen.

Klicken Sie **Enable All**, um alle Einträge zu aktivieren.

Klicken Sie **Disable All**, um alle Einträge zu deaktivieren.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

Klicken Sie **Next**, um auf die nächste Seite zu blättern oder **Previous**, um auf die vorige Seite zurückzukehren.

5.12.2 System Routing Table

Über das Menü **Advanced Routing** → **System Routing Table** sehen Sie das im Bild 5-64 gezeigte. Die Tabelle zeigt die aktuell verwendeten Statischen Routen mit **Destination Network** (Zielnetz), **Subnet Mask** (Subnetzmaske), **Gateway** und **Interface** (Schnittstelle).

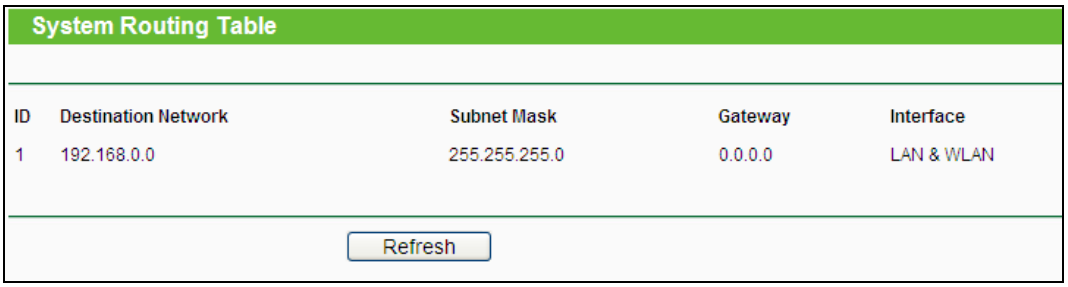


Bild 5-64 System Routing Table

- **Destination Network** - Die Adresse des Netzes, das das Ziel der Statischen Route darstellt.
- **Subnet Mask** - Die Subnetzmaske bestimmt, welcher Teil der IP-Adresse das Netz und welcher den Host definiert.
- **Gateway** - Die IP-Adresse des Gateways, der den Weg zum Ziel zur Verfügung stellt.
- **Interface** - Zeigt an, ob das Ziel über die **WAN**(Internet)- oder die lokale Seite (**LAN & WLAN**) erreichbar ist.

5.13 Bandwidth Control

Bild 5-65 Bandwidth Control

Das Menü **Bandwidth Control** erlaubt die Konfiguration der Upload- und der Download-Datenrate (Bild 5-65).

5.13.1 Control Settings

Das Menü **Bandwidth Control → Control Settings** ermöglicht die Konfiguration der Upload- und der Download-Datenrate. Zugelassen sind Werte von bis zu 100000kbps. Zur optimalen Kontrolle der Bandbreite wählen Sie bitte den richtigen Leitungstyp aus und fragen Sie bei Ihrem ISP bezüglich der jeweiligen Maximalbandbreite nach.

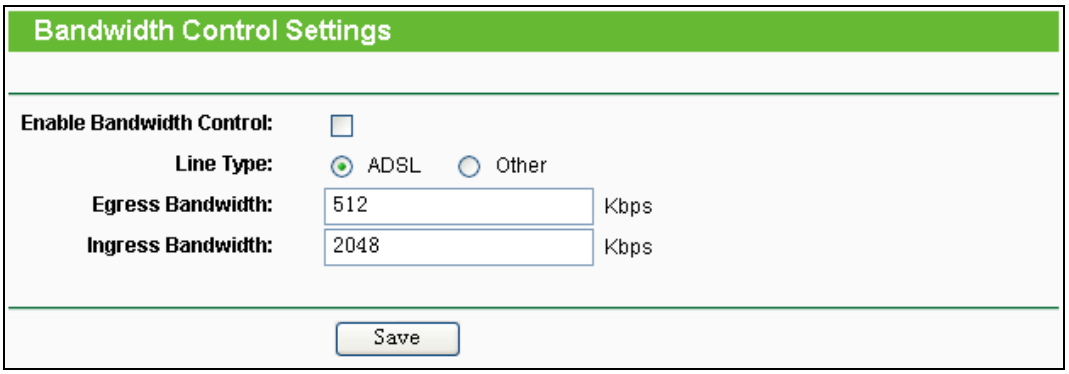


Bild 5-66 Bandwidth Control Settings

- **Enable Bandwidth Control -** Funktion aktivieren oder deaktivieren.
- **Line Type -** Wählen Sie hier Ihre Zugangsart aus. Sind Sie diesbezüglich unsicher, fragen Sie bitte bei Ihrem Internetdiensteanbieter nach.
- **Egress Bandwidth -** Uploadgeschwindigkeit des WAN-Ports.
- **Ingress Bandwidth -** Downloadgeschwindigkeit des WAN-Ports.

5.13.2 Rules List

Im Menü **Bandwidth Control → Rules List** können Sie die QoS-Regeln ansehen und bearbeiten (siehe folgende Abbildung).

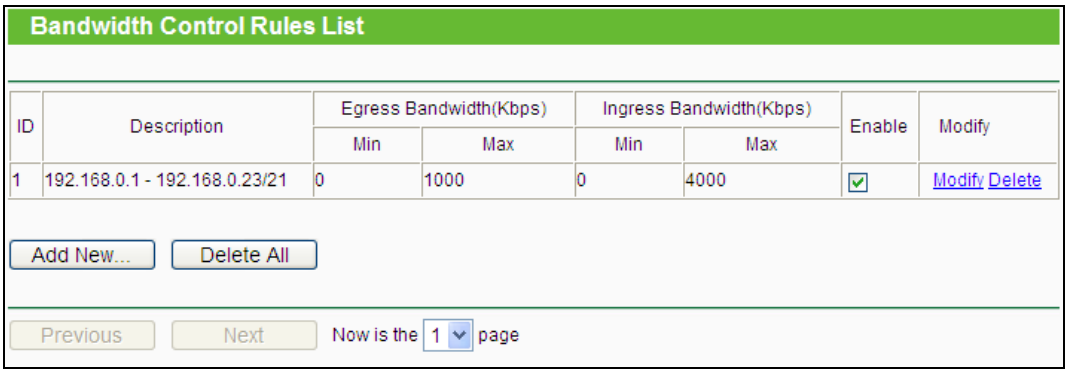


Bild 5-67 Bandwidth Control Rules List

- **Description -** Eine einfache Regelbeschreibung, z,B. der Adressbereich.
- **Egress bandwidth -** Maximale und minimale Uploadgeschwindigkeit am WAN-Port. Standard ist 0.
- **Ingress bandwidth -** Maximale und minimale Downloadgeschwindigkeit am WAN-Port. Standard ist 0.
- **Enable -** Zeigt an, ob die Regel aktiv ist.

➢ **Modify -** Klicken Sie **Modify** zum Bearbeiten der Regel oder **Delete**, um sie zu löschen.

Um eine Bandbreitenkontrollregel anzulegen, tun Sie dies.

1. Klicken Sie **Add New…** (Bild 5-67). Sie sehen Bild 5-68.
2. Geben Sie die im Folgenden gezeigten Informationen ein.

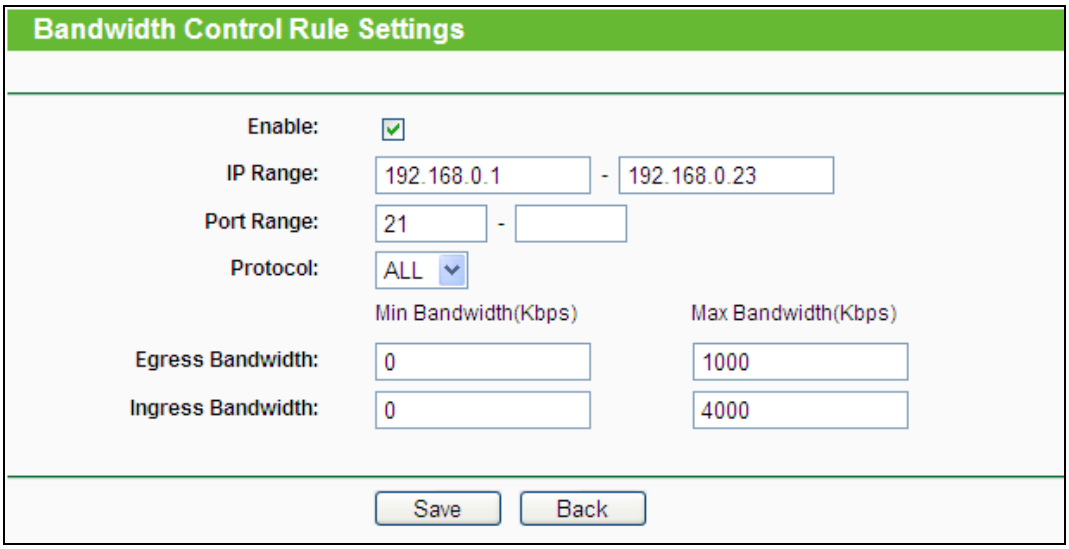


Bild 5-68 Bandwidth Control Rule Settings

3. Klicken Sie **Save**.

5.14 IP & MAC Binding Setting

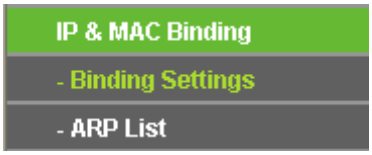


Bild 5-69 Bindungsmenü

Unter dem Bindungsmenü gibt es zwei Untermenüs (Bild 5-69): **Binding Settings** und **ARP List**.

5.14.1 Binding Settings

Diese Seite zeigt Ihnen die IP- und MAC-Adressbindungstabelle (Bild 5-70).

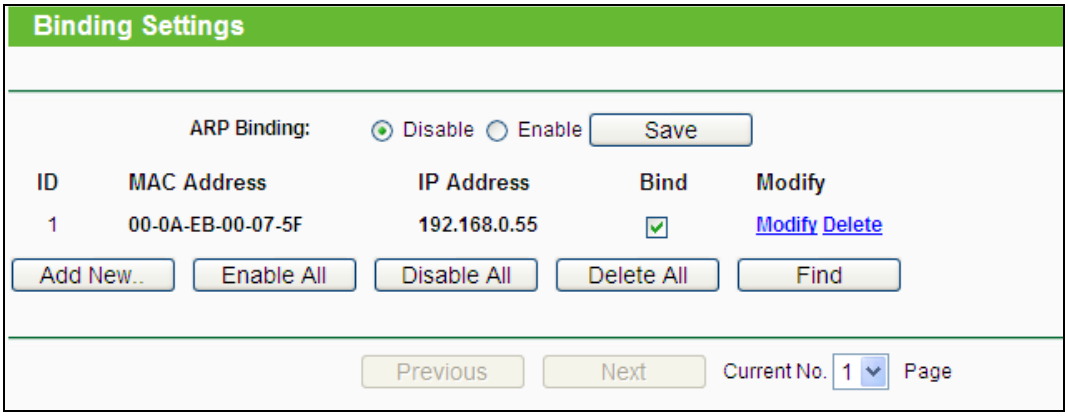


Bild 5-70 Binding Setting

- **MAC Address -** Die MAC-Adresse des kontrollierten LAN-Computers.
- **IP Address -** Die IP-Adresse des kontrollierten LAN-Computers.
- **Bind -** Wählen Sie dies an, um die ARP-Bindung für dieses Gerät zu aktivieren.
- **Modify -** Bearbeiten oder Löschen eines Eintrags.

Möchten Sie einen IP-/MAC-Adressbindungseintrag hinzufügen oder bearbeiten, können Sie **Add New…** oder **Modify** klicken. Sie werden dann auf die nächste Seite weitergeleitet (Bild 5-71).

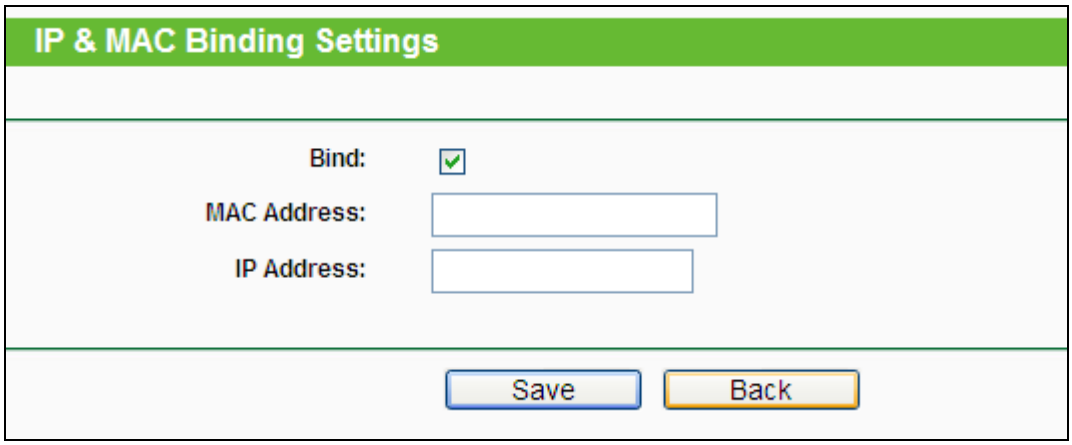


Bild 5-71 IP-/MAC-Adressbindungseinstellungen hinzufügen/bearbeiten

So fügen Sie Einträge zur IP-/MAC-Adressbindung hinzu:

1. Klicken Sie **Add New...** (Bild 5-70).
2. Geben Sie MAC- und IP-Adresse ein.
3. Wählen Sie **Bind** an.
4. Klicken Sie **Save**.

Um einen bestehenden Eintrag zu bearbeiten oder löschen, klicken Sie einfach in der entsprechenden Zeile auf **Modify** oder **Delete** in der Spalte **Modify**.

Um eine Suche nach einem Eintrag durchzuführen.

1. Klicken Sie **Find** (Bild 5-70).
2. Geben Sie die MAC-Adresse oder die IP-Adresse ein.
3. Klicken Sie **Find**, wie in Bild 5-72 gezeigt.

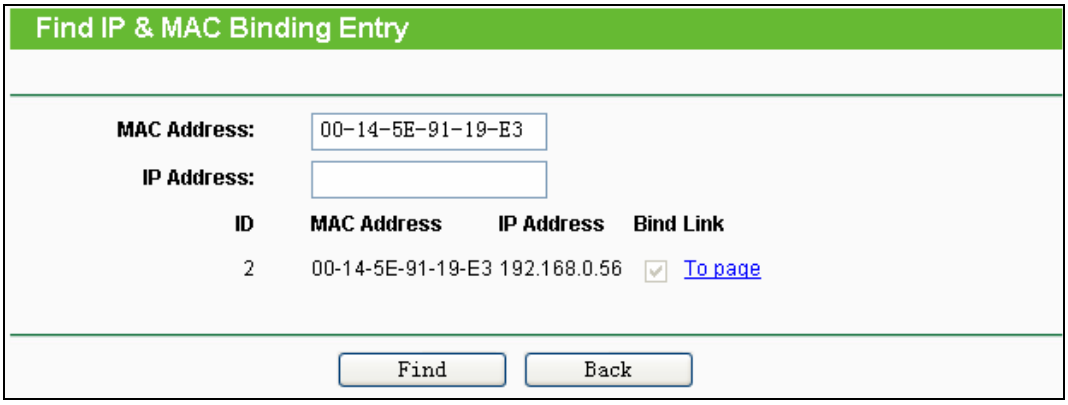


Bild 5-72 Find IP & MAC Binding Entry

Klicken Sie **Enable All**, um alle Einträge zu aktivieren.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

5.14.2 ARP List

Zur Computerverwaltung können Sie die Zusammenhänge zwischen MAC- und IP-Adresse auf der ARP-Liste überwachen und die Einträge in der ARP-Liste bearbeiten. Diese Seite zeigt die ARP-Liste mit allen existierenden IP- und MAC-Adressbindungseinträgen (Bild 5-73).

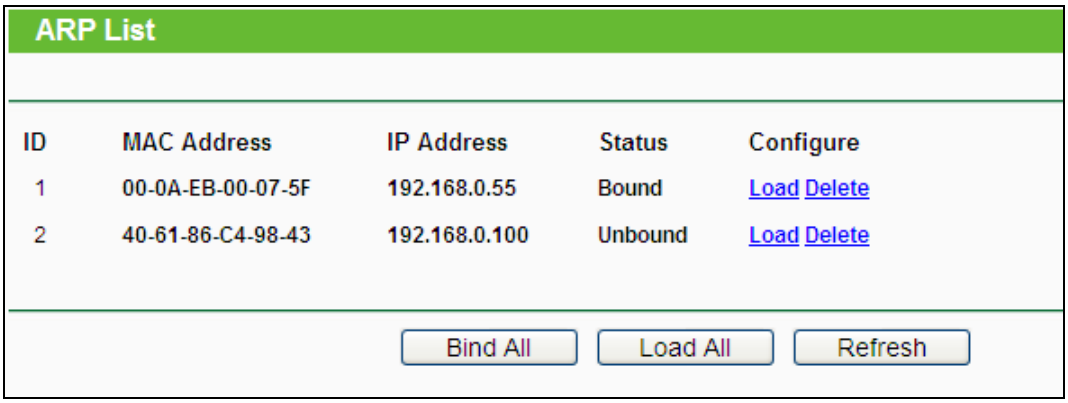


Bild 5-73 ARP List

1. **MAC Address -** Die MAC-Adresse des kontrollierten LAN-Computers.
2. **IP Address -** Die zugewiesene IP-Adresse des kontrollierten LAN-Computers.
3. **Status -** Status der Bindung: **Bound** (Gebunden) oder **Unbound** (Ungebunden).
4. **Configure -** Eintrag laden (**Load**) oder löschen (**Delete**).
   - **Load -** Element in die IP-/MAC-Adressbindungsliste aufnehmen.
   - **Delete -** Element aus der Liste entfernen.

Klicken Sie **Bind All**, um alle aktuellen Einträge zu binden. Diese Funktion ist nur für aktive Einträge verfügbar.

Klicken Sie **Load All**, um alle Einträge in die Bindungsliste zu laden.

Klicken Sie **Refresh**, um die Ansicht zu aktualisieren.

Bemerkung:

Ein Eintrag könnte unter Umständen nicht in die Bindungsliste geladen werden, wenn dessen IP-Adresse schon geladen ist. In diesem Fall informiert Sie eine Warnung. Entsprechend lädt **Load All** nur die konfliktfreien Elemente in die Bindungsliste.

5.15 Dynamic DNS

Im Menü **Dynamic DNS** können Sie die Funktionalität des Dynamischen DNS einstellen.

Der Router verfügt über die DDNS(Dynamic Domain Name System)-Funktionalität. Mit DDNS können Sie Ihrer dynamisch zugeteilten Internet-IP-Adresse einen festen Host-/Domänennamen zuordnen. Dies ist sehr nützlich, wenn Sie Ihre Website selbst hosten oder Serverdienste wie z.B. FTP hinter dem Router laufen lassen wollen. Bevor Sie diese Funktionalität nutzen können, müssen Sie sich bei einem DDNS-Dienst wie z.B. dyndns.org, no-ip.com oder comexe.cn anmelden. Der Anbieter gibt Ihnen dann ein Passwort oder einen Schlüssel.

5.15.1 Comexe.cn

Haben Sie als DDNS-Anbieter comexe.cn gewählt, erscheint folgende Seite Bild 5-74.

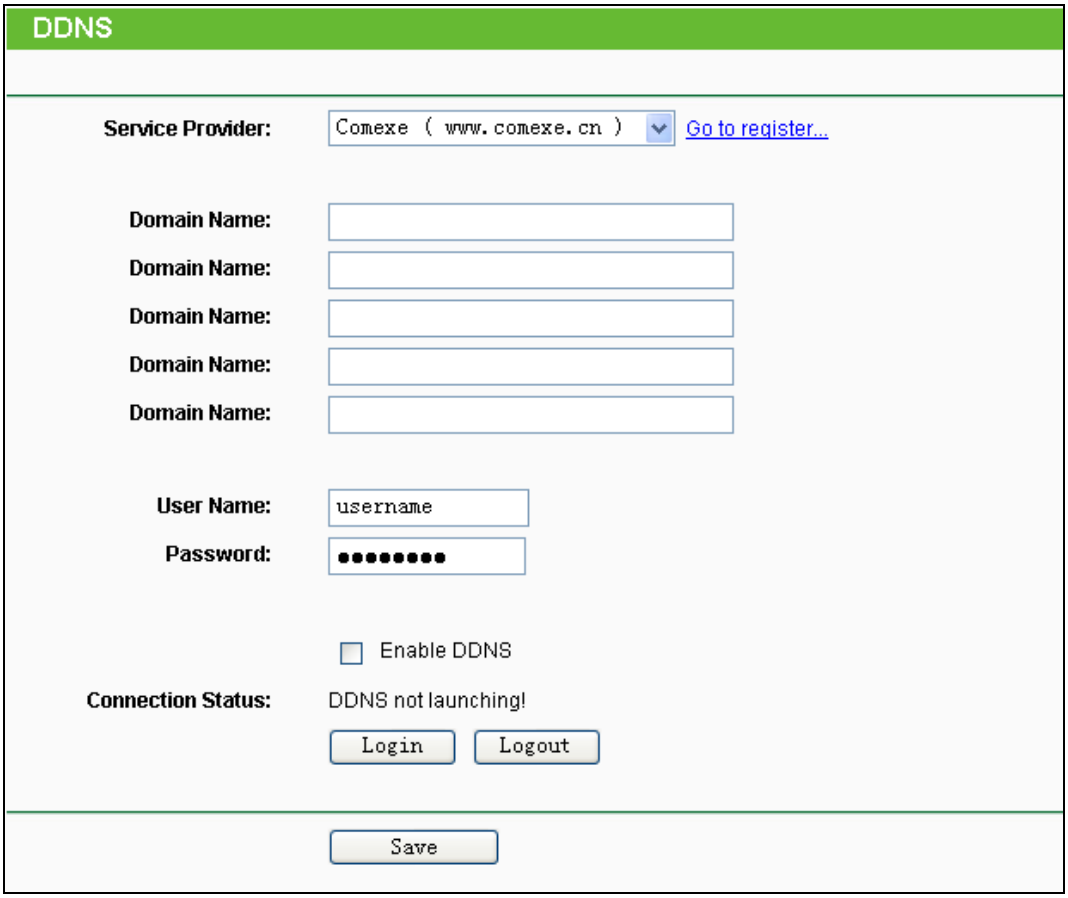


Bild 5-74 DDNS mit Comexe.cn

Um DDNS einzurichten, tun Sie Folgendes:

1. Geben Sie den Domänennamen unter **Domain Name** an.
2. Geben Sie unter **User Name** den Benutzernamen Ihres DDNS-Accounts ein.
3. Geben Sie unter **Password** das Passwort Ihres DDNS-Accounts ein.
4. Klicken Sie **Login**, um sich in den DDNS-Dienst einzuloggen.

Klicken Sie **Logout**, um sich aus dem DDNS-Dienst auszuloggen.

☞ **Bemerkung:**

Möchten Sie vom Router irgendwann einen anderen dynamischen Host aktualisieren lassen, müssen Sie sich zunächst **Logout**, bevor Sie Ihren neuen Benutzernamen und Ihr neues Passwort eingeben und sich danach **Login**.

5.15.2 DynDNS

Haben Sie als DDNS-Anbieter dyndns.org ausgewählt, erscheint folgende Seite (Bild 5-75).

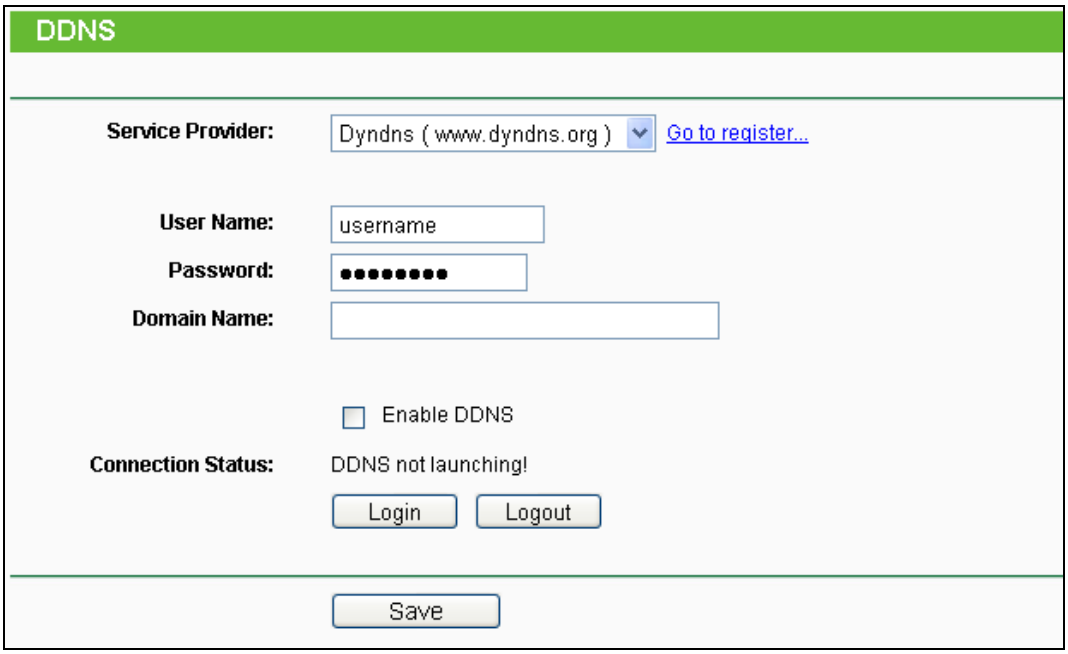


Bild 5-75 DDNS mit DynDNS

Um DDNS einzurichten, tun Sie Folgendes:

1. Geben Sie unter **User Name** den Benutzernamen Ihres DDNS-Accounts ein.
2. Geben Sie unter **Password** das Passwort Ihres DDNS-Accounts ein.
3. Geben Sie den Domänennamen unter **Domain Name** ein.
4. Klicken Sie **Login**, um sich in den DDNS-Dienst einzuloggen.

Klicken Sie **Logout**, um sich aus dem DDNS-Dienst auszuloggen.

☞ **Bemerkung:**

Möchten Sie vom Router irgendwann einen anderen dynamischen Host aktualisieren lassen, müssen Sie sich zunächst **Logout**, bevor Sie Ihren neuen Benutzernamen und Ihr neues Passwort eingeben und sich danach **Login**.

5.15.3 No-IP

Haben Sie als DDNS-Anbieter no-ip.com ausgewählt, erscheint folgende Seite (Bild 5-76).

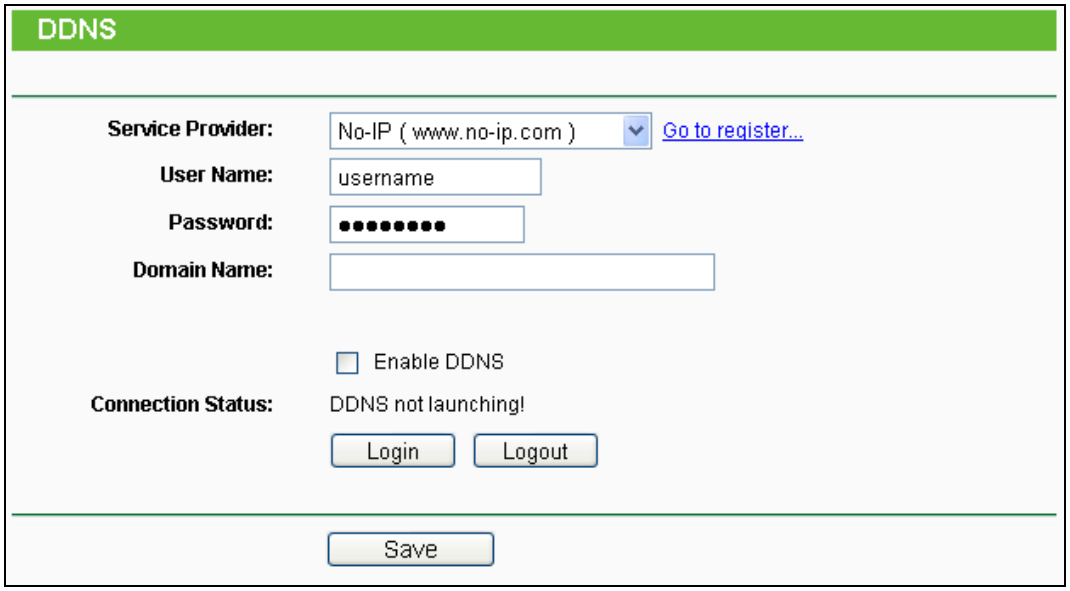


Bild 5-76 DDNS mit No-IP

Um DDNS einzurichten, tun Sie Folgendes:

1. Geben Sie unter **User Name** den Benutzernamen Ihres DDNS-Accounts ein.
2. Geben Sie unter **Password** das Passwort Ihres DDNS-Accounts ein.
3. Geben Sie den Domänennamen unter **Domain Name** ein.
4. Klicken Sie **Login**, um sich in den DDNS-Dienst einzuloggen.

Connection Status - Der Verbindungsstatus des DDNS-Dienstes.

Klicken Sie **Logout**, um sich aus dem DDNS-Dienst auszuloggen.

☞ **Bemerkung:**

Möchten Sie vom Router irgendwann einen anderen dynamischen Host aktualisieren lassen, müssen Sie sich zunächst **Logout**, bevor Sie Ihren neuen Benutzernamen und Ihr neues Passwort eingeben und sich danach **Login**.

5.16 System Tools

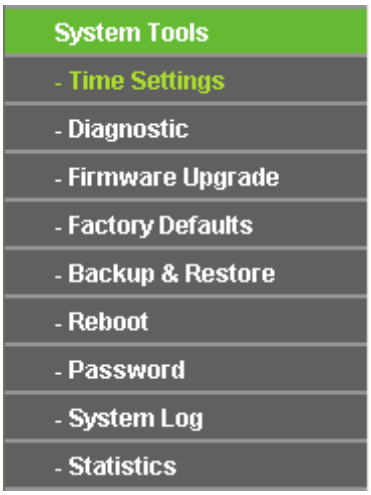


Bild 5-77 Das Menü **System Tools**

Im Menü **System Tools** gibt es folgende Untermenüs: **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults, Backup & Restore, Reboot, Password, System Log** und **Statistics**.

5.16.1 Time Setting

Im Menü **System Tools** → **Time Setting** können Sie die Echtzeituhr des Routers von Hand oder mittels der aus dem Internet abgefragten GMT einstellen.

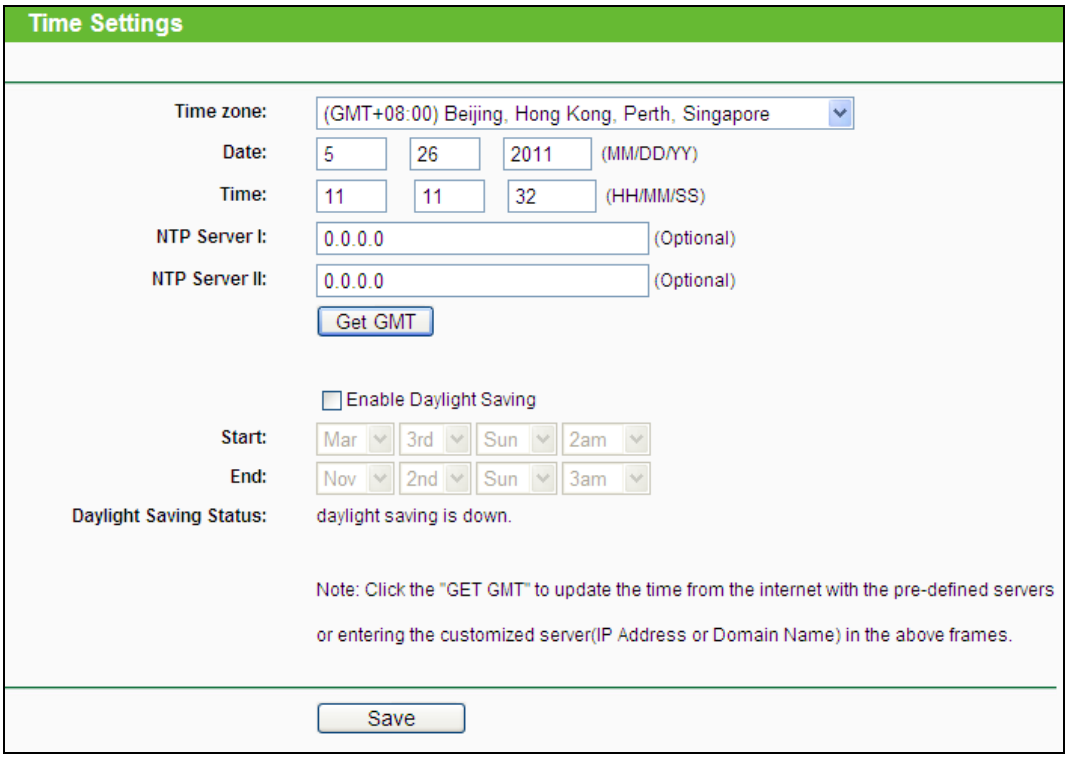


Bild 5-78 Time settings

- **Time Zone -** Wählen Sie hier die Zeitzone aus, in der der Router steht.
- **Date -** Geben Sie das aktuelle Datum im Format „MM/TT/JJJJ“ ein.
- **Time -** Geben Sie die aktuelle Uhrzeit im Format „hh/mm/ss“ ein.
- **NTP Server I, NTP Server II -** Geben Sie hier die Adresse(n) eines NTP-Servers oder zweier NTP-Server ein, wird der Router von diesem die Uhrzeit abfragen, sobald er eine Internetverbindung hergestellt hat. Zusätzlich zu diesen konfigurierbaren sind einige weitere NTP-Server in der Routersoftware hart kodiert, so dass er auch von diesen die Uhrzeit automatisch abfragen kann.
- **Enable Daylight Saving -** Hiermit beachtet der Router die weiter unten definierte Sommerzeitregelung.
- **Start -** Beginn der Sommerzeit. Wählen Sie nacheinander Monat, Woche, Tag und Stunde.
- **End -** Ende der Sommerzeit. Wählen Sie nacheinander Monat, Woche, Tag und Stunde.
- **Daylight Saving Status -** Zeigt an, ob die Sommerzeit gerade aktiv ist.

Die Zeit können Sie auch von Hand mit folgenden Schritten einstellen:

1. Wählen Sie die zutreffende Zeitzone aus.
2. Geben Sie das Datum (als **Date**) im Format „MM/TT/JJJJ“ und die aktuelle Uhrzeit (als **Time**) im Format „HH/MM/SS“ ein.
3. Klicken Sie **Save**.

Zur automatischen Zeiteinstellung konfigurieren Sie Ihren Router bitte so:

1. Wählen Sie die zutreffende Zeitzone aus.
2. Geben Sie unter **NTP Server I** oder **NTP Server II** eine oder zwei NTP-Server-Adressen ein.
3. Klicken Sie **Get GMT**, um die GMT bei bestehender Internetverbindung abzurufen.

Zur automatischen Umstellung zwischen Sommer- und Winterzeit tun Sie dies:

1. Aktivieren Sie Sommerzeit (**Enable Daylight Saving**).
2. Wählen Sie den **Start**- und den **End**zeitpunkt der Sommerzeit aus.
3. Klicken Sie **Save**.

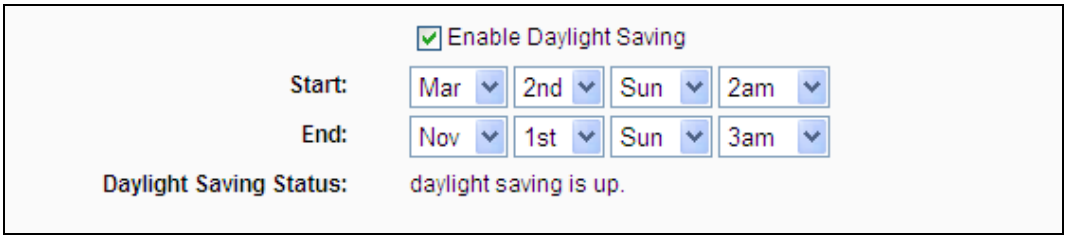


Bild 5-79 Sommerzeiteinstellungen

Bemerkungen:

1) Diese Einstellung beeinflusst einige zeitbasierende Funktionen wie z.B. die Firewall.

Hierfür müssen die Uhrzeit und die Zeitzone zwingend gesetzt werden.

2) Die Uhrzeit geht verloren, wenn die Spannungsversorgung getrennt wird.
3) Der Router setzt die Systemzeit automatisch, wenn er eine Internetverbindung bekommt und entsprechend konfiguriert ist.
4) Es dauert nach dem Speichern ca. eine Minute, bis die Sommerzeiteinstellung wirksam wird.

5.16.2 Diagnostic

Das Menü **System Tools** → **Diagnostic** erlaubt die Ausführung von Ping- und Traceroute-Befehlen zur Überprüfung der Konnektivität.

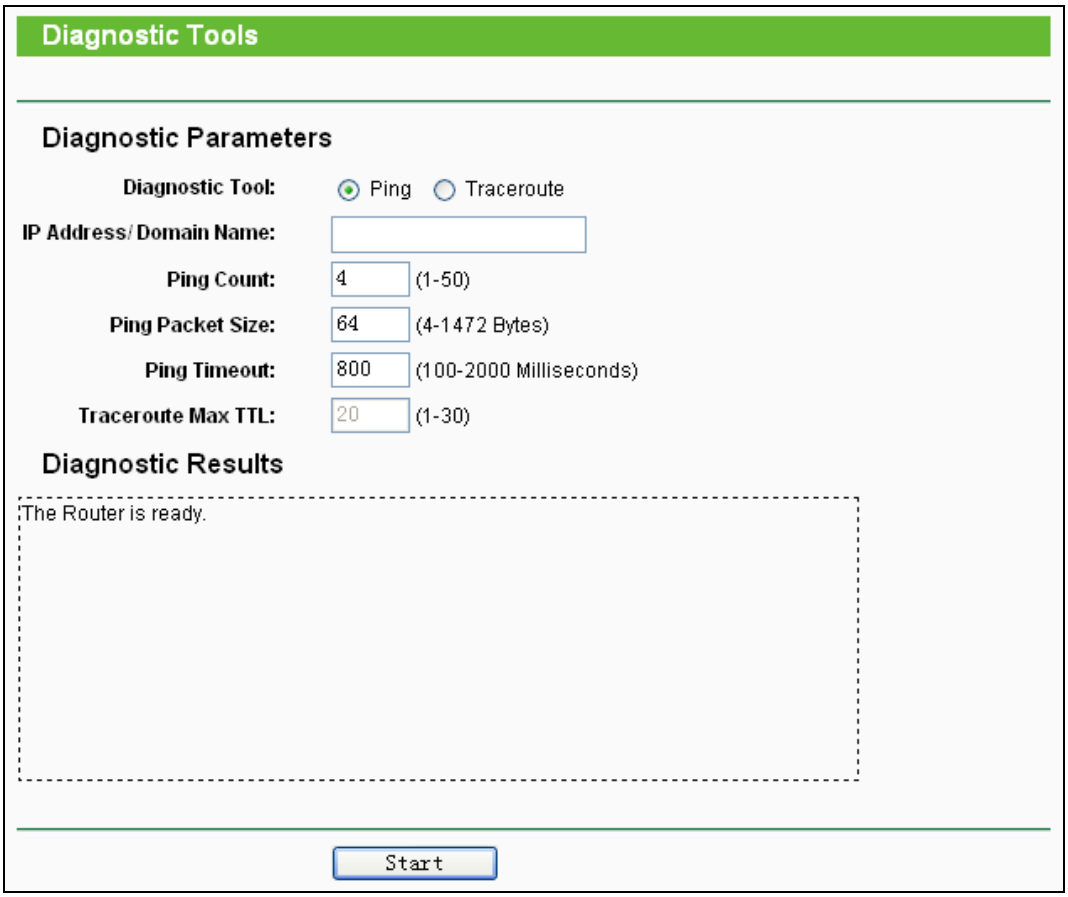


Bild 5-80 Diagnostic Tools

- **Diagnostic Tool** - Wählen Sie zwischen **Ping** und **Traceroute**.
- **Ping** - Hiermit können Sie die Konnektivität, die Erreichbarkeit und die Namensauflösung für einen gegebenen Host testen.
- **Traceroute** - Dieses Tool ist in der Lage, die Performance der verschiedenen Verbindungsabschnitte zu testen.

Bemerkung:

Ping und Traceroute akzeptieren sowohl IP-Adressen als auch Domänennamen. Können Sie eines der Tools für eine IP-Adresse erfolgreich laufen lassen, für einen Domänennamen aber nicht, deutet dies darauf hin, dass die Namensauflösung (DNS) nicht funktioniert.

- **IP Address/Domain Name** - Geben Sie das Ziel als IP-Adresse (z.B. 202.108.22.5) oder als Domänenname (z.B. www.tp-link.com) an.
- **Pings Count -** Die Anzahl der zu sendenden Ping-Pakete. Standard: 4.
- **Ping Packet Size -** Die Größe eines Pingpakets. Standard: 64.
- **Ping Timeout -** Setzen Sie hier die Wartezeit für ein Pingpaket. Kommt innerhalb dieser Zeit keine Antwort, gilt der Ping als fehlgeschlagen. Standard: 800.
- **Traceroute Max TTL -** Die maximale Knotenanzahl (Hops) für eine Traceroute-Verbindung. Standardwert: 20.

Klicken Sie **Start**, um die Konnektivität zu testen.

Der Abschnitt **Diagnostic Results** zeigt die Ergebnisse der Diagnose an. Bei einem Ergebnis ähnlich wie diesem ist die Internetkonnektivität gut.

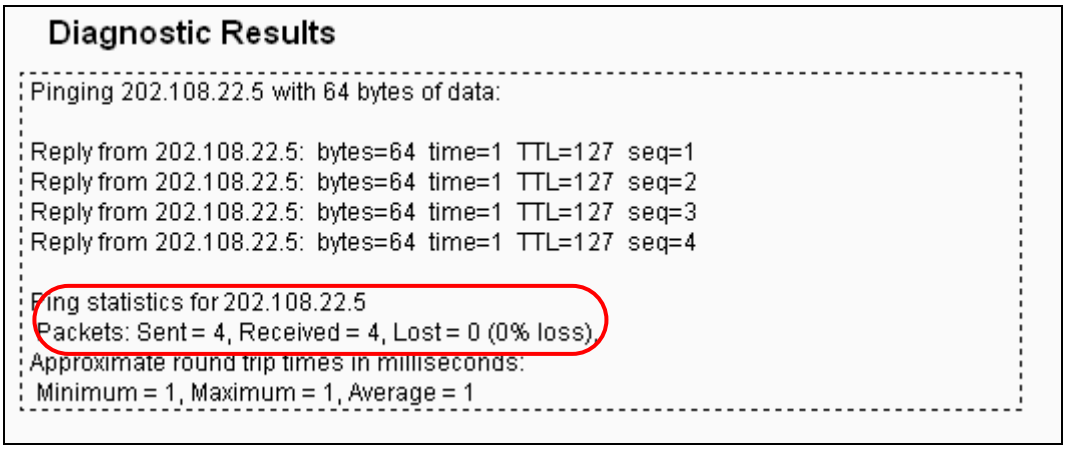


Bild 5-81 Diagnoseergebnisse

Bemerkung:

Diese Tools können nur von einem Computer aus zur gleichen Zeit gestartet werden. Die Optionen **Ping Count**, **Ping Packet Size** und **Ping Timeout** werden von der **Ping**-Funktion verwendet, während **Traceroute Max TTL** von der **Traceroute**-Funktion genutzt wird.

5.16.3 Firmware Upgrade

Diese Seite erlaubt Firmwareupgrades, um den Router aktuell zu halten.

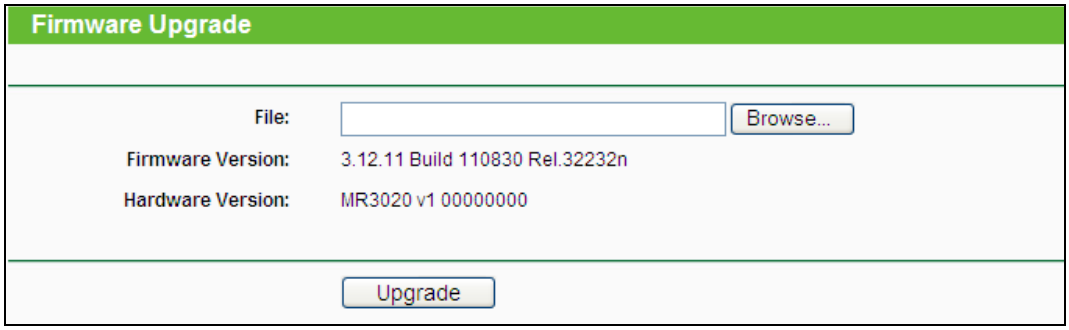


Bild 5-82 Firmware Upgrade

- **Firmware Version -** Zeigt Ihnen die aktuell installierte Firmwareversion.

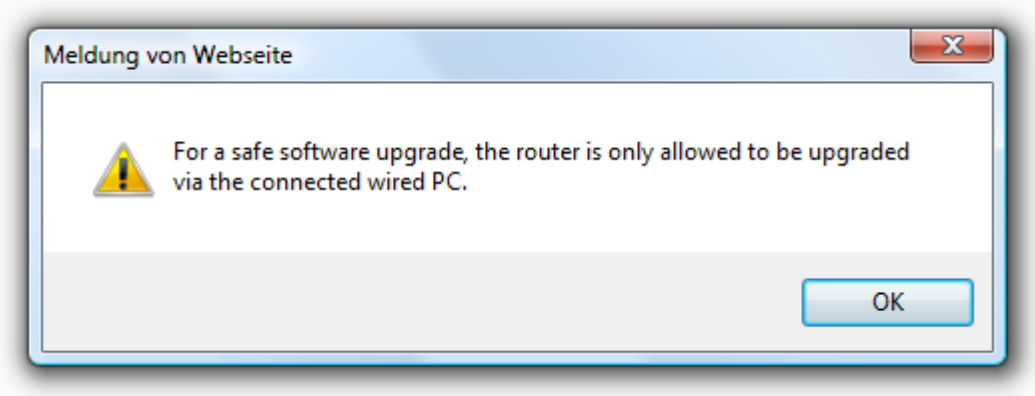
- **Hardware Version -** Zeigt Ihnen die aktuelle Hardwareversion. Diese muss unbedingt mit der Hardwareversion der Update-Datei übereinstimmen.

Um die Firmware zu aktualisieren, gehen Sie so vor:

1. Laden Sie sich eine Firmwaredatei für Ihr Modell von der TP-LINK-Webseite **www.tp-link.com** herunter und entpacken Sie sie.
2. Verbinden Sie sich mit dem Router über eine Kabelverbindung, nicht über WLAN. Klicken Sie im Webinterface **Durchsuchen**, um die heruntergeladene Datei auszuwählen.
3. Klicken Sie **Upgrade**.
4. Der Router verarbeitet die Datei und startet anschließend neu.

Hinweis:

1) Führen Sie das Upgrade nie über eine WLAN-Verbindung durch, sondern nur über Kabel. Beim Versuch eines Upgrades über WLAN erscheint diese Meldung.



2) Neue Firmware ist auf **www.tp-link.com** zu finden und kann kostenlos heruntergeladen werden. Haben Sie mit dem Router keine Probleme und bietet die neue Firmware keine unbedingt benötigten neuen Funktionalitäten, brauchen Sie die Firmware nicht zwingend zu aktualisieren.
3) Beim Firmwareupgrade kann Ihre aktuelle Konfiguration verloren gehen. Stellen Sie also sicher, dass Sie sie in einer Datei gespeichert haben, bevor Sie mit dem Upgrade beginnen.
4) Während des Firmwareupgrades darf der Router keinesfalls von der Versorgungsspannung getrennt oder mittels der Reset-Taste zurückgesetzt werden.
5) Beachten Sie die Hardwareversion der Firmwaredatei. Diese muss unbedingt mit der Hardwareversion des Routers identisch sein.
6) Nach erfolgreichem Upgrade (nach wenigen Minuten) startet der Router automatisch neu.

5.16.4 Factory Defaults

Die Seite **System Tools → Factory Defaults** ermöglicht das Wiederherstellen der Standardeinstellungen des Routers.

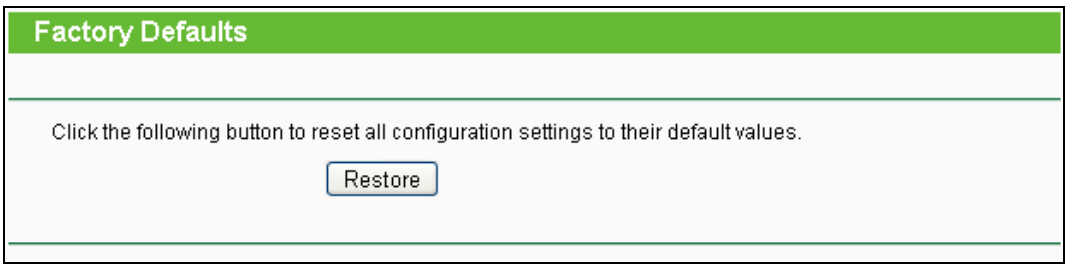


Bild 5-83 Standardeinstellungen wiederherstellen

Klicken Sie **Restore**, um alle Einstellungen zurückzusetzen. Danach gelten:

- Benutzername (**User Name**): admin
- Passwort (**Password**): admin
- Subnetzmaske (**Subnet Mask**): 255.255.255.0

Bemerkung:

Prinzipbedingt gehen bei diesem Vorgang alle im Router gespeicherten Einstellungen verloren.

5.16.5 Backup & Restore

Unter **System Tools** → **Backup & Restore** können Sie die Routerkonfiguration lokal speichern sowie eine zuvor gespeicherte Konfiguration wiederherstellen (Bild 5-84).

Bild 5-84 Backup & Restore der Routerkonfiguration

- Klicken Sie **Backup**, um die aktuelle Konfiguration herunterzuladen und lokal zu speichern.
- Um eine alte Konfiguration wiederherzustellen, tun Sie Folgendes.
  - Klicken Sie **Durchsuchen…**, um die Backup-Datei auszuwählen.
  - Klicken Sie **Restore**.

Bemerkung:

Beim Wiederherstellungsprozess geht die aktuell im Router befindliche Konfiguration verloren. Der Prozess dauert ca. 20 Sekunden. Anschließend startet der Router neu. Bitte lassen Sie den Router während der Wiederherstellung eingeschaltet, um Schäden zu vermeiden.

5.16.6 Reboot

Unter **System Tools** → **Reboot** können Sie durch Klick auf **Reboot** den Router neustarten.

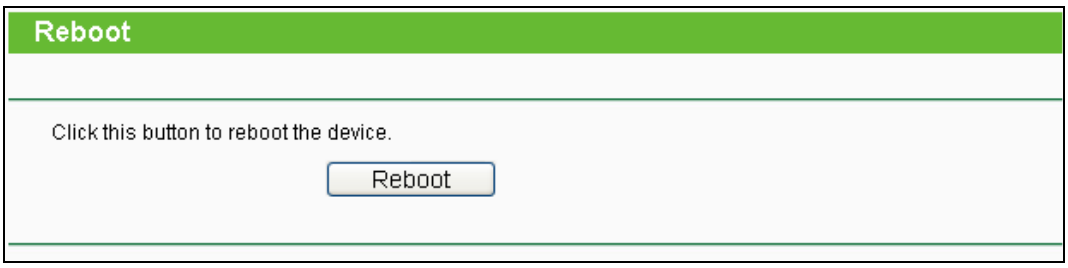


Bild 5-85 Reboot

Einige Einstellungen des Routers können nur durch einen Neustart übernommen werden:

- Ändern der LAN-IP-Adresse (der Router startet automatisch neu).
- DHCP-Konfigurationsänderungen.
- Änderungen an der Drahtloskonfiguration.
- Ändern des Ports für die Fernwartung.
- Firmwareupgrade (der Router startet automatisch neu).
- Zurücksetzen der Routereinstellungen (der Router startet automatisch neu).
- Wiederherstellen einer alten Konfiguration mittels Dateiupload (der Router startet automatisch neu).

5.16.7 Password

Auf **System Tools** → **Password** können Sie die Router-Zugangsdaten ändern (Bild 5-86).

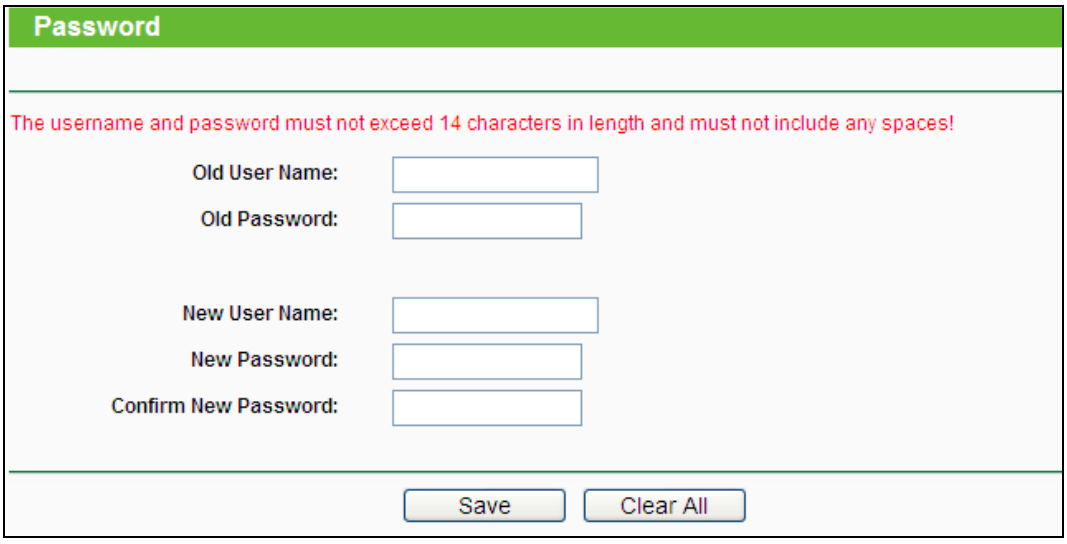


Bild 5-86 Password

Es wird empfohlen, die Zugangsdaten abzuändern. Diese werden von alle Benutzern abgefragt, die versuchen, auf das webbasierende Konfigurationstool zuzugreifen.

Bemerkung:

Benutzername und Passwort dürfen nicht länger als jeweils 14 Zeichen sein und keine Leerzeichen enthalten. Um Tippfehler auszuschließen, muss das Passwort zweimal

eingegeben werden.

Klicken Sie **Save**, wenn Sie die Daten eingegeben haben.

Klicken Sie **Clear All**, um die Feldinhalte zu löschen.

5.16.8 System Log

Über die Seite **System Tools** → **System Log** können Sie die Routerprotokolle abfragen.

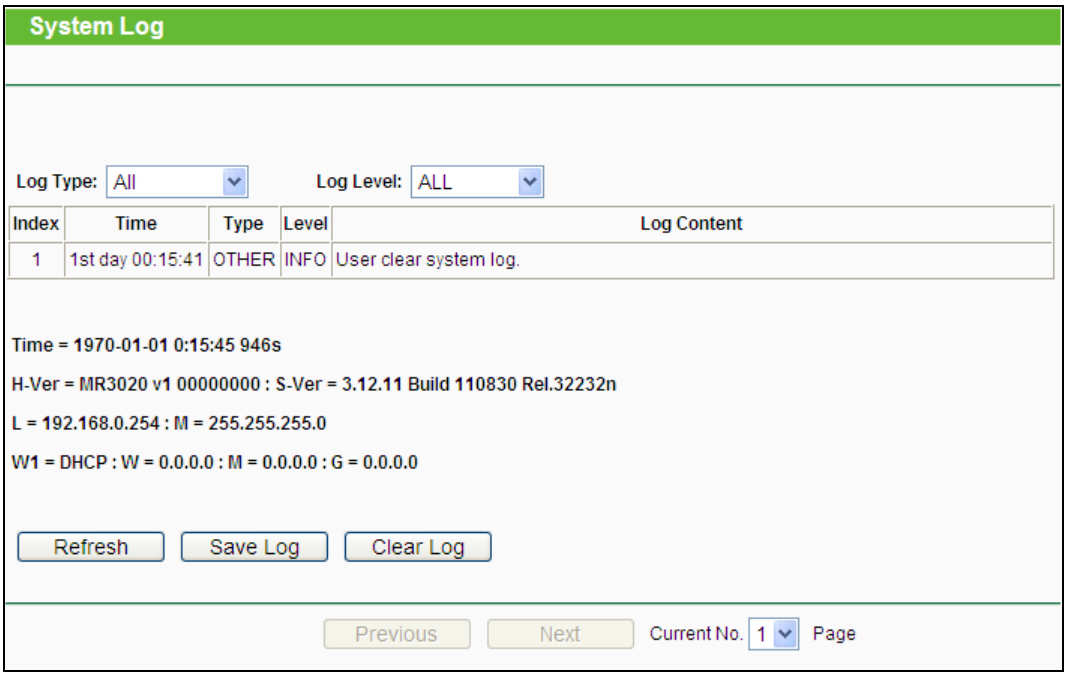


Bild 5-87 System Log

- **Log Type -** Filtern nach Protokolltyp (PPP, Wireless, …).
- **Log Level -** Filtern nach Protokollebene (Fehler, Warnung, …).
- **Refresh -** Ansicht aktualisieren.
- **Save Log -** Protokoll als Textdatei lokal speichern.
- **Mail Log -** Klicken Sie hier, um das Protokoll gemäß den Maileinstellungen per E-Mail zu verschicken.
- **Clear Log -** Endgültiges Löschen der Protokolle aus dem Router.

Klicken Sie **Next**, um zur nächsten Seite zu gehen oder **Previous**, um auf die vorige Seite zurückzukehren.

5.16.9 Working Mode

Über die Seite **System Tools** → **Working Mode** können Sie den Betriebsmodus Ihres Geräts einsehen.

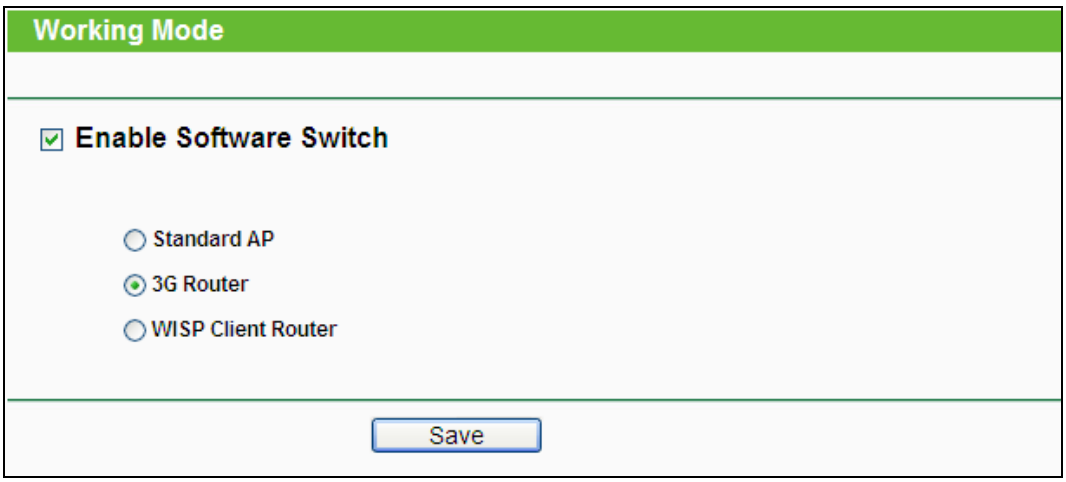


Bild 5-88 Working Mode

- **Standard AP -** Dieser Modus erlaubt es drahtlosen Geräten, sich mit dem AP zu verbinden. Als Accesspoint sendet das Gerät ein eigenes WLAN aus.
- **3G Router -** Dieser Modus erlaubt es mehreren Usern eine Verbindung zum Internet über ADSL/Kabelmodem aufzubauen.
- **WISP Client Router -** Dieser Modus erlaubt es mehreren Usern eine Verbindung zum Internet über WISP aufzubauen.

☞ **Bemerkung:**

Der Router startet automatisch neu, wenn Sie auf **Save** klicken.

5.16.10 Statistics

Unter **System Tools** → **Statistics** können Sie die Routerstatistiken einsehen. Diese umfassen: Gesamtdatenverkehr und Datenverkehr während des letzten „Packet Statistics Interval“.

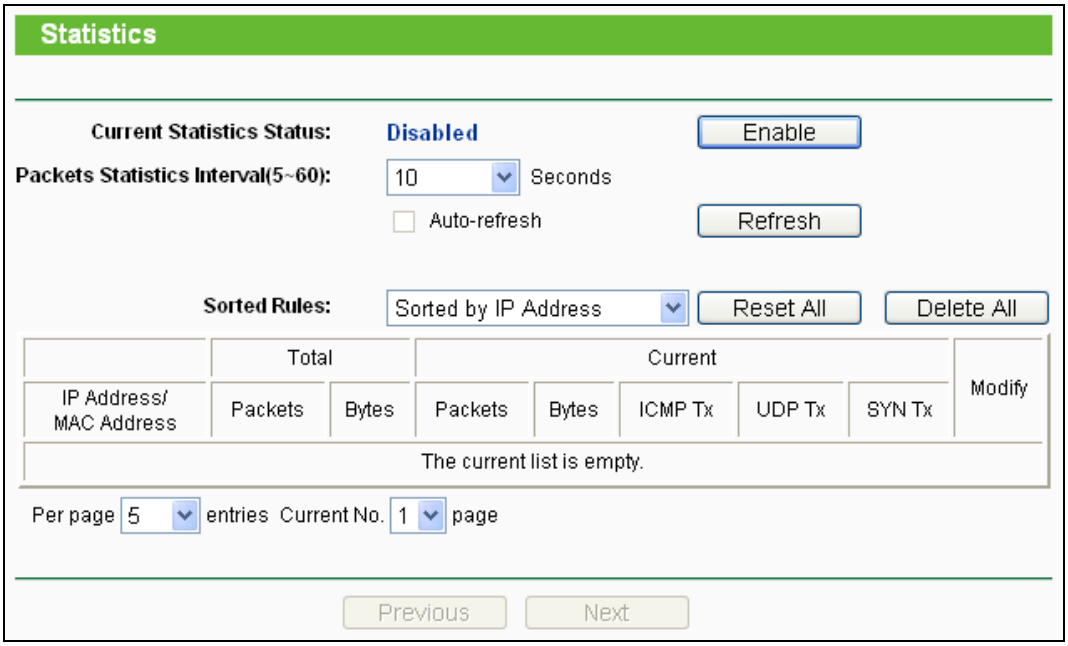


Bild 5-89 Statistics

- **Current Statistics Status -** Kann hier aktiviert oder deaktiviert werden.
- **Packets Statistics Interval(5-60) -** Die Dauer eines Zeitabschnittes, den eine Paketstatistik geführt wird, in Sekunden. Standardwert ist 10. Gültige Werte sind von 5 bis 60.
- **Sorted Rules -** Hiermit können Sie die Regeln nach Ihren Vorstellungen ordnen.

Aktivieren Sie **Auto-refresh**, um die Ansicht periodisch neu zu laden.

Klicken Sie **Refresh**, um die Ansicht sofort zu aktualisieren.

Klicken Sie **Reset All**, um alle Werte auf null zu setzen.

Klicken Sie **Delete All,** um alle Einträge aus der Tabelle zu entfernen.

Statistiktabelle:

IP/MAC Address		Die IP-/MAC-Adresse, zu der diese Statistiken gehören.
Total	**Packets**	Gesamtanzahl der vom Router übertragenen Pakete.
	Bytes	Vom Router übertragene Gesamtdatenmenge.
Current	**Packets**	Anzahl übertragener Pakete während des letzten Paketstatistikintervalls.
	Bytes	Während des letzten Paketstatistikintervalls übertragene Datenmenge.
	ICMP Tx	Anzahl zum WAN-Port gesendeter ICMP-Pakete während des letzten Paketstatistikintervalls.
	UDP Tx	Anzahl zum WAN-Port gesendeter UDP-Pakete während des letzten Paketstatistikintervalls.
	TCP SYN Tx	Anzahl zum WAN-Port gesendeter TCP-SYN-Pakete während des letzten Paketstatistikintervalls.
Modify	**Reset**	Wert des Eintrags auf Null zurücksetzen.
	Delete	Diesen Eintrag aus der Tabelle löschen.

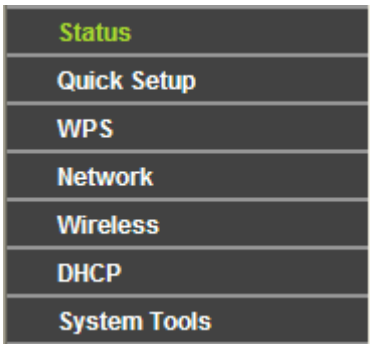
Standardmäßig sind 5 Einträge pro Seite zu sehen. Klicken Sie **Next**, um zur nächsten Seite zu blättern oder **Previous**, um zur vorigen Seite zurückzukehren.

Kapitel 6. AP-Modus

Dieses Kapitel zeigt Ihnen die Schlüsselfunktionalitäten und Konfigurationsmöglichkeiten jedes Menüs.

6.1 Login

Nachdem Sie sich erfolgreich eingeloggt haben, sehen Sie die sieben Hauptmenüs auf der linken Bildschirmseite. Im rechten HTML-Frame ist der Hilfetext zu sehen.



Im Folgenden werden diese Hauptmenüs detailliert behandelt.

6.2 Status

Die Seite **Status** zeigt Statusinformationen zum Router. Diese Informationen können hier nicht geändert werden.

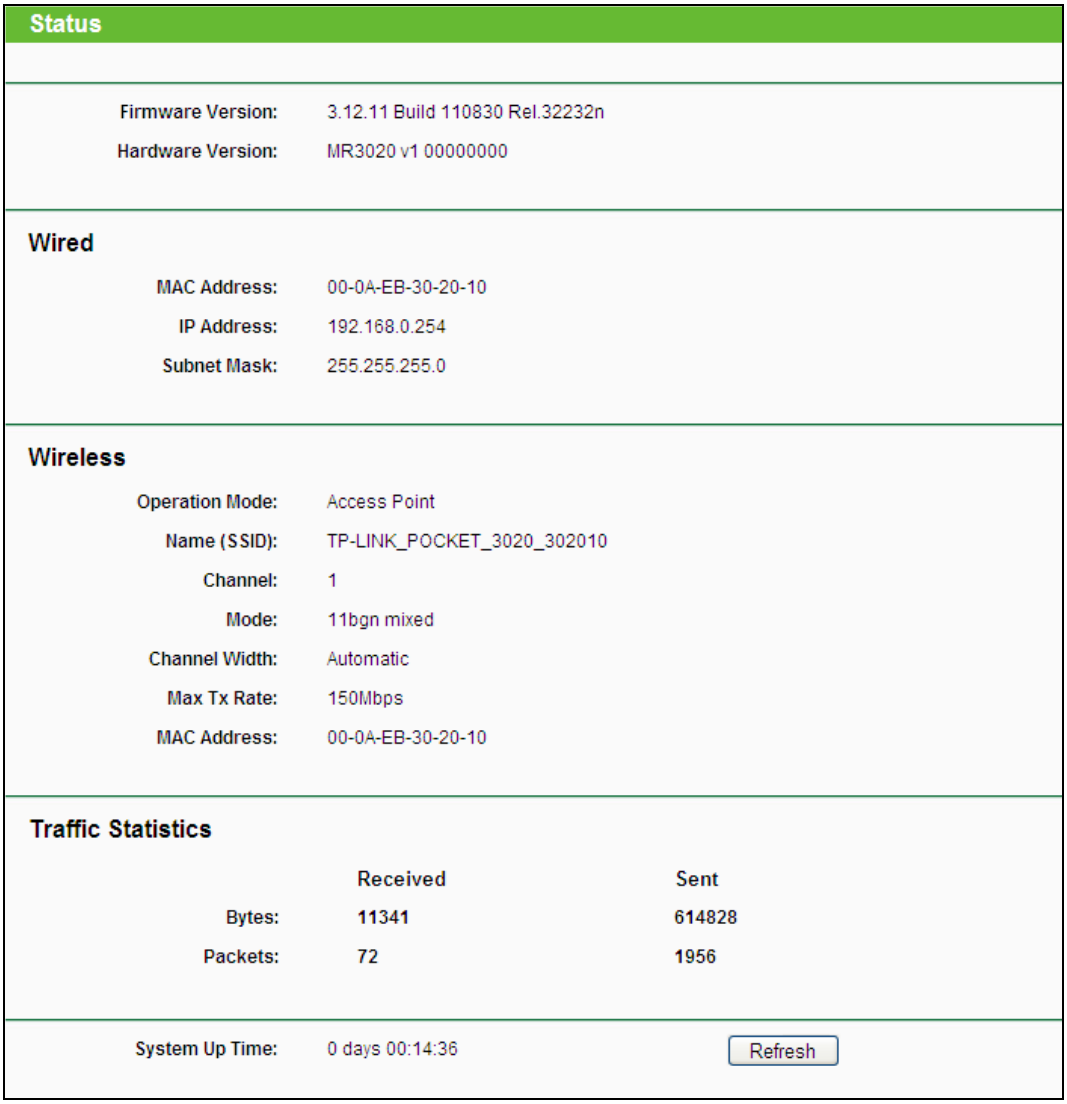


Bild 6-1 Statusseite

- **Firmware Version -** Zeigt die aktuell installiere Firmware vom AP an.
- **Hardware Version -** Zeigt die Hardwareversion des AP an.
- **Wired -** Hier werden die folgenden aktuellen Einstellungen angezeigt **MAC address**, **IP address** und **Subnet Mask**.
- **Wireless -** Hier werden die folgenden aktuellen Einstellungen angezeigt **Operating Mode, SSID, Channel, Mode, Channel Width, Max Tx Rate** und **MAC Address.**
- **Traffic Statistics -** Zeigt die **Traffic Statistic** des APs an.
- **System Up Time -** Zeigt an, wie lange der AP seit dem Start oder Reset läuft.

6.3 WPS

WPS (**Wi-Fi Protected Setup**), früher QSS **(Quick Secure Setup)** genannt, ermöglicht es Ihnen, ohne viel Arbeit ein weiteres drahtloses Gerät Ihrem verschlüsselten WLAN hinzuzufügen. Die WPS-Funktion steht nur in den Modi **Access Point** und **Multi-SSID** zur

Verfügung.

1) Gehen Sie in das Menü **WPS**. Sie sehen Folgendes (Bild 6-2).

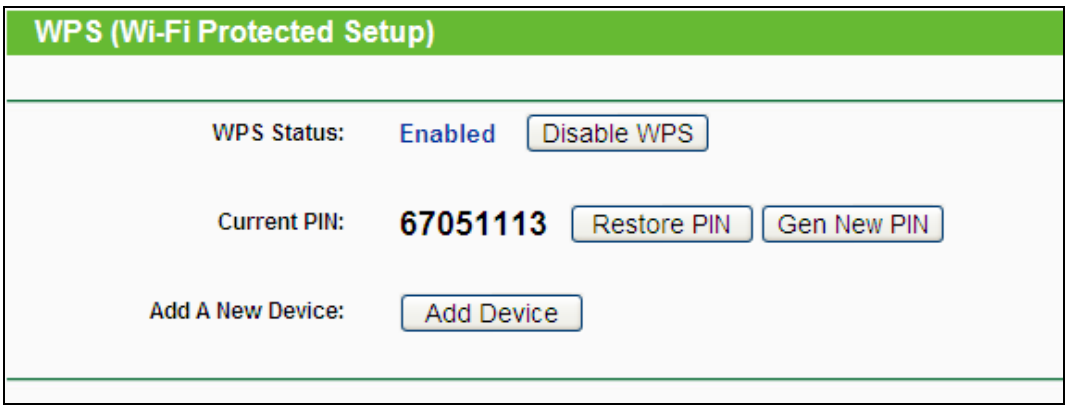


Bild 6-2 WPS

- Fehler! AutoText-Eintrag nicht definiert. **Status -** WPS aktivieren oder deaktivieren.
- **Current PIN -** Aktuelle Router-PIN. Die Standard-PIN kann auf dem Etikett auf der Geräterückseite oder auf dem Handbuch gefunden werden.
- **Restore PIN -** Standard-PIN des Routers wiederherstellen.
- **Gen New PIN -** Neue PIN per Zufallsgenerator erstellen. Damit können Sie die Sicherheit wiederherstellen, wenn die alte PIN Unbefugten bekannt wurde.
- **Add device -** Mit dieser Schaltfläche können Sie neue Geräte von Hand einbinden.

2) Um ein neues Gerät hinzuzufügen**:**

Unterstützt der Drahtlosadapter WPS (Wi-Fi Protected Setup), können Sie die Verbindung entweder mit der Tastendruckmethode (PBC) oder der PIN-Methode herstellen.

☞ Bemerkung:

Um mittels WPS erfolgreich eine Verbindung herzustellen, sollten Sie zeitgleich die entsprechende QSS-Konfiguration des Adapters durchführen.

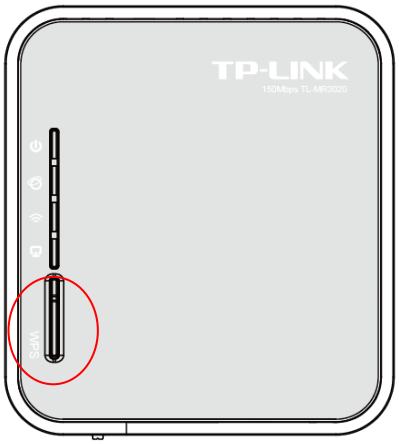
Als Beispiel dient im Folgenden ein QSS-fähiger TP-LINK-Adapter.

I. Mittels PBC

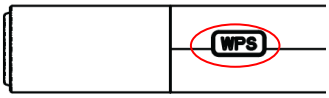
Unterstützt der drahtlose Adapter Wi-Fi Protected Setup und die Tastendruck-Konfigurationsmethode (PBC), können Sie diesen auf folgenden beiden Wegen in das WLAN einbinden.

Methode 1:

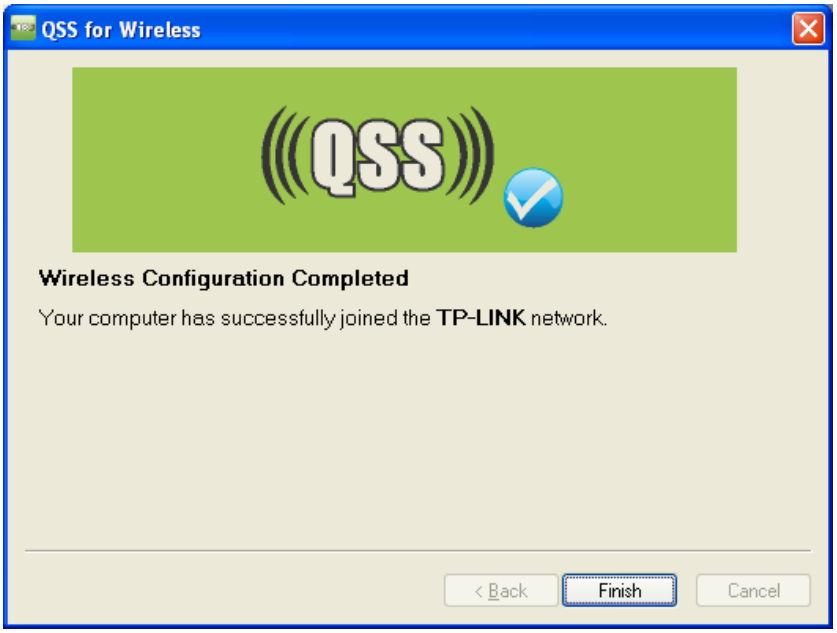
Schritt 1: Drücken Sie die WPS-Taste auf der Vorderseite des Routers.



Schritt 2: Drücken Sie die WPS-Taste des Adapters und halten Sie sie für 2 oder 3 Sekunden.



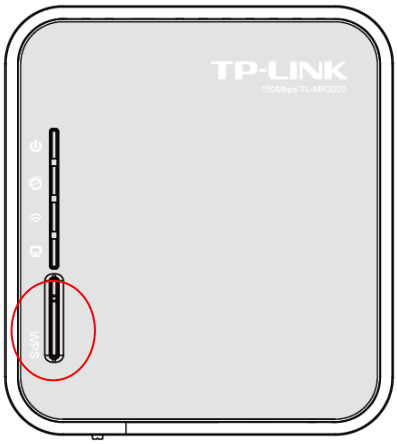
Schritt 3: Warten Sie, bis auf dem Bildschirm Folgendes erscheint. Klicken Sie **Finish**.



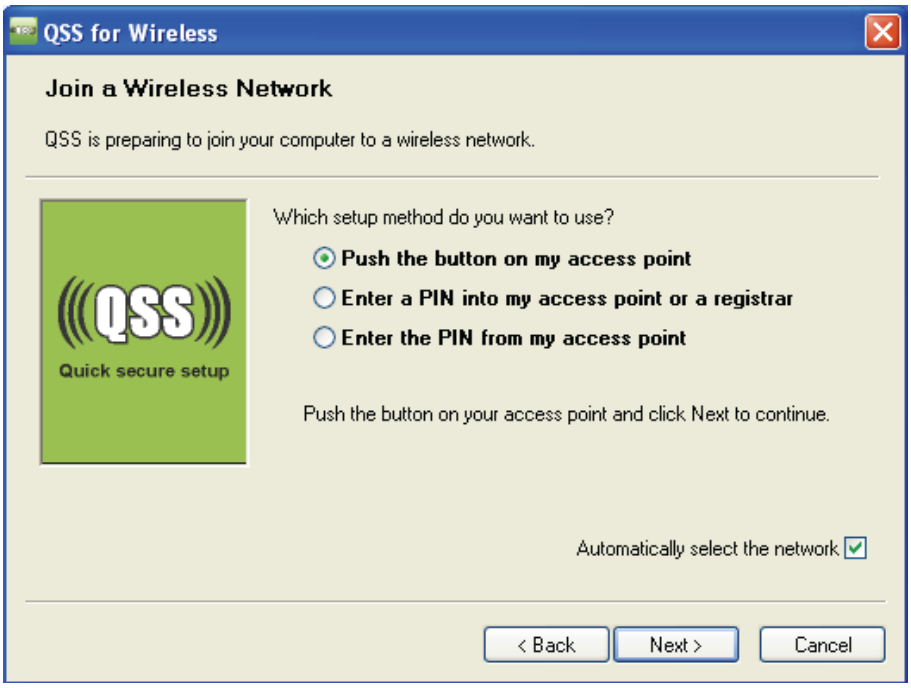
QSS-Konfigurationssoftware des Adapters

Methode 2:

Schritt 1: Drücken Sie die QSS-Taste auf der Vorderseite des Routers.

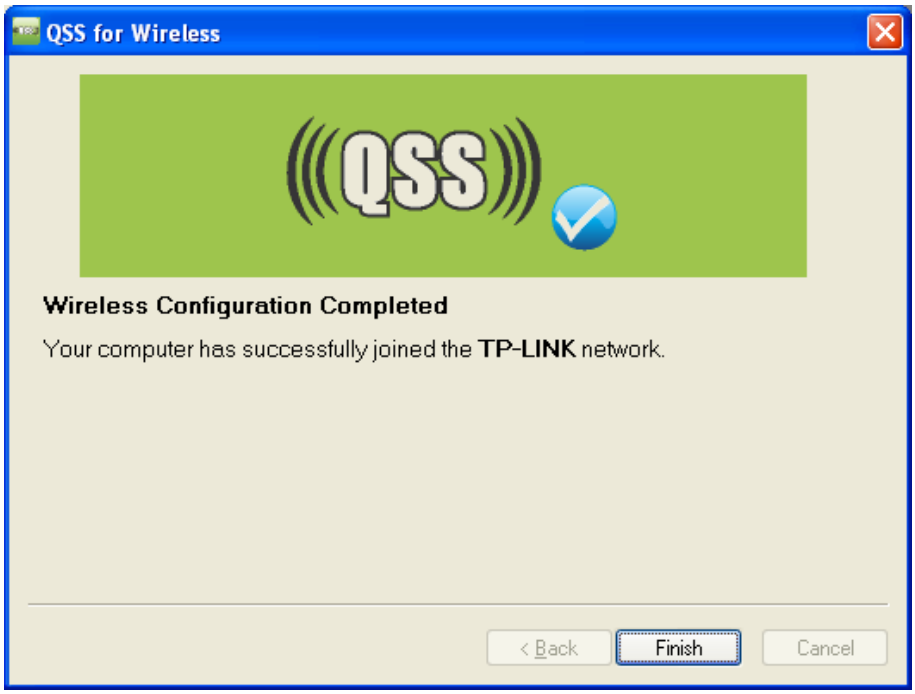


Schritt 2: Zur Konfiguration des Adapters wählen Sie in der QSS-Software bitte **Push the button on my access point** und klicken Sie **Weiter**.



QSS-Konfigurationssoftware des Adapters

Schritt 3: Warten Sie, bis Sie auf dem Bildschirm Folgendes sehen. Klicken Sie **Finish**.



QSS-Konfigurationssoftware des Adapters

Methode 3:

Schritt 1: Stellen Sie sicher, dass WPS aktiviert ist und klicken Sie **Gerät hinzufügen**, wie in Bild 6-2. Folgendes Bild erscheint.

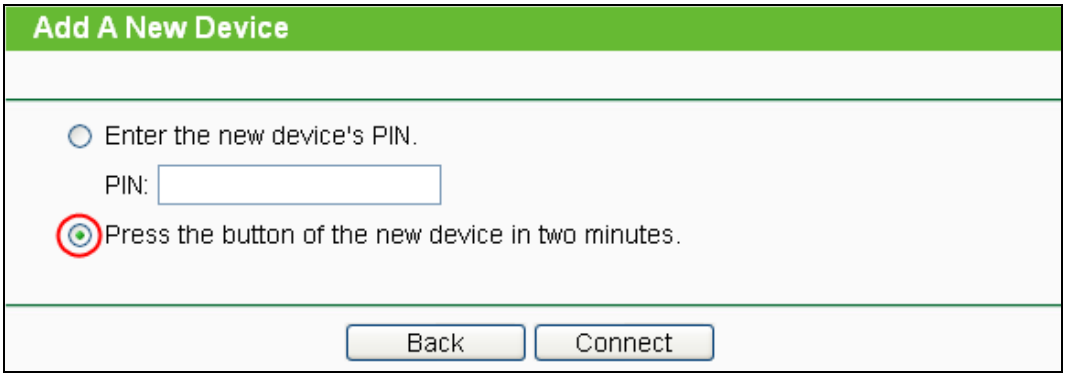
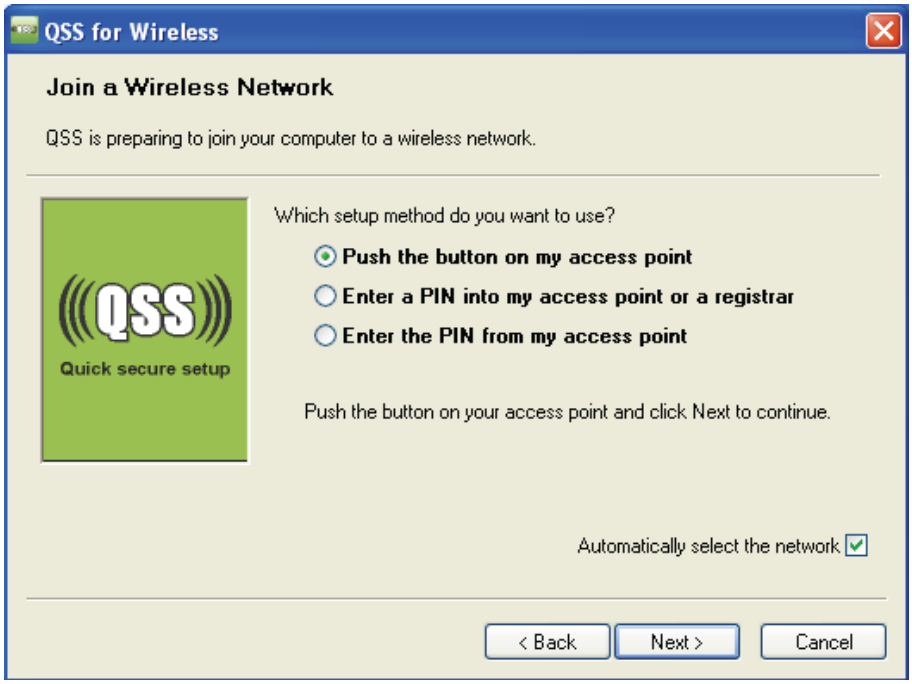


Bild 6-3 Hinzufügen eines neuen Geräts

Schritt 2: Wählen Sie **Press the button of the new device in two minutes** und klicken Sie **Connect**.

Schritt 3: Zur Konfiguration des drahtlosen Adapters wählen Sie bitte im QSS-Konfigurationstool **Push the button on my access point** und klicken Sie **Next**.



QSS-Konfigurationssoftware des Adapters

Schritt 4: Warten Sie, bis folgendes Fenster erscheint. Klicken Sie **Finish**, um die QSS-Konfiguration abzuschließen.

QSS-Konfigurationssoftware des Adapters

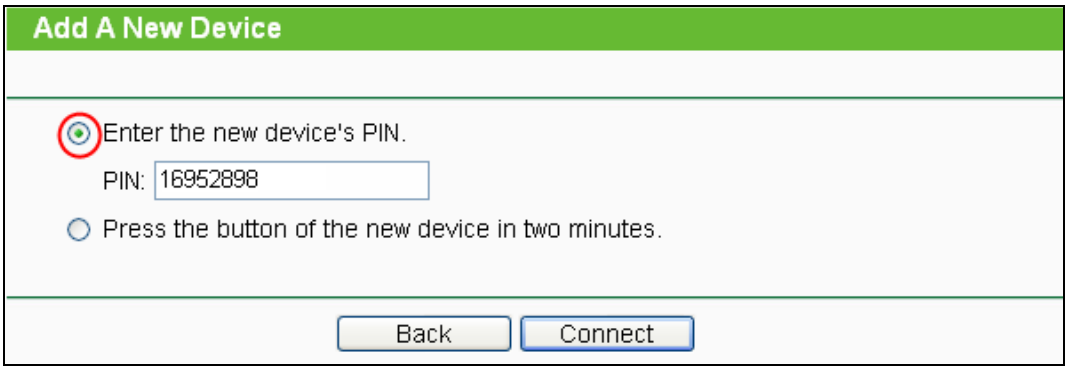
II. Mittels PIN

Unterstützt das neue Gerät WPS (Wi-Fi Protected Setup) und die PIN-Methode, können Sie es mittels der folgenden beiden Methoden durch PIN-Eingabe in das WLAN integrieren.

Methode 1: PIN in den Router eingeben

Schritt 1: Belassen Sie den Standard-QSS-Status (**Enabled**) und klicken Sie **Add device** (Bild

6-2). Folgendes Bild erscheint.

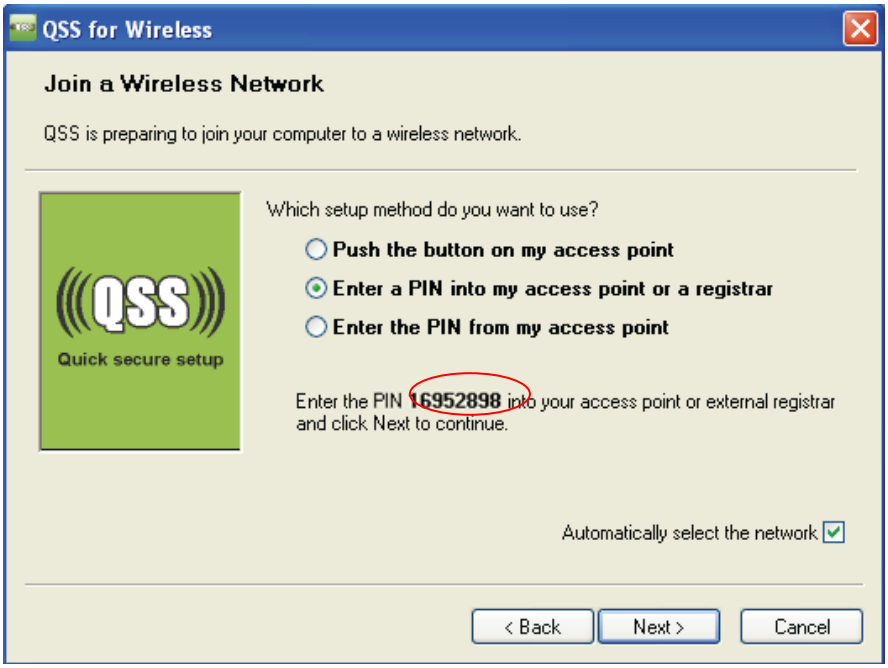


Schritt 2: Wählen Sie **Enter the new device's PIN** und geben Sie die PIN des Adapters in das Feld **PIN** ein. Klicken Sie **Connect.**

Bemerkung:

Die PIN des Adapters wird im QSS-Konfigurationsprogramm angezeigt.

Schritt 3: Zur Konfiguration des Adapters wählen Sie bitte **Enter a PIN into my access point or a registrar** aus und klicken Sie **Next.**



QSS-Konfigurationssoftware des Adapters

Bemerkung:

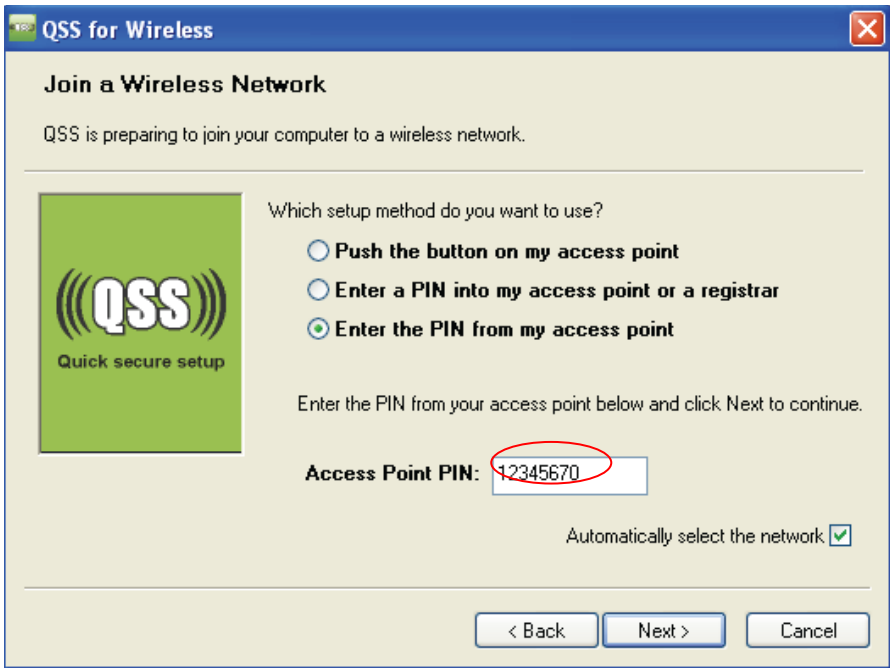
Die PIN des Adapters lautet in diesem Beispiel 16952898, wie oben ersichtlich.

Methode 2: PIN des Routers eingeben

Schritt 1: Lesen Sie die aktuelle Router-PIN in Bild 6-2 ab. Jeder Router hat eine andere PIN. In diesem Beispiel lautet sie 12345670.

Schritt 2: Zur Konfiguration des Adapters wählen Sie im QSS-Konfigurationsprogramm **PIN meines Accesspoints eingeben** und geben Sie sie bei **Accesspoint-PIN** ein. Klicken

Sie **Weiter**.

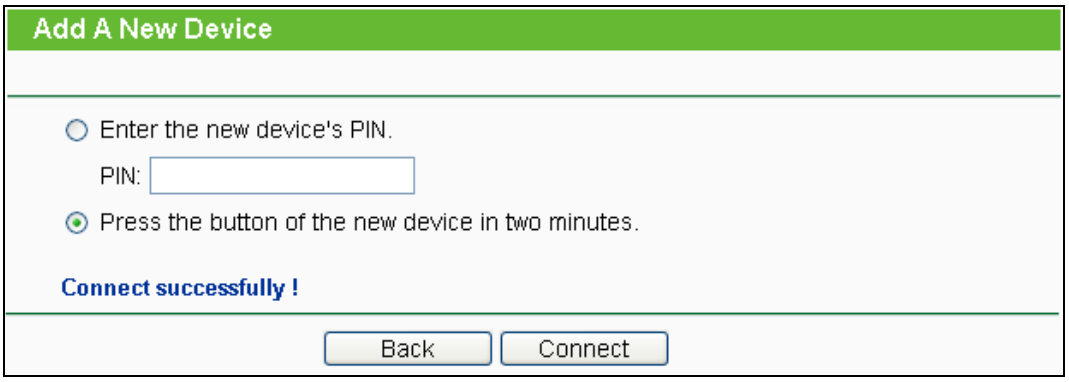


QSS-Konfigurationssoftware des Adapters

Bemerkung:

Die Standard-PIN des Routers kann auf einem Aufkleber auf der Geräterückseite oder im Webinterface wie in Bild 6-2 abgelesen werden.

Haben Sie ein Gerät erfolgreich in das Netz gebracht, sehen Sie folgende Meldung.



Bemerkungen:

1) Die Router-LED **QSS** leuchtet für einige Minuten grün, nachdem das Gerät erfolgreich dem Netz hinzugefügt wurde.
2) Die QSS-Funktionalität steht nicht zur Verfügung, wenn die WLAN-Schnittstelle des Routers deaktiviert ist. Bitte stellen Sie sicher, dass diese aktiv ist, bevor Sie QSS verwenden.

6.4 Network

Bild 6-4 Das Menü **Network**

Das Menü **Network** (Bild 6-4) verfügt im AP-Modus nur über den Unterpunkt **LAN**.

Unter **Network** → **LAN** können Sie die LAN-IP-Parameter wie unten beschrieben konfigurieren.

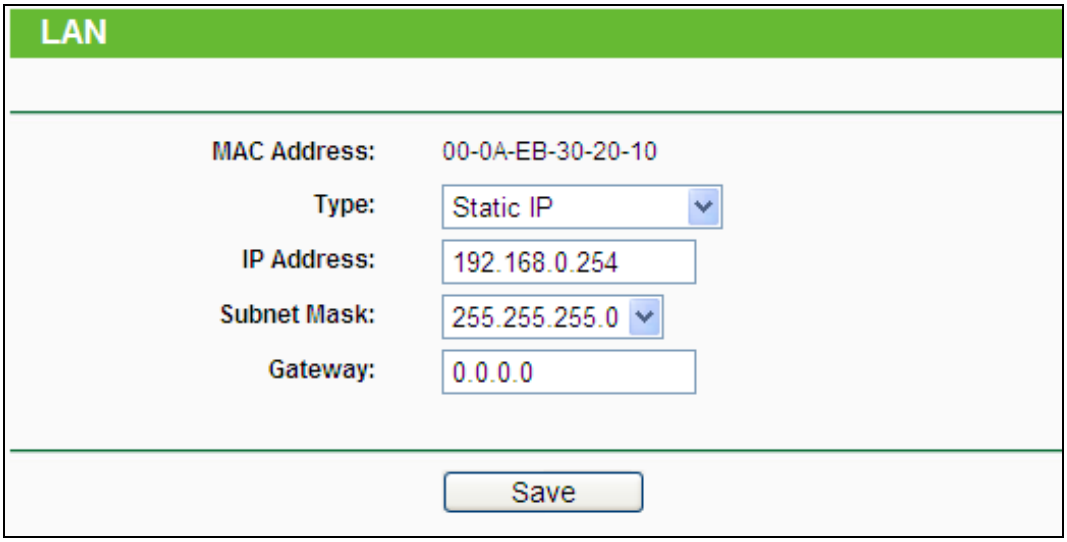


Bild 6-5 LAN

- **MAC Address -** Die physische Adresse des Routers, wie sie vom LAN aus gesehen werden kann. Diese kann nicht geändert werden.
- **IP Address -** Hier können Sie die Router-IP-Adresse festlegen (Standard: 192.168.1.1).
- **Subnet Mask -** Ein Adresscode, der die Größe Ihres Netzes angibt. Normalerweise ist die Subnetzmaske 255.255.255.0.
- **Gateway -** Hier können Sie das Gateway-IP festlegen.

☞ **Bemerkungen:**

1) Ändern Sie die LAN-IP-Adresse, muss ab dann die neue IP-Adresse verwendet werden, um den Router zu administrieren.
2) Liegt die neue LAN-IP-Adresse in einem anderen Subnetz als die alte, ändert der Adresspool des DHCP-Servers sich automatisch entsprechend, während die Einstellungen zu Virtuellen Servern und DMZ-Host neu konfiguriert werden müssen.

6.5 Wireless

Unter **Wireless** können Sie in wenigen Schritten ein WLAN anlegen und Grundeinstellungen tätigen. Die Drahtlossicherheit bietet drei verschieden starke Sicherheitsstufen, um Ihr Netz den Clientfähigkeiten entsprechend abzusichern. MAC-Adressfilterung ermöglicht die Kontrolle darüber, welche Stationen auf das WLAN des APs zugreifen dürfen. Weiterhin ist die

Einstellung einiger erweiterter WLAN-Parameter möglich. Der **Throughput Monitor** ermöglicht Ihnen die Beobachtung des Datendurchsatzes.

Im Menü **Wireless** gibt es fünf Untermenüs (Bild 6-6): **Wireless Settings**, **Wireless Security**, **Wireless MAC Filtering**, **Wireless Advanced** und **Wireless Statistics**.

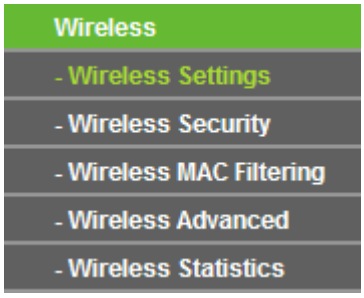


Bild 6-6 Das Menü **Wireless**

6.5.1 Wireless Settings

Wählen Sie **Wireless** -> **Wireless Settings**, können Sie die Grundeinstellungen Ihres WLANs tätigen (Bild 6-7). Auf dieser Seite können Sie den Betriebsmodus Ihres Gerätes einstellen. Es werden sechs Betriebsarten unterstützt: **Access Point**, **Client**, **Repeater** and **Bridge with AP**. Jeder Modus bringt andere Optionen mit.

1) Access Point: Dieser Modus erlaubt es drahtlosen Geräten, sich mit dem AP zu verbinden. Als Accesspoint sendet das Gerät ein eigenes WLAN aus.

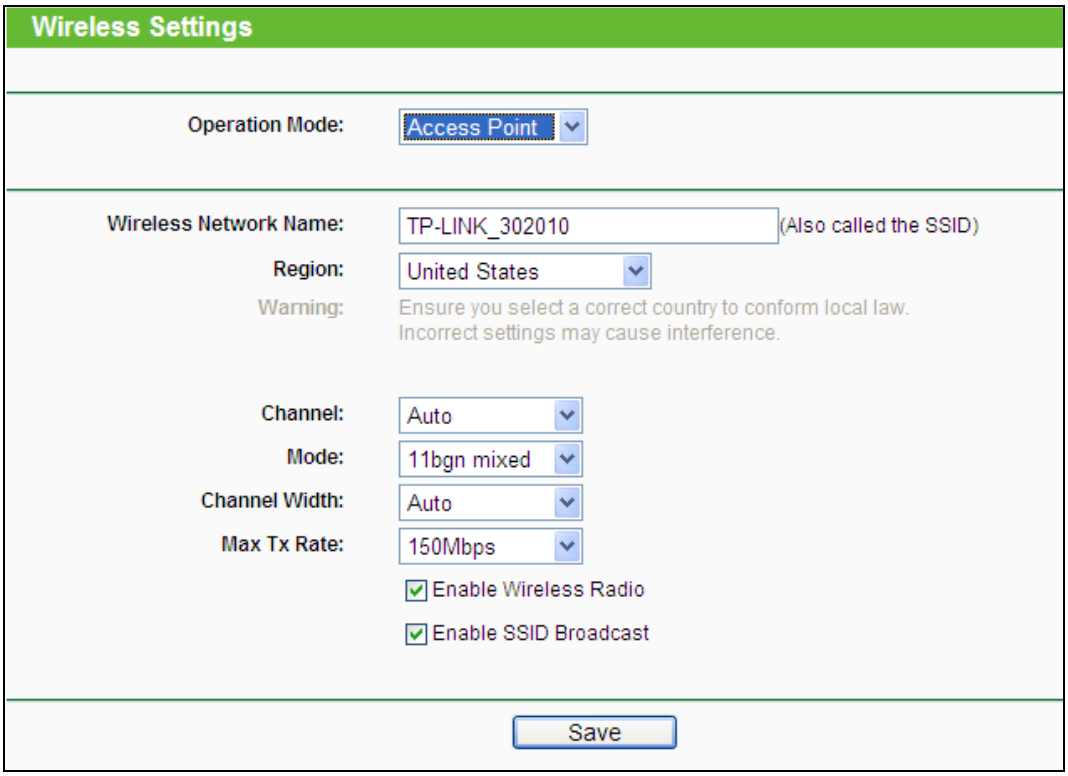


Bild 6-7 Einstellungen im Modus Accesspoint

- **Wireless Network Name (auch SSID genannt) -** Vergeben Sie Ihrem WLAN einen Namen

von bis zu 32 Zeichen an (SSID). Dieser muss von allen anderen Geräten in Ihrem WLAN verwendet werden. Standardwert ist TP-LINK_xxxxxx, doch sollte dieser geändert werden. Hier wird zwischen Groß- und Kleinschreibung unterschieden, z.B. bezeichnen *TP-LINK* und *tp-link* unterschiedliche Netze.

- **Region -** Wählen Sie hier den Standort des Routers aus. Eine falsche Auswahl könnte gegen geltende Gesetze verstoßen. Ist Ihre Region nicht aufgeführt, wenden Sie sich bitte an die zuständigen Behörden. In Deutschland ist **Germany**, in der Schweiz **Switzerland** und in Österreich **Austria** einzustellen.

  Wird diese Einstellung geändert, erscheint nach Klick auf **Save** folgende Meldung, die Sie mit **OK** bestätigen.

  Bemerkung:

  Aufgrund gesetzlicher Restriktionen verfügt die Nordamerika-Version des Produktes nicht über diese Option.

- **Channel -** Dieses Feld legt die Betriebsfrequenz des Routers fest. In der Standardeinstellung **Auto** wählt der Router automatisch einen Kanal aus. Es ist nicht erforderlich, diese zu ändern, es sei denn, Sie stellen Interferenzen von einem nahen Accesspoint fest.

- **Mode -** Wählen Sie den gewünschten Modus aus. Standardwert: **11bgn mixed**:
  - **11b only -** Wählen Sie dies nur aus, wenn alle Clients in Ihrem WLAN 802.11b-Clients sind.
  - **11g only -** Wählen Sie dies nur aus, wenn alle Clients in Ihrem WLAN 802.11g-Clients sind.
  - **11n only -** Wählen Sie dies nur aus, wenn alle Clients in Ihrem WLAN 802.11n-Clients sind.
  - **11bg mixed -** Diese Option ist die richtige, wenn Sie sowohl 802.11b- als auch 802.11g-Clients in Ihrem Netz betreiben..

- **Channel Width -** Wählen Sie die Kanalbreite aus. Standardeinstellung ist **Automatic**

  Bemerkung:

  Diese Option kann nicht geändert werden, wenn über **Modus** 802.11n-Clients ausgeschlossen wurden. Der Kanalbreitenwert ist dann auf 20MHz eingestellt.

- **Max Tx Rate -** Die WLAN-Datentransferrate kann hiermit begrenzt werden.

- **Enable Wireless Radio -** Die WLAN-Funktion des Routers kann ein- und ausgeschaltet werden, um drahtlosen Zugriff zu ermöglichen oder zu verhindern.
- **Enable SSID Broadcast -** Wird dies ausgewählt, sendet der Router den WLAN-Namen (SSID) aus und Clients können das Netz in ihrer Übersicht anzeigen.

☞ **Bemerkung:**

Um die auf dieser Seite getätigten Einstellungen zu übernehmen, muss der Accesspoint nach Klicken auf **Save** neugestartet werden. Ein Hinweis wird Sie zusätzlich daran erinnern.

2) Client: In dieser Betriebsart dient der AP dazu, ein Ethernetgerät als WLAN-Station Ihrem drahtlosen Netz hinzuzufügen

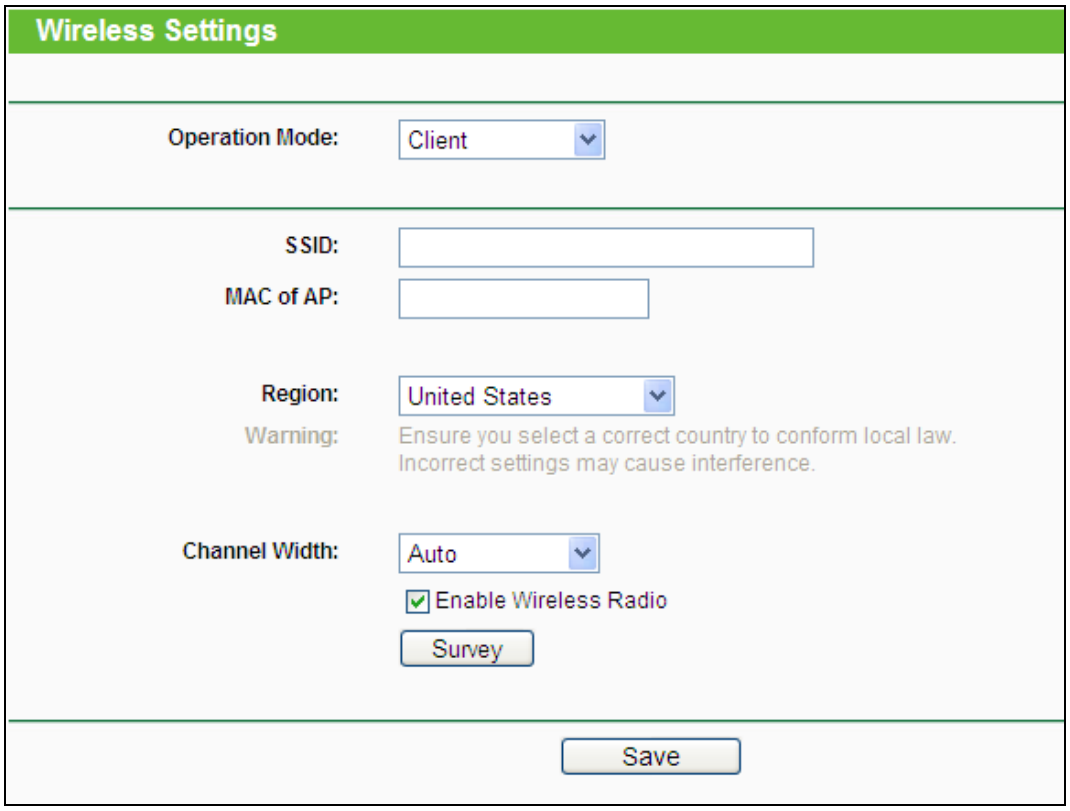


Bild 6-8 Einstellungen im **Client**-Modus

- **SSID -** Wählen Sie diese Option aus, verbindet der Client sich anhand der SSID mit dem AP. Hierfür geben Sie bitte die dem AP zugehörige SSID in das Feld ein.
- **MAC of AP -** Wählen Sie diese Option aus, verbindet der Client sich anhand der MAC-Adresse mit dem AP. Hierfür geben Sie bitte die MAC-Adresse des APs ein .
- **Region -** Wählen Sie aus der Drop-Down-Liste die Region aus, in der der AP sich befindet. Damit verbunden sind Spezifikationen für die vom AP verwendeten Kanäle und Weiteres. Daher kann hier eine falsche Einstellung einen nicht gesetzeskonformen Betrieb verursachen. Ist die Region, in der der Router steht, nicht in dieser Liste aufgeführt, wenden Sie sich bitte an die zuständigen Behörden.

Haben Sie Ihre Region ausgewählt und **Save** geklickt, erscheint folgender Hinweis. Stellen Sie aus obigen Gründen sicher, dass die Einstellung **Region** stimmt und klicken Sie **OK**.

☞ Bemerkung:

Aus rechtlichen Gründen verfügt die Nordamerika-Version dieses Accesspoints nicht über die Möglichkeit, die Region einzustellen.

- **Channel Width -** Legt die verwendete Kanalbreite fest. Es ist in der Regel nicht erforderlich, diese abzuändern.
- **Enable Wireless Radio -** WLAN-Zugriff zulassen oder nicht.

Klicken Sie **Search**, um in der näheren Umgebung nach SSIDs zu suchen..

☞ Bemerkung:

Um die auf dieser Seite getätigten Einstellungen zu übernehmen, muss der Accesspoint nach Klicken auf **Save** neugestartet werden. Ein Hinweis wird Sie zusätzlich daran erinnern.

3) Repeater: In diesem Modus gibt der AP Daten an einen verbundenen, WDS-fähigen Root-AP weiter. Der Repeater erweitert also die Reichweite des Root-APs.

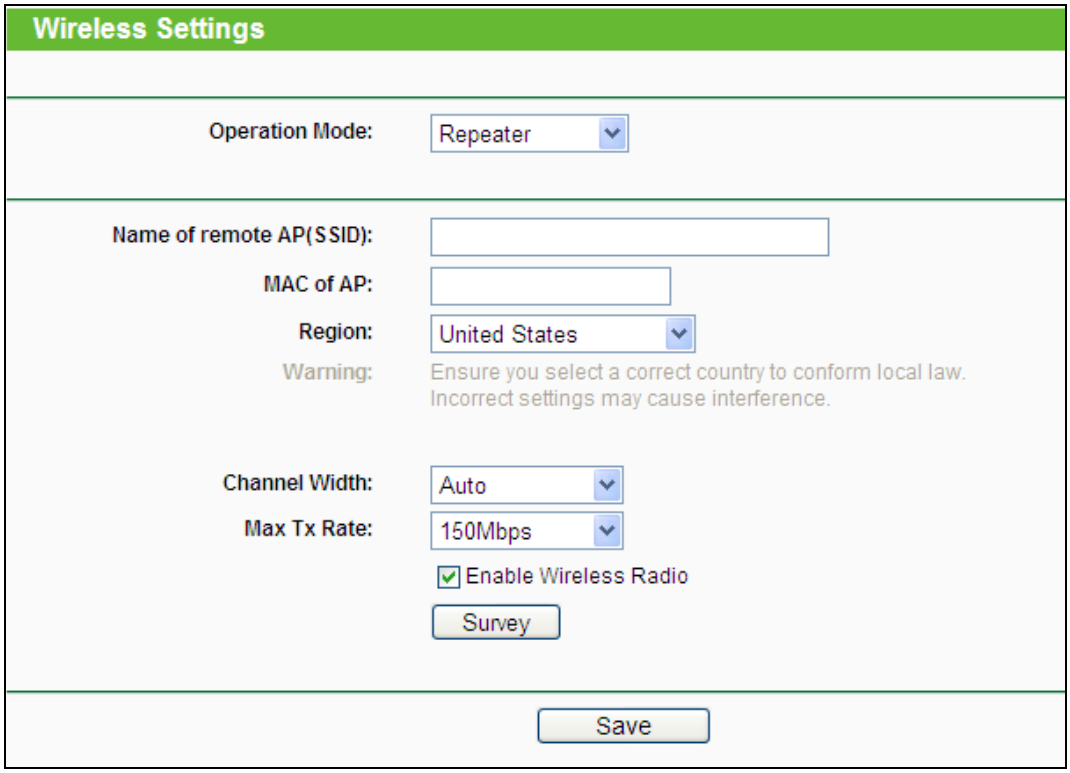


Bild 6-9 Repeatereinstellungen

- **MAC of AP -** Geben Sie die MAC-Adresse des Root-APs, dessen Reichweite Sie vergrößern möchten, in dieses Feld ein.
- **Region -** Wählen Sie aus der Drop-Down-Liste die Region aus, in der der AP sich befindet. Damit verbunden sind Spezifikationen für die vom AP verwendeten Kanäle und Weiteres. Daher kann hier eine falsche Einstellung einen nicht gesetzeskonformen Betrieb verursachen. Ist die Region, in der der Router steht, nicht in dieser Liste aufgeführt, wenden Sie sich bitte an die zuständigen Behörden

  Haben Sie Ihre Region ausgewählt und **Save** geklickt, erscheint folgender Hinweis. Stellen Sie aus obigen Gründen sicher, dass die Einstellung **Region** stimmt und klicken Sie **OK**.

☞ Bemerkung:

Aus rechtlichen Gründen verfügt die Nordamerika-Version dieses Accesspoints nicht über die Möglichkeit, die Region einzustellen.

- **Channel Width -** Legt die verwendete Kanalbreite fest. Es ist in der Regel nicht erforderlich, diese abzuändern.
- **Max Tx Rate -** Stellt die maximale WLAN-Übertragungsrate des Gerätes ein.
- **Enable Wireless Radio -** WLAN-Zugriff zulassen oder nicht.

Klicken Sie **Search**, um in der näheren Umgebung nach SSIDs zu suchen..

☞ Bemerkung:

Um die auf dieser Seite getätigten Einstellungen zu übernehmen, muss der Accesspoint nach Klicken auf **Save** neugestartet werden. Ein Hinweis wird Sie zusätzlich daran erinnern.

4) **Bridge with AP:** In diesem Modus können dieser AP und bis zu 4 weitere 4 APs, die sich ihrerseits im Bridgemodus befinden, benutzt werden, um mehrere Draht-LANs miteinander zu verbinden.

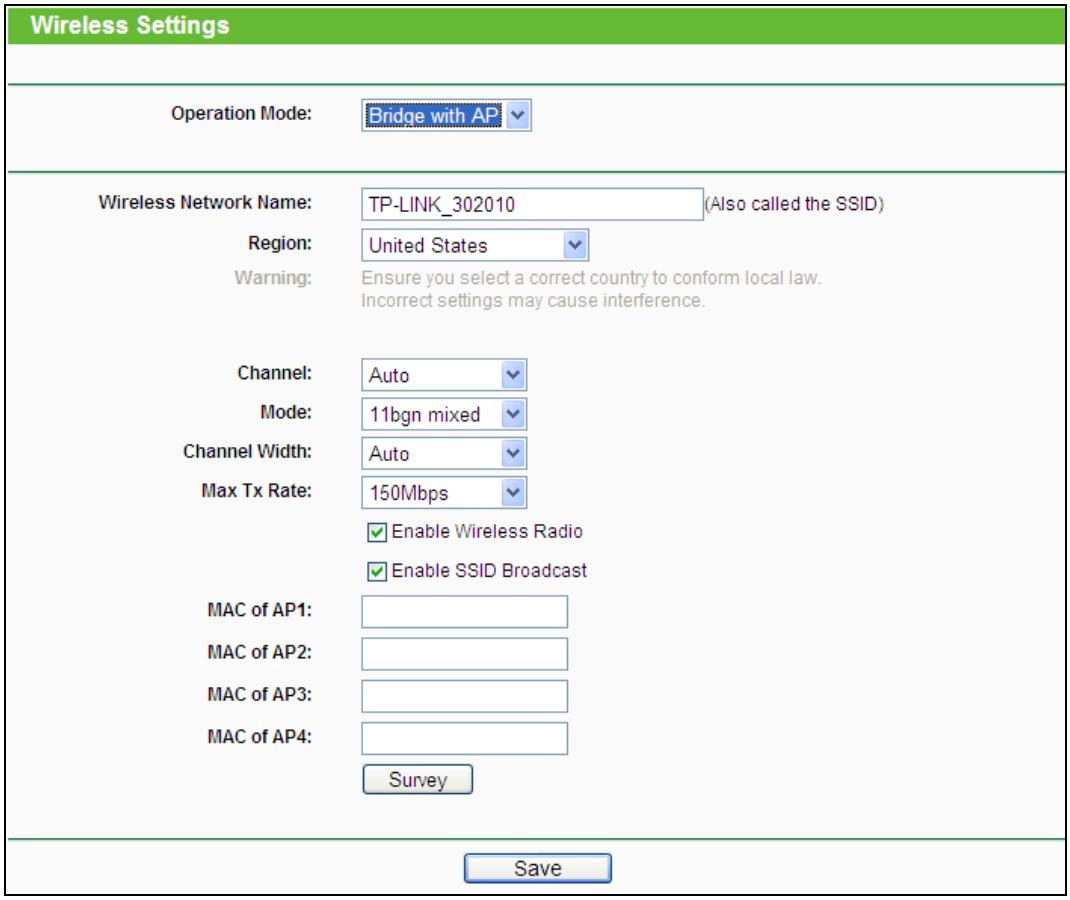


Bild 6-10 Einstellungen im Modus Bridge with AP

- **Wireless Network Name (auch SSID genannt) -** Dies ist der Name Ihres drahtlosen Netzes. Er darf bis zu 32 Zeichen lang sein. Alle Geräte, die zu Ihrem Netz gehören (sollen), müssen mit diesem Namen konfiguriert werden. Die Standard-SSID lautet „TP-LINK_XXXXXX“, wobei „XXXXXX“ für die letzten sechs Zeichen der MAC-Adresse des APs steht. Hierbei wird zwischen Groß- und Kleinschreibung unterschieden. Beispielsweise bezeichnen die SSIDs *TP-LINK* und *tp-link* unterschiedliche Netze
- **Region -** Wählen Sie aus der Drop-Down-Liste die Region aus, in der der AP sich befindet. Damit verbunden sind Spezifikationen für die vom AP verwendeten Kanäle und Weiteres. Daher kann hier eine falsche Einstellung einen nicht gesetzeskonformen Betrieb verursachen. Ist die Region, in der der Router steht, nicht in dieser Liste aufgeführt, wenden Sie sich bitte an die zuständigen Behörden.

Haben Sie Ihre Region ausgewählt und **Save** geklickt, erscheint folgender Hinweis. Stellen Sie aus obigen Gründen sicher, dass die Einstellung **Region** stimmt und klicken Sie **OK**.

Bemerkung:

Aufgrund gesetzlicher Restriktionen verfügt die Nordamerika-Version des Produktes nicht über diese Option.

- **Channel -** Dieses Feld legt die Betriebsfrequenz des Routers fest. In der Standardeinstellung **Auto** wählt der Router automatisch einen Kanal aus. Es ist nicht erforderlich, diese zu ändern, es sei denn, Sie stellen Interferenzen von einem nahen Accesspoint fest.
- **Mode -** Wählen Sie den gewünschten Modus aus. Standardwert: **11bgn mixed**.
  - **11b only -** Wählen Sie dies nur aus, wenn alle Clients in Ihrem WLAN 802.11b-Clients sind.
  - **11g only -** Wählen Sie dies nur aus, wenn alle Clients in Ihrem WLAN 802.11g-Clients sind.
  - **11n only -** Wählen Sie dies nur aus, wenn alle Clients in Ihrem WLAN 802.11n-Clients sind.
  - **11bg mixed -** Diese Option ist die richtige, wenn Sie sowohl 802.11b- als auch 802.11g-Clients in Ihrem Netz betreiben.
  - **11bgn mixed -** Wählen Sie diese Option in allen anderen Fällen (empfohlene Standardeinstellung). Damit können sowohl b- und g- als auch n-Clients Verbindung aufnehmen.
- **Channel Width -** Wählen Sie die Kanalbreite aus. Standardeinstellung ist **Automatic**

  Bemerkung:

  Diese Option kann nicht geändert werden, wenn über **Modus** 802.11n-Clients ausgeschlossen wurden. Der Kanalbreitenwert ist dann auf 20MHz eingestellt.
- **Max Tx Rate -** Die WLAN-Datentransferrate kann hiermit begrenzt werden.
- **Enable Wireless Radio -** Die WLAN-Funktion des Routers kann ein- und ausgeschaltet werden, um drahtlosen Zugriff zu ermöglichen oder zu verhindern.
- **Enable SSID Broadcast -** Wird dies ausgewählt, sendet der Router den WLAN-Namen (SSID) aus und Clients können das Netz in ihrer Übersicht anzeigen.
- **MAC of AP (1-4) -** Die MAC-Adresse des/der anderen AP(s).

Klicken Sie **Survey**, um in der näheren Umgebung nach SSIDs zu suchen.

Bemerkung:

Um die auf dieser Seite getätigten Einstellungen zu übernehmen, muss der Accesspoint nach Klicken auf **Save** neugestartet werden. Ein Hinweis wird Sie zusätzlich daran erinnern.

6.5.2 Wireless Security

Im Menü **Wireless** → **Wireless Security** können Sie die Sicherheitseinstellungen ändern. Der AP beherrscht drei Sicherheitstypen: WEP, WPA/WPA2 und WPA-PSK/WPA2-PSK. Die Sicherheit kann auf der Seite in Bild 6-11 eingestellt werden. Die Sicherheitsoptionen können sich abhängig von der Betriebsart voneinander unterscheiden.

1) Access Point

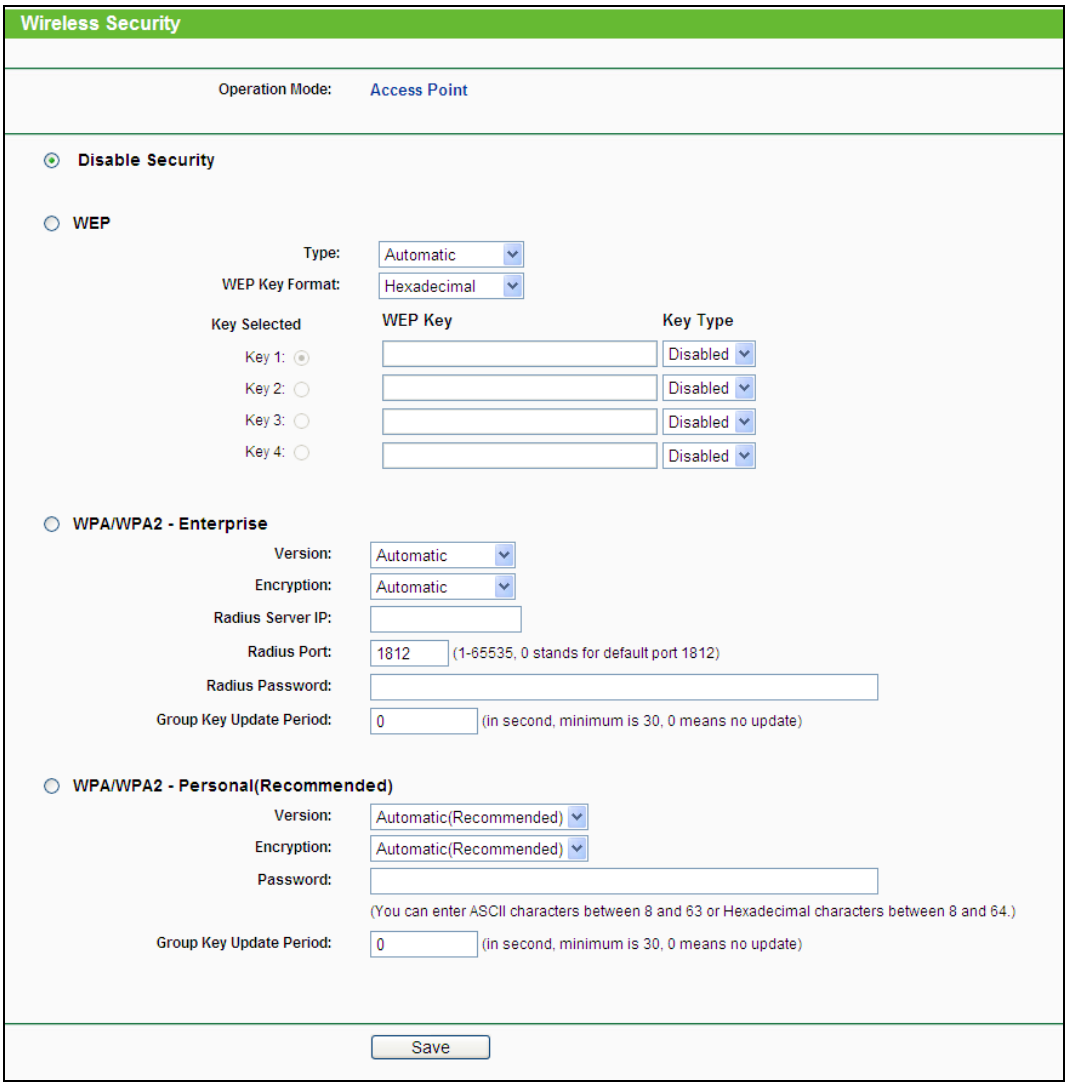


Bild 6-11 Sicherheitseinstellungen Accesspoint

- **Operation Mode -** Zeigt die aktuelle Betriebsart an.
- **Disable Security -** Hiermit können Sie verfügen, dass der AP ganz ohne Verschlüsselung arbeitet. Damit kann jeder in Reichweite sich mit dem AP verbinden. Es wird wärmstens empfohlen, dass Sie statt dieser Option eine mit Sicherheit wählen.

- **WEP** - WEP-Sicherheit nach IEEE 802.11.
  - **WEP -** Der WEP-Authentifizierungstyp kann auf **Automatic** (Standard), **Open System** oder **Shared Key** eingestellt werden. **Automatic** lässt den Client den Typ auswählen.
  - **WEP Key Format -** Als Schlüsselformat können Sie zwischen **ASCII** und **Hexadecimal** wählen. Im Fall von **ASCII** können Sie mit beliebigen Zeichen arbeiten. Haben Sie **Hexadecimal** gewählt, können Sie nur Buchstaben von A bis F und arabische Ziffern verwenden. Der Wert 0 ist allerdings unzulässig. Bitte beachten Sie die vorgegebene Schlüssellänge.
  - **WEP Key** - Wählen Sie einen der vier Schlüssel aus, um diesen zu verwenden.
  - **Key Type** - Hier können Sie die Schlüssellänge (64, 128 oder 152 Bit) auswählen. Der Wert „**Disabled**" bedeutet hier, dass der Schlüssel ungültig ist .
  - Bei **64-Bit**-Verschlüsselung sind 10 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 5 ASCII-Zeichen einzugeben.
  - Bei **128-Bit**-Verschlüsselung sind 26 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 13 ASCII-Zeichen einzugeben.
  - Bei **152-Bit**-Verschlüsselung sind 32 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 16 ASCII-Zeichen einzugeben.

☞ **Bemerkung:**

Wurde kein WEP-Schlüssel gesetzt, ist das Netz immer noch unverschlüsselt, selbst wenn als Sicherheitstyp **WEP** ausgewählt ist.

- **WPA/WPA2 – Enterprise -** Basiert auf einem Radius-Server.
  - **Version -** Hier können Sie die WPA-Version auswählen. Die Standardeinstellung ist **Automatic**, womit entsprechend der Fähigkeiten/Anforderungen der Clients entweder mit **WPA** (Wi-Fi Protected Access) oder **WPA2** (WPA Version 2) gearbeitet wird.
  - **Encryption** - Hier können Sie zwischen **Automatic**, **TKIP** und **AES** wählen.
  - **Radius Server IP** - IP-Adresse des Radius-Servers.
  - **Radius Port** - Port, auf dem der Radius-Dienst läuft.
  - **Radius Password** - Das Passwort des Radius-Servers.
  - **Group Key Update Period** - Geben Sie die Dauer der Gültigkeit eines einzigen Gruppenschlüssels in Sekunden an. Dieser Wert sollte 0 (=deaktiviert) oder mindestens 30 betragen. Empfohlen sind Werte von 500 oder 600.
- **WPA/WPA2 – Personal (Recommended) -** WPA/WPA2-Authentifizierung, basierend auf einem Passwort. Empfohlene Einstellung.
  - **Version -** WPA-PSK-Version. Die Standardeinstellung ist **Automatic**, womit entsprechend der Fähigkeiten/Anforderungen der Clients entweder mit **WPA-PSK** (Wi-Fi Protected Access) oder **WPA2-PSK** (WPA Version 2) gearbeitet wird.

- **Encryption** - Hier können Sie zwischen **Automatic**, **TKIP** und **AES** wählen.
- **PSK Passphrase** - Das Passwort kann 8 bis 63 ASCII- oder 8 bis 64 Hexadezimalzeichen lang sein.
- **Group Key Update Period** - Geben Sie die Dauer der Gültigkeit eines einzigen Gruppenschlüssels in Sekunden an. Dieser Wert sollte 0 (=deaktiviert) oder mindestens 30 betragen. Empfohlen sind Werte von 500 oder 600.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

2) Client

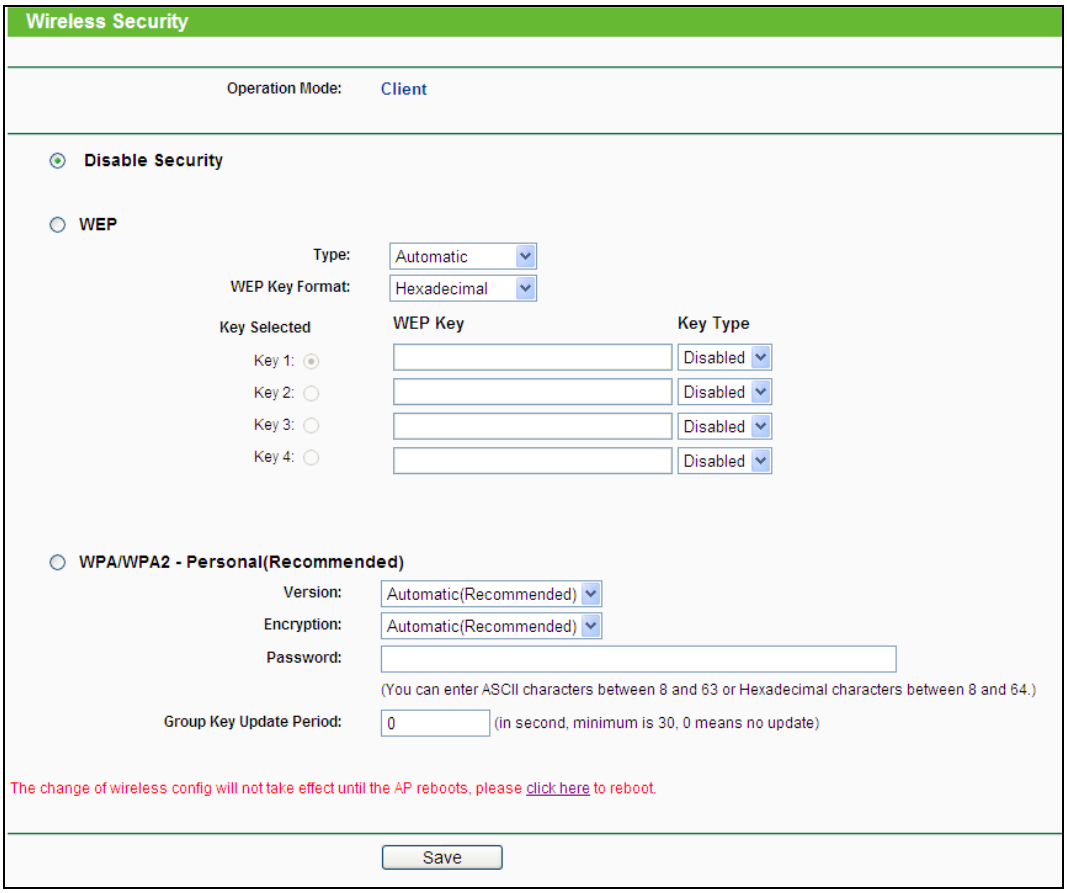


Bild 6-12 Wireless Security – Client

- **Operation Mode -** Zeigt die aktuelle Betriebsart an.
- **Disable Security -** Hiermit können Sie verfügen, dass der AP ganz ohne Verschlüsselung arbeitet. Damit kann jeder in Reichweite sich mit dem AP verbinden. Es wird wärmstens empfohlen, dass Sie statt dieser Option eine mit Sicherheit wählen.
- **WEP -** WEP-Sicherheit nach IEEE 802.11.
  - **Type** - Der WEP-Authentifizierungstyp kann auf **Automatic** (Standard), **Open System** oder **Shared Key** eingestellt werden. **Automatic** lässt den Client den Typ auswählen.

- **WEP Key Format** - Es können die Formate **Hexadecimal** und **ASCII** ausgewählt werden. Im Fall von **Hexadecimal** können Sie eine Folge Hexadezimalziffern (0..9, a..f) in der angegebenen Länge eingeben. Bei **ASCII**-Format können Sie alle Zeichen nehmen.
- **WEP Key** - Wählen Sie aus, welcher der vier Schlüssel verwendet werden soll, und geben Sie den passenden WEP-Schlüssel ein. Stellen Sie sicher, dass Sie diese auf allen Geräten in Ihrem WLAN korrekt eingeben.
- **Key Type** - Hier können Sie die WEP-Schlüssellänge (64 Bit, 128 Bit oder 152 Bit) auswählen. **Disabled** sagt aus, dass der eingegebene WEP-Schlüssel ungültig ist.
- Bei **64-Bit**-Verschlüsselung sind 10 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 5 ASCII-Zeichen einzugeben.
- Bei **128-Bit**-Verschlüsselung sind 26 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 13 ASCII-Zeichen einzugeben.
- Bei **152-Bit**-Verschlüsselung sind 32 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 16 ASCII-Zeichen einzugeben.

Bemerkung:

Wird hier kein Schlüssel angegeben, wird die WLAN-Sicherheit nicht aktiviert, selbst wenn dies so eingestellt ist.

➢ **WPA/WPA2 – Personal (Recommended) -** WPA/WPA2-Authentifizierung, basierend auf einem Passwort. Empfohlene Einstellung.

- **Version -** WPA-PSK-Version. Die Standardeinstellung ist **Automatic**, womit entsprechend der Fähigkeiten/Anforderungen der Clients entweder mit **WPA-PSK** (Wi-Fi Protected Access) oder **WPA2-PSK** (WPA Version 2) gearbeitet wird
- **Encryption** - Hier können Sie zwischen **Automatic**, **TKIP** und **AES** wählen.
- **PSK Passphrase** - Das Passwort kann 8 bis 63 ASCII- oder 8 bis 64 Hexadezimalzeichen lang sein.
- **Group Key Update Period** - Geben Sie die Dauer der Gültigkeit eines einzigen Gruppenschlüssels in Sekunden an. Dieser Wert sollte 0 (=deaktiviert) oder mindestens 30 betragen. Empfohlen sind Werte von 500 oder 600.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

3) Repeater

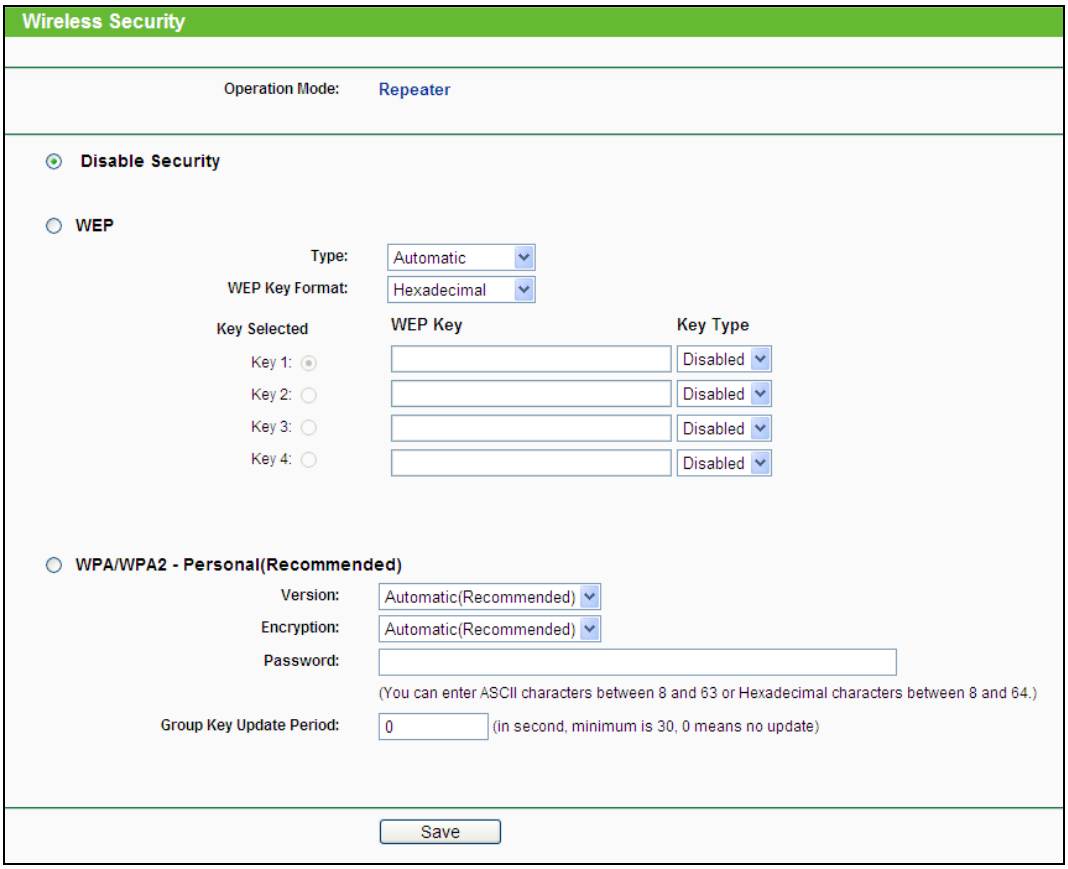


Bild 6-13 Sicherheitseinstellungen des Repeaters

- **Operation Mode -** Zeigt die aktuelle Betriebsart an.
- **Disable Security -** Hiermit können Sie verfügen, dass der AP ganz ohne Verschlüsselung arbeitet. Damit kann jeder in Reichweite sich mit dem AP verbinden. Es wird wärmstens empfohlen, dass Sie statt dieser Option eine mit Sicherheit wählen.
- **WEP -** WEP-Sicherheit nach IEEE 802.11.
  - **Type -** Der WEP-Authentifizierungstyp kann auf **Automatic** (Standard), **Open System** oder **Shared Key** eingestellt werden. **Automatic** lässt den Client den Typ auswählen.
  - **WEP Key Format** - Es können die Formate **Hexadecimal** und **ASCII** ausgewählt werden. Im Fall von **Hexadecimal** können Sie eine Folge Hexadezimalziffern (0..9, a..f) in der angegebenen Länge eingeben. Bei **ASCII**-Format können Sie alle Zeichen nehmen.
  - **WEP Key** - Wählen Sie aus, welcher der vier Schlüssel verwendet werden soll, und geben Sie den passenden WEP-Schlüssel ein. Stellen Sie sicher, dass Sie diese auf allen Geräten in Ihrem WLAN korrekt eingeben.
  - **Key Type** - Hier können Sie die WEP-Schlüssellänge (64 Bit, 128 Bit oder 152 Bit) auswählen. **Disabled** sagt aus, dass der eingegebene WEP-Schlüssel ungültig ist.
  - Bei **64-Bit**-Verschlüsselung sind 10 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 5 ASCII-Zeichen einzugeben.

- Bei **128-Bit**-Verschlüsselung sind 26 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 13 ASCII-Zeichen einzugeben.
- Bei **152-Bit**-Verschlüsselung sind 32 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 16 ASCII-Zeichen einzugeben

☞ **Bemerkung:**

Wird hier kein Schlüssel angegeben, wird die WLAN-Sicherheit nicht aktiviert, selbst wenn dies so eingestellt ist.

➢ **WPA/WPA2 – Personal (Recommended) -** WPA/WPA2-Authentifizierung, basierend auf einem Passwort. Empfohlene Einstellung.

- **Version** - WPA-PSK-Version. Die Standardeinstellung ist **Automatic**, womit entsprechend der Fähigkeiten/Anforderungen der Clients entweder mit **WPA-PSK** (Wi-Fi Protected Access) oder **WPA2-PSK** (WPA Version 2) gearbeitet wird.
- **Encryption** - Hier können Sie zwischen **Automatic**, **TKIP** und **AES** wählen.
- **PSK Passphrase** - Das Passwort kann 8 bis 63 ASCII- oder 8 bis 64 Hexadezimalzeichen lang sein.
- **Group Key Update Period** - Geben Sie die Dauer der Gültigkeit eines einzigen Gruppenschlüssels in Sekunden an. Dieser Wert sollte 0 (=deaktiviert) oder mindestens 30 betragen. Empfohlen sind Werte von 500 oder 600.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

4) Bridge with AP

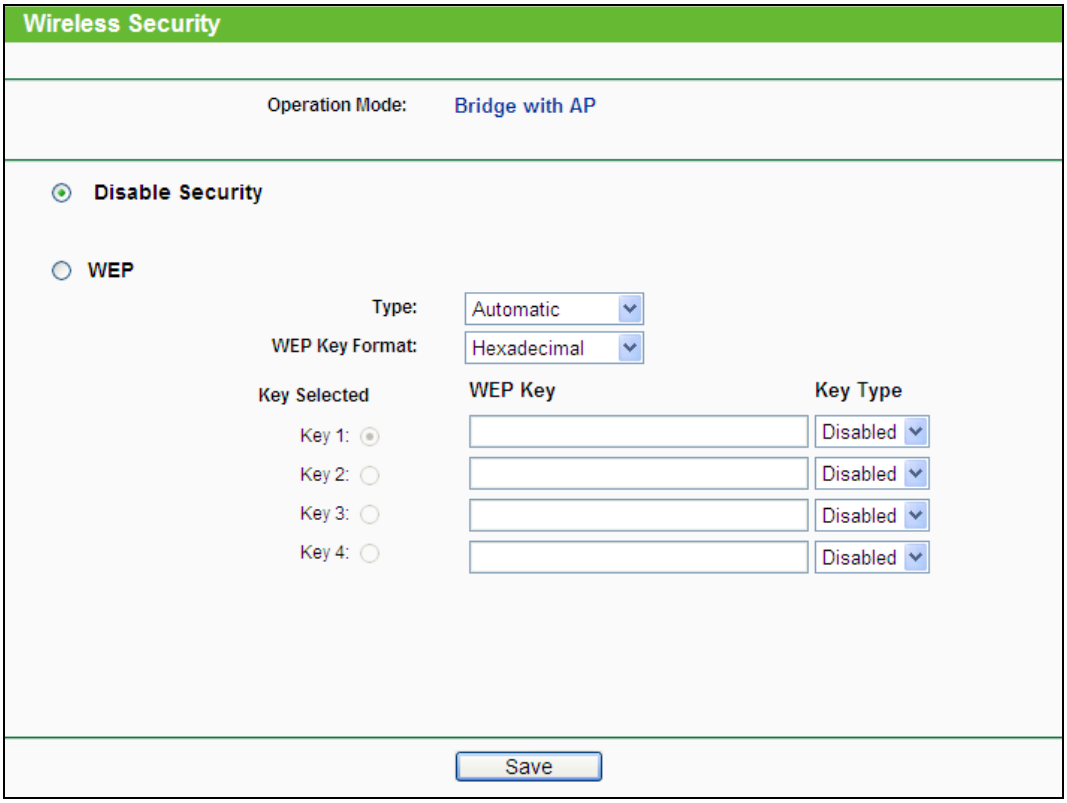


Bild 6-14 Wireless Security – Bridge with AP

- **Operation Mode -** Zeigt die aktuelle Betriebsart an.
- **Disable Security -** Hiermit können Sie verfügen, dass der AP ganz ohne Verschlüsselung arbeitet. Damit kann jeder in Reichweite sich mit dem AP verbinden. Es wird wärmstens empfohlen, dass Sie statt dieser Option eine mit Sicherheit wählen.
- **WEP** - WEP-Sicherheit nach IEEE 802.11
  - **Type -** Der WEP-Authentifizierungstyp kann auf **Automatic** (Standard), **Open System** oder **Shared Key** eingestellt werden. **Automatic** lässt den Client den Typ auswählen.
  - **WEP Key Format** - Es können die Formate **Hexadecimal** und **ASCII** ausgewählt werden. Im Fall von **Hexadecimal** können Sie eine Folge Hexadezimalziffern (0..9, a..f) in der angegebenen Länge eingeben. Bei **ASCII**-Format können Sie alle Zeichen nehmen.
  - **WEP Key** - Wählen Sie aus, welcher der vier Schlüssel verwendet werden soll, und geben Sie den passenden WEP-Schlüssel ein. Stellen Sie sicher, dass Sie diese auf allen Geräten in Ihrem WLAN korrekt eingeben.
  - **Key Type** - Hier können Sie die WEP-Schlüssellänge (64 Bit, 128 Bit oder 152 Bit) auswählen. **Disabled** sagt aus, dass der eingegebene WEP-Schlüssel ungültig ist.
  - Bei **64-Bit**-Verschlüsselung sind 10 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 5 ASCII-Zeichen einzugeben.

- Bei **128-Bit**-Verschlüsselung sind 26 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 13 ASCII-Zeichen einzugeben.
- Bei **152-Bit**-Verschlüsselung sind 32 Hexadezimalziffern (0..9 und a..f, Wert 0 ist nicht erlaubt) oder 16 ASCII-Zeichen einzugeben.

Bemerkung:

Wird hier kein Schlüssel angegeben, wird die WLAN-Sicherheit nicht aktiviert, selbst wenn dies so eingestellt ist.

Klicken Sie **Save**, um Ihre Einstellungen zu speichern.

6.5.3 Wireless MAC Filtering

Im Menü **Wireless** -> **Wireless MAC Filtering** können Sie in Abhängigkeit von der jeweiligen MAC-Adresse Filterregeln zum Limitieren des Zugriffs auf das WLAN einstellen, wie in Bild 6-15. gezeigt. Diese Funktion ist im Client-Modus nicht verfügbar. Hier wird die Betriebsart **Bridge with AP** als Beispiel genommen.

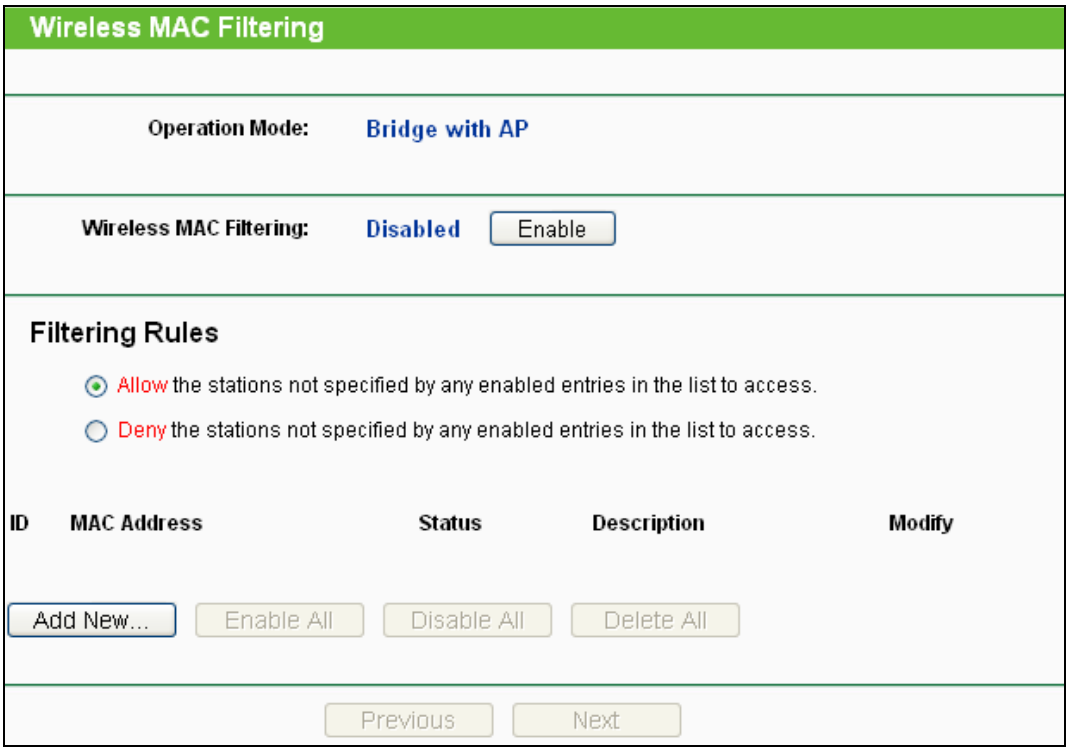


Bild 6-15 MAC-Adressfilterung

Die WLAN-MAC-Adressenfilterung erlaubt Ihnen die Kontrolle darüber, welche WLAN-Stationen (abhängig von der MAC-Adresse) sich mit Ihrem WLAN verbinden können.

- **Operation Mode -** Zeigt die aktuelle Betriebsart an.
- **Wireless MAC Filtering -** Klicken Sie **Enable**, um die MAC-Adressfilterung zu aktivieren. In den Standardeinstellungen ist diese abgeschaltet (**Disabled**).

Um einen Eintrag hinzuzufügen, klicken Sie **Add New…**. Der Dialog **Add or Modify Wireless**

MAC Address Filtering entry erscheint (Bild 6-16).

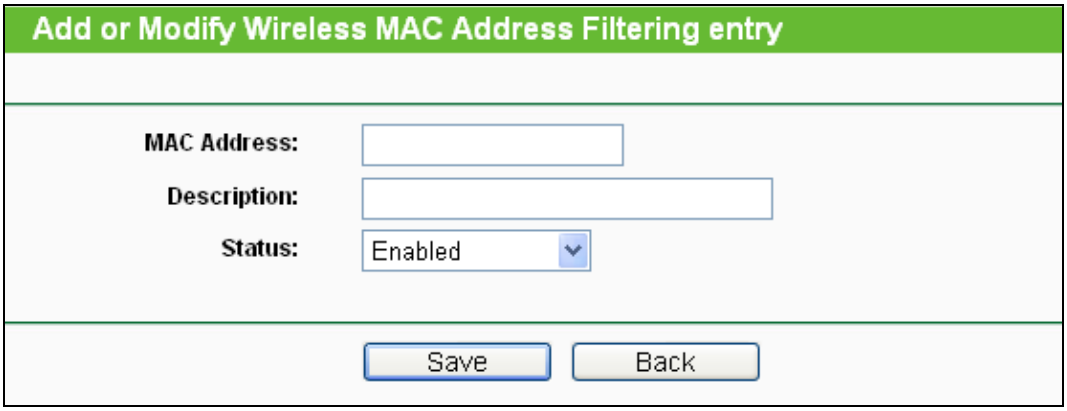


Bild 6-16 Hinzufügen oder Bearbeiten eines MAC-Adressfiltereintrags

- **MAC Address -** Die MAC-Adresse des WLAN-Gerätes, das Sie filtern möchten.
- **Status -** Der Status dieses Eintrags (**Enabled** oder **Disabled**).
- **Description -** Eine einfache Beschreibung der WLAN-Station.

Um einen neuen Eintrag anzulegen, folgen Sie bitte diesen Schritten:

Zunächst ist es wichtig, zu wissen, ob Sie eine Whitelist oder eine Blacklist anlegen möchten. Sollen die nicht angegebenen Geräte Zugriff auf das WLAN bekommen (Blacklist), markieren Sie **Allow the stations not specified by any enabled entries in the list to access**. Sollen dagegen nur die angegebenen Stationen Zugriff auf das WLAN haben können und alle anderen nicht (Whitelist), wählen Sie **Deny the stations not specified by any enabled entries in the list to access** aus.

Um einen Eintrag in der MAC-Adressfilterungsliste zu erstellen oder zu bearbeiten:

1. Geben Sie die entsprechende MAC-Adresse in das Feld **MAC Address** im Format „XX-XX-XX-XX-XX-XX“ ein („X“ repräsentiert eine Hexadezimalziffer). Beispiel: „00-0A-EB-B0-00-0B“.
2. Geben Sie eine frei wählbare Beschreibung der WLAN-Station (Bsp.: „Kurts PC“) in das Feld **Description** ein.
3. **Status - Enabled** oder **Disabled** sind auswählbar.
4. Klicken Sie **Save**, um den Eintrag zu speichern.

Um weitere Einträge hinzuzufügen, wiederholen Sie die obige Prozedur.

Um einen Eintrag zu bearbeiten oder zu löschen, tun Sie bitte Folgendes:

1. Klicken Sie für den entsprechenden Eintrag **Modify**, wenn Sie ihn bearbeiten wollen und **Delete, um ihn zu löschen.**

2. Bearbeiten Sie die Informationen, falls erforderlich.
3. Klicken Sie **Save**.

Klicken Sie **Enable All**, um alle Einträge zu aktivieren.

Klicken Sie **Disable All**, um alle Einträge zu deaktivieren.

Klicken Sie **Delete All,** um alle Einträge zu löschen.

Klicken Sie **Next**, um zur nächsten Seite zu blättern oder **Previous**, um zur vorigen Seite zurückzukehren.

Beispiel: Soll die WLAN-Station A mit der MAC-Adresse 00-0A-EB-00- 07-BE Zugriff bekommen, während alle anderen Geräte nicht in das WLAN dürfen, sollte die Filterliste folgendermaßen konfiguriert werden:

1. Klicken Sie **Enable**, um die MAC-Adressfilterung zu aktivieren.
2. Wählen Sie die Option **Deny the stations not specified by any enabled entries in the list to access** an.
3. Löschen oder deaktivieren Sie alle bereits vorhandenen Einträge der Liste. .
4. Klicken Sie **Add New...** und geben Sie die MAC-Adresse „00-0A-EB-00-07-BE“ in das Feld **MAC Address** ein und beispielsweise „Mein PC“ in das Feld **Description**. Wählen Sie als **Status Enabled**. Klicken Sie **Save**.

Die damit konfigurierten Filterregeln sollten zusammengefasst in etwa so aussehen:

ID	MAC Address	Status	Description	Modify
1	00-0A-EB-00-07-BE	Enabled	wireless station A	Modify Delete

☞ **Bemerkung:**

Ist die Option **Deny the stations not specified by any enabled entries in the list to access** bei aktiver MAC-Adressfilterung ausgewählt und in der Liste sind keine aktiven Einträge, kann überhaupt nicht auf das WLAN des Accesspoints zugegriffen werden.

6.5.4 Wireless Advanced

Im Menü **Wireless** -> **Wireless Advanced** können Sie einige erweiterte Einstellungen tätigen Bild 6-17. Da dies für die verschiedenen Betriebsarten fast identisch abläuft, wird hier der Accesspoint-Modus als Beispiel genommen.

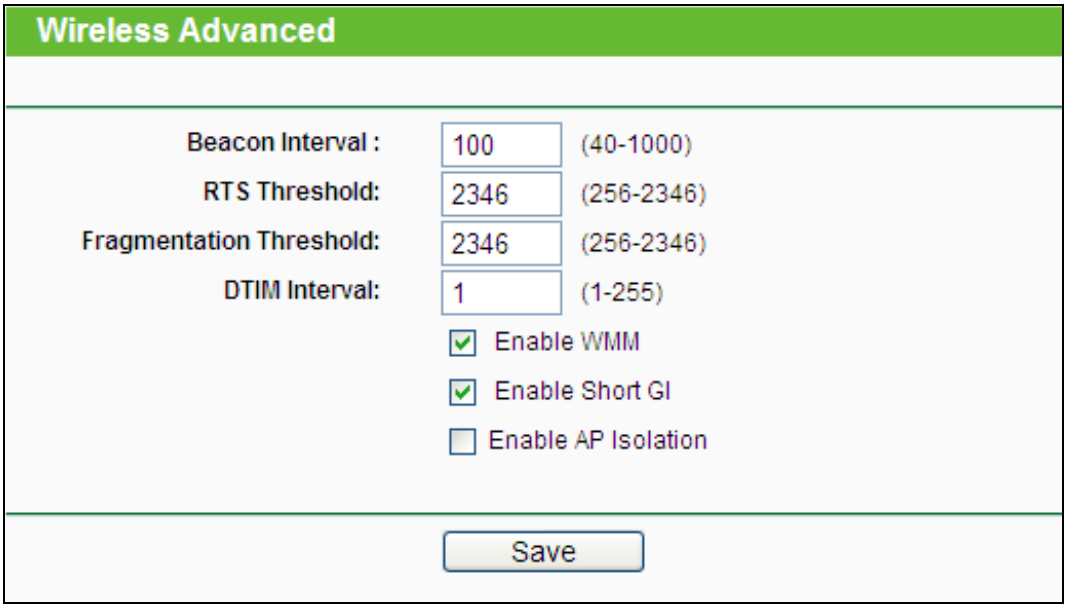


Bild 6-17 Einstellungen Wireless Advanced

- **Beacon Interval -** Geben Sie einen Wert von 20 bis 1000 (Millisek.) ein. Ortungspakete werden vom Router zur Synchronisierung des WLANs ausgesendet. Standardwert ist 100.
- **RTS Threshold -** Hier können Sie den RTS(Request to Send)-Grenzwert angeben. Ist ein Paket größer als dieser Wert, sendet der Router RTS-Frames zu einer bestimmten Empfangsstation, um den Versand eines Datenframes abzustimmen. Standardwert: 2346.
- **Fragmentation Threshold -** Dieser Wert ist die Maximalgröße, ab der Pakete fragmentiert werden. Eine zu niedrige Einstellung dieses Wertes könnte sich negativ auf die Performance auswirken. Standardwert: 2346 (empfohlen).
- **DTIM Interval -** Dieser Wert bezeichnet die Intervalllänge zwischen zwei aufeinanderfolgenden Delivery Traffic Indication Messages (DTIMs). Ein DTIM-Feld ist ein Countdown, der die Clients des nächsten Fensters anweist, auf Broadcasts und Multicasts zu hören. Hat der Router Broadcasts oder Multicasts für verbundene Clients gepuffert, sendet er den nächsten DTIM. Sie können diese Dauer in Ortungsintervallen (1..255) angeben. Standard ist 1, d.h. das DTIM-Intervall ist genauso lang wie ein Ortungsintervall.
- **Enable WMM -** WMM garantiert, dass Nachrichten hoher Priorität bevorzugt übertragen werden. Es wird wärmstens empfohlen, diese Option aktiviert zu lassen.
- **Enable Short GI -** Die Verwendung dieser Funktion wird empfohlen, da sie die Übertragungskapazitäten auf Kosten der Schutzintervallzeit vergrößert.

- **Enable AP Isolation -** Diese Funktion kann WLAN-Stationen innerhalb Ihres Netzes untereinander unsichtbar machen. Damit können Sie nur mit dem Router, aber nicht miteinander kommunizieren. AP-Isolation ist standardmäßig deaktiviert.

6.5.5 Wireless Statistics

Auf der Seite **Wireless** -> **Wireless Statistics** sehen Sie Informationen über die verbundenen drahtlosen Geräte (Bild 6-18).

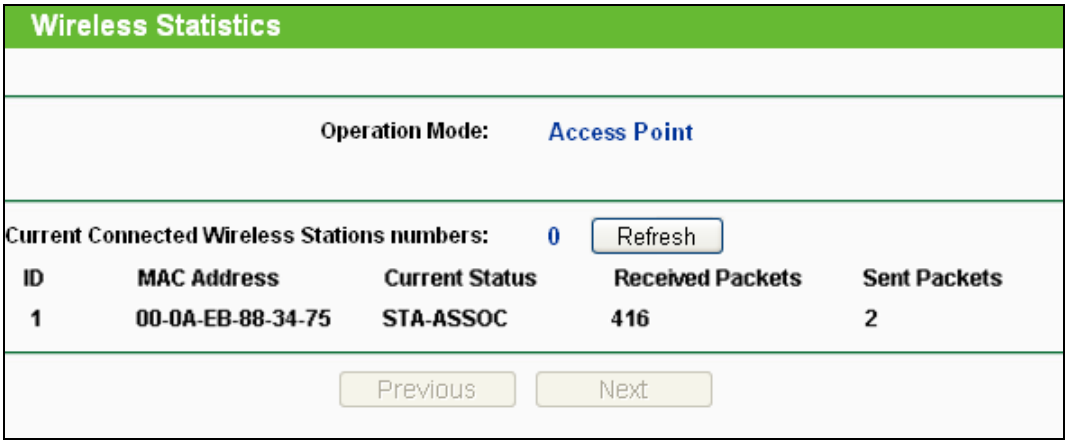


Bild 6-18 Statistiken zu den verbundenen WLAN-Stationen

- **Operation Mode -** Zeigt die aktuell aktive Betriebsart. Ist diese **Multi-SSID**, werden alle verbundenen WLAN-Geräte angezeigt.
- **MAC Address -** MAC-Adresse des Gerätes.
- **Current Status -** Status des verbundenen Gerätes: **AP-UP**, **AP-DOWN**, **STA-AUTH**, **STA-ASSOC**, **STA-JOINED**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK** oder **Disconnected**
- **Received Packets -** Durch die Station empfangene Pakete.
- **Sent Packets -** Durch die Station gesendete Pakete.

Auf dieser Seite können keine Werte geändert werden. Um die Anzeige zu aktualisieren, klicken Sie **Refresh**.

Passen alle Einträge nicht auf eine Seite, können Sie mit der Schaltfläche **Next** auf die nächste Seite wechseln und mit **Previous** auf die vorige Seite zurückkehren.

Bemerkung:

Diese Seite lädt sich alle 5 Sekunden neu.

6.6 DHCP

DHCP steht für „Dynamic Host Configuration Protocol“ (Protokoll zur dynamischen Hostkonfiguration). Der DHCP-Server vergibt Computern im LAN auf Anfrage automatisch dynamische IP-Adressen. Mit diesem Protokoll wird der Verwaltungsaufwand im Netz erheblich verringert.

Im DHCP-Menü finden Sie drei Untermenüs (Bild 6-19): **DHCP Settings**, **DHCP Clients List** und **Address Reservation**.

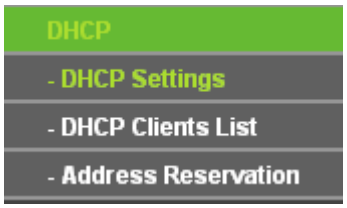


Bild 6-19 Das Menü **DHCP**

6.6.1 DHCP Settings

Im Menü **DHCP** → **DHCP Settings** können Sie den DHCP-Server konfigurieren (Bild 6-20). Der DHCP(Dynamic Host Configuration Protocol)-Server des Routers ist im AP-Modus standardmäßig inaktiv und stellt DHCP-Clients im LAN ihre TCP/IP-Konfiguration bereit.

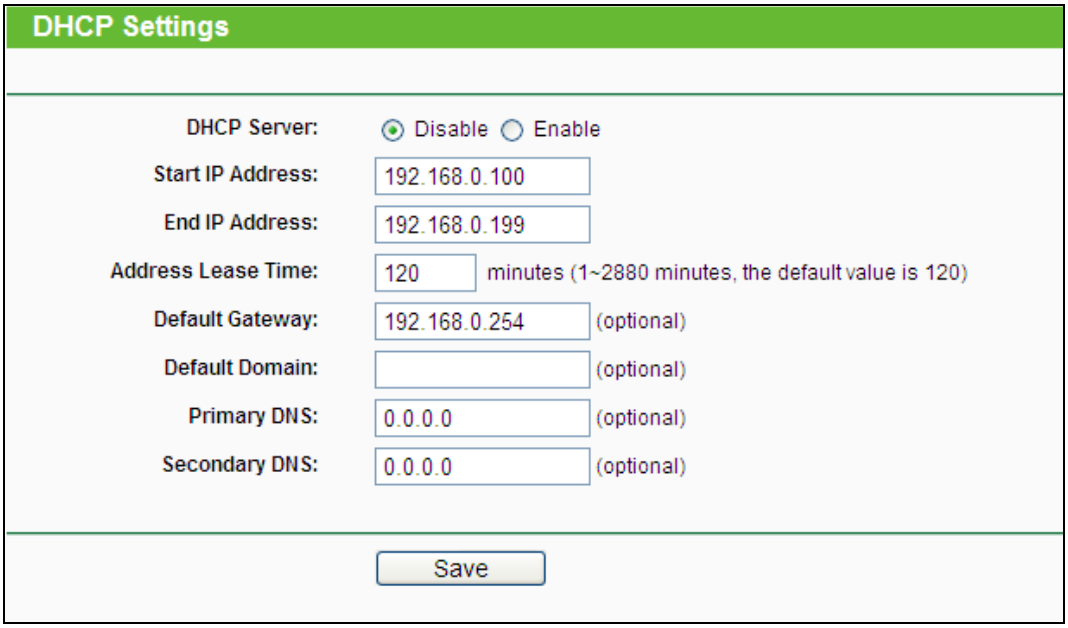


Bild 6-20 DHCP-Einstellungen

- **DHCP Server -** DHCP-Server **aktivieren** oder **deaktivieren**. Deaktivieren Sie den DHCP-Server, benötigen Sie einen anderen in Ihrem LAN oder Sie müssen die IP-Konfiguration jedes Clients in Ihrem Netz von Hand vornehmen.
- **Start IP Address -** Die erste vergebbare IP-Adresse. Standard ist 192.168.1.100.
- **End IP Address** - Die letzte IP-Adresse im Adresspool. Standard: 192.168.1.199.
- **Address Lease Time -** Die Dauer (in min.), für die ein Netzbenutzer seine IP-Konfiguration behalten darf, in Minuten. Gültig sind Werte von 1 bis 2880. Standard: 120.
- **Default Gateway (optional) -** Es wird empfohlen, hier die LAN-IP-Adresse des Routers (Standard: 192.168.1.1) einzugeben.
- **Default Domain (optional) -** Hier sollte der Domänenname Ihres Netzes eingegeben

werden.

- **Primary DNS (optional) -** Geben Sie eine von Ihrem ISP erhaltene DNS-Server-IP-Adresse ein. Sollten Sie keine erhalten haben, fragen Sie bitte nach.
- **Secondary DNS (optional) -** Geben Sie hier die eventuell von Ihrem ISP erhaltene zweite DNS-Server-IP-Adresse ein, falls vorhanden.

Klicken Sie **Save**, um die Änderungen zu speichern.

Bemerkung:

1. Ist das Gerät als DHCP-Client konfiguriert, kann der DHCP-Server nicht aktiviert werden.
2. Damit ein DHCP-Server Adressen vergeben kann, müssen die zugehörigen Computer dafür eingestellt sein: „IP-Adresse automatisch beziehen“.
3. Um die Änderungen auf dieser Seite zu übernehmen, muss der AP neugestartet werden.

6.6.2 DHCP Clients List

Unter **DHCP → DHCP Clients List** können Sie Informationen über die gerade verbundenen DHCP-Clients abfragen (Bild 6-21).

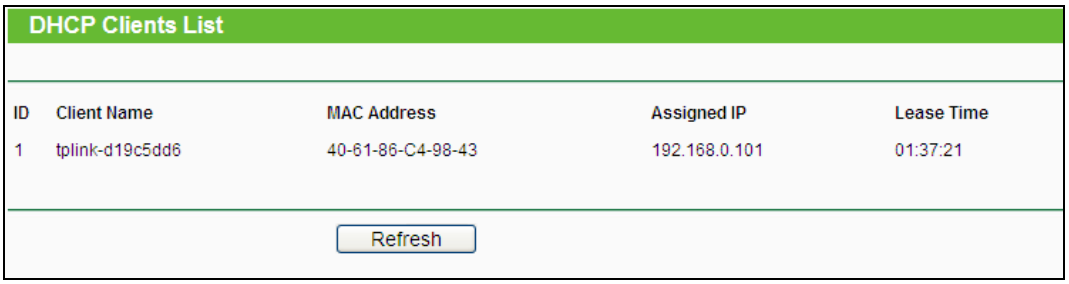


Bild 6-21 DHCP-Clientliste

- **ID -** Eine eindeutige Nummer des DHCP Clients
- **Client Name -** Name des DHCP-Clients
- **MAC Address -** MAC-Adresse des DHCP-Clients
- **Assigned IP -** Die IP-Adresse, die der Router diesem Client gegeben hat.
- **Lease Time -** Die verbleibende Zeit, die der DHCP-Client die aktuelle Konfiguration noch behalten kann. Nach Ablauf dieser Zeit bekommt dieser automatisch eine neue IP-Adresse.

Die auf dieser Seite angezeigten Werte können nicht hier direkt geändert werden. Um die Ansicht zu aktualisieren, klicken Sie **Refresh**.

6.6.3 Address Reservation

Das Menü **DHCP → Address Reservation** befasst sich mit der Reservierung von IP-Adressen für Clients (Bild 6-22). Geben Sie hier eine reservierte IP-Adresse für einen LAN-PC an, wird dieser immer diese Adresse zugeteilt bekommen. Diese Funktionalität ist hilfreich, wenn Sie

einen Server im LAN betreiben wollen.

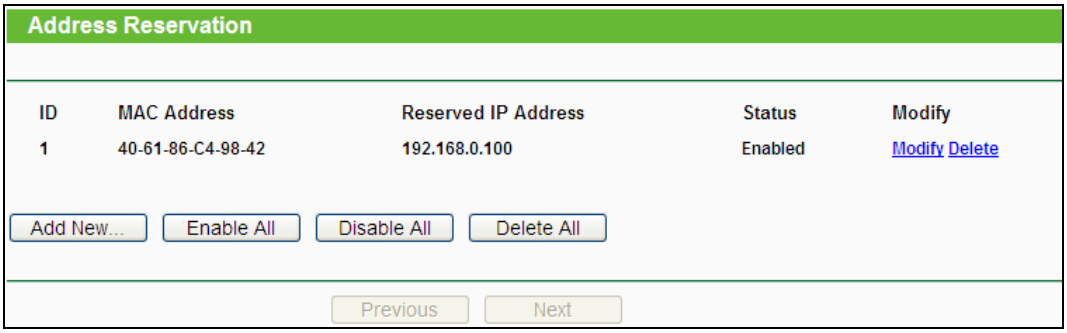


Bild 6-22 Address Reservation

- **MAC Address -** MAC-Adresse des PCs, für den Sie eine IP-Adresse reservieren möchten.
- **Assigned IP Address -** IP-Adresse, die für diesen Host reserviert wurde.
- **Status -** Status dieses Eintrags: **Enabled** (aktiv) oder **Disabled** (inaktiv
- **Modify -** Bearbeiten oder Löschen des entsprechenden Eintrages

Um IP-Adressen zu reservieren:

1. Klicken Sie **Add New…**.
2. Geben Sie die MAC-Adresse (Format „XX-XX-XX-XX-XX-XX“) und die IP-Adresse des betreffenden Computers ein.
3. Klicken Sie **Save**, wenn Sie fertig sind.

Um einen Eintrag zu bearbeiten oder zu löschen:

1. Klicken Sie für den zu bearbeitenden Eintrag. Klicken Sie **Delete**, wenn Sie ihn löschen möchten.
2. Bearbeiten Sie die Informationen, wie gewünscht.
3. Klicken Sie **Save**.

Klicken Sie **Enable All/Disable All**, um alle Einträge zu (de)aktivieren.

Klicken Sie **Delete All**, um alle Einträge zu löschen.

Klicken Sie **Next**, um auf die nächste Seite zu blättern oder **Previous**, um auf die vorige Seite zurückzukehren.

6.7 System Tools

Das Menü **System Tools** erlaubt Ihnen die Optimierung der Gerätekonfiguration. Mittels SNMP können Sie das Gerät auch aus der Ferne überwachen. Diagnosetools (Ping und Traceroute) ermöglichen Ihnen Fehlerdiagnose auf der Leitung zu den angeschlossenen Geräten. Der AP kann hier auch auf den neuesten Firmwarestand gebracht und die Gerätekonfiguration gesichert und wiederhergestellt werden. Der **Ping Watch Dog** ist in der Lage, ein bestimmtes Ziel über längere Zeit anzupingen. Hier können Sie auch die Zugangsdaten zum AP ändern.

Dies wird wärmstens empfohlen, damit Unbefugte nichts an der Konfiguration ändern können. Darüber hinaus können Sie das Systemprotokoll einsehen.

Das Menü **System Tools** verfügt über zehn Untermenüs (Bild 6-23): **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults**, **Backup & Restore**, **Reboot**, **Password**, **System Log**, **Working Mode** und **Statistics**.

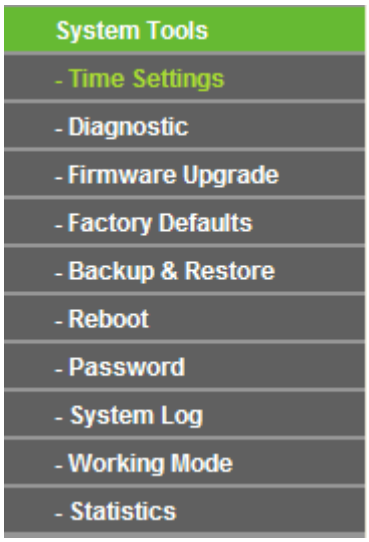


Bild 6-23 Das Menü **System Tools**

6.7.1 Time Setting

Im Menü **System Tools** → **Time Settings** können Sie die Echtzeituhr des Routers von Hand oder mittels der aus dem Internet abgefragten GMT einstellen.

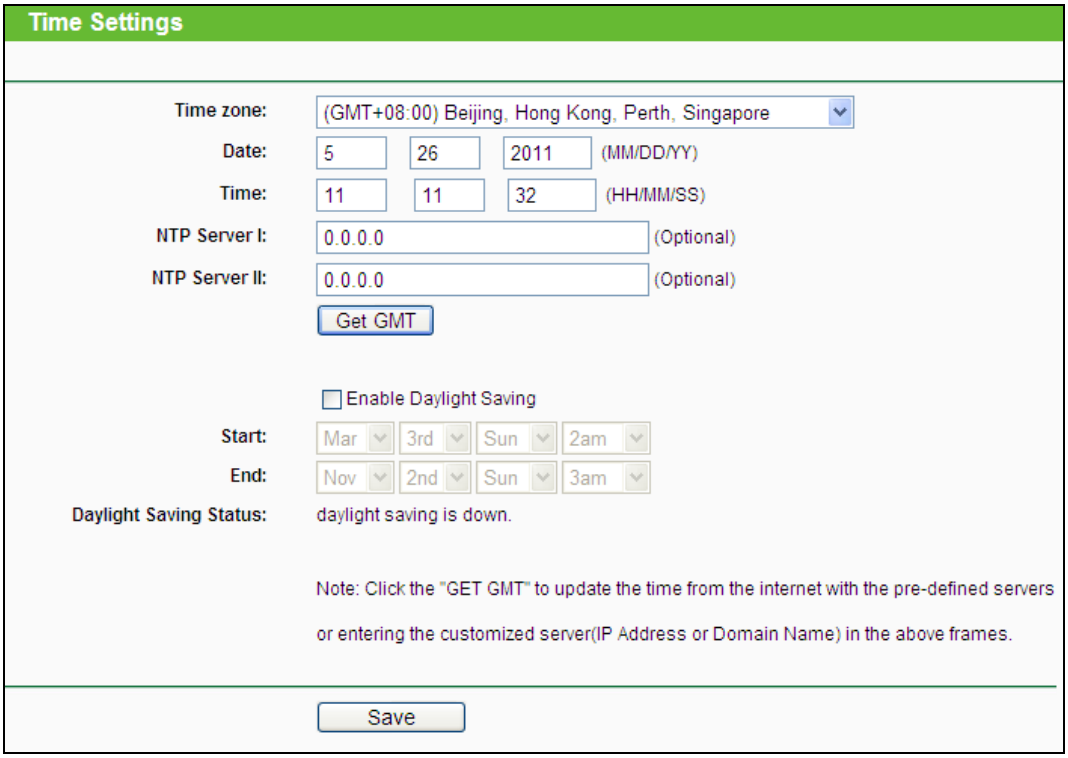


Bild 6-24 Zeiteinstellungen

- **Time Zone -** Wählen Sie hier die Zeitzone aus, in der der Router steht.
- **Date -** Geben Sie das aktuelle Datum im Format „MM/TT/JJJJ“ ein.
- **Time -** Geben Sie die aktuelle Uhrzeit im Format „hh/mm/ss“ ein.
- **NTP Server I/II -** Geben Sie hier die Adresse eines NTP-Servers oder zweier NTP-Server ein, wird der Router von diesem die Uhrzeit abfragen, sobald er eine Internetverbindung hergestellt hat. Zusätzlich zu diesem konfigurierbaren sind einige weitere NTP-Server in der Routersoftware hart kodiert, so dass er auch von diesen die Uhrzeit automatisch abfragen kann.
- **Enable Daylight Saving -** Hiermit beachtet der Router die weiter unten definierte Sommerzeitregelung.
- **Start -** Beginn der Sommerzeit. Wählen Sie nacheinander Monat, Woche, Tag und Stunde.
- **End -** Ende der Sommerzeit. Wählen Sie nacheinander Monat, Woche, Tag und Stunde.
- **Daylight Saving Status -** Zeigt an, ob die Sommerzeit gerade aktiv ist.

Die Zeit können Sie auch von Hand mit folgenden Schritten einstellen:

1. Wählen Sie die zutreffende Zeitzone aus.
2. Geben Sie das Datum (als **Date**) im Format „MM/TT/JJJJ“ und die aktuelle Uhrzeit (als **Time**) im Format „HH/MM/SS“ ein.
3. Klicken Sie **Save**.

Zur automatischen Zeiteinstellung konfigurieren Sie Ihren Router bitte so:

1. Wählen Sie die zutreffende Zeitzone aus.
2. Geben Sie unter **NTP Server I** oder **NTP Server II** eine oder zwei NTP-Server-Adressen ein.
3. Klicken Sie **Get GMT**, um die GMT bei bestehender Internetverbindung abzurufen.

Zur automatischen Umstellung zwischen Sommer- und Winterzeit tun Sie dies:

1. Aktivieren Sie Sommerzeit (**Enable Daylight Saving**).
2. Wählen Sie den **Start**- und den **End**zeitpunkt der Sommerzeit aus.
3. Klicken Sie **Save**.

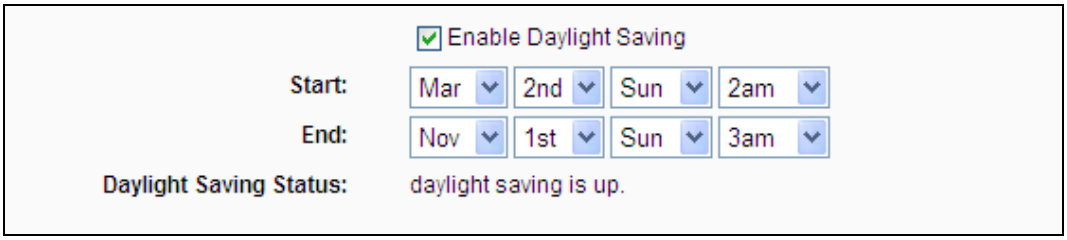


Bild 6-25 Sommerzeiteinstellungen

Bemerkungen:

1) Diese Einstellung beeinflusst einige zeitbasierende Funktionen wie z.B. die Firewall.

Hierfür müssen die Uhrzeit und die Zeitzone zwingend gesetzt werden.

2) Die Uhrzeit geht verloren, wenn die Spannungsversorgung getrennt wird.
3) Der Router setzt die Systemzeit automatisch, wenn er eine Internetverbindung bekommt und entsprechend konfiguriert ist.
4) Es dauert nach dem Speichern ca. eine Minute, bis die Sommerzeiteinstellung wirksam wird.

6.7.2 Diagnostic

Das Menü **System Tools** → **Diagnostic** erlaubt die Ausführung von Ping- und Traceroute-Befehlen zur Überprüfung der Konnektivität.

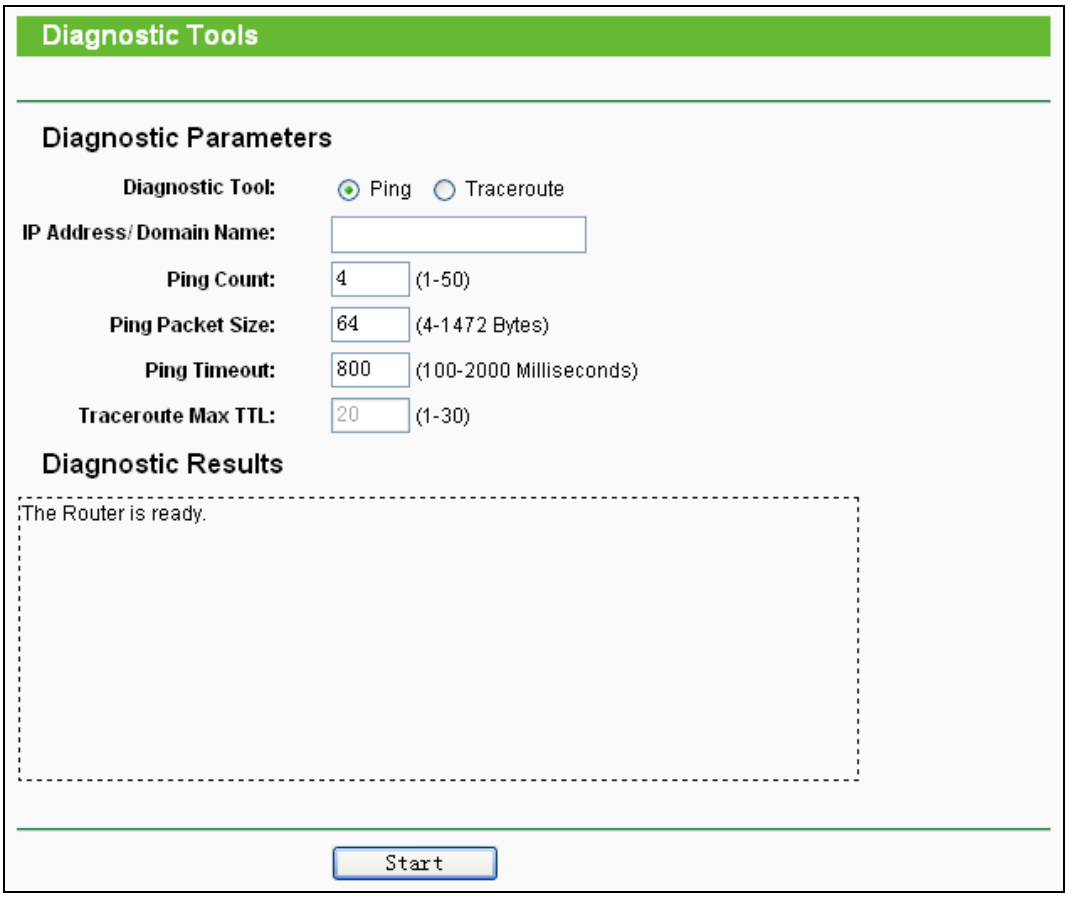


Bild 6-26 Diagnostic Tools

- **Diagnostic Tool** - Wählen Sie zwischen **Ping** und **Traceroute**.
- **Ping** - Hiermit können Sie die Konnektivität, die Erreichbarkeit und die Namensauflösung für einen gegebenen Host testen.
- **Traceroute** - Dieses Tool ist in der Lage, die Performance der verschiedenen Verbindungsabschnitte zu testen.

Bemerkung:

Ping und Traceroute akzeptieren sowohl IP-Adressen als auch Domänennamen. Können Sie eines der Tools für eine IP-Adresse erfolgreich laufen lassen, für einen Domänennamen aber nicht, deutet dies darauf hin, dass die Namensauflösung (DNS) nicht funktioniert.

- **IP Address/Domain Name** - Geben Sie das Ziel als IP-Adresse (z.B. 202.108.22.5) oder als Domänenname (z.B. www.tp-link.com) an.
- **Pings Count -** Die Anzahl der zu sendenden Ping-Pakete. Standard: 4.
- **Ping Packet Size -** Die Größe eines Pingpakets. Standard: 64.
- **Ping Timeout -** Setzen Sie hier die Wartezeit für ein Pingpaket. Kommt innerhalb dieser Zeit keine Antwort, gilt der Ping als fehlgeschlagen. Standard: 800.
- **Traceroute Max TTL -** Die maximale Knotenanzahl (Hops) für eine Traceroute-Verbindung. Standardwert: 20.

Klicken Sie **Start**, um die Konnektivität zu testen.

Der Abschnitt **Diagnostic Results** zeigt die Ergebnisse der Diagnose an. Bei einem Ergebnis ähnlich wie diesem ist die Internetkonnektivität gut.

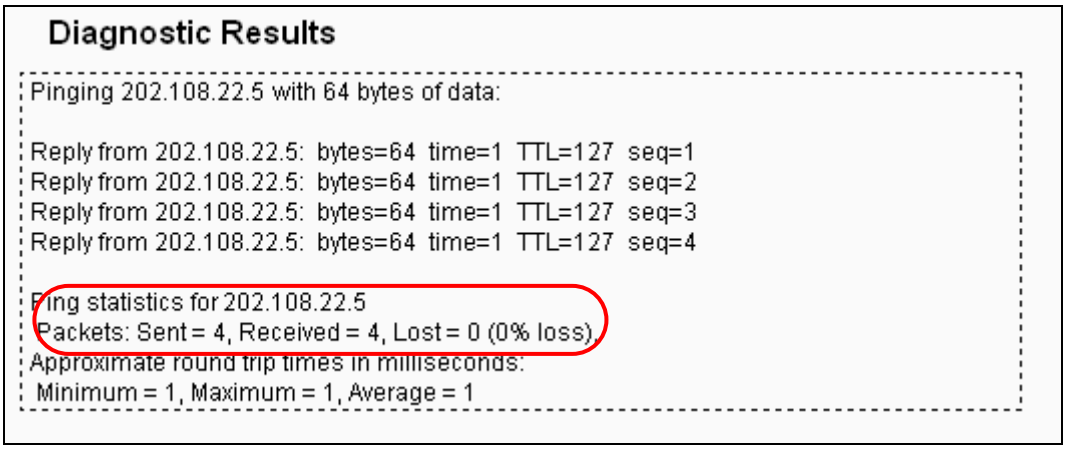


Bild 6-27 Diagnoseergebnisse

Bemerkung:

Diese Tools können nur von einem Computer aus zur gleichen Zeit gestartet werden. Die Optionen **Ping Count**, **Ping Packet Size** und **Ping Timeout** werden von der **Ping**-Funktion verwendet, während **Traceroute Max TTL** von der **Traceroute**-Funktion genutzt wird.

6.7.3 Firmware Upgrade

Diese Seite erlaubt Firmwareupgrades, um Ihren Router aktuell zu halten.

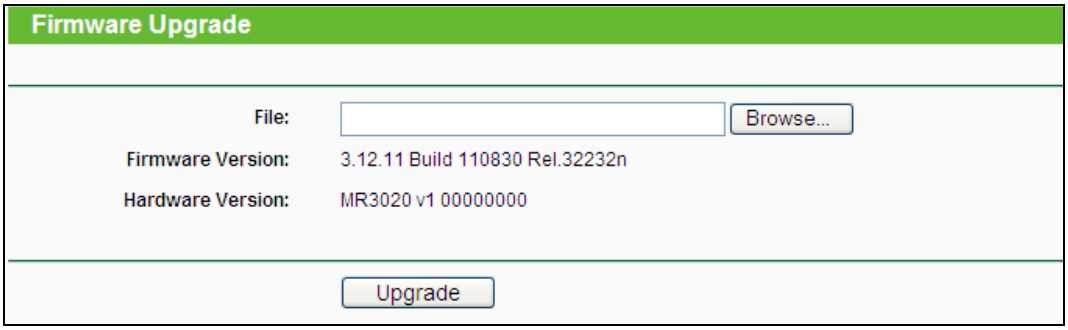


Bild 6-28 Firmware Upgrade

- **Firmware Version -** Zeigt Ihnen die aktuell installierte Firmwareversion.

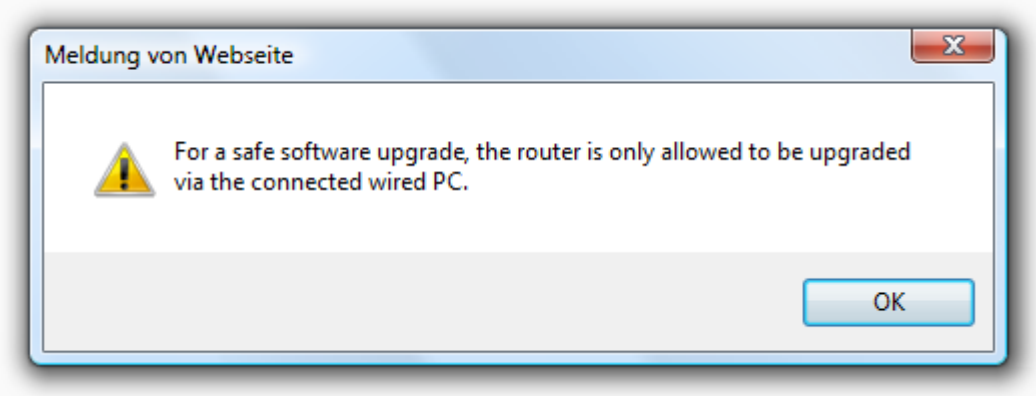
- **Hardware Version -** Zeigt Ihnen die aktuelle Hardwareversion. Diese muss unbedingt mit der Hardwareversion der Update-Datei übereinstimmen.

Um die Firmware zu aktualisieren, gehen Sie so vor:

1. Laden Sie sich eine Firmwaredatei für Ihr Modell von der TP-LINK-Webseite **www.tp-link.com** herunter und entpacken Sie sie.
2. Verbinden Sie sich mit dem Router über eine Kabelverbindung, nicht über WLAN. Klicken Sie im Webinterface **Durchsuchen**, um die heruntergeladene Datei auszuwählen.
3. Klicken Sie **Upgrade**.
4. Der Router verarbeitet die Datei und startet anschließend neu.

Bemerkungen:

1) Führen Sie das Upgrade nie über eine WLAN-Verbindung durch, sondern nur über Kabel. Beim Versuch eines Upgrades über WLAN erscheint diese Meldung:



2) Neue Firmware ist auf **www.tp-link.com** zu finden und kann kostenlos heruntergeladen werden. Haben Sie mit dem Router keine Probleme und bietet die neue Firmware keine unbedingt benötigten neuen Funktionalitäten, brauchen Sie die Firmware nicht zwingend zu aktualisieren.

3) Beim Firmwareupgrade kann Ihre aktuelle Konfiguration verloren gehen. Stellen Sie also sicher, dass Sie sie in einer Datei gespeichert haben, bevor Sie mit dem Upgrade beginnen.

4) Während des Firmwareupgrades darf der Router keinesfalls von der Versorgungsspannung getrennt oder mittels der Reset-Taste zurückgesetzt werden.

5) Beachten Sie die Hardwareversion der Firmwaredatei. Diese muss unbedingt mit der Hardwareversion des Routers identisch sein.

6) Nach erfolgreichem Upgrade (nach wenigen Minuten) startet der Router automatisch neu.

6.7.4 Factory Defaults

Die Seite **System Tools** → **Factory Defaults** ermöglicht das Wiederherstellen der Standardeinstellungen des Routers.

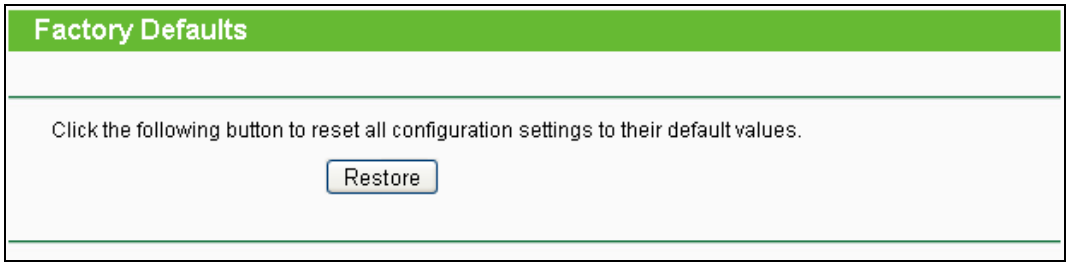


Bild 6-29 Standardeinstellungen wiederherstellen

Klicken Sie **Restore**, um alle Einstellungen zurückzusetzen. Danach gelten:

- Benutzername (**User Name**): admin
- Passwort (**Password**): admin
- IP-Adresse (**IP Address**): 192.168.0.254
- Subnetzmaske (**Subnet Mask**): 255.255.255.0

Bemerkung:

Hierbei gehen prinzipbedingt alle im Router gespeicherten Einstellungen verloren.

6.7.5 Backup & Restore

Unter **System Tools** → **Backup & Restore** können Sie die Routerkonfiguration lokal speichern sowie eine zuvor gespeicherte Konfiguration wiederherstellen (Bild 6-30).

Bild 6-30 Konfiguration sichern und wiederherstellen

- Klicken Sie **Backup**, um die aktuelle Konfiguration herunterzuladen und lokal zu speichern.
- Um eine alte Konfiguration wiederherzustellen, tun Sie Folgendes.
  - Klicken Sie **Durchsuchen**, um die Backup-Datei auszuwählen.
  - Klicken Sie **Restore**.

Bemerkung:

Beim Wiederherstellungsprozess geht die aktuell im Router befindliche Konfiguration verloren. Der Prozess dauert ca. 20 Sekunden. Anschließend startet der Router neu. Bitte lassen Sie den Router während der Wiederherstellung eingeschaltet, um Schäden zu vermeiden.

6.7.6 Reboot

Unter **System Tools** → **Reboot** können Sie durch Klick auf **Reboot** den Router neustarten.

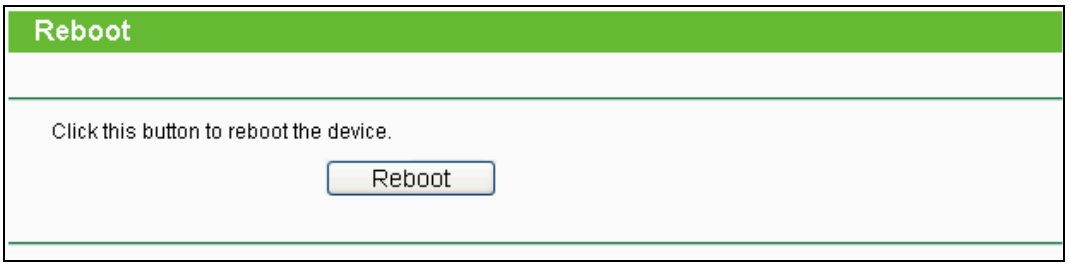


Bild 6-31 Routerneustart

Einige Einstellungen des Routers können nur durch einen Neustart übernommen werden:

- Ändern der LAN-IP-Adresse (der Router startet automatisch neu).
- DHCP-Konfigurationsänderungen.
- Änderungen an der Drahtloskonfiguration.
- Ändern des Ports für die Fernwartung.
- Firmwareupgrade (der Router startet automatisch neu).
- Zurücksetzen der Routereinstellungen (der Router startet automatisch neu).
- Wiederherstellen einer alten Konfiguration mittels Dateiupload (der Router startet automatisch neu).

6.7.7 Password

Auf **System Tools** → **Password** können Sie die Router-Zugangsdaten ändern (Bild 6-32).

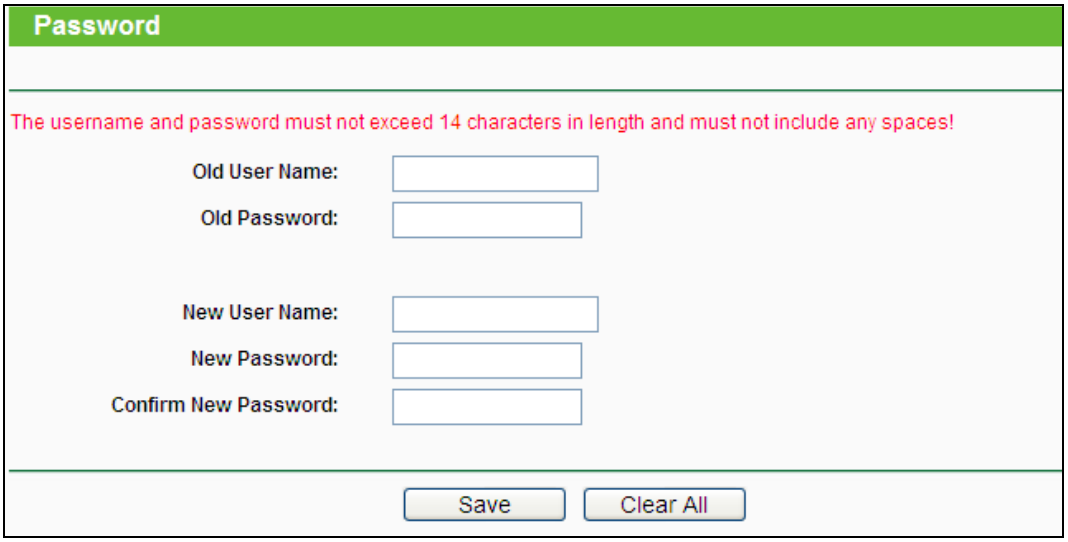


Bild 6-32 Password

Es wird empfohlen, die Zugangsdaten abzuändern. Diese werden von alle Benutzern abgefragt, die versuchen, auf das webbasierende Konfigurationstool zuzugreifen.

Bemerkung:

Benutzername und Passwort dürfen nicht länger als jeweils 14 Zeichen sein und keine Leerzeichen enthalten. Um Tippfehler auszuschließen, muss das Passwort zweimal eingegeben werden.

Klicken Sie **Save**, wenn Sie die Daten eingegeben haben.

Klicken Sie **Clear All,** um die Feldinhalte zu löschen.

6.7.8 System Log

Über die Seite **System Tools** → **System Log** können Sie die Routerprotokolle abfragen.

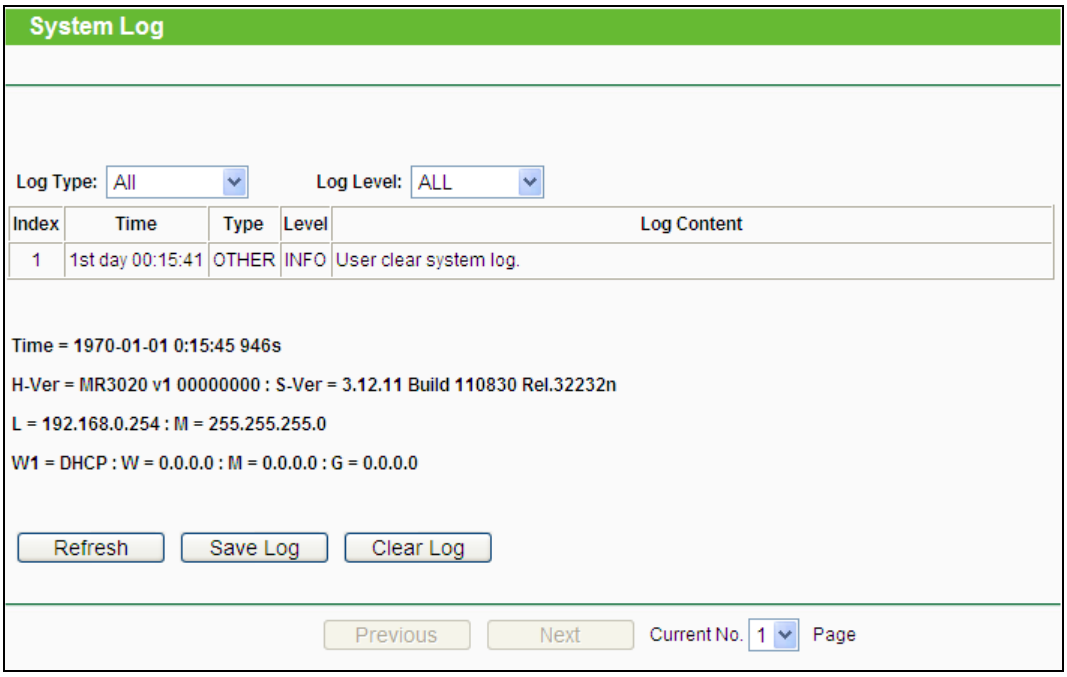


Bild 6-33 Systemprotokoll

- **Log Type -** Filtern nach Protokolltyp (PPP, Wireless, …).
- **Log Level -** Filtern nach Protokollebene (Fehler, Warnung, …).
- **Refresh -** Ansicht aktualisieren.
- **Save Log -** Protokoll als Textdatei lokal speichern.
- **Mail Log -** Klicken Sie hier, um das Protokoll gemäß den Maileinstellungen per E-Mail zu verschicken.
- **Clear Log -** Endgültiges Löschen der Protokolle aus dem Router.

Klicken Sie **Next**, um zur nächsten Seite zu gehen oder **Previous**, um auf die vorige Seite zurückzukehren.

6.7.9 Working Mode

Über die Seite **System Tools** → **Working Mode** können Sie die Router-Betriebsart einstellen.

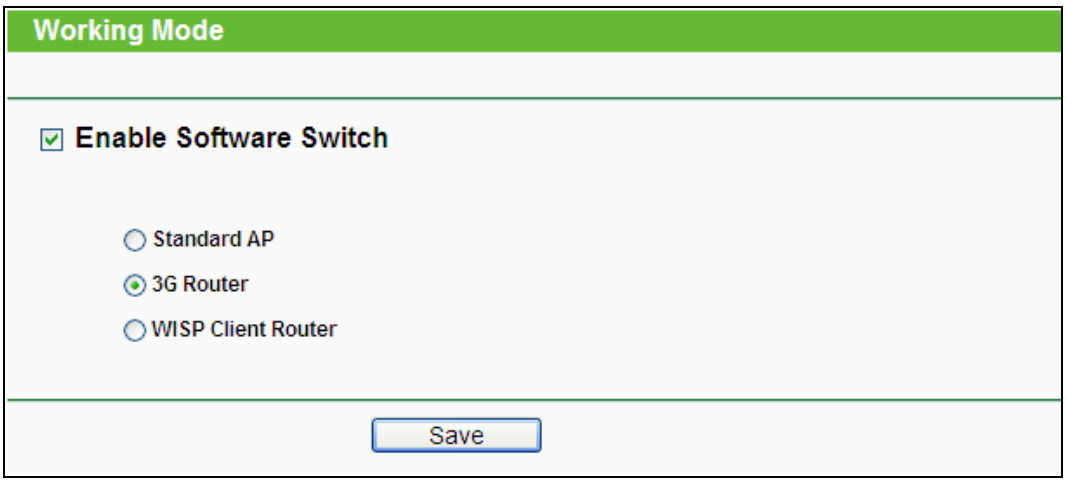


Bild 6-34 Working Mode

- **Standard AP -** Dieser Modus erlaubt es drahtlosen Geräten, sich mit dem AP zu verbinden. Als Accesspoint sendet das Gerät ein eigenes WLAN aus.
- **3G Router -** Dieser Modus erlaubt es mehreren Usern, eine Verbindung zum Internet über ADSL/Kabelmodem aufzubauen.
- **WISP Client Router -** Dieser Modus erlaubt es mehreren Usern eine Verbindung zum Internet über einen WISP aufzubauen.

☞ **Bemerkung:**

Der Router startet automatisch neu, wenn Sie auf **Save** klicken.

6.7.10 Statistics

Unter **System Tools** → **Statistics** können Sie die Routerstatistiken einsehen. Diese umfassen: Gesamtdatenverkehr und Datenverkehr während des letzten „Packet Statistics Interval“.

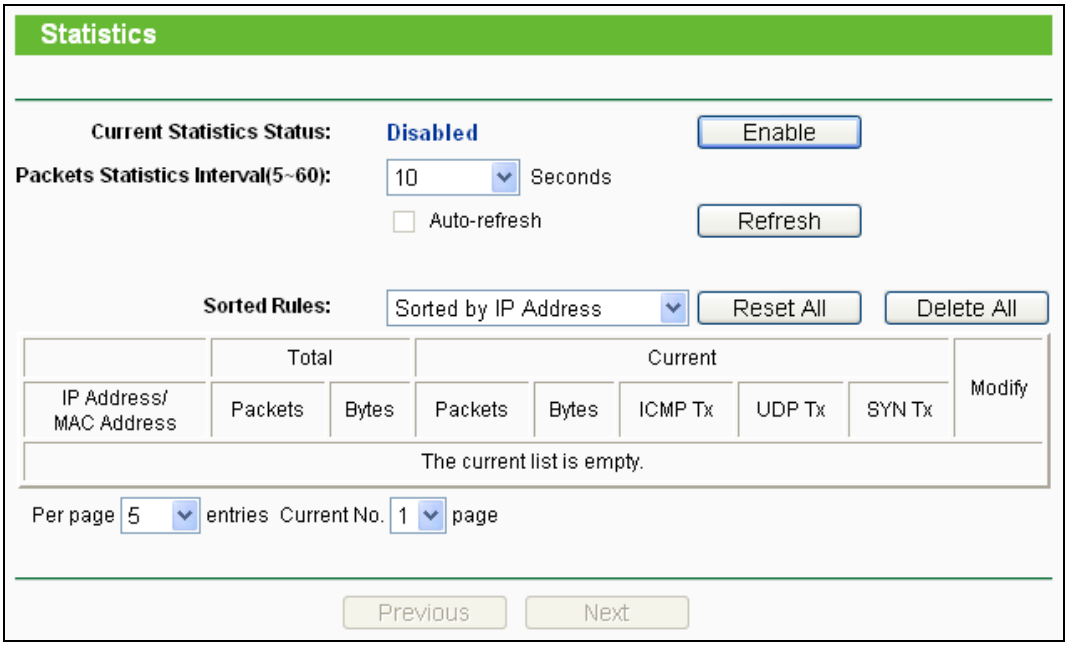


Bild 6-35 Statistiken

- **Current Statistics Status -** Kann hier aktiviert oder deaktiviert werden.
- **Packets Statistics Interval(5~60) -** Die Dauer eines Zeitabschnittes, den eine Paketstatistik geführt wird, in Sekunden. Standardwert ist 10. Gültige Werte sind von 5 bis 60.
- **Sorted Rules -** Hiermit können Sie die Regeln nach Ihren Vorstellungen ordnen.

Aktivieren Sie **Auto-refresh**, um die Ansicht periodisch neu zu laden.

Klicken Sie **Refresh**, um die Ansicht sofort zu aktualisieren.

Klicken Sie **Reset All**, um alle Werte auf null zu setzen.

Klicken Sie **Delete All,** um alle Einträge aus der Tabelle zu entfernen.

Statistiktabelle:

IP/MAC Address		Die IP-/MAC-Adresse, zu der diese Statistiken gehören.
Total	**Packets**	Gesamtanzahl der vom Router übertragenen Pakete.
	Bytes	Vom Router übertragene Gesamtdatenmenge.
Current	**Packets**	Anzahl übertragener Pakete während des letzten Paketstatistikintervalls.
	Bytes	Während des letzten Paketstatistikintervalls übertragene Datenmenge.
	ICMP Tx	Anzahl zum WAN-Port gesendeter ICMP-Pakete während des letzten Paketstatistikintervalls.
	UDP Tx	Anzahl zum WAN-Port gesendeter UDP-Pakete während des letzten Paketstatistikintervalls.
	TCP SYN Tx	Anzahl zum WAN-Port gesendeter TCP-SYN-Pakete während des letzten Paketstatistikintervalls.
Modify	**Reset**	Wert des Eintrags auf Null zurücksetzen.
	Delete	Diesen Eintrag aus der Tabelle löschen.

Standardmäßig sind 5 Einträge pro Seite zu sehen. Klicken Sie **Next**, um zur nächsten Seite zu blättern oder **Previous**, um zur vorigen Seite zurückzukehren.

Anhang A: FAQ

1. Wie kann ich den Router für den Internetzugang über ADSL konfigurieren?

1) Konfigurieren Sie Ihr ADSL-Modem entsprechend des Bridge-Modells RFC1483.

2) Verbinden Sie Ihr ADSL-Modem mittels eines Ethernet-Kabels mit dem WAN-Port des Routers. Stecken Sie das Telefonkabel in den Line-Port des ADSL-Modems.

3) Loggen Sie sich in den Router ein und navigieren Sie zum Menü **Network** (siehe linke Seite der angezeigten Webseite). Klicken Sie hier auf **WAN**. Auf der WAN-Seite wählen Sie „PPPoE" als WAN-Verbindungstyp aus. Geben Sie einen Benutzernamen und ein Passwort ein und klicken Sie dann **Connect**.

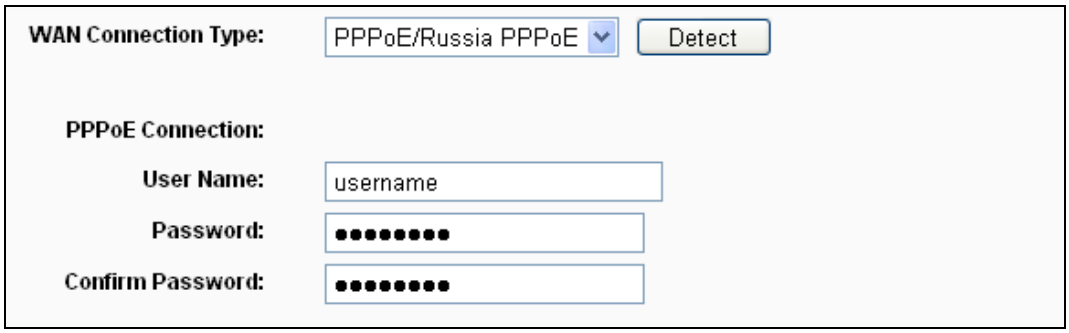


Bild A-1 PPPoE-Verbindungstyp

4) Haben Sie einen DSL-Zeitvertrag, sollten Sie **Verbinden bei Bedarf** oder **Manuell verbinden** benutzen. Geben Sie als **Max Idle Time** eine angemessene Zeitspanne ein, um nicht unnötig für ungenutzte Zeit zahlen zu müssen. Ansonsten können Sie **Connect Automatically** auswählen.

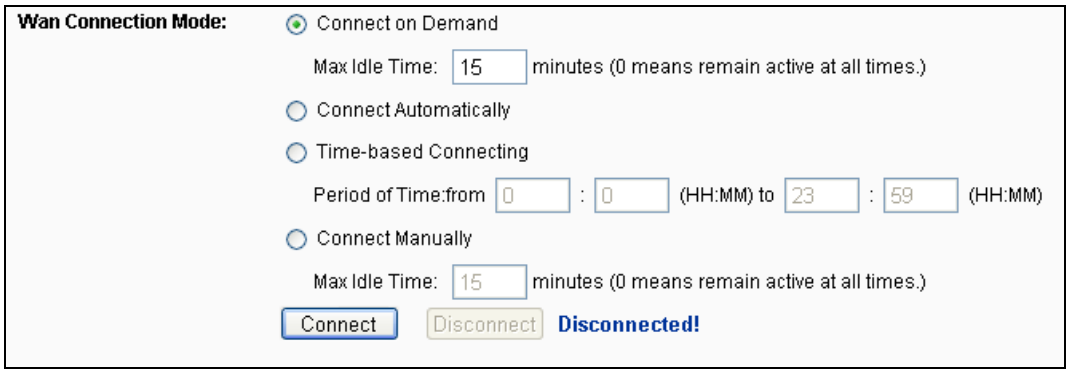


Bild A-2 PPPoE-Verbindungsmodus

☞ **Bemerkungen:**

1) Die Verbindung wird unter Umständen nach Ablauf der **Max Idle Time** nicht getrennt, nämlich dann, wenn einige Applikationen im Hintergrund Datenverkehr erzeugen.
2) Als Kabelmodembenutzer konfigurieren Sie Ihren Router bitte nach obigem Punkt 2.

2. Wie konfiguriere ich den Router für Internetzugang über Ethernet?

1) Loggen Sie sich in den Router ein und navigieren Sie zum Menü (siehe linke Seite der angezeigten Webseite). Klicken Sie hier auf **WAN**. Auf der WAN-Seite wählen Sie **Dynamic IP** als **WAN Connection Type** und klicken Sie **Save**.

2) Einige ISPs verlangen eine Registrierung der MAC-Adresse Ihres Adapters, der während der Installation mit dem Kabel-/DSL-Modem verbunden ist. Ist dies bei Ihnen der Fall, loggen Sie sich in den Router ein und rufen Sie das Menü **Network** auf. Klicken Sie auf **Clone MAC Address**. Auf dieser Seite (sofern Sie an dem entsprechenden PC sitzen) klicken Sie **Clone MAC Address**. Die MAC-Adresse Ihres PCs wird in das Feld **WAN MAC Address** kopiert. Falls nicht, geben Sie sie bitte von Hand ein. Format: „XX-XX-XX-XX-XX-XX“. Klicken Sie dann **Save**. Die neue MAC-Adresse gilt ab dem nächsten Routerstart.

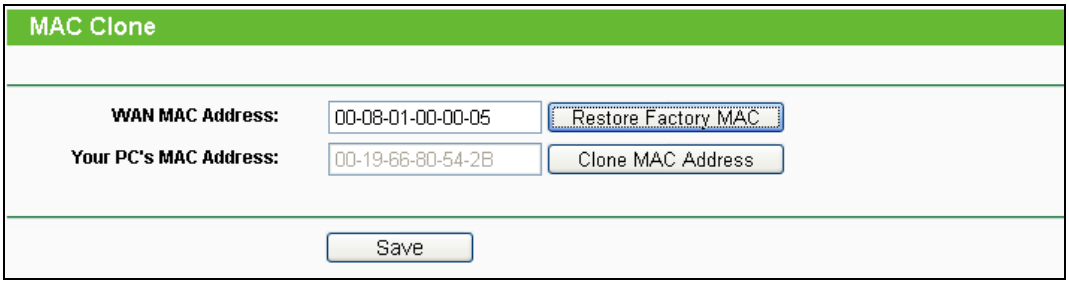


Bild A-3 MAC-Adresse klonen

3. Ich muss mit NetMeeting arbeiten. Was ist zu tun?

1) Sind Sie in der Rolle des NetMeeting-Hosts, braucht der Router nicht speziell dafür konfiguriert werden.

2) Wurden Sie eingeladen, müssen Sie entweder einen Virtuellen Server oder einen DMZ-Host einrichten und sicherstellen, dass das H323-ALG aktiv ist.

3) Wie man einen Virtuellen Server einrichtet: Loggen Sie sich in den Router ein und klicken Sie links in dem Navigationsframe **Forwarding**. Auf der Seite **Virtual Servers** klicken Sie **Add New…** und geben Sie „1720” als **Service Port** und Ihre IP-Adresse als **IP Address** ein, z.B. 192.168.1.169. Betätigen Sie **Save** mit **Status** auf „Aktiviert“.

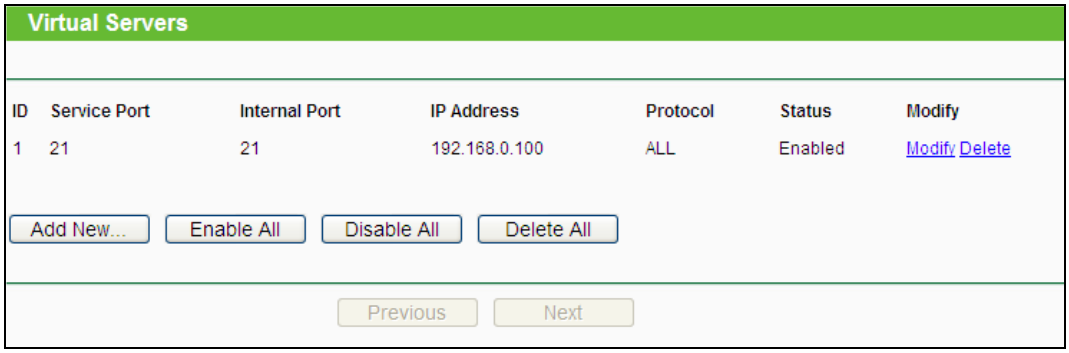


Bild A-4 Virtuelle Server

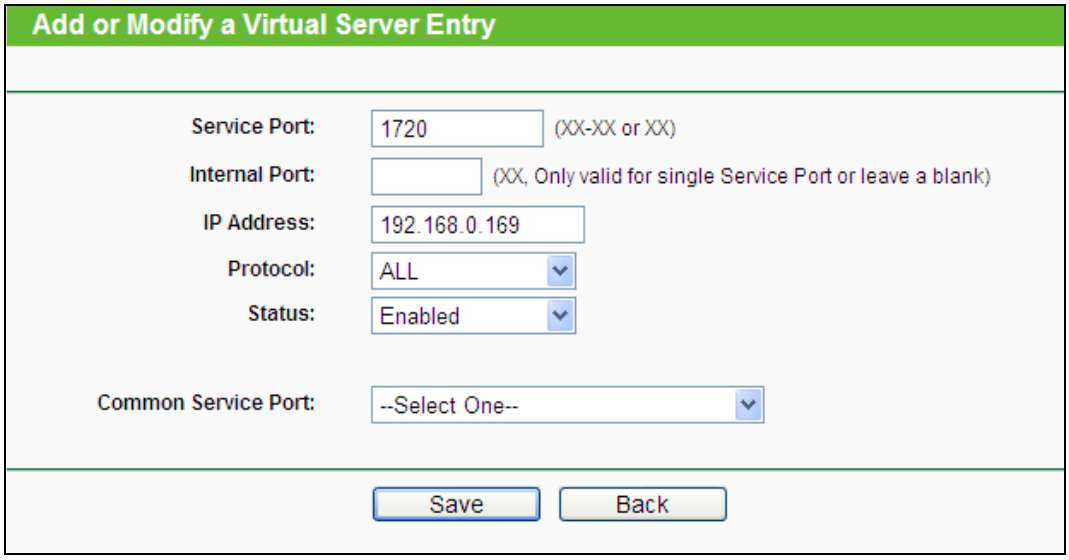


Bild A-5 Virtuellen Server hinzufügen oder bearbeiten

☞ **Bemerkung:**

Ihr NetMeeting-Partner muss Ihre auf der Statusseite zu findende WAN-IP-Adresse anrufen.

4) Wie man einen DMZ-Host aktiviert: Loggen Sie sich in den Router ein und klicken Sie klicken Sie links in dem Navigationsframe **Forwarding** und dann **DMZ** an. Auf der Seite **DMZ** klicken Sie **Enable** an und geben Sie Ihre IP-Adresse in das Feld **DMZ Host IP Address** ein, z.B. 192.168.1.169. Klicken Sie dann **Save**.

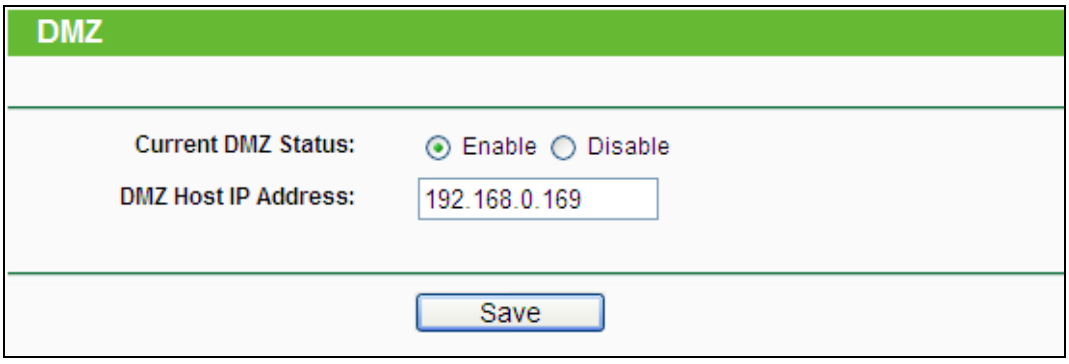


Bild A-6 DMZ

5) Wie der H323-ALG aktiviert wird: Loggen Sie sich in den Router ein und klicken Sie im Menü **Security** auf **Basic Security**. Auf dieser Seite aktivieren (**Enable**) Sie unter **ALG H323 ALG**. Klicken Sie dann **Save**.

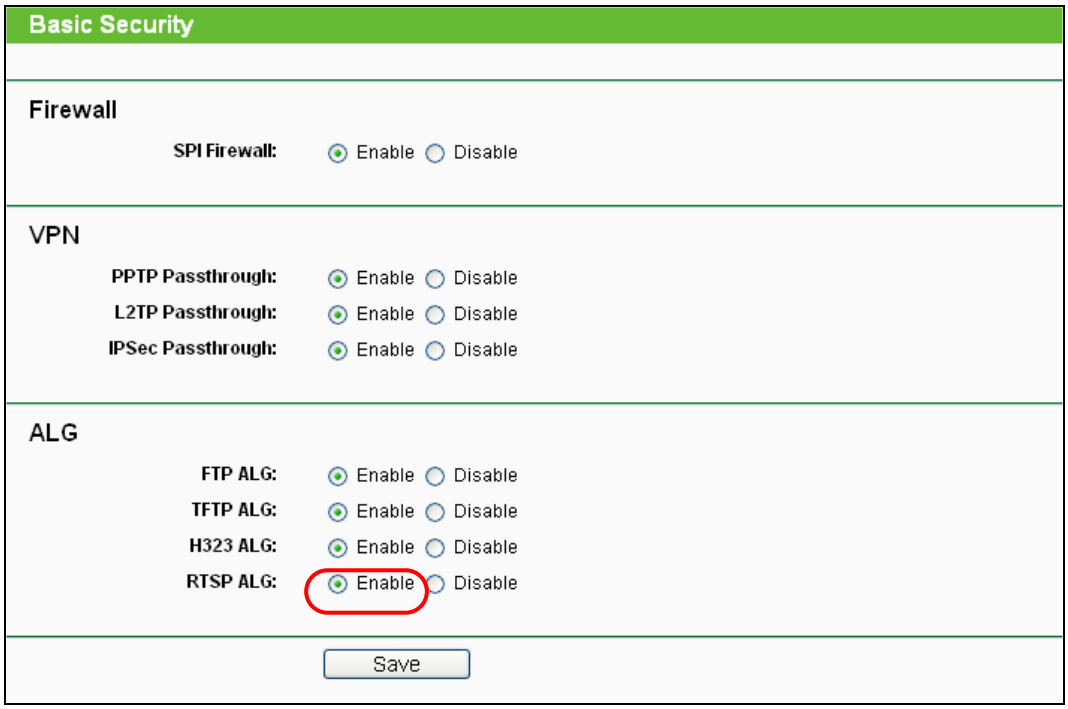


Bild A-7 Basissicherheit

4. Ich möchte in meinem LAN einen von außen erreichbaren Webserver betreiben?

1) Da der Port des Webservers (80) zunächst für die Fernwartung des Routers belegt ist, muss dieser umgelegt werden.

2) Hierfür loggen Sie sich in den Router ein, klicken in der Navigationsleiste auf **Security** und dann auf **Remote Management**. Hier geben Sie für die Fernwartung einen anderen Port als 80 an, z.B. 88. Klicken Sie **Save** und starten Sie den Router neu.

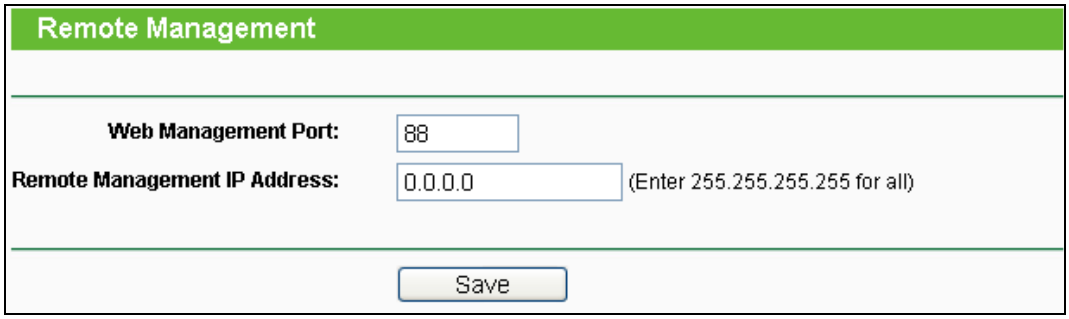


Bild A-8 Fernwartung

☞ **Bemerkung:**

Ist obige Konfiguration übernommen worden, muss zur Administration des Routers ab sofort beispielsweise http://192.168.1.1:88 („http://“, LAN-IP-Adresse des Routers, „:“, gerade angegebene Webmanagementportnummer) eingegeben werden.

3) Loggen Sie sich in den Router ein und klicken Sie das Menü **Forwarding** und dann **Virtual Servers** an. Auf der Seite **Virtual Servers** klicken Sie **Add New…**, geben Sie dann auf der Seite **Add or Modify a Virtual Server** 80 in das Feld **Service Port** und Ihre IP-Adresse in das Feld **IP Address** ein. Beispiel: 192.168.1.188. Stellen Sie den

Eintrag auf **Enabled** und klicken Sie **Save**.

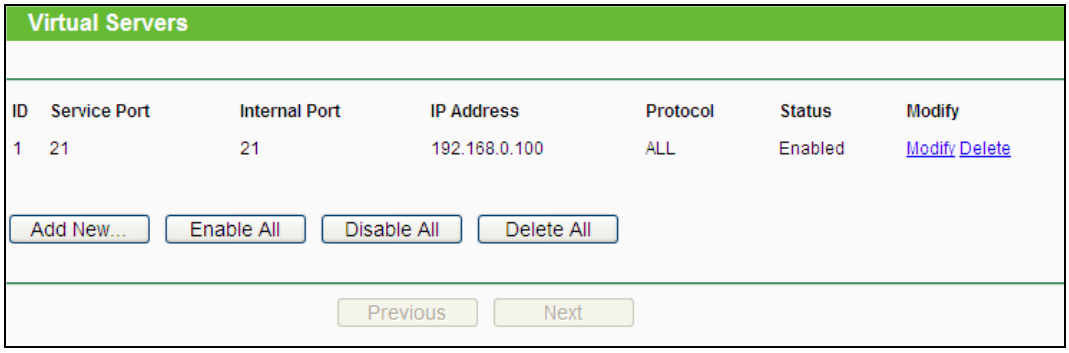


Bild A-9 Virtuelle Server

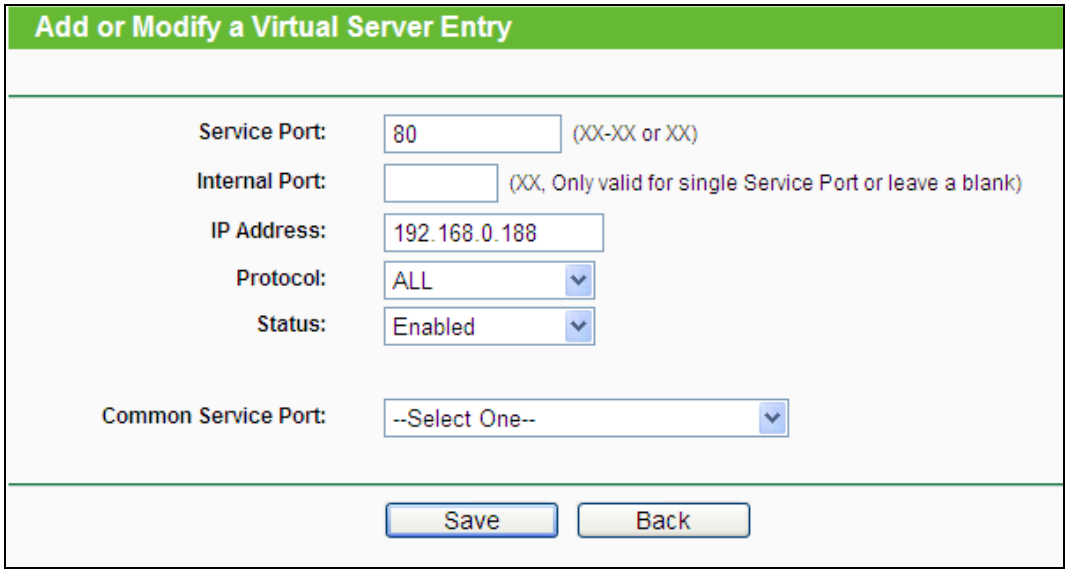


Bild A-10 Virtuellen Server hinzufügen oder bearbeiten

5. WLAN-Stationen können sich nicht mit dem Router verbinden. Was tun.

1) Stellen Sie sicher, dass die WLAN-Funktion aktiviert ist.

2) Stellen Sie sicher, dass die Clients versuchen, sich mit der richtigen SSID zu verbinden.

3) Stellen Sie sicher, dass die WLAN-Stationen den richtigen Schlüssel verwenden, falls Ihr WLAN verschlüsselt ist. Eventuell ist es ratsam, das WLAN-Profil aus dem WLAN-Gerät zu löschen und neu anzulegen.

4) Überprüfen Sie, ob Ihre WLAN-Stationen sich im gleichen Subnetz wie der Router aufhalten (siehe Anhang B).

5) Überprüfen Sie, ob der MAC-Adressenfilter inaktiv oder für die Zulassung der entsprechenden WLAN-Geräte konfiguriert ist.

Anhang B: PCs konfigurieren

Dieser Abschnitt erklärt Ihnen, wie unter Windows XP TCP/IP korrekt konfiguriert wird. Stellen Sie zunächst sicher, dass Ihr Ethernet-Adapter funktioniert. Schauen Sie ggf. in dessen Handbuch.

1. TCP/IP einrichten

1) Klicken Sie **Start** -> **Einstellungen** -> **Systemsteuerung**.

2) Klicken Sie **Netzwerkverbindungen** an. Sie sehen eine Verbindungsübersicht.

3) Rechtsklicken Sie auf das Symbol Ihrer LAN-Verbindung. Wählen Sie **Eigenschaften**.

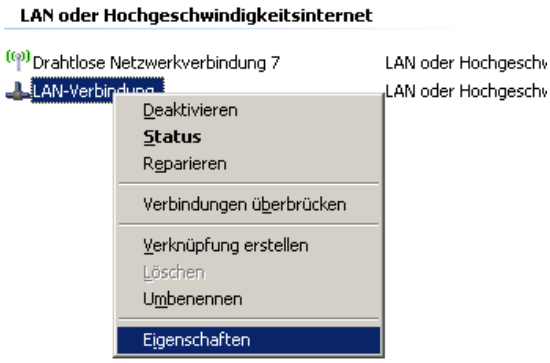


Bild B-1

4) Im dann erscheinenden Fenster doppelklicken Sie auf **Internetprotokoll (TCP/IP)**.

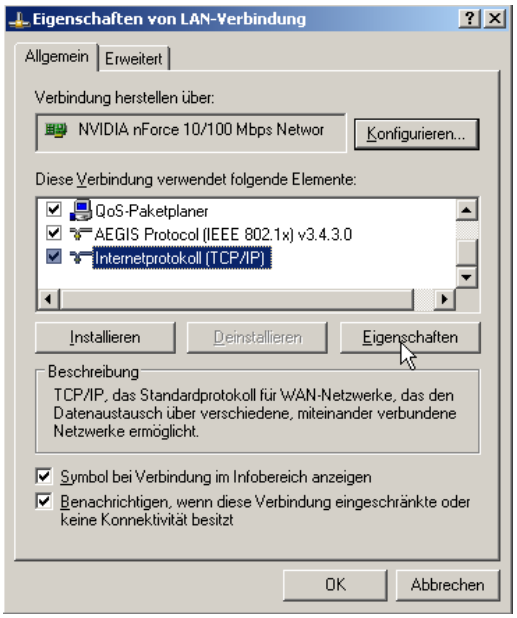


Bild B-2

5) Das Fenster **TCP/IP-Eigenschaften** öffnet sich.

Nun gibt es zwei Möglichkeiten, TCP/IP zu konfigurieren:

➢ **Automatisch**

Wählen Sie **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen**:

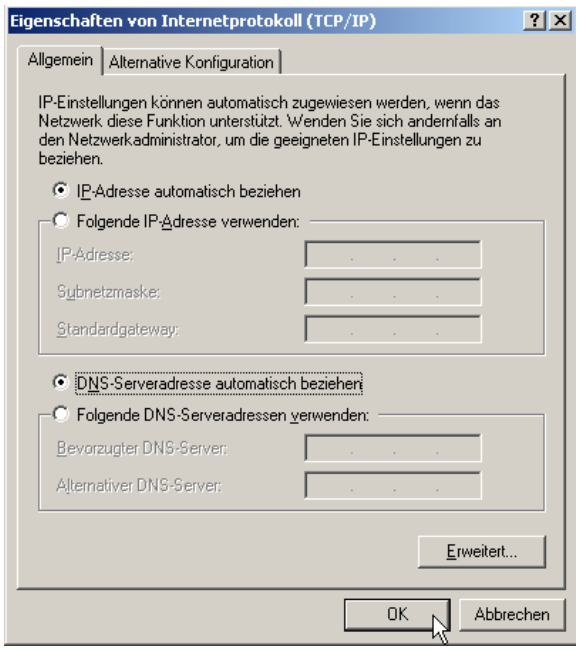


Bild B-3

➢ **Manuell**

1 Wählen Sie **Folgende IP-Adresse verwenden**. Folgende Felder werden verfügbar.

2 Hat der Router die LAN-IP-Adresse 192.168.1.1, geben Sie eine IP-Adresse der Form 192.168.1.x ein. x bezeichnet eine Zahl von 2 bis 254. **Subnetzmaske** ist 255.255.255.0.

3 Geben Sie des Routers LAN-IP-Adresse (Standard: 192.168.1.1) als **Standardgateway** ein.

4 Wählen Sie **Folgende DNS-Server verwenden**. Als **Bevorzugten DNS-Server** geben Sie die DNS-Server-Adresse, die Sie von Ihrem ISP erhalten haben, ein.

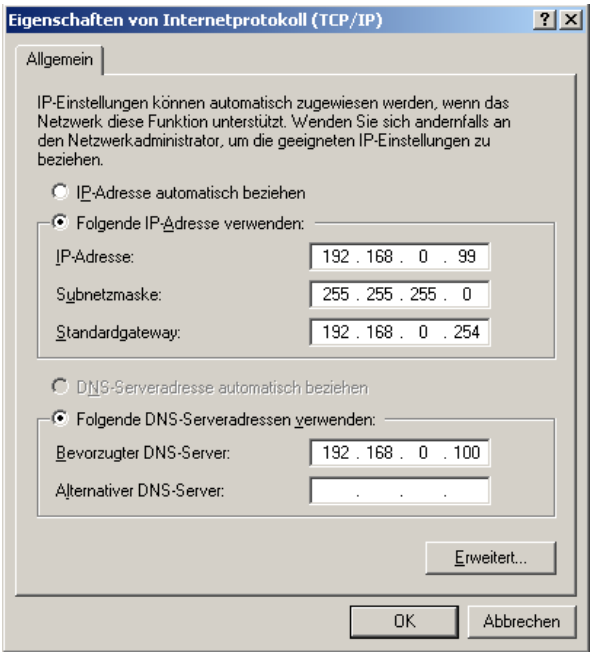


Bild B-4

Anhang C: Spezifikationen

Allgemein	
Standards	IEEE 802.3, 802.3u, 802.11b, 802.11g und 802.11n
Protokolle	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Anschlüsse	Ein 10/100M-RJ45-Port (WAN/LAN) mit Autoabstimmung
Kabel	10BASE-T: UTP-Kategorien 3, 4, 5 (max. 100m) EIA/TIA-568 100Ω STP (max. 100m)
	100BASE-TX: UTP-Kategorien 5, 5e (max. 100m) EIA/TIA-568 100Ω STP (max. 100m)
LEDs	PWR, Internet, WLAN, Ethernet, WPS
Sicherheit und Emissionen	FCC, CE
WLAN	
Frequenzband	2,4..2,4835GHz
Datenraten über Funk	11n: bis zu 150Mbps (automatisch) 11g: 54/48/36/24/18/12/9/6M (automatisch) 11b: 11/5,5/2/1M (automatisch)
Frequenzverteilung	DSSS (Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Sicherheit	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Empfindlichkeit bezogen auf Paketfehlerrate (PER)	130M: -68dBm bei 10% PER 108M: -68dBm bei 10% PER 54M: -68dBm bei 10% PER 11M: -85dBm bei 8% PER 6M: -88dBm bei 10% PER 1M: -90dBm bei 8% PER
Antennengewinn	5dBi
Physisch und Umgebung	
Temperaturgrenzen	Betrieb: 0°C..40°C
	Lager: -40°C..70°C
Relative Feuchtigkeit	Betrieb: 10%..90%, nicht kondensierend
	Lager: 5%..90%, nicht kondensierend

Anhang D: Glossar

- **802.11n -** Der Standard 802.11n erweitert frühere 802.11-Standards durch MIMO (multiple input, multiple output). MIMO benutzt mehrere Sender und Empfänger, um den Durchsatz zu erhöhen und die Reichweite zu erhöhen. Das Enhanced Wireless Consortium (EWC) [3] wurde ins Leben gerufen, um die Entwicklung des IEEE-802.11n-Standards zu beschleunigen und eine technische Spezifikation für die Interoperabilität der WLAN-Geräte der nächsten Generation zu erstellen.
- **802.11b -** Der Standard 802.11b spezifiziert drahtloses Netzwerken mit 11 Mbps durch Benutzung von Direct-Sequence-Spread-Spectrum(DSSS)-Technologie und Funkverbindungen im lizenzfreien Frequenzbereich bei 2.4GHz sowie WEP-Verschlüsselung. 802.11b-Netze sind auch als Wi-Fi-Netze bekannt.
- **802.11g -** Spezifikation für drahtloses Netzwerken mit 54 Mbps durch Benutzung von Direct-Sequence-Spread-Spectrum(DSSS)-Technologie mit OFDM-Modulation und Funkverbindungen im lizenzfreien Frequenzbereich bei 2,4GHz sowie WEP-Verschlüsselung. Es besteht Abwärtskompatibilität zu IEEE-802.11b-Geräten.
- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** Die Möglichkeit, einen festen Hostnamen einer dynamischen IP-Adresse zuzuordnen.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol)**:** Ein Protokoll, das automatisch die TCP-IP-Parameter eines mit dem DHCP-Server verbundenen PCs setzt.
- **DMZ** (**D**e**m**ilitarized **Z**one)**:** Eine Demilitarisierte Zone erlaubt es, einen lokalen PC für einen speziellen Zweck ungeschützt ans Internet anzuschließen, um als Gamingserver oder für Videokonferenzen zu agieren.
- **DNS** (**D**omain **N**ame **S**ystem) **-** Die IP-Adresse des Servers bei Ihre ISP, der Domänennamen in IP-Adressen auflöst.
- **Domain Name/Domänenname -** Ein „sprechender“ Name für eine Internet-Adress(grupp)e.
- **DSL** (**D**igital **S**ubscriber **L**ine)**:** Eine Technik, die es erlaubt, Daten über traditionelle Telefonleitungen zu transportieren.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** Eine Firma, die Internetzugang anbietet.
- **MTU** (**M**aximum **T**ransmission **U**nit) **-** Maximale Paketgröße in Byte.
- **NAT** (**N**etwork Adresse **T**ranslation) **-** NAT wandelt IP-Adressen eines lokalen Netzes in eine Internet-IP-Adresse um.
- **PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE ist ein Protokoll zur Verbindung zwischen Hosts und dem Internet mittels einer Standleitung und einer simulierten Wählverbindung.

- **SSID** (**S**ervice **S**et **Id**entification) **-** Eine SSID identifiziert ein WLAN. Sie ist maximal 32 alphanumerische Zeichen lang. Um im selben WLAN arbeiten zu können, müssen alle Geräte mit derselben SSID konfiguriert sein. Sie entspricht der ESSID eines Accesspoints und dem WLAN-Namen.
- **WEP** (**W**ired **E**quivalent **P**rivacy) **-** Ein Datenverschlüsselungsmechanismus, basierend auf einem 64-Bit-, 128-Bit- oder 152-Bit-Shared-Key-Algorithmus, siehe IEEE 802.11.
- **Wi-Fi -** Eine Handelsmarke für den Standard 802.11b, herausgegeben von der Wireless Ethernet Compatibility Alliance (WECA, siehe http://www.wi-fi.net), einer Industriestandardgruppe, die die Zusammenarbeit der verschiedenen 802.11b-WLAN-Geräte gewährleistet.
- **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork) **-** Eine Gruppe Computer oder sonstiger Geräte, die drahtlos miteinander kommunizieren und deren Nutzer auf ein relativ kleines Gebiet konzentriert sind.

Anhang E: Kompatible 3G/3,75G-USB-Modems

In der folgenden Tabelle finden Sie die von uns getesteten UMTS/HSPA/EVDO-USB-Modems. Die neueste Kompatibilitätsliste kann auf **http://www.tp-link.com** gefunden werden.

Kompatible 3G/3,75G-USB-Modems (im Feld getestet)

HUAWEI	E122, E1262, E1550, E1552, E156, E156B, E156C, E156G, E160, E160E, E160G, E169, E1692, E169G, E173, E1750, E1752, E1756, E1762, E1782, E180, E1800, E1820, E182E, E220, E226, E230, E270, E272, E870, EC122, EC1260, EC1261, EC169, K3520, K3565, K3715, K3765, K4505, UMG1691
ZTE	AC2726, AC2726i, AC2736, AC2766, AC581, K3565-Z, K3765-Z, K4505-Z, MF100, MF102, MF110, MF112, MF160, MF161, MF180, MF190, MF626, MF627, MF636, MF637, MF637U, MF645, MF668, MF668+, MU351
NOVATEL	U760
NOKIA	CS-10, CS-12, CS-15
ONDA	MSA501HS, MT833UP, MW100HS, MW833UP
ALCATEL	X060S, X070S, X080S
4G SYSTEM	XSStick W12
CSL	U1-TF, U1
SAMSUNG	SGH-H128
BANDRICH	BANDLUXE C321, C120
BLUE CUBE	H01
Blue-Link	BL-HD72A
BM	WM78
CENTENNIAL	FlyingAngel HSUPA
DLINK	DWM-151, DWM-152, DWM-156, DWM-652
E-TOUCH	WM78
GLBETRTTER	GI0452

HAIER	CE100, OLIVE VME110, WM200
HSDC	Hsdc-03
MWALKER	MBD-100HU
MYWAVE	FW2012T
OPTION	iCon 401
PANTECH	PX500
QISDA	H21
SIERRA WIRELESS	AC306, AirCard 881U, Compass 885U, Compass 889
SPRINT	U600
TELSEY	EVERYWEB HSUPA
T-MOBILE	USB STICK 120
VENUS	VT18
VIRGIN	MC760