

## Beveiliging van de Netgear Router

### 1. Inleiding

Mocht men een Netgear (modem-)router willen beveiligen tegen onbevoegd 'medegebruik' van het internet door burelen of onbekenden dan dient men na aanschaf nog de beveiliging te activeren.

De beveiliging kan worden onderverdeeld in een

- beveiliging van het draadloze deel van de router en een
- uitgebreide beveiliging die zowel draadloos als ook de bekabelde verbinding beveiligt.

Alle hieronder genoemde beveiligingen werken onafhankelijk van elkaar op een zeer specifiek vlak. Hierdoor kunnen deze elkaar aanvullen en de router nog veiliger maken. Echter, voor normaal gebruik hoeft men niet meer toe te passen dan "encryptie" en/of een "Access List"

**LET OP:** configuratie van deze draadloze instellingen kan men beter doen via een bekabelde verbinding tussen de router en de PC aangezien de draadloze verbinding na activering van een beveiligingsmethode (tijdelijk) zal wegvallen.

Men dient op de router in te loggen op de beveiliging te kunnen activeren. Dit doet men via een internetbrowser zoals Firefox, Netscape of Internet Explorer. Op de adresbalk van de browser tikt men voor een ongeconfigureerde router (direct na een reset): <http://192.168.1.1/basicsetting.htm> of <http://www.routerlogin.com/basicsetting.htm>



Voor een al werkende en/of geconfigureerde router tikt men <http://192.168.1.1> of <http://www.routerlogin.com> in. De iets oudere Netgear routers hebben nog het toegangsadres <http://192.168.0.1> of <http://192.168.0.1/basicsetting.htm>

Het kan zijn dat men na de login gevraagd wordt om een gebruikersnaam en een wachtwoord. Deze zijn:

	Standaard router	UPC	@home
Gebruikersnaam	admin	admin	admin
Wachtwoord	password	UPC	draadloos

Na succesvolle inlog ziet men dan het scherm "Basic Settings" verschijnen met de vraag: "Does Your Internet Connection Require A Login". Dit scherm laat men voor wat het is en men gaat naar het menu "Setup Wireless Settings".

### 1. Draadloze Beveiliging

De draadloze beveiliging kan worden onderverdeeld in Encryptie, toegangslijsten en verbergen van het signaal. Hieronder zullen deze methoden worden behandeld.

#### 1.1 Encryptie

Encryptie is een versleutelingsmethode die men activeert in het routermenu "Setup Wireless Settings" via WEP of WPA-PSK.

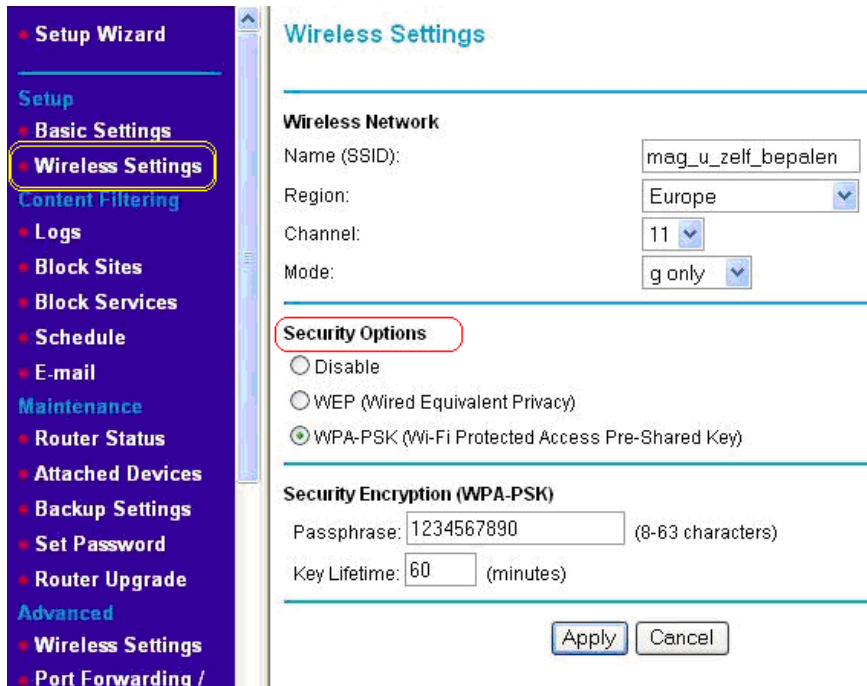
De WEP encryptie kan met moderne software binnen een half uur worden "gehacked" maar wordt vanwege zijn compatibiliteit met andere oudere apparatuur toch nog toegepast. Het beschermt afdoende tegen "gelegenheids internetters".

WPA is veiliger, moeilijker te "hacken", simpeler te installeren en geeft tussen Netgear apparatuur onderling en de meeste moderne netwerkkaarten absoluut geen probleem.

**1.1.1 WPA encryptie**

We beginnen hier met de behandeling van de veiligste draadloze bescherming: De WPA.

Voor het instellen hiervan kiest men wederom het eerder genoemde menu [Setup Wireless settings](#). Men gaat dan naar “[Security options](#)” en activeert WPA-PSK. In het veld “[passphrase](#)” geeft men een wachtwoord in en klikt men op “[apply](#)”.



De [passphrase](#) die wordt ingevoerd mag men zelf bepalen en is een controle password van de router op de draadloze adapters die toegang willen; Vergelijkbaar met een pincode bij de bank. Dezelfde passphrase voert men dan in in de draadloze adapter(s), hetzij de USB adapter, hetzij de PCI -kaart hetzij de PCMCIA (laptop) kaart, via onderstaand principe:



Let wel: de “passphrase” is hier hoofdletter gevoelig, dus dient men goed te noteren wat wordt ingevoerd. Maak ook hier wachtwoorden nooit te makkelijk. Laat ze bestaan uit combinaties van letters en cijfers.

Na voltooiing is de router beveiligd tegen inbraak.

Mocht men onverhoopt draadloos geen toegang meer krijgen tot internet en de router dan kan men met een bekabelde verbinding (zoals bij de eerste installatie) weer toegang krijgen tot de router.

### 1.1.2 WEP encryptie

Wil men ondanks de nadelen van WEP toch de WEP encryptie gebruiken (vanwege bijvoorbeeld compatibiliteit met niet-Netgear draadloze apparatuur die geen WPA ondersteunt) dan dient men op het volgende te letten: Zorg dat de “[Encryption Strength](#)” zowel in de router alsook in de draadloze netwerkkaart beiden identiek staan ingesteld: 64bit – 64 bit of 128bit – 128bit. De 128bit mode is het meest veilig.

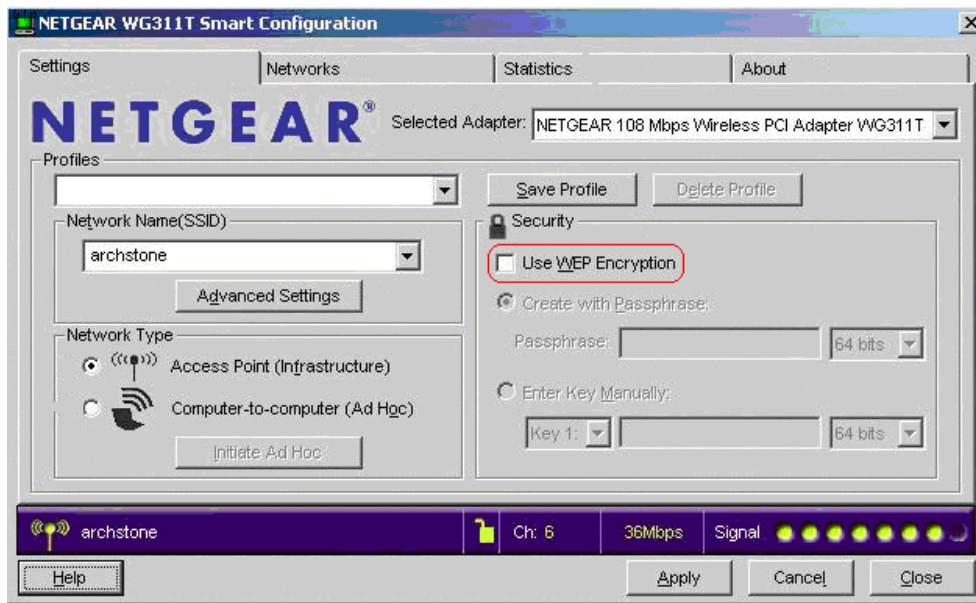
The screenshot shows the 'Wireless Settings' page of a Netgear router. It is divided into three main sections: 'Wireless Network', 'Security Options', and 'Security Encryption (WEP)'.  
1. **Wireless Network:** Name (SSID) is 'mag\_u\_zelf\_bepalen', Region is 'Europe', Channel is '11', and Mode is 'g and b'.  
2. **Security Options:** 'WEP (Wired Equivalent Privacy)' is selected with a radio button.  
3. **Security Encryption (WEP):** Authentication Type is 'Automatic', and Encryption Strength is '64bit'.  
4. **Security Encryption (WEP) Key:** A passphrase 'password' is entered. A 'Generate' button is next to it. Below, four keys are listed: Key 1 (selected) is 'F2C7BB35B9', Key 2 is '858EDAB02E', Key 3 is '27914293E5', and Key 4 is 'CE63E8FB8B'.  
At the bottom, there are 'Apply' and 'Cancel' buttons.

Verder dient men er voor te zorgen dat u de in de router gegenereerde [key](#) overbrengt naar de kaart's “[smart configuration utility](#)” ofwel dezelfde [passphrase](#) overzet en daarmee in de “[smart configuration utility](#)” de key laat genereren.

Let wel: de “[passphrase](#)” is hoofdletter gevoelig, dus men dient goed te noteren wat men invoert. De “key” daarentegen is niet hoofdletter gevoelig.

Maak ook hier wachtwoorden nooit te makkelijk. Laat ze bestaan uit combinaties van letters en cijfers.

In de Netgear netwerkkaart activeert u de WEP beveiliging onder het tabblad “Settings” waar u bij “Security” kiest om of de “Key” in te voeren of te werken met de “Passphrase”.



### 1.2 Access List

Een tweede soort van beveiliging voor draadloze beveiliging is de “access list” (toegangslijst). Deze lijst van in de router geregistreerde MAC-adressen weigert de toegang tot de router aan MAC-adressen van draadloze netwerkkaarten die niet in deze lijst voorkomen. De toegang tot de router en tot internet wordt deze apparaten simpelweg geweigerd.

Deze lijst kan men bereiken in het menu “Advanced Wireless Settings” onder de knop “Setup Access List”.

#### Advanced Wireless Settings

##### Wireless Router Settings

- Enable Wireless Router Radio
- Enable SSID Broadcast
- Fragmentation Threshold (256 - 2346):
- CTS/RTS Threshold (256 - 2346):
- Preamble Mode:

##### 108Mbps Settings

- Disable Advanced 108Mbps Features
- Enable Adaptive Radio(AR) Feature
- Enable eXtended Range(XR) Feature

##### Wireless Card Access List

Na op de knop gedrukt te hebben krijgt men het onderstaande scherm. Via de knop “Add” voegt men nieuwe MAC-adressen toe.

Turn Access Control On

	Device Name	Mac Address

Add Edit Delete

Apply Cancel

Het scherm wordt dan als volgt

### Wireless Card Access Setup

Available Wireless Cards

	Device Name	MAC Address
<input type="radio"/>	PC 1	00:00:00:00:00:01

Wireless Card Entry

Device Name:

MAC Address:

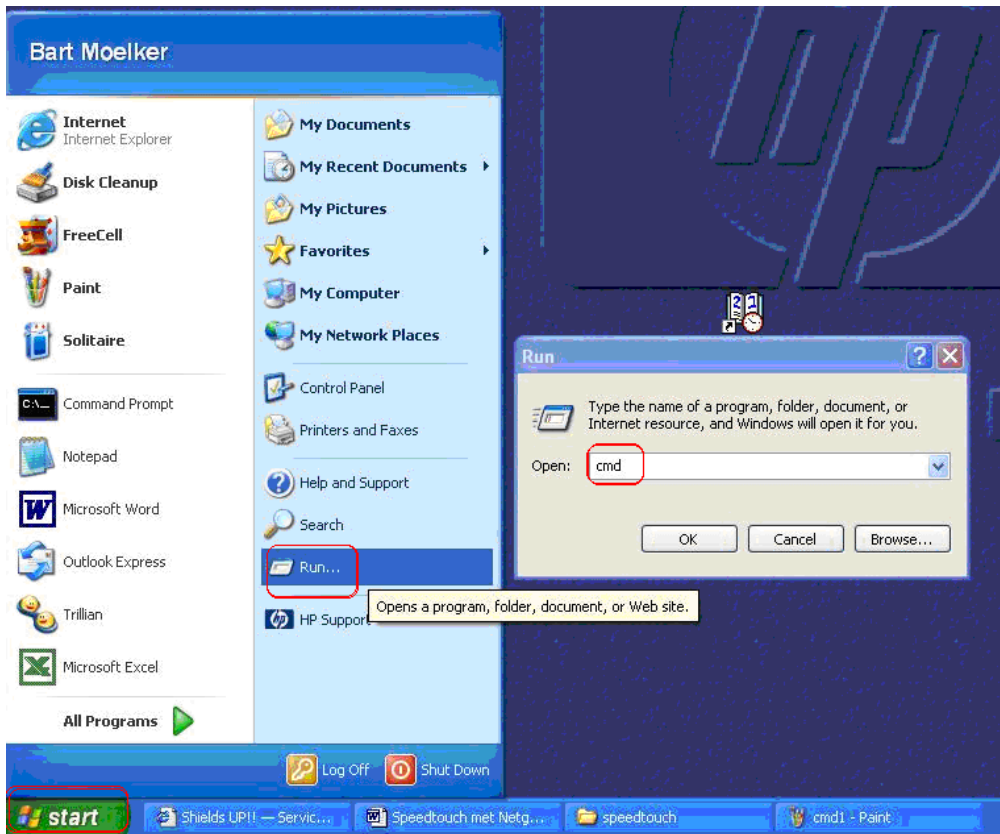
Add Cancel Refresh

Als alles goed verloopt zal men in dit scherm de mogelijkheid zien om een “[available wireless station](#)” te selecteren en automatisch toe te voegen. Let u wel op dat het station dat men automatisch toevoegt niet van een onbeveegde is.

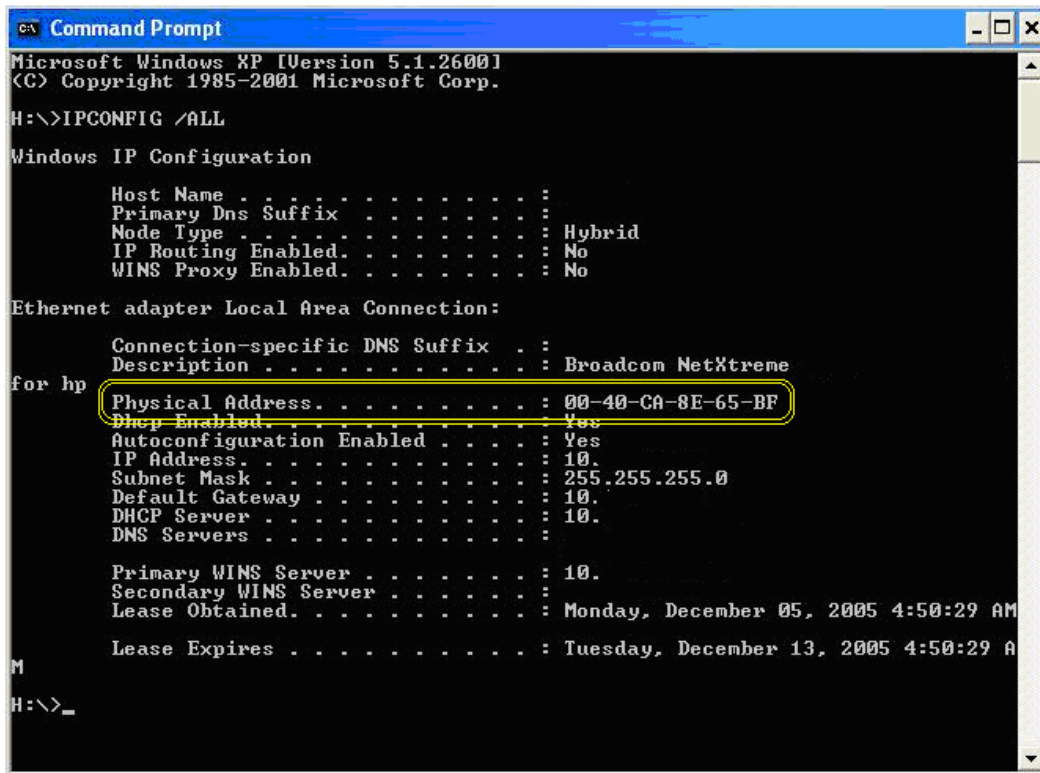
Indien men het niet automatisch wil doen maar handmatig voegt men via “[Device name](#)” een naam toe die men zelf mag bepalen, zoals bijvoorbeeld werkkamer, kinderkamer, etc.

Via “[MAC-Address](#)” voegt men dan handmatig het specifieke MAC adres in van de draadloze netwerkkaart. Dit staat meestal afgedrukt op het apparaat zelf. Indien u het MAC-adres van de draadloze netwerkkaart niet bekend is dan gaat men naar:

Start → Uitvoeren → cmd en drukt u op OK



In het volgende scherm tikt men dan het MS-dos commando: "IPCONFIG /ALL"



Het Fysieke adres (Physical Address) dat bij de draadloze LAN verbinding wordt vermeld is het MAC-adres dat wordt gezocht. Let dan wel op dat hier het adres wordt overgenomen van de geïnstalleerde draadloze

netwerkadapter en niet per ongeluk van een andere adapter. De overige MAC adressen van deze PC kunnen worden overgenomen voor de overige beveiligingen die verderop in deze handleiding worden besproken.

Na invoeren van de MAC-gegevens voltooit men het toevoegen en zet men in het beginscherm van “[Setup Access List](#)” een vinkje (markering) in het veld: “[Turn Access Control On](#)”. Hierdoor wordt de toegevoegde lijst geactiveerd.

Mocht het zo zijn dat de router hierna draadloos ineens niet meer bereikbaar is dan heeft men het MAC-adres van dit apparaat niet goed overgenomen en dient dat te worden gecorrigeerd in de router. Soms kan het opnieuw opstarten van de PC en router ook uitkomst bieden.

### 1.3 Uitschakelen SSID

Het uitschakelen van de uitzending van de stationsnaam door de router, zoals deze gezien kan worden onder “[Setup Wireless Settings](#)”, kan een goede additionele beveiliging zijn. De stationsnaam wordt dan verborgen door de router en onbekenden kunnen de router dan niet benaderen.

Deze functie wordt geactiveerd onder “[Advanced Wireless Settings](#)” door het vinkje weg te halen bij “[Enable SSID Broadcast](#)”. Men dient echter wel de stationsnaam in de netwerkkaart in te geven onder het kopje “[Network name\(SSID\)](#)”.

Let wel: Niet alle netwerkkaarten ondersteunen deze functie en het kan zijn dat men niet meer kan verbinden met de router wanneer dit niet wordt ondersteund door uw netwerkkaart.

Indien men ook het vinkje weghaalt bij “[Enable Wireless Router Radio](#)” houdt de router op draadloos te functioneren. Dit kan handig zijn wanneer de router niet draadloos gebruikt zal worden maar slechts bekabeld.

#### Advanced Wireless Settings

---

**Wireless Router Settings**

Enable Wireless Router Radio

Enable SSID Broadcast

Fragmentation Threshold (256 - 2346):

CTS/RTS Threshold (256 - 2346):

Preamble Mode

---

**108Mbps Settings**

Disable Advanced 108Mbps Features

Enable Adaptive Radio(AR) Feature

Enable eXtended Range(XR) Feature

---

**Wireless Card Access List**

---

## 2. Uitgebreide beveiliging

Behalve draadloze beveiligingen zijn er nog extra beveiligingen die kunnen worden toegepast om ongewenste toegang zoveel mogelijk te beperken. Deze zijn vaak niet noodzakelijk voor de huiselijke gebruiker.

### 2.1 Standaard Wachtwoord veranderen

Het veranderen van het standaard router wachtwoord "password" in een eigen gekozen wachtwoord kunt men doen in het menu "[Maintenance Set Password](#)". Verandering van dit wachtwoord beveiligt alleen de toegang tot de router en onbevoegde veranderingen in de router. Deze methode beveiligt niet de toegang tot internet of het netwerk.

Vergeet dit nieuwe router wachtwoord echter niet. Bij verlies is de enige methode om weer toegang te krijgen tot het router menu door een reset van de router met de reset-knop. Hiermee verliest men al de gedane instellingen en keert de router weer terug naar de fabrieksinstellingen.

### 2.2 Hoeveelheid IP adressen beperken

De hoeveelheid beschikbare IP adressen kan men bijvoorbeeld beperken tot de werkelijke hoeveelheid aangesloten computers op de router. Mocht er ooit iemand in slagen door de bovenstaande beveiligingen heen te komen dan kan de persoon geen IP adres van de router toegewezen krijgen aangezien deze niet meer beschikbaar zijn.

Deze beveiliging wordt eveneens geactiveerd in het menu "[Advanced LAN IP setup](#)". Daar kiest men "[Use Router as DHCP Server](#)". Het bereik van "[Starting IP address](#)" en "[Ending IP address](#)" wordt hier dan veranderd. In het geval van 3 computers die zijn aangesloten op de router wordt dit dus voor "[Starting IP address](#)": 192.168.1.2 en voor "[Ending IP address](#)": 192.168.1.4.

### LAN IP Setup

---

**LAN TCP/IP Setup**

IP Address  .  .  .

IP Subnet Mask  .  .  .

RIP Direction  ▾

RIP Version  ▾

---

**Use Router as DHCP Server**

Starting IP Address  .  .  .

Ending IP Address  .  .  .

---

**Address Reservation**

#	IP Address	Device Name	Mac Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

---

Hiermee voorkomt men dat de router 254 adressen beschikbaar houdt waarvan er maar 2 of 3 bezet zullen worden. De overigen zouden gebruikt kunnen worden door een Hacker.

### 2.3 Statische IP adressen

Een vervolg methode op de bovenstaande methode is de hoeveelheid IP adressen te beperken door statische (vaste) IP adressen uit te geven waarin elke PC (draadloos en bekabeld) altijd zijn eigen vaste IP adres krijgt. Mocht er een PC onder paragraaf 2.2 zijn uitgeschakeld dan zou het theoretisch toch nog kunnen gebeuren dat iemand toegang zou kunnen krijgen door op die gereserveerde plaats in te haken. Middels statische IP adressen wordt dit moeilijker. Statische IP adressen zijn in te stellen in het menu "Advanced LAN IP setup". Hier kiest men dan onder "Address Reservation" de knop "Add".

#### LAN IP Setup

**LAN TCP/IP Setup**

IP Address: 192 . 168 . 1 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: None

RIP Version: Disabled

---

Use Router as DHCP Server

Starting IP Address: 192 . 168 . 1 . 2

Ending IP Address: 192 . 168 . 1 . 4

---

**Address Reservation**

#	IP Address	Device Name	Mac Address
1	192.168.1.2	COSMICLAPTOP	00:0d:9d:5c:05:d8

Add Edit Delete

---

Apply Cancel

Nadat op "Add" wordt gedrukt krijgt men het volgende scherm om het MAC-adres toe te voegen. Hierin voegt men dan het MAC-adres van de betreffende netwerkkaart en men geeft deze een eigen vast IP-adres.

**Address Reservation**

---

**Address Reservation Table**

#	IP Address	Device Name	MAC Address
1	192.168.1.3	COSMICCOMPUTER	00:09:5b:00:22:03
2	192.168.1.2	UNKNOWN NAME	00:0d:9d:5c:05:d8

---

IP Address: [ ] . [ ] . [ ] . [ ]

MAC Address: [ ]

Device Name: [ ]

---

Add Cancel Refresh

Het adres 192.168.1.1 is standaard gereserveerd voor de router en hier dus niet door de gebruiker te gebruiken. Het eerst volgende vrije adres is derhalve 192.168.1.2. De adressen hoeven niet per sé te beginnen met xxx.xxx.xxx.2. Men kan ze desgewenst ook hoger in de range plaatsen met het maximum van xxx.xxx.xxx.254

Het is te adviseren bij het toekennen van deze statische adressen wel met enig systeem te werk te gaan zodat de IP adressen dicht bij elkaar liggen. Dit kan namelijk zeer handig zijn voor de stap: "Hoeveelheid IP adressen beperken" in paragraaf 2.2.

## 2.4 IP adres uitgifte stoppen (Uitschakelen DHCP-server)

De bovenstaande methoden staan nog steeds toe dat een zeer professionele hacker kan inbreken op het apparaat. Als we het vinkje uit "Use Router As DHCP Server" in het menu "LAN IP Setup" weghalen stopt ook de automatische uitgifte van IP adressen. De router is hiermee compleet statisch geworden en hanteert alleen nog maar de adressen die voorkomen in de lijst van "Address Reservation".

**Let wel:** Een groot deel van de bovenstaande methoden zijn voor de huiselijke sfeer niet strikt noodzakelijk en bemoeilijken de probleemoplossing door een Netgear medewerker in het geval van een probleem. Vaak zal er dan door de medewerker worden verzocht om de router weer te resetten naar de fabrieksinstellingen.