



[www.windows-netzwerke.de](http://www.windows-netzwerke.de)

° Diese Artikel wurde an uns per Mail zugesendet.

Quelle: Unbekannt  
Autor: Unbekannt

## IP Forwarding

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q230082>

Wenn in einem Host mehrere Netzwerkkarten eingebaut sind, kann dieser als statischer Router eingesetzt werden, wozu IP-Forwarding aktiviert werden muss.

### Advanced Features:

Der DSL-Router hat noch viele Einstellmöglichkeiten die wir Ihnen hier kurz erläutern möchten. Um diese Funktionen zu benutzen müssen Sie dem PCs an dem Sie die Funktionen nutzen möchten eine feste IP zuteilen. Sie können DHCP und statische/feste IP gleichzeitig nutzen - dies stellt sicher, daß der PC egal ob Sie ihm eine IP Adresse zuteilen oder nicht eine IP Adresse erhält.

Der DSL-Router benutzt IP Adressen die mit 192.168.1.X starten. Wenn Sie IP Adresse STATISCH/FEST ist, ist die letzte Nummer im Bereich von 2 bis 99. Wenn Die IP Adresse dynamisch vergeben wird ist sie 100 und/oder größer.

### Beispiel:

192.168.1.43 ist eine feste IP Adresse

192.168.1.127 ist eine dynamische IP Adresse.

Um eine feste IP Adresse zu setzen, versichernn Sie sich, daß alle angegebenen Daten im SETUP eingegeben sind.

IP Adresse  
192.168.1.2 bis 99

Subnet Mask  
255.255.255.0

Default Gateay  
192.168.1.1

DNS Server

vom IPS\* zugeteilt

\* DNS Daten finden Sie auf der Statusseite im Konfigurationsprogramm oder bei Ihrem Internet Anbieter. Unser Support kann Ihnen diese Angaben nicht geben.

Unter Umständen bekommen Sie mehrere DNS Server mitgeteilt die Sie dann auch eingeben können. In den Netzwerkeinstellungen unter TCP/IP "enablen" Sie DNS. Unter "HOST" geben Sie einen Namen ein (kann der Name des Rechners sein).

Unter Domain Name geben Sie den Namen Ihres Serviceproviders ein und unter DNS geben Sie alle DNS Daten ein.

Prüfen Sie alle Eingaben genau bevor Sie das Fenster schließen. Diese Angaben können je nach Anbieter abweichen, der technische Support Ihres Internetserviceproviders sollte Ihnen hierzu Auskünfte geben können !

### **DMZ Hosting:**

Durch die Funktion DMZ können Sie einen PC komplett nach aussen hin öffnen und die Firewall des DSL Routers umgehen während der Rest des Netzwerkes geschützt bleibt. Diese Funktion ist z.B. bei Videokonferenzsystemen nützlich die mehr als 10 Ports nutzen. Internetspiele und Videokonferenzen sind typische Nutzer der DMZ Funktion

### **Achtung:**

Wenn Sie die DMZ Funktion nutzen, haben Sie keinen Schutz durch die Firewall für den entsprechenden PC. Im Router SETUP klicken Sie auf ADVANCED und dann auf FORWARDING.

Geben Sie die IP Adresse des Rechners ein denn Sie in den DMZ-Mode setzen wollen - dann klicken Sie APPLY.

### **IP – FORWARDING:**

IP Forwarding kann benutzt werden für E-Mail Server, Web Server oder Fernwartungsprogramme die Zugriff auf einen Rechner haben sollen.

Im Konfigurationsprogramm des Routers wählen Sie ADVANCED und dann FORWARDING. Geben Sie die PORT-Nummern an die Ihre Anwendung benutzt (denken Sie daran, daß alle TCP und UDP Ports geöffnet werden wenn Sie diese Eingaben machen)

Geben Sie dann die IP Adresse des Rechners an welcher die Daten empfangen soll. Denken Sie daran diesem Rechner eine STATISCHE/FESTE IP Adresse zuzuteilen. Klicken Sie APPLY !

## **IP Filtering:**

Diese Funktion läßt es zu bestimmten Rechnern im Netzwerk den Zugang zum Internet sperren. Sie können nur den generellen Zugang sperren nicht aber den Zugang zu bestimmten Seiten.

Geben Sie die IP Adresse des PCs an welchen Sie sperren möchten und klicken Sie APPLY. Dieser Rechner kann nicht mehr auf das Internet zugreifen.  
(Achtung, wenn sie den DHCP Server nutzen kann sich die IP Adresse des Rechners nach einem Neustart ändern- diese Funktion empfiehlt sich nur mit statischen IP Adressen)

Sie können auch einen PORT des Routers sperren, geben Sie dabei die PORT Nummer des zu sperrenden Ports in das PORT-Number Feld ein.

## **BLOCKING WAN REQUESTS:**

Wenn Sie die Funktion Block WAN Requests aktivieren (ENABLE) können Sie von aussen nicht mehr "gepingt" werden oder durch sogenannte Portscans aufgespürt werden. Dies ist ein zusätzlicher Sicherheitsfaktor.