



Small ICT Projects

## **Thuisnetwerken**

Philippe Baeten & Dries Van Brussel

3 TI, Reeks 3

Semester 5

Katholieke Hogeschool Leuven  
Departement Rega  
Sint-Maartensstraat 55d • 3000 Leuven  
Tel. +32 16 29 85 11  
Fax +32 16 20 44 17  
rega@khleuven.be

# Inhoudstafel

<a href="#">Inleiding.....</a>	<a href="#">3</a>
<a href="#">Hoofdstuk 1: Het nut van een thuisnetwerk.....</a>	<a href="#">4</a>
<a href="#">Hoofdstuk 2: Welke apparaten kunnen voorkomen in een netwerk?.....</a>	<a href="#">5</a>
<a href="#">Hub.....</a>	<a href="#">5</a>
<a href="#">Switch.....</a>	<a href="#">5</a>
<a href="#">Router (uitspraak: roeter).....</a>	<a href="#">5</a>
<a href="#">Access Point.....</a>	<a href="#">5</a>
<a href="#">Netwerkadapter.....</a>	<a href="#">6</a>
<a href="#">Modem.....</a>	<a href="#">6</a>
<a href="#">Hoofdstuk 3: Waarmee beveilig ik mijn netwerk?.....</a>	<a href="#">7</a>
<a href="#">Alle mogelijkheden op een rijtje:.....</a>	<a href="#">7</a>
<a href="#">Verbergen van de SSID.....</a>	<a href="#">7</a>
<a href="#">Uitschakelen van DHCP.....</a>	<a href="#">8</a>
<a href="#">Lijst met toegelaten MAC-adressen.....</a>	<a href="#">8</a>
<a href="#">WEP.....</a>	<a href="#">8</a>
<a href="#">WPA-PSK (WPA2).....</a>	<a href="#">9</a>
<a href="#">Hoe beveilig ik mijn computer?.....</a>	<a href="#">10</a>
<a href="#">Hoofdstuk 4: Wat moet ik aanschaffen voor mijn netwerk?.....</a>	<a href="#">11</a>
<a href="#">Voorbeeld 1: Appartement.....</a>	<a href="#">11</a>
<a href="#">Voorbeeld 2: Huis.....</a>	<a href="#">12</a>
<a href="#">Hoofdstuk 5: Hoe installeer en configureer ik mijn apparaten? .....</a>	<a href="#">13</a>
<a href="#">Installatie van de router.....</a>	<a href="#">13</a>
<a href="#">SSID verbergen.....</a>	<a href="#">15</a>
<a href="#">Uitschakelen van de DHCP.....</a>	<a href="#">18</a>
<a href="#">Lijst met toegelaten MAC-adressen.....</a>	<a href="#">21</a>
<a href="#">WEP .....</a>	<a href="#">22</a>
<a href="#">WPA-PSK (WPA2).....</a>	<a href="#">24</a>
<a href="#">Hoofdstuk 6: Eventuele problemen.....</a>	<a href="#">26</a>
<a href="#">Verbindt de computer rechtstreeks met de modem.....</a>	<a href="#">27</a>
<a href="#">Heeft de computer een geldig IP-adres?.....</a>	<a href="#">27</a>
<a href="#">Controleer de IP-instellingen op de computer.....</a>	<a href="#">27</a>
<a href="#">Zet alle beveiligingsmaatregelen op de router uit.....</a>	<a href="#">29</a>
<a href="#">Woordenlijst.....</a>	<a href="#">30</a>
<a href="#">Bijlage Gezondheidsrisico's.....</a>	<a href="#">32</a>

# Inleiding

Het eerste hoofdstuk geeft een kort overzicht van de verschillende functionaliteiten en aandachtspunten van een thuisnetwerk.

In hoofdstuk 2 vind je een overzicht van de apparaten die kunnen voorkomen in een computernetwerk. De functie van een router, switch, acces point, [netwerkadapter](#), modem en hub worden er bondig uitgelegd. In hoofdstuk 4 krijg je te horen welke van deze apparaten in jou situatie nodig zijn en het daarop volgende deel behandelt de installatie van je aankopen.

Aan de hand van hoofdstuk 3 gaan we je draadloos netwerk beveiligen. Naast encryptietechnologiën, bekijken we ook de beveiliging van de computer zelf, door middel van een firewall en anti-virussoftware.

Er kan altijd iets fout lopen tijdens de **installatieprocedure (hoofdstuk 5)**, voor de meest voorkomende problemen wordt er een oplossing aangeboden in hoofdstuk 6.

Om meer duidelijkheid te scheppen, wordt er gebruik gemaakt van de volgende in het oog springende kadertjes:

- Dit wijst op een valkuil, belangrijke informatie die in acht moet genomen worden.

- Overzicht van de nadelen van een specifieke techniek.

- Nuttige informatie met een link naar relevante websites op het internet.

Achteraan (vóór de bijlage) vind je een **verklarende woordenlijst**, hierin vind je alle woorden die in het blauw gemarkeerd staan. Voor meer informatie of als er nog begrippen onduidelijk zijn kan je terecht op <http://nl.wikipedia.org/wiki/Portaal:Informatica> .

# Hoofdstuk 1: Het nut van een thuisnetwerk

Steeds meer mensen installeren thuis een internetverbinding. Meestal is dit beperkt tot één computer, hoewel er soms **meerdere computers** in het huis aanwezig zijn. Door de creatie van een thuisnetwerk kunnen deze computers zowel met elkaar als met het internet communiceren. En het kost bovendien helemaal niet veel.

De eerste en heel belangrijke keuze is het type van verbinding die we tussen onze verschillende computers willen leggen.

Als er twee computers op een vaste plaats in het huis staan, is het een goede keuze om een **bekabeld netwerk** te nemen. Soms is dit echter niet mogelijk (bijvoorbeeld: huurhuis) of maken er ook laptops deel uit van het netwerk, in dat geval is het makkelijker om een **draadloos netwerk** te configureren.

Het allerbeste is de combinatie van de twee, omdat je dan de voordelen van beide combineert. Uiteraard is dit iets duurder en kost het ook meer moeite.

Wanneer je een draadloos netwerk wil installeren, moet je met verschillende zaken rekening houden:

- De constructie van het huis, meerdere verdiepingen met dikke betonlagen belemmeren het draadloos signaal aanzienlijk.
- De afstand die overbrugd moet worden.
- De snelheid van de verbinding tussen de verschillende apparaten vb.: je wil grote bestanden zoals films en muziek over het netwerk verzenden. Dan haalt een bekabeld netwerk een hogere en stabielere verbindingssnelheid en is dus beter in deze situatie.
- De beveiliging: bij een netwerk met kabels is het in mindere mate nodig om uw verbinding te beveiligen. Het is immers niet voor de hand liggend voor een vreemde om een kabel in uw netwerk te komen gebruiken. Bij een draadloze verbinding kan iedereen het signaal van uw netwerk binnen een bepaalde straal opvangen. Hier is het dus van groot belang dat je maatregelen treft om te voorkomen dat een vreemde jouw bestanden en internet kan gebruiken.

Er zijn uiteraard veel voordelen aan een netwerk tussen je verschillende computers. Je kan makkelijk bestanden verzenden, om bijvoorbeeld reservekopieën van belangrijke bestanden te nemen. Je moet ook niet langer dubbele bestanden houden op de verschillende pc's, je kan rechtstreeks van de ene computer naar de andere computer zijn harde schijf om bestanden te gebruiken.

- Programma's dienen nog steeds op elke computer apart geïnstalleerd te zijn. Je kan een programma van een andere pc niet op de jouwe openen.

Ook voor de kinderen zijn er voordelen verbonden aan een netwerk. Er zijn duizenden spelletjes die je over een netwerk tegen elkaar kan spelen. Wat veel leuker is dan alleen spelen.

## Hoofdstuk 2: Welke apparaten kunnen voorkomen in een netwerk?

In een computernetwerk krijg je te maken met heel wat gespecialiseerde apparatuur. Om een goede keuze te maken bij de aankoop, volgt een beschrijving van de verschillende apparaten. Op de netwerkkaart na, zijn dit allemaal apparaten die niet in een computer zitten.

### **Hub**

Hub is het engelse woord voor "naaf". Het is één van de meest eenvoudige apparaten uit een computernetwerk. Het verbindt fysisch meerdere computers met elkaar. Maar verandert niets aan de gegevens die verzonden worden. Wanneer er bijvoorbeeld vijf computers op de hub aangesloten worden en één computer verstuurt gegevens naar een andere, dan zal de hub die gegevens naar de vier andere computers sturen. Het is dus aan de computer zelf om uit te maken of het bericht al dan niet voor hem bestemd is.

### **Switch**

Een switch is een veredelde hub. In die zin dat een switch wel kijkt naar de bestemming van de gegevens en leert langs welke weg hij een bepaalde computer kan bereiken. Eens hij dit weet, stuurt hij de gegevens enkel naar de juiste computer.

### **Router (uitspraak: roeter)**

Dit apparaat is in staat om verschillende netwerken met elkaar te verbinden, zoals een thuisnetwerk aan het internet. Het verzorgt de communicatie tussen netwerken in plaats van tussen computers, zoals bij de twee voorgaanden wel het geval is. Zoals de naam doet vermoeden, zorgt dit schakelapparaat ervoor dat gegevens via de correcte weg verzonden worden naar de bestemming. Er is in se geen verschil tussen een draadloze en niet-draadloze router, buiten de manier waarop je er verbinding mee maakt. Dankzij de router lijkt het voor de buitenwereld (dus ook je [internet service provider](#)) alsof je met slechts één computer met het internet verbonden bent. Je moet wel opletten dat je het juiste type router koopt, er is wel degelijk een verschil tussen een router voor een kabelverbinding (telenet, chello,...) en adsl-verbinding (skynet, scarlet,...)

### **Access Point**

Een access point is een apparaat dat draadloze toegang op een bestaand bekabeld netwerk mogelijk maakt of gebruikt wordt ter uitbreiding van een [WLAN](#). Het apparaat sluit je met een kabel aan op het netwerk en laat

vervolgens de computer toe draadloos te communiceren. Bijkomende configuratie is niet vereist, de beveiling is nog steeds in handen van de router.

## ***Netwerkadapter***

Onderdeel van een computer dat de mogelijkheid biedt met een netwerk te verbinden. Afhankelijk van het type gebeurt dit met kabel of draadloos. Meestal zit in een computer bij aankoop al een netwerkkaart voor de toegang met een kabel.

Bij desktops dient het draadloze type vaak achteraf nog aangekocht en geïnstalleerd worden.

## ***Modem***

### ***MOdulator-DEModulator***

Door middel van een modem kan een computer communiceren over een analoge telefoonverbinding. Dit apparaat wordt geleverd door je [ISP](#).

- Je moet / mag hier meestal zelf niets aan instellen. Enkel aansluiten!

## Hoofdstuk 3: Waarmee beveilig ik mijn netwerk?

Wat wordt er eigenlijk bedoeld met "beveiliging van een draadloos netwerk"? Een draadloos netwerk maakt gebruik van radiosignalen, die door de lucht verspreid worden.

In tegenstelling tot bekabelde netwerken, waar de signalen door een draadje lopen, is het bij draadloze netwerken heel eenvoudig om de signalen op te pikken en berichten mee te lezen. Natuurlijk wil je niet dat iemand je emails meeleest, of erger nog, al je wachtwoorden te weten komt.

Door **encryptiealgoritmes** toe te passen, maak je van deze signalen een warboeltje. Enkel de computer waarvoor de berichten bestemd zijn, beschikt over een **sleutel** om van het signaal iets zinvol te maken. Er zijn verscheidene oplossingen voor handen om je netwerk te beveiligen. De eerste drie mogelijkheden van het lijstje hieronder zijn voorzorgsmaatregelen die je als beheerder kan instellen. De twee laatste, **WEP** en **WPA**, zijn encryptiealgoritmes die toepasbaar zijn op draadloze netwerken. Natuurlijk is het niet voldoende om er eentje te kiezen uit de lijst, ideaal is het combineren van meerdere technieken om het zo moeilijk mogelijk te maken voor de inbreker. Aan de hand van de sterretjes kan je zien hoe relevant de mogelijkheden zijn.

- Verbergen van de **SSID** ★★★★★
- Uitschakelen van **DHCP** ★
- Lijst met toegelaten MAC-adressen ★★
- **WEP** ★★★★★
- **WPA** ★★★★★★

### ***Alle mogelijkheden op een rijtje:***

#### **Verbergen van de SSID**

★★★

De **SSID** is de naam die je draadloos netwerk met zich meedraagt, door deze niet uit te zenden, maak je het al heel wat moeilijker voor iemand anders om op je netwerk te geraken. Op deze manier, kunnen computers dit netwerk niet detecteren zonder een beetje hulp van de gebruiker. Om als nieuwe gebruiker met het netwerk te verbinden, moet je zelf de **SSID** meegeven van het betreffende netwerk. Voor gebruikers die er voorheen al gebruik van hebben gemaakt, gebeurt dit automatisch.

- Gebruik geen al te voor de hand liggende naam voor je computernetwerk, zoals Thuis, of de merknaam van je router.

## Uitschakelen van DHCP



Door middel van **DHCP** zal door de draadloze router automatisch een **IP-adres** toegewezen worden. Op deze manier kunnen er geen conflicten optreden bij de verdeling van adressen. Wanneer je het automatisch proces uitschakelt, laat je het aan de gebruiker over om zelf zulk een **IP-adres** te kiezen, dus moet deze al weten welk **IP-adres** aanvaard zal worden door de router.

- Enige kennis van IP-adressering is wel vereist.
- De inhoud van de verzonden berichten wordt niet onleesbaar gemaakt. Het is enkel de toegang tot het netwerk die beveiligd wordt.

## Lijst met toegelaten MAC-adressen



Door in de router een lijst op te slaan van de toegelaten computers, door middel van hun fysiek adres, zal deze geen verbindingen met andere computers toelaten.

Het is een goed systeem, dat door professionelen wel te omzeilen valt, maar tegen 99% van de computergebruikers waterdicht is.

- Het nadeel hieraan is dat het enige moeite vraagt om een nieuwe computer in het netwerk op te nemen.
- Net als bij DHCP wordt de inhoud van de verzonden berichten niet veranderd. Het is enkel de toegang tot het netwerk die beveiligd wordt.

## WEP



**WEP** (Wired Equivalent Privacy) is een **eenvoudig encryptiealgoritme**. Er zijn twee niveaus van veiligheid, namelijk de 64 en de 128-bit versleuteling.

Hoe hoger het aantal bits, des te moeilijker het algoritme te kraken is. Het is dus aangeraden om bij het gebruik van **WEP** voor de 128-bit versleuteling te kiezen.

De techniek baseert zich op het feit dat beide partijen een gemeenschappelijke sleutel bezitten. Hiermee wordt de inhoud, van elk bericht dat verstuurd wordt, bewerkt tot deze onleesbaar is. De ontvanger (die dezelfde sleutel bezit als de verzender) kan met zijn sleutel de boodschap terug ontcijferen en de originele inhoud achterhalen.

Omdat elk bericht versleuteld is, kunnen gebruikers zonder sleutel de inhoud van de berichten niet achterhalen en dus ook geen deel uitmaken van het netwerk.

- De sleutels bij communicatie tussen computer A en B, zijn verschillend van de sleutels die gebruikt worden voor de beveiliging van communicatie tussen A en C. Deze sleutels worden elke keer opnieuw door de computers gegenereerd op basis van de ingevoerde netwerksleutel.

- WEP is niet van de jongste. Toen het algoritme ontworpen werd, voldeed het aan de eisen van zijn tijd. Maar door de grote toename van de reken capaciteit van de computers is het nu een kwestie van enkele minuten om te kraken.
- De ingebruikname van WEP is niet zo voor de hand liggend. Omdat het gekozen paswoord aan bepaalde specificaties moet voldoen.

## WPA-PSK (WPA2)



WPA (Wireless Protected Access) is een veel ingewikkelder algoritme dan WEP, door het gebruik van verschillende sleutels die snel na elkaar gewisseld worden gedurende het verzenden van berichten. Deze sleutels worden door de computer zelf gegenereerd. De gebruiker moet maar één sleutel invoeren die de computer gebruikt als basis.

Ook hier geldt dat enkel de gebruikers die de sleutel kennen toegang tot het netwerk kunnen krijgen. WPA bestaat in twee vormen:

- WPA-PSK: "Pre-Shared Key"
- WPA-enterprise

De eerste versie wordt vooral door thuisgebruikers en binnen kleine ondernemingen toegepast, omdat de sleutel handmatig ingevoerd moet worden. De enterprise-versie vereist een complexe infrastructuur waaronder een RADIUS-verificatieserver, wat voor een thuisnetwerk niet van toepassing is.

De nieuwe versie van WPA, WPA2 werkt op gelijkaardige manier, maar heeft als encryptiealgoritme AES toegevoegd. Hierdoor voldoet het aan de 802.11i standaard.

- Ook al is dit de beste beschikbare beveiligingsmethode voor draadloze netwerken, toch is ook deze methode niet 100% veilig. Maar het kraken ervan vereist een zeer goede kennis van netwerktechnologieën en goede apparatuur om te omzeilen.

## Hoe beveilig ik mijn computer?

Niet alleen de veiligheid in een netwerk is van belang. Ook de computer zelf moet beschermd zijn tegen verschillende gevaren, zoals virussen, [Trojaanse paarden](#), wormen, ad-ware, spyware...

Om je te beschermen tegen deze indringers, zijn er verschillende soorten programma's beschikbaar, hier zijn alvast een aantal gratis programma's:

1. **Anti-virussoftware:** Onmisbaar op elke computer die met het internet verbonden is.

- Avast Home Edition: na registratie een gratis te gebruiken anti-virus programma

Link: [http://www.avast.com/eng/avast\\_4\\_home.html](http://www.avast.com/eng/avast_4_home.html)

2. **Anti-spyware:** Al surfend wordt er heel wat informatie op je computer opgeslagen. Niet al deze bestanden zijn even onschuldig, af en toe is het aangeraden je computer te controleren op de aanwezigheid ervan.

Er zijn heel wat programma's beschikbaar tegen spyware, hier zijn alvast een aantal voorbeelden:

- Hitman

Link: <http://www.hitmanpro.nl>

- Ad-aware

Link: <http://www.lavasoft.nl/dutch/support/download/>

- Spybot Search & Destroy

Link: <http://www.spybot.info/nl/mirrors/index.html>

3. Een **persoonlijke firewall** beschermt de toegang tot je computer. Ongewenste bezoekers wordt de toegang geweigerd en programma's die ongevraagd verbinding proberen maken met het internet worden geblokkeerd. Windows XP SP2 bezit standaard een firewall, deze is echter van mindere kwaliteit dan gespecialiseerde software.

- Sunbelt Kerio Personal Firewall schakelt automatisch de standaard Windowsfirewall uit.

Link: <http://www.sunbelt-software.com/kerio.cfm>

- Zonealarm van ZoneLabs is eveneens een uitstekende gratis firewall.

Link: <http://www.zonelabs.com>

## Hoofdstuk 4: Wat moet ik aanschaffen voor mijn netwerk?

Het is begrijpelijk dat elke situatie min of meer verschillende implementatie vereist. Woon je bijvoorbeeld in een appartement, dan hoeft je bereik niet uitermate groot te zijn om zo te voorkomen dat je burens er eveneens gebruik van kunnen maken. Of wens je net het tegenovergestelde en moet het netwerk meerdere verdiepingen bestrijken. Natuurlijk is de positie van je router essentieel om voor de laagste kost het meeste eruit te halen. Probeer dan ook deze te plaatsen op een plaats die centraal ligt ten opzichte van elke ruimte van waaruit je op het netwerk wilt. Indien de afstand te groot zou zijn, dan zou je kunnen overwegen om sommige plaatsen te bekabelen of door middel van één of meerdere access points je draadloos netwerk uit te breiden.

Storing van het signaal is na het beveiligingsprobleem van draadloze LAN's, de belangrijkste factor om rekening mee te houden. Meestal is dit bij thuisnetwerken minder belangrijk dan voor ondernemingen, maar het is hoe dan ook nefast voor de signaalsterkte. De voornaamste oorzaak van storing is de aanwezigheid van metaal, want dat **reflecteert** de signalen. In gebouwen zit er heel wat van verwerkt, denk maar aan staalnetten in funderingen. Maar ook materialen met een hoge dichtheid, zoals beton, maken het voor signalen heel wat moeilijker om te penetreren dan door bijvoorbeeld een gipsmuur.

Volgens de [802.11b](#) standaard gebruikt een WiFi-sigitaal een frequentie van 2,4 GHz, net als microgolfovens, sommige GSM's, ... Door het delen van deze frequentie is het niet meer dan normaal dat ze **elkaars signaal nadelig beïnvloeden**.

Om te voorkomen dat je overbodige investeringen zou maken, staan er in dit hoofdstuk een aantal richtlijnen die je in acht kan nemen bij de aankoop van je toestellen. De voorbeeldsituaties kunnen je helpen bij deze keuzes.

### ***Voorbeeld 1: Appartement***

Indien je in een appartement woont, is het absoluut niet nodig om de allernieuwste draadloze router te kopen. Naarmate de aankoopprijs van zulk een apparaat stijgt, zal het bereik toenemen. Eigenlijk is het hier dus heel eenvoudig:

- Je zorgt ervoor dat je computer over de mogelijkheid beschikt om draadloos te kunnen surfen
- Je plaatst de router bij de modem (de positie is helemaal niet zo belangrijk, aangezien je bereik ruim zal volstaan om je appartement te bedekken)

- Over het algemeen is elke draadloze router gelijkwaardig op het vlak van veiligheid.

## ***Voorbeeld 2: Huis***

Als je naast de werkruimte ook netwerktoegang wenst in de kamers op de bovenverdieping van je huis, moet je al beter nadenken over de plaatsing van de router. In de meeste gevallen is het voldoende om de router centraal in huis te plaatsen, maar soms heb je bijkomende apparatuur nodig om je netwerk uit te breiden.

Wil je bijvoorbeeld twee verdiepingen overbruggen is het aangeraden van een kabel te leggen naar je bovenverdieping. Hiermee kan je de computer rechtstreeks verbinden of je plaatst er een acces point. Als je van plan bent meerdere computers op verschillende plaatsen te gebruiken, gebruik je best een acces point.

- Plafonds laten radiosignalen heel moeilijk door, een extra investering is meestal noodzakelijk.

# Hoofdstuk 5: Hoe installeer en configureer ik mijn apparaten?

## *Installatie van de router*

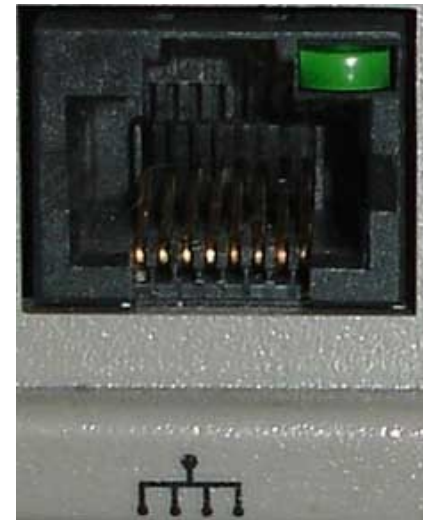
Bij de installatie van de router moeten we het onderscheid maken tussen een router, zonder meer, en een router met geïntegreerde modem. In het laatste geval moet de router geplaatst worden bij het aansluitpunt van de telefoonlijn of kabel distributie.

- Let op het dat je het juiste routertype koopt. Er is wel degelijk een verschil tussen een adsl en kabel aansluiting.

Wanneer met een aparte modem gewerkt wordt, kan je de router eender waar plaatsen, zolang je een ( kabel-) verbinding tussen router en modem kan maken.

Een draadloze router heeft tegenwoordig meestal vier aansluitpunten voor een ethernetkabel. In die poort dient de aansluiting met de modem gemaakt te worden. De rest van de verbindingen gebeurt draadloos. Wanneer je de kabel tussen de twee apparaten aansluit moet het controlelampje ofwel constant branden, ofwel knipperen.

Nu is de fysieke verbinding gemaakt. De router is met de modem verbonden en de modem op zijn beurt met de telefoonlijn of de kabel distributie. Het is tijd om de verbinding door te trekken naar de computers.



**Ethernetpoort**

- Om de router te configureren sluiten we de computer met een ethernetkabel aan.

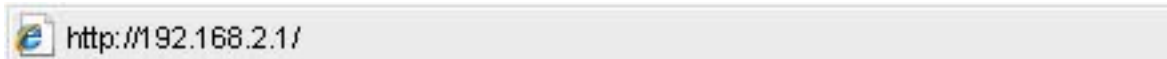
Omdat de interface van elke producent er verschillend uitziet kunnen we deze uiteraard niet allemaal behandelen. We geven één uitgebreid voorbeeld aan de hand van de interface van een *Belkin wireless* router + adsl modem. Tijdens dit voorbeeld komen veel van de reeds behandelde thema's terug. Dus lees, indien u dit nog niet gedaan heeft, voorgaande hoofdstukken eerst!

Om aan de configuratie van je router te kunnen beginnen is het best dat je je computer rechtstreeks aansluit via een kabel. Dit om te voorkomen dat, wanneer je een instelling aanpast, je jezelf buitensluit.

Om je router te kunnen bereiken heb je zijn [ip-adres](#) nodig. Dit kan je makkelijk vinden aan de hand van volgende handelingen:

- Start >> Alle programma's >> Bureau-accessoires >> Opdrachtprompt
- In dit venster typ je: ipconfig
- Het **ip-adres** van je router is te vinden achter "standaardgateway" of "defaultgateway"
- Als hier geen **ip-adres** staat, heb je waarschijnlijk een fout **ip-adres** op je computer. Je moet dan de instellingen van je **netwerkadapter** aanpassen.

Nu je het juiste **ip-adres** gevonden hebt, kan je met je browser surfen naar dat adres:



Het resultaat hiervan is dat je belandt op de basispagina van je router. Doorgaans wordt hier om een wachtwoord gevraagd. Als je router nog niet eerder geconfigureerd is, vind je dit wachtwoord in de handleiding van je router.

### Het beginscherm:

**BELKIN** Wireless ADSL Modem Router Setup Utility

**LAN Setup**

- LAN Settings
- DHCP Client List

**Internet WAN**

- Connection Type
- DDNS
- DDNS

**Wireless**

- Channel and SSID
- Security
- Wireless Bridge

**Firewall**

- Virtual Servers
- Client IP Filters
- MAC Address Filtering
- DMZ
- WAN Ping Blocking
- Security Log

**Utilities**

- Restart Router
- Restore Factory Default
- Save/Backup Settings
- Restore Previous Settings
- Firmware Update
- System Settings

**Login**

Before you can change any settings, you need to log in with a password. If you have not yet set a custom password, then leave this field blank and click "Submit".

**Password**

Default = leave blank

- Het is zeer belangrijk dat je het wachtwoord van de router onmiddellijk aanpast

Meestal vind je dit onder "system settings".

Het volgende wat je moet doen zijn de beveiligingsinstellingen, de uitleg over de verschillende mogelijkheden vind je in hoofdstuk drie.

## **SSID verbergen**

Deze instelling vind je onder het menu "channel en SSID" of iets gelijkaardig.

### **Wireless > Channel and SSID**

This page allows you to enter the Wireless Network Name (SSID in Wi-fi terminology) and the Wi-Fi Channel number. In the wireless environment the router can also act as an wireless internet access point. These parameters are used for a wireless computer to connect to this wireless base station. [More Info](#)

SSID >	<input type="text" value="netwerknaam123"/>
ESSID Broadcast >	<input checked="" type="radio"/> ENABLE <input type="radio"/> DISABLE
Wireless Mode >	<input type="text" value="Mixed (11b+11g)"/>
Wireless Channel >	<input type="text" value="4"/>

Naast het vinden van een goede netwerknaam (SSID) is het nuttig om deze niet uit te zenden.

Dit bekom je door naast "SSID broadcast" de optie "disable" aan te vinken.

Om vanaf dit moment moeten nieuwe gebruikers om toegang tot je netwerk te krijgen deze netwerknaam invoeren.

Dit doe je door naar

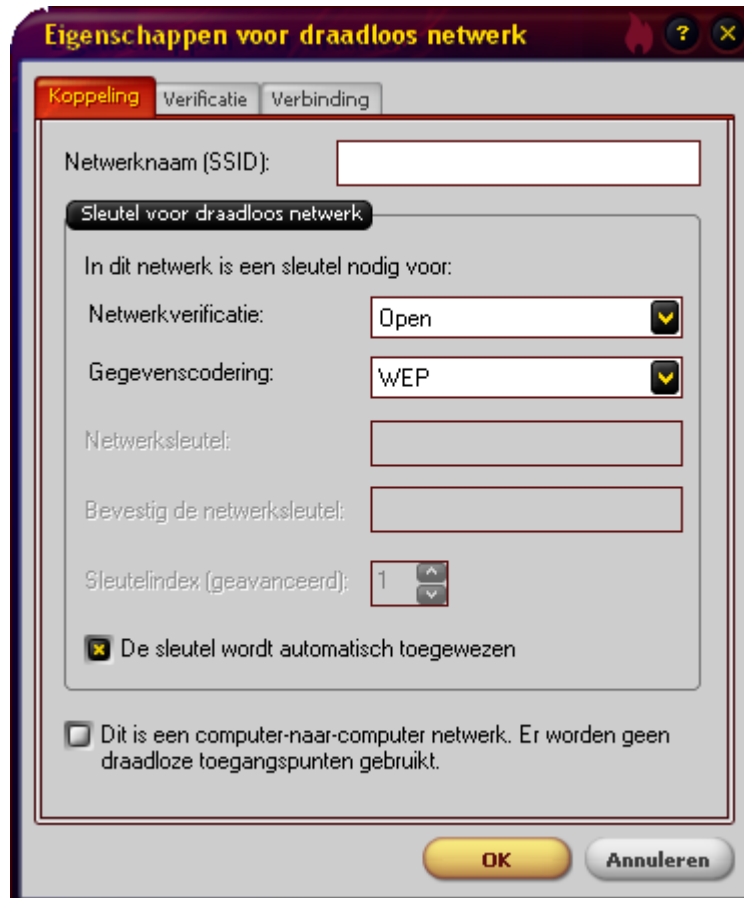
- *Start >> configuratiescherm >> netwerkverbindingen*

te gaan. Daar vind je een icoontje met de naam: draadloze netwerkverbinding. Klik met de rechtermuisknop op dit icoontje en kies "eigenschappen".

Een nieuw venster heeft zich geopend. Hierin dien je het tweede tabblad te selecteren.



Hier moet je het netwerk toevoegen om er toegang tot te krijgen. Dit doe je door op de knop "Toevoegen..." te klikken.



Vul de netwerknaam in en kies de overeenkomstige beveiligingsmethode. Indien je enkel de **SSID** verbergt als beveiliging, dan moet je de opties "Open" en "Uitgeschakeld" kiezen. Let er wel op dat je de netwerknaam exact invoert, pas dus ook op voor hoofdletters - kleine letters.

Als je het netwerk toegevoegd hebt en op de router geen verdere beveiliging ingesteld hebt, kan je nu op je netwerk. De verbinding gaat automatisch gemaakt worden als je binnen het bereik van je router zit.

## Uitschakelen van de DHCP

Als je DHCP op de router uitschakelt, betekent dit dat je zelf een IP-adres aan je computer moet toekennen. En dat dit bovendien een juist IP-adres is. Deze methode is vooral voor gebruikers die de principe van IP-adressering onder de knie hebben.

Het doel is uiteraard van je draadloos netwerk veiliger te maken, dus moet je ervoor zorgen dat je geen standaard IP-adres neemt.

Vb. 192.168.0.1 voor de router en 192.168.0.2-.. voor de computers  
10.0.0.1 voor de router en 10.0.0.2-.. voor de computers

Deze adressen zijn de eerste die iemand zal proberen te gebruiken om toegang tot je netwerk te krijgen.

Wat je dus beter doet is een ander adres gebruiken, je verandert hiervoor het getal op de plaats van de laatste "0" in het adres.

Vb. 192.168.8.1 voor de router en 192.168.8.2-.. voor de computers  
10.0.7.1 voor de router en 10.0.7.2-.. voor de computers

Om deze instellingen te maken dien je eerst je router correct te configureren:

### LAN > LAN Settings

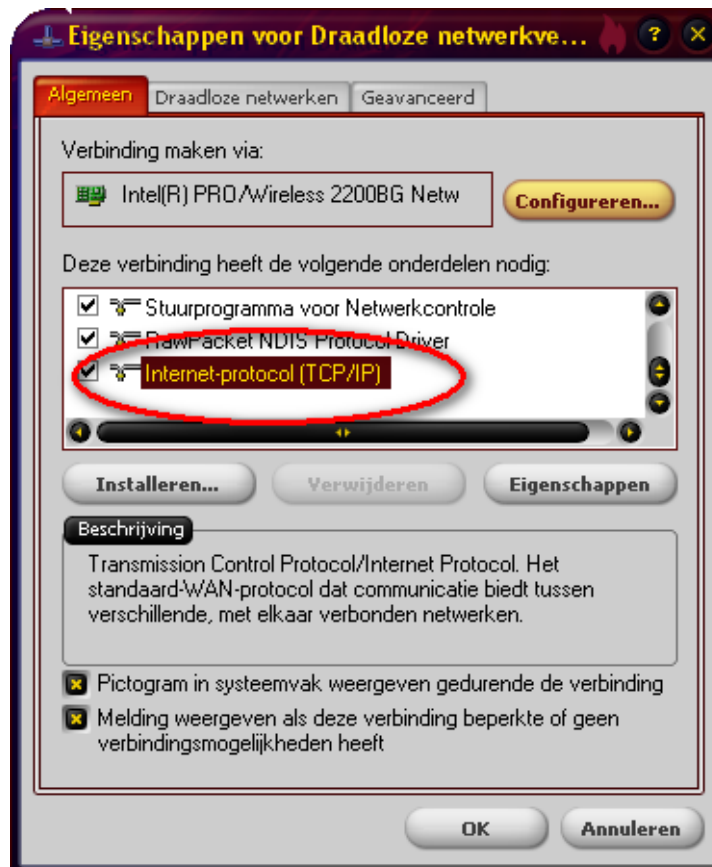
You can make changes to the Local Area Network (LAN) here. For changes to take effect, you must press the "Apply Changes" button at the bottom of the screen.

<b>IP Address &gt;</b>	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="2"/> <input type="text" value="1"/>
<a href="#">More Info</a>	
<b>Subnet Mask &gt;</b>	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/>
<a href="#">More Info</a>	
<b>DHCP server &gt;</b>	<input checked="" type="radio"/> On <input type="radio"/> Off
The DHCP server function makes setting up a network very easy by assigning IP addresses to each computer on the network. It is not necessary to make any changes here. <a href="#">More Info</a>	
<b>IP Pool Starting Address &gt;</b>	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="2"/> <input type="text" value="2"/>
<b>IP Pool Ending Address &gt;</b>	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="2"/> <input type="text" value="100"/>
<b>Lease Time &gt;</b>	<input type="text" value="One Day"/> <input type="button" value="v"/>
The length of time the DHCP server will reserve the IP address for each computer.	
<b>Local Domain Name &gt;</b> (Optional)	<input type="text" value="Belkin"/>
A feature that lets you assign a name to your network. <a href="#">More Info</a>	
<input type="button" value="Clear Changes"/> <input type="button" value="Apply Changes"/>	

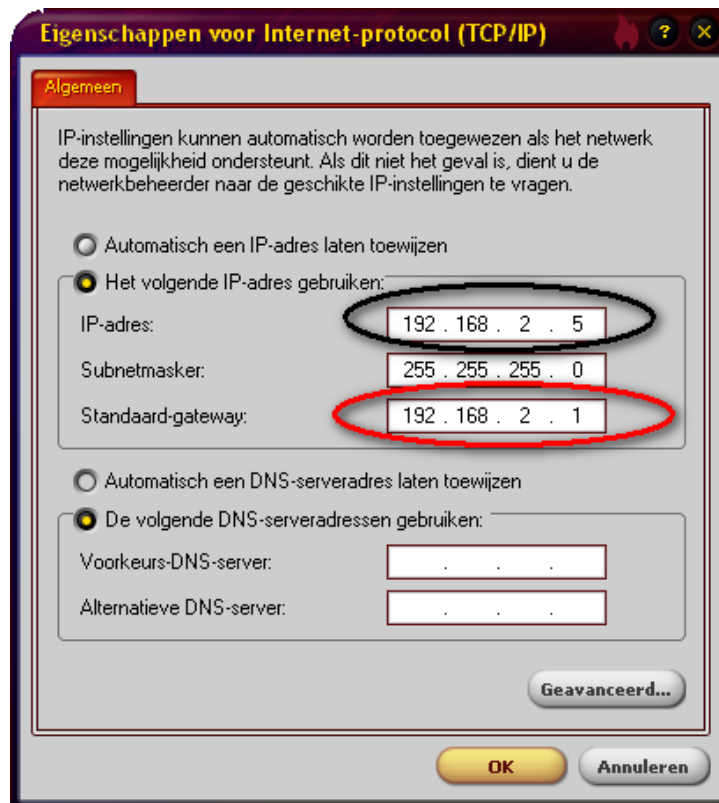
Je vindt op de router de mogelijkheid om bij DHCP "disable" te selecteren. Wanneer je dit doet zullen de computers die op het netwerk willen dus niet langer hun IP-adres toegewezen krijgen door de router. Vergeet ook niet je router zelf een IP-adres te geven.

Nu je router juist is ingesteld moet je het IP-adres van je computer ook juist instellen. In dit voorbeeld zie je dat de router het adres 192.168.2.1 heeft gekregen. We zullen op de computer het adres 192.168.2.5 instellen.

Ga daarvoor terug naar de eigenschappen van de draadloze verbinding:



Dubbelklik op "Internet-protocol(TCP/IP)".



Het zwart omcirkelde tekstvenster is het **IP-adres** van je computer. Hier vullen we in dit geval dus 192.168.2.5 in. Het venster "subnetmasker" wordt automatisch ingevuld wanneer we ons **IP-adres** hebben ingevoerd. Het is van groot belang bij het venster van "Standaard-gateway" het **IP-adres** van je router in te vullen.

- Computers binnen hetzelfde netwerk mogen nooit hetzelfde IP-adres toegewezen krijgen. Het IP-adres dient net om elke computer uniek te kunnen identificeren!

Als je meerdere computers op het netwerk wil toevoegen, dien je dus op elke computer de IP-instellingen manueel aan te passen. Dit is niet het geval als je **DHCP** wel gebruikt, daarom is deze methode niet meteen aangeraden. Het brengt heel wat configuratie met zich mee en het gevaar bestaat dat verschillende gebruikers (= computers) hetzelfde **IP-adres** gaan instellen.

## Lijst met toegelaten MAC-adressen

Deze manier is wel redelijk veilig, maar is vooral geschikt voor een statisch netwerk (een netwerk dat niet vaak van structuur verandert): het toevoegen van nieuwe computers op het netwerk vereist dat je de instellingen van de router aanpast.

Op de router zal een lijst worden opgeslagen met de **MAC-adressen** van de computers die toegelaten moeten worden. Aangezien elke computer vanaf de fabricage een uniek **MAC-adres** gegeven wordt, zal de toegang voor vreemden niet toegelaten worden.

Ga naar de configuratie van je router:

Firewall > MAC Address Filtering

This feature lets you set up a list of allowed clients. When you enable this feature, you must enter the MAC address of each client on your network to allow network access to each. [More Info](#)

Enable MAC Address Filtering >  Enable  Disable

Access Rule for registered MAC address >  Allow  Deny

DHCP Client List: ip=192.168.2.5 name=laptopbati  1

MAC Address Filtering List > (up to 32 computers)

ID	MAC Address
1	: : : : : : :
2	: : : : : : :
3	: : : : : : :
4	: : : : : : :
5	: : : : : : :
6	: : : : : : :
7	: : : : : : :
8	: : : : : : :
9	: : : : : : :
10	: : : : : : :
11	: : : : : : :
12	: : : : : : :
13	: : : : : : :

Je ziet dat de MAC-adressen van de computers die momenteel met het netwerk verbonden zijn, in een lijstje aan te klikken zijn. Achter het **MAC-adres** staat de naam van de computer. Je kiest hieruit het juiste **MAC-adres** en klikt op "toevoegen" of "copy to" om het naar de lijst te kopiëren.

- Let erop dat de regel voor de lijst ingesteld staat op "toelaten" ("allow"), anders loop je het risico dat je jezelf uit je draadloos netwerk sluit.

Wil je een nieuwe gebruiker toevoegen, moet je deze procedure opnieuw uitvoeren, en het **MAC-adres** van de nieuwe gebruiker ook toevoegen.

## WEP

Dit is de eerste vorm van beveiliging die niet enkel de toegang tot het netwerk beperkt, maar ook de gegevens die erover verzonden worden gaat coderen. Indringers kunnen op die manier ook niet het verzonden verkeer afluisteren en analyseren.

De configuratie begint zoals steeds weer op de router:

**Wireless > Security**

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

**Allowed Client Type >** WEP

**WEP Mode >**  64 bit  128 bit

**Key Entry Method >**  HEX  ASCII

**Key Provisioning >**  Static  Dynamic

**Key 1 >** 148852F2CB

**Key 2 >** FE5DCB91F9

**Key 3 >** C6C2540008

**Key 4 >** 387E1F0E3D

**Default Key ID >** 1

**Passphrase >**

[Apply Changes](#) [Clear Changes](#)

Het instellen van WEP is redelijk verwarrend. Het is makkelijker en beter om WPA-PSK in te stellen. De encryptie van WPA is beter en door het gebruik van PSK (pre-shared key) is het veel eenvoudiger als het gebruik van de sleutels van WEP.

Je ziet dat er automatisch sleutels gegenereerd worden, je moet de sleutel die bij "Key1" staat even overschrijven want deze heb je later op de computer nog nodig.

Vanaf het moment dat je op "Apply changes" klikt, verlies je de verbinding met je netwerk, dit is normaal aangezien je netwerk nu beveiligd is en je nog niet de juiste instellingen op je computer hebt aangebracht.

Om dit te doen moet je naar de instellingen van "draadloze verbinding":



Je kiest hier "toevoegen" als de naam van je netwerk nog niet in de lijst staat. Als hij er wel staat klik je op de naam en dan op "Eigenschappen".



Als je "Open" en "WEP" selecteert moet je nog kijken of "De sleutel wordt automatisch toegewezen" niet aangevinkt staat. Sleutelindex mag je op "1" laten staan.

Daarna kan je de sleutel die je van op de router hebt, tweemaal invullen in de voorziene tekstvakken. Klik op "Ok" en je zou terug toegang tot je draadloos netwerk moeten hebben.


## WPA-PSK (WPA2)

Dit is een zeer goede keuze qua beveiliging, ze is makkelijk in te stellen er relatief veilig.

Bij de instellingen van de router ga je naar "Security" en daar kan je "WPA" of "WPA/WPA2" kiezen.

### Wireless > Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. [More Info](#)

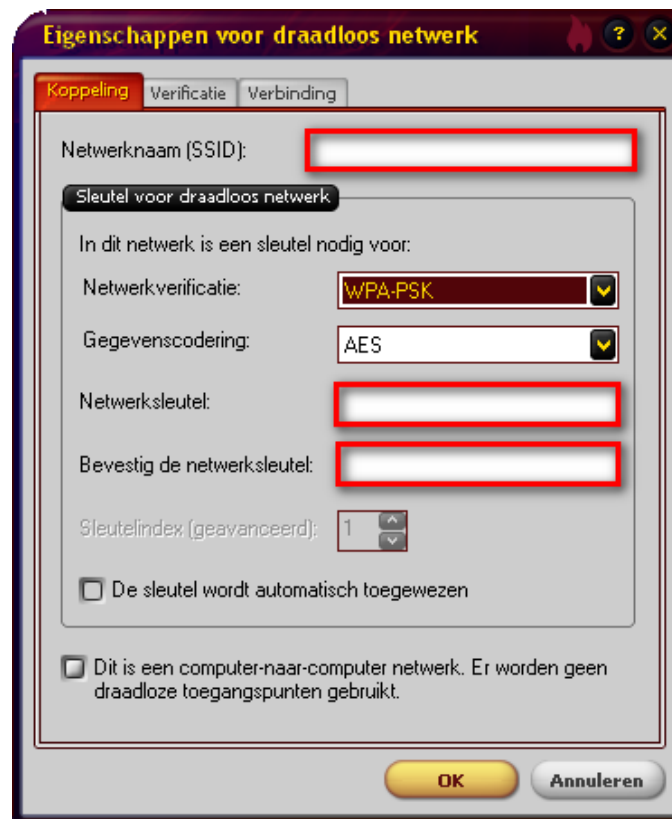
**Allowed Client Type >**  

**Authentication >**  802.1X  Pre-shared Key

**Pre-shared Key >**

Belangrijk is dat je de optie "Pre-shared key" aanduidt. Dit geeft de mogelijkheid om een sleutel in te voeren naar keuze. Uiteraard moet je deze sleutel goed onthouden, wil je terug toegang tot je netwerk krijgen.

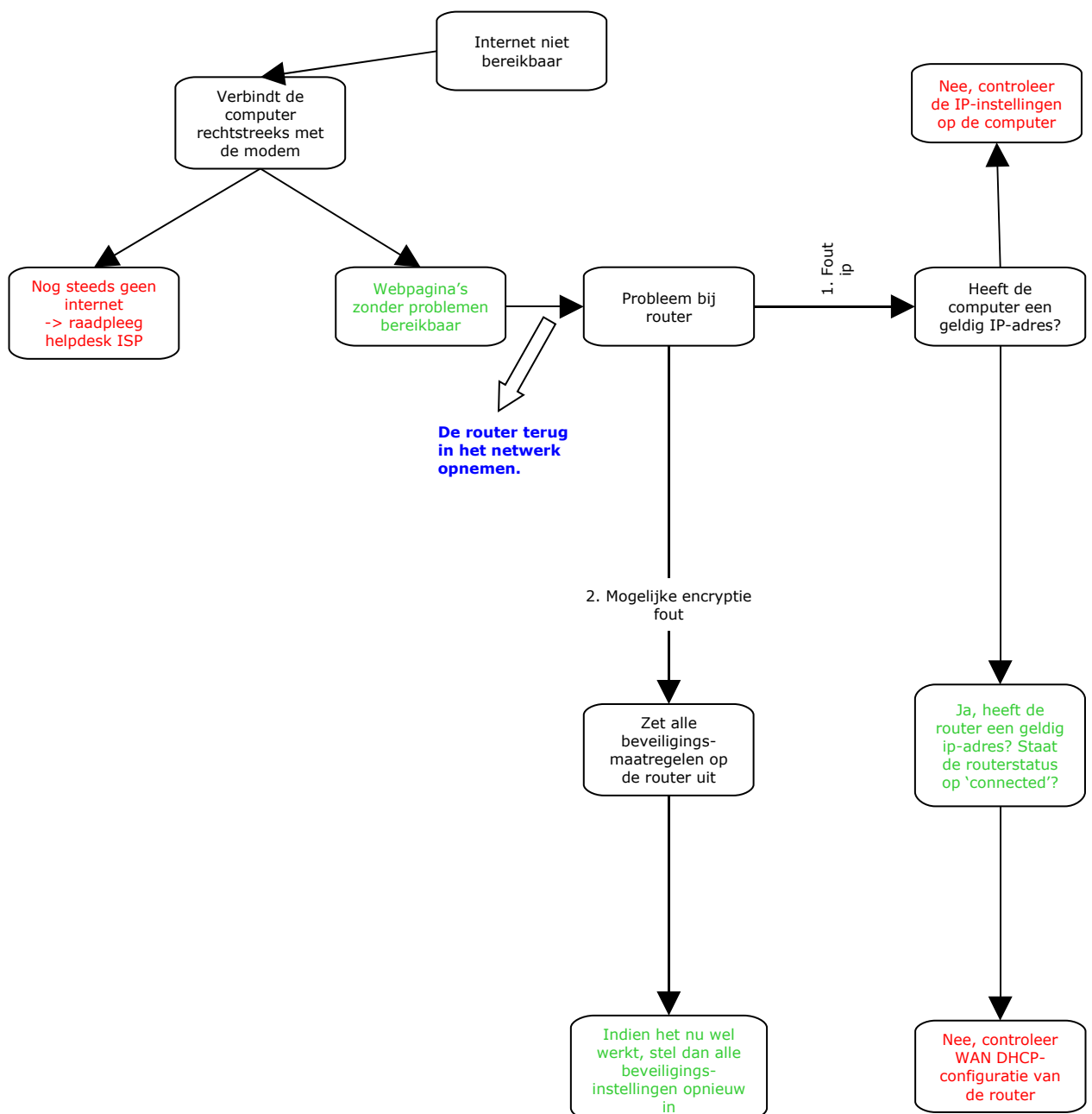
De instelling op de computer begint door naar de instellingen voor draadloos netwerk te gaan, daar je netwerk te kiezen uit de lijst of een nieuw netwerk toe te voegen.



De vakken in het rood moeten ingevuld worden. De netwerknamen en de zelfgekozen sleutel moeten uiteraard dezelfde zijn als op de router. Als deze zaken juist ingesteld zijn, kan je terug verbinding maken met je router.

## Hoofdstuk 6: Eventuele problemen

Bij het opstellen van een thuisnetwerk kan er één en ander mislopen. Zelfs als je de installatieprocedure nauwkeurig uitgevoerd hebt. In dit hoofdstuk worden de meest voorkomende problemen aangekaart. Voor elk probleem kunnen er verschillende oorzaken zijn, aan de hand van je configuratie zal je moeten uitmaken welke oplossing voor jou van toepassing is. Gebruik dit schema om zo de oorzaak van je probleem snel te vinden. Als het probleem gekend is, kan je de oplossing ervan opzoeken in de onderstaande tekst.



## Verbindt de computer rechtstreeks met de modem

Het eerste wat je moet doen is controleren of je op internet geraakt als je je computer rechtstreeks met de modem verbindt (zoals de oorspronkelijke situatie, zonder router). Als dit werkt kan je de router terug aansluiten en de volgende stappen overlopen. Bij problemen is het aangeraden om de helpdesk van je [internetprovider](#) te raadplegen.

## Heeft de computer een geldig IP-adres?

Is de verbinding tussen de computer en de router in orde? Met andere woorden, kan je van op je computer de router pingen?

Om dit te testen ga je naar

- `start >> uitvoeren (sneltoets Windowsknop + "r")`

Typ in het geopende venstertje "cmd" en druk op de enter-toets.

Een command-prompt wordt geopend, hierin moet je het [ping](#) commando typen.

- `ping ip-adres (vb: "ping 192.168.8.1")`

Als je het [ip-adres](#) niet kent, kijk dan terug in hoofdstuk 5.

De [ping](#) is succesvol als je de volgende boodschap krijgt:

```
Pingen naar 10.0.0.42 met 32 byte gegevens:
Antwoord van 10.0.0.42: bytes=32 tijd=1 ms TTL=255
Antwoord van 10.0.0.42: bytes=32 tijd<1 ms TTL=255
Antwoord van 10.0.0.42: bytes=32 tijd<1 ms TTL=255
Antwoord van 10.0.0.42: bytes=32 tijd<1 ms TTL=255
Ping-statistieken voor 10.0.0.42:
  Pakketten: verzonden = 4, ontvangen = 4, verloren = 0
  (<0% verlies>).De gemiddelde tijd voor het uitvoeren van één bewerking in milliseconden:
  Minimum = 0ms, Maximum = 1ms, Gemiddelde = 0ms
```

Een succesvolle [ping](#) betekent dus dat je [ip-adres](#) in orde is.

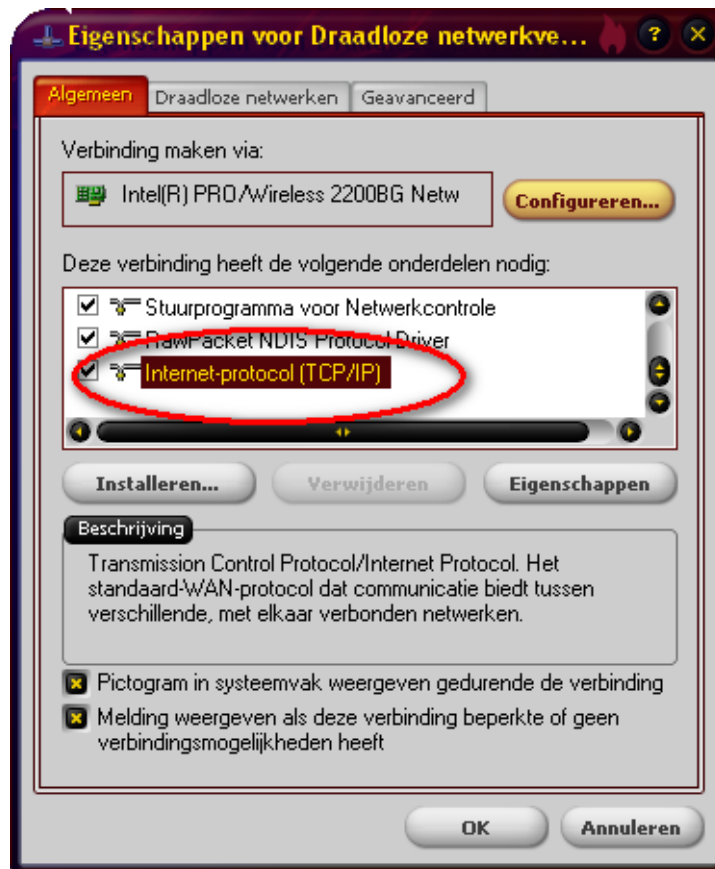
Wanneer deze boodschap niet verschijnt (*time-out bij opdracht*), is er geen juist [ip-adres](#) ingesteld.

## Controleer de IP-instellingen op de computer

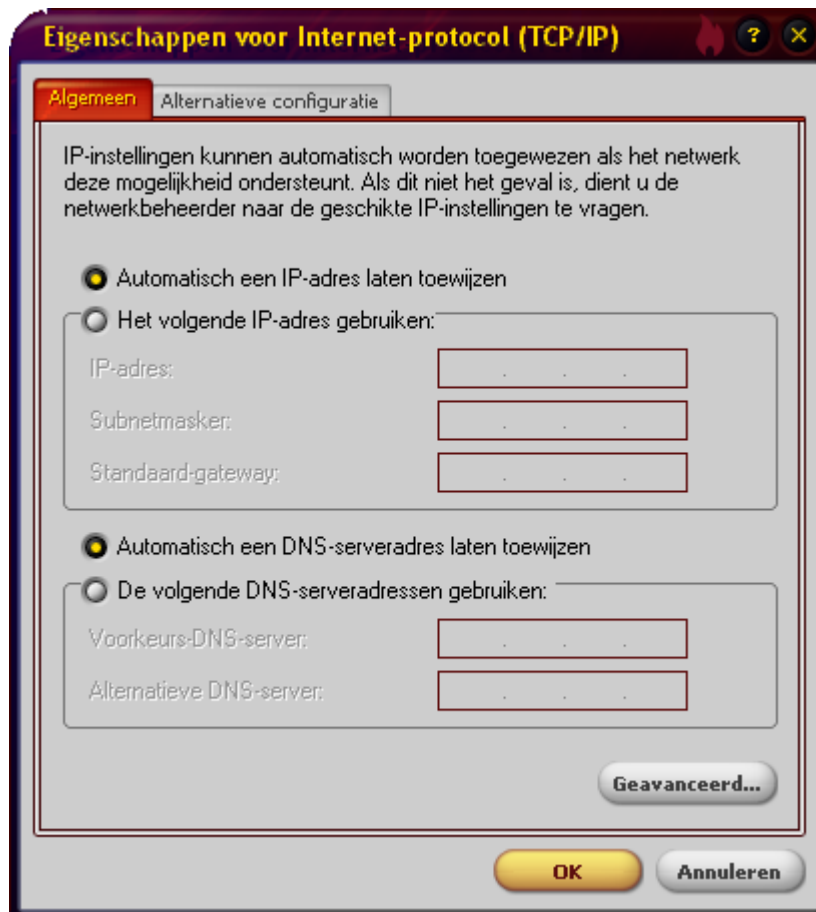
Afhankelijk van de ip-adresverdeling op je router moet je hier nakijken of enerzijds [DHCP](#) ingeschakeld staat, anderzijds of je een geldig<sup>1</sup> [ip-adres](#) gekozen hebt. Je vindt dit door naar "configuratiescherm >> netwerkverbindingen" te

<sup>1</sup> Met een geldig [ip-adres](#) wordt bedoeld dat het [ip-adres](#) binnen hetzelfde domein is als het [ip-adres](#) van de router. Indien dit niet het geval is, kan de router onmogelijk met jou computer communiceren. Zoals eerder vermeld is hier een goede kennis van ip-adressering vereist!

gaan en daar met de rechtermuisknop op "draadloze verbinding" te klikken en eigenschappen te nemen.



Kies "Internetprotocol (TCP/IP)" en klik vervolgens op "Eigenschappen"



## ***Heeft de router een geldig ip-adres? Staat de routerstatus op "connected"?***

Hiervoor moet je naar de administratiepagina van de router gaan, bij *Connection Type*, *WAN settings* of iets dergelijks kan je de connectie-instelling van je router met het internet (je [internetprovider](#)) verifiëren. Indien de routerstatus "connected" is, moet je hier niet verder naar fouten zoeken.

Staat er geen fout bij de [WAN](#)-instellingen van je router? In de meeste gevallen moet de router de gebruikersnaam en het wachtwoord kennen om een verbinding met de [provider](#) te maken. Zorg ervoor dat deze gegevens correct ingevuld zijn!

## ***Zet alle beveiligingsmaatregelen op de router uit***

Als de internetconnectie ondanks al de voorgaande maatregelen nog steeds niet werkt, of als er zich daar geen problemen bevinden, ligt de fout hoogstwaarschijnlijk bij de ingestelde encryptie. Het is noodzakelijk dat de instellingen op de computer overeenkomen met die op de router. Zoniet kunnen beide apparaten niet met elkaar communiceren, waardoor er niet eens verbinding met het lokaal netwerk tot stand kan komen. Om er voor te zorgen dat je de instelling juist configureerd, kijk je best even terug naar hoofdstuk 5.

# Woordenlijst

## 802.11b/i standaard

*Deze standaard laat gecertificeerde toestellen toe een radiosignaal te produceren binnen een frequentie van 2,4 GHz. Naast WLAN's maken microgolfovens, GSM's... gebruik van deze standaard.*

## Computerworm

*Dit is een soort virus dat zich verspreidt via o.a. email.*

## DHCP

*Het Dynamic Host Configuration Protocol (DHCP) is een computerprotocol dat de toewijzing van IP-adressen automatisch afhandelt.*

## Ethernet

*Ethernet is het onderliggende netwerk waarmee computers met elkaar communiceren als ze hardwarematig met elkaar in een netwerk verbonden zijn met behulp van netwerkkaarten en netwerkkabels.*

## Hexadecimale nummering

*Naast het decimale rekenstelsel bestaat ook de hexadecimale notatie, met andere woorden zijn er geen 10, maar 16 verschillende waardes.*

*0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*

*Waarbij A evenveel voorstelt als het decimale 10, B is 11... tot F dat 15 is. In plaats van 48 keer een 0 of een 1 te moeten lezen, maakt de computer deze beter leesbare voorstelling voor ons.*

## Internet Service Provider (ISP)

*De ISP verzorgt je toegang tot het internet (vb. Telenet, Skynet, Chello...).*

## IP-adres

*Dit is een adres dat bestaat uit 32 bits, dus een combinatie van 32 nullen en éénen. Op deze manier kan een ander apparaat binnen het netwerk duidelijk maken dat de verstuurd berichten enkel voor jouw computer bestemd zijn en dat alle andere deze moeten negeren. Opzoeken van jouw IP-adres kan als volgt:*

**Start >> Alle programma's >> Bureau-accessoires >> Opdrachtprompt**

*In dit venster typ je **ipconfig /all***

## LAN (Local Area Network)

*Netwerken van kleine ondernemingen en thuisnetwerken worden ook wel eens LAN's genoemd, verwijzend naar de beperkte grootte van het netwerk.*

## MAC-adres

*Medium Acces Control -adres, in het Nederlands wordt hiernaar verwezen als fysiek adres, omdat dit verwijst naar een wereldwijd uniek nummer op de netwerkadapter. Om dit op te zoeken doe je hetvolgende:*

**Start >> Alle programma's >> Bureau-accessoires >> Opdrachtprompt**

*In dit venster typ je **ipconfig /all***

*Dit adres is geschreven met hexadecimale cijfers en staat gegroepeerd in zes groepjes van 2 hexadecimale nummers (0A-87-B3-44-00-CF).*

## Netwerkadapter

*Op deze adapter zit de apparatuur die je computer toelaat om netwerkverkeer uit te wisselen.*

## Ping-commando

*Met het ping-commando kan je op een eenvoudige manier een verbinding testen.*

## SSID

*Service Set Identifier, een naam van maximaal 32 karakters die je aan je draadloos netwerk toewijst.*

## Trojaanse paarden

*Er wordt een klein programma op de computer geïnstalleerd, zonder medeweten van de gebruiker. Dit programma zorgt ervoor dat hacker via het internet toegang tot de bestanden verkrijgt.*

## WAN

*Wide Area Network. De benaming WAN Link wordt regelmatig gebruikt voor de connectie naar de buitenwereld (het internet).*

## WEP

*Wired Equivalent Privacy, standaard beveiligingsalgoritme voor draadloze netwerken.*

## WLAN (Wireless LAN)

*Het draadloze equivalent van LAN.*

## WPA

*Wireless Protected Access-encryptie wordt als veiliger beschouwd ten opzichte van WEP-encryptie.*

## Bijlage Gezondheidsrisico's

Meer en meer mensen klagen over de gezondheidsrisico's van alle draadloze toepassingen die ontwikkeld worden vandaag de dag. We halen enkele voorbeelden uit de media ter illustratie hiervan. Tot nu toe is er echter nog geen sluitend bewijs over de schadelijke gevolgen van deze technologieën.

### Britse scholen bannen 'on gezond' draadloos internet

In Groot-Brittannië is er een nieuwe paniekgolf ontstaan over de effecten van elektronische straling op de gezondheid. Ditmaal gaat het om draadloos internet: enkele Britse scholen hebben hun draadloze computernetwerk afgebroken omdat leerlingen er onwel van zouden worden.

Ook in andere landen, zoals Oostenrijk, zijn er polemieken ontstaan over de mogelijk schadelijke gevolgen van straling door wifi (de industrienaam voor draadloos internet). De discussie is ongeveer dezelfde als die over schadelijke gevolgen van gsm-straling op het lichaam. Het antwoord dus

ook: men weet het nog niet.

Al jaren volgen studies elkaar op die een verband tussen gsm-stralingen kanker aantonen, die daarna worden tegengesproken door onderzoeken die pal het tegendeel beweren. Het is ook moeilijk te zeggen hoeveel van die studies gesponsord zijn door de telecomindustrie.

De radiogolven die een wifi-basisstation uitzendt, zijn ongeveer dezelfde als degene die door gsm's worden gebruikt. Maar straling die wifi afgeeft, is veel minder krachtig dan die van een gsm-mast. Bovendien warmt de straling van een gsm-toestel het

hoofd van zijn eigenaar veel sterker op - in de eerste plaats omdat het toestel tegen het oor wordt gehouden.

Maar net als bij de gsm zijn er bij een wifinetwerk twee elementen die straling afgeven: de zender en de ontvanger. Wifi en gsm verschillen sterk van elkaar qua zender: voor draadloos internet staat die bijna per definitie dicht bij de gebruiker, terwijl gsm-masten ettelijke kilometers ver reiken. De wifi-ontvanger bevindt zich in de regel niet dicht bij het oor, maar zit wel in een laptop of een ander toestel, dat zich meestal dicht bij het lichaam bevindt. (RME)

Artikel uit De Morgen 26-11-2006

---

### Zeg nee tegen DECT, WiFi, Digitenne en UMTS

Friday, June 20 2003

Zeg nee tegen DECT, WiFi, Digitenne en UMTS Ik ben Ed en ik studeer informatica (univ. Utrecht). Een paar maanden geleden woonde ik nog in een flat in Utrecht. Ik werd vaak geplaagd door slaapproblemen, hoofdpijn, concentratieproblemen en vooral een tekort aan energie. Studeren werd bijna onmogelijk. Toen ik een keer een paar weken op vakantie ging naar Frankrijk, bleken deze problemen ineens te verdwijnen. Weer terug in Utrecht kwamen de problemen bijna direct weer terug. Toen ik een keer bij mijn ouders ging logeren, verdwenen de problemen echter weer.

Ik ben toen op onderzoek gegaan en kwam er via internet achter dat mijn klachten wel eens met zogenaamde electrosmog te maken zou kunnen hebben. Om de proef op de som te nemen, heb ik toen in Duitsland een hoogfrequente veldsterkte meter gekocht. Met dit apparaat kan de kracht van de hoogfrequente golven in de lucht gemeten worden.

Ik woonde in Overvecht op de 3e verdieping. Als ik met de meter in mijn hand de trap op liep, zag ik de veldsterkte per verdieping sterk oplopen. Op de 3e verdieping bleek de waarde zo hoog, dat alle rode lampjes gingen branden. Ter vergelijking heb ik toen ook de waarden bij het huis van mijn ouders gemeten en deze waren binnenshuis vele malen (meer dan faktor 200) lager.

Ik heb toen de meest geschikte kamer uitgezocht en die ingericht als slaapkamer en ben toen verhuisd naar het electrosmog-vrije platteland. Na een paar dagen kreeg ik steeds meer energie en ging ik ook weer veel beter slapen. Mijn studie ging ook meteen een stuk beter.

Maanden hierna begon ik echter weer het duffe gevoel in mijn hoofd te krijgen. Ik heb toen weer de meter uit de kast gehaald en ben gaan testen. Wat blijkt: De waarden zijn meer dan het honderdvoudige dan wat ze eerst waren. Zelfs op het "platteland" is niet meer aan electrosmog te ontkomen. Wat nu? Verdere uitwijkmogelijkheden heb ik niet meer. Ik kan overwegen te verhuizen naar het platteland in Frankrijk. Daar is er geen GSM-zendmast te bekennen, van DECT telefoons hebben mensen nog nooit gehoord en de meter geeft alleen

maar groene waarden aan. Daar voel ik me dan ook altijd opperbest. Helaas is dat om meerdere redenen geen praktische oplossing, zoals de lezer zal begrijpen.

Ik besluit om maar snel de studie af te ronden, de duifheid maar te accepteren en na de studie zien we wel weer verder. Maar, bedenk ik me, er is wel iets wat ik hieraan kan doen. Ik kan proberen de burgers te overtuigen van de gevaren van electrosmog. Hoewel ik bovenmatig veel last heb van electrosmog, schaadt het zonder twijfel de gezondheid van ieder mens en dier.

In Duitsland zijn zo'n vijftig professoren en doktoren begonnen met een actie. Ze hebben namelijk geconcludeerd dat electrosmog in zeer veel gevallen de oorzaak is van moderne degeneratieve ziekten. Het simpelweg uitzetten van de DECT-telefoon doet in veel gevallen alle ziekteverschijnselen verdwijnen. Denk hierbij aan ziektes als chronische vermoeidheid, M.E., fibromyalgie, allergieën, en nog wat meer ziekten waar de reguliere medische wetenschap maar geen oplossing voor kan vinden.

Nagenoeg iedereen heeft inmiddels wel een of meerdere draadloze, digitale telefoons in huis. Het probleem zit hem in het basisstation / oplaadstation van deze overigens zeer handige draadloze telefoons. Het DECT basisstation zendt 24 uur per dag een sterk gepulseerd signaal de ether in. Zelfs wanneer het toestel in het basisstation staat of zelfs wanneer het handtoestel uit staat, blijft het doorzenden. De DECT standaard voorziet namelijk in de communicatie met maximaal acht handtoestellen en het basisstation moet "dus" constant een bericht uitzenden in de trend van: "Hier is het basisstation.. Maak met mij verbinding als je met een nieuw handtoestel naar binnen loopt".. De kracht waarmee een DECT basisstation zendt is zeer hoog. Zonder obstakels kan tot op meer dan honderd meter gecommuniceerd worden en de straling reikt dwars door dikke betonnen muren heen en bereikt met gemak de slaapkamers.

Zoals wel bekend is, gebeurt de communicatie in het menselijk lichaam met kleine elektrische stroompjes. Tijdens de slaap probeert het lichaam te herstellen en gaat deze proberen te synchroniseren met het aardmagnetisch veld. Wanneer dan een DECT basisstation continu staat te zenden, kan er van dit herstel geen sprake zijn. De persoon stapt vermoeid uit bed, alsof hij/zij helemaal niet geslapen heeft. Dag na dag gaat dit proces voort, totdat de een of andere ziekte zijn intrede doet. Vooral kinderen zijn erg gevoelig voor dit soort straling. Groot was dan ook mijn verbazing toen Philips introduceerde een op DECT-gebaseerde babyfoon te introduceren.

Nu zijn dit wel genoeg details. Mijn oproep aan iedereen is het volgende: Wilt u alstublieft uw DECT telefoon uitschakelen en weer overschakelen naar een "ouderwetse" telefoon met een draad eraan. Wilt u toch echt draadloos telefoneren, dan is een analoge draadloze telefoon nog een optie. Deze heeft twee voordelen: Deze telefoons en basisstations zenden alleen wanneer dat nodig is (wanneer u telefoneert) en ze sturen een zwakker, ongepulst signaal, wat veel minder negatieve effecten heeft op de biochemische processen in een lichaam.

Uw voordeel is dat u geen risico meer loopt om electrosmog gerelateerde ziekten op te lopen. Het mogelijke voordeel voor uw kinderen is dat de kans op leukemie en andere kwaadaardige ziekten vele malen kleiner wordt en dat hun hersenen niet aangetast worden. Deze straling zorgt er namelijk voor dat de hersen-bloedbarrière niet meer goed werkt. Wanneer bepaalde eiwitdeeltjes in de hersenen terecht komen, kunnen deze (aantoonbaar uit dierproeven) zeer grote schade aanrichten. Autopsie na de dierproeven toont zelfs aan dat op de hersenen grote zwarte vlekken ontstaan.

Houd ook in ogenschouw dat u met de aanschaf van wat extra luxe (draadloos bellen, draadloos netwerk, etc) ook nog iets anders in huis haalt: Veel extra risico's. Weeg de twee dus goed af: Welk risico wil ik lopen voor welke toename van luxe ?

Het aardmagnetisch veld is de laatste twee decennia 200.000 maal in kracht toegenomen. De hoeveelheid negatieve ionen, meetbaar in de lucht, is van 4000 deeltjes per kubieke centimeter gedaald naar zo'n 300 deeltjes. De populatie kleine vogels is gedaald naar bijna nul (herinnert u zich nog de tjirpende mussen van zo'n 10 jaar terug ?). Als in 2004 de UMTS-masten beginnen met zenden, zal het echt problematisch worden. Onderzoekers voorspellen dat tot 60% van de bevolking ziek zal worden.

De voorspellingen van deze onderzoekers worden genegeerd en tegengesproken door zowel de regering (ja, zelfs de "groene" partijen) als natuurlijk de telecomproviders zelf. En dan zijn er de (vele) studies die objectief aantonen dat er een sterk verhoogde kans op kanker is bij muizen die blootgesteld worden aan stralingen van een normale GSM telefoon. Hierop reageert de telecomindustrie met door hun gefinancierde studies die aantonen dat er geen verschil zou zijn tussen de blootgestelde en de controle groep. Wat blijkt, de controle groep bestaat voor 75% uit muizen die genetisch reeds een hoge kans op kanker hadden. Beide groepen krijgen kanker en dus is er geen verschil tussen beide groepen. En zo zijn er nog veel meer voorbeelden. Welke groep wetenschappers u vertrouwt, moet u zelf beslissen, maar het is in ieder geval duidelijk dat de ene groep veel grotere economische belangen heeft dan de andere. Dit doet ook denken aan de tabaksindustrie, die keer na keer bleef ontkennen dat er enige schadelijke effecten voor de gezondheid zouden zijn bij het roken.

Ed.

Bron: <http://www.electroallergie.org/downloads/Ervaringsverhalen/Zeg%20nee%20tegen%20DECT.pdf>

Indien u zelf ook de negatieve gevolgen van straling in uw omgeving vreest, kan u hier terecht voor een aantal beschermende producten:

<http://www.vitalitools.nl/>

In de academische wereld neemt niet iedereen de dreiging van de radiogolven even serieus. De volgende paper van het MIT drijft de spot met de groeiende onrust omtrent radiogolven.



**"On the Effectiveness of Aluminium Foil Helmets: An Empirical Study"**

<http://people.csail.mit.edu/rahimi/helmet/>