Overal wifi: 25 tips voor je draadloze netwerk

Door: Toon van Daele | 02 februari 2018 11:49

HOW TO

Inhoudsopgave

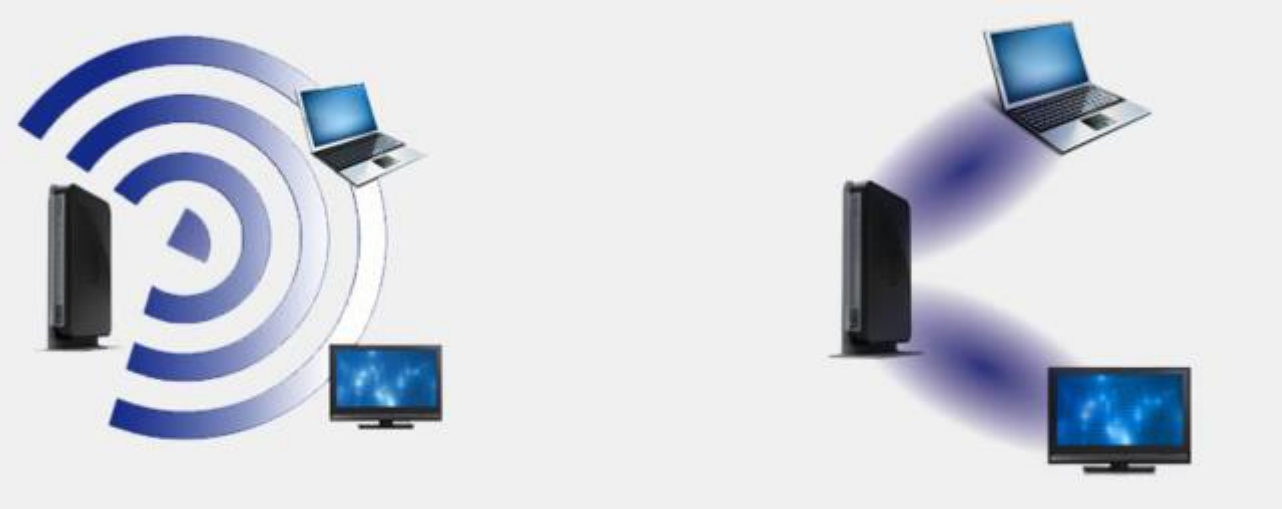
Een (draadloos) netwerk is een complex samenspel van allerlei hardware, drivers, protocollen en software. Zodoende kan het verdraaid lastig zijn een oplossing te vinden als je ergens vastzit of er iets fout loopt. Je wilt immers overal wifi hebben. In dit artikel hebben we maar liefst 25 wifi-perikelen verzameld en van mogelijke oplossingen voorzien. Je zult zien dat de oorzaak van een wifi-probleem ook best elders in je netwerk kan liggen.

1 Optimale positie

Wat is de optimale positie voor mijn draadloze router of toegangspunt?

Om uit te vissen waar je je draadloze router of toegangspunt het best kunt plaatsen, kun je een ‘site survey’ uitvoeren, bijvoorbeeld met het gratis Ekahau Heatmapper of met de betaalde variant van NetSpot. Het komt erop neer dat je de software op een laptop installeert, waarna je door je woning wandelt en veelvuldig je actuele locatie aanduidt. Na afloop geeft de tool de sterkte van het wifi-signaal op al die locaties weer (‘heatmap’). Herhaal deze procedure nadat je bijvoorbeeld de router of het toegangspunt hebt verplaatst, zodat je weer de optimale positie kunt bepalen.
Overigens moet je wel weten dat een draadloze router een min of meer bolvormig signaal in nagenoeg alle richtingen uitzendt, zodat er doorgaans heel wat signalen verloren gaan. Ben je van plan een 802.11ac-router aan te schaffen, dan kun je een model met ‘beamforming’ overwegen. Die stuurt de signalen dan automatisch zo veel mogelijk richting je (ac-)clients.

Wat trouwens de beste positie voor de routerantennes betreft: daar kunnen we helaas geen eenduidig op geven, zoals ook wel hieruit blijkt.



Links een ‘klassiek’ bolvormig wifi-signaal, rechts een router met beamforming.

2 Beperkt bereik

Het signaal van mijn draadloze router komt niet tot in de slaapkamer.

Er zijn diverse (mogelijke) oplossingen voor dit probleem, gesteld dat een herpositionering van je router niet helpt of niet mogelijk is (zie vraag 1). Je kunt overwegen een range-extender of repeater in te zetten, een oplossing die momenteel wordt gepromoot door provider Ziggo. Zo’n apparaat plaats je doorgaans op een plek waar het nog minstens 50 procent van het signaal van je router oppikt. Houd er echter rekening mee dat zo’n repeater de snelheid van het wifi-signaal doorgaans halveert. Dat geldt niet per se voor multiband-repeaters (zoals de ASUS ExpressWay), die één radio toewijzen aan de verbinding met de router en de andere gebruiken voor de verbinding met de client.

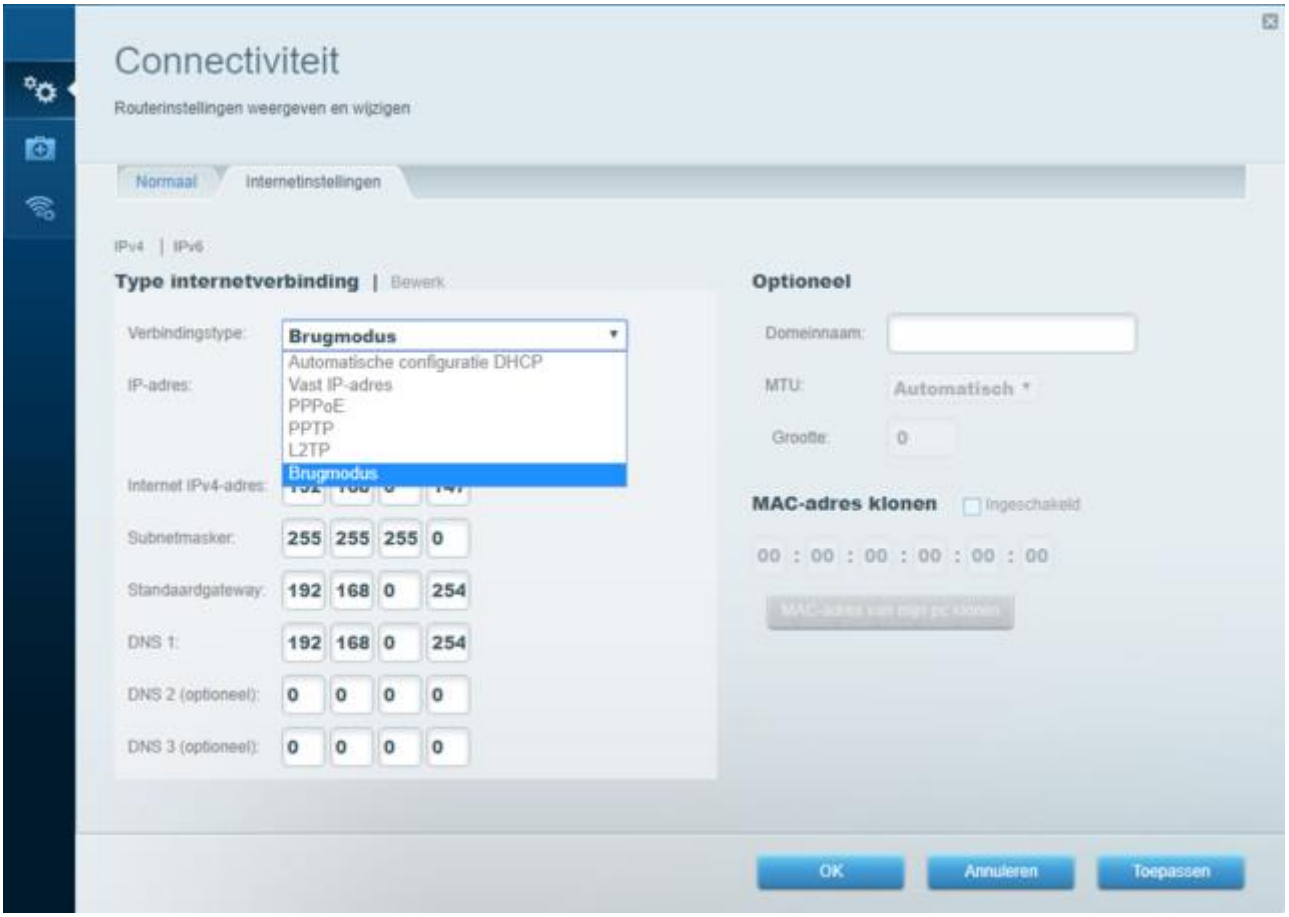
Een alternatief is een Homeplug (AV)/Powerline-set, die handig gebruik kan maken van het stroomnet. Een derde mogelijkheid is het inzetten van een tweede router of toegangspunt (zie ook vraag 3). Tot slot kun je nog investeren in een heus mesh-netwerk, waarbij één router-unit op je modem is aangesloten en het wifi-signaal tussen de andere units wordt gecommuniceerd, wat zorgt voor een beter bereik (zie het artikel rond wifi-mesh elders in dit nummer).

Multiband-repeaters kunnen twee radio’s inzetten zodat de volledige bandbreedte behouden blijft.

3 Tweede router

Ik heb nog een (oude) router liggen. Kan ik die inzetten om het draadloze bereik te vergroten?

Dat is inderdaad mogelijk. Dat gaat het makkelijkst als je tweede router een bridge- of repeater-modus ondersteunt, maar je kunt die ook zo instellen dat die als een draadloos toegangspunt fungeert. De eenvoudigste opzet is die waarbij je een lan-poort op elk van beide routers via een utp-kabel (en een switch) met elkaar verbindt. Je zorgt er tevens voor dat het wan-ip-adres van de tweede router, die niet rechtstreeks met je modem is verbonden, binnen hetzelfde subnet ligt als dat van je eerste router – bijvoorbeeld 192.168.0.200 wanneer router 1 als lan-ip-adres 192.168.0.1 heeft. Let er wel op dat het adres dat je aan router 2 geeft niet binnen het dhcp-bereik van router 1 valt. Je geeft beide wel hetzelfde subnetmasker mee (wellicht 255.255.255.0 of /24). Schakel bovendien de dhcp-service op router 2 uit.



Wel zo makkelijk wanneer je (tweede) router een bridge-modus ondersteunt.

4 Automatisch overschakelen

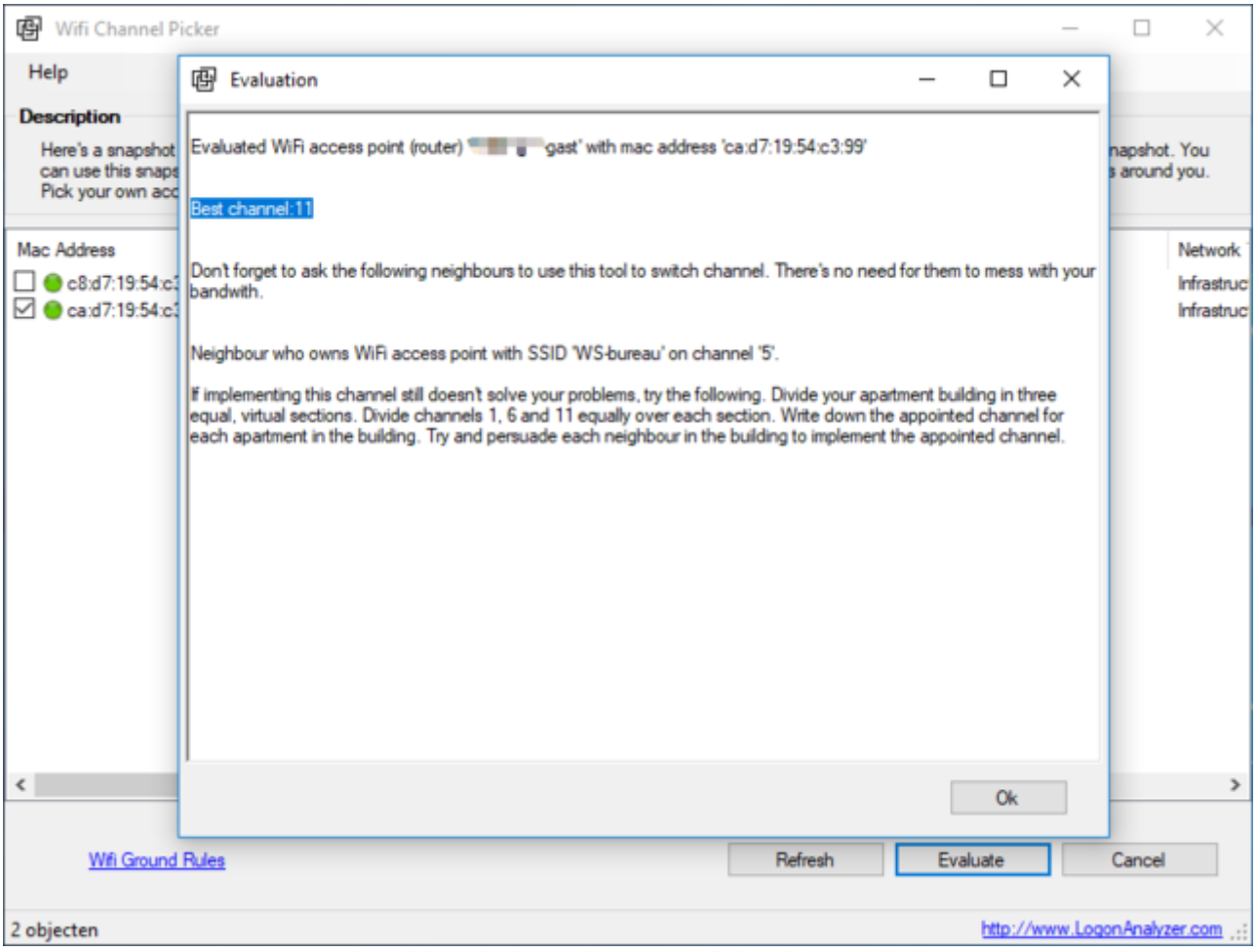
Als ik met mijn mobiele toestel naar boven ga, schakelt die niet (altijd) automatisch over naar het toegangspunt op de eerste verdieping.

In de meeste gevallen is het aan te raden op beide toegangspunten hetzelfde ssid in te stellen, net als dezelfde encryptiestandaard en hetzelfde wachtwoord. Stel elk van beide echter in op een (zo) verschillend (mogelijk) kanaal. Wanneer je je nu naar het andere toegangspunt begeeft, zal een client die continu checkt of er toegangspunten met hetzelfde ssid in de nabijheid zijn dankzij het sterkste signaal automatisch overschakelen naar dat toegangspunt Afhankelijk van de draadloze netwerkadapter op je laptop kun je dat automatisch overschakelen ook iets sneller laten verlopen. Open **Apparaatbeheer** (**devmgmt.msc**) en roep het eigenschappenvenster van je draadloze netwerkadapter op. Met wat geluk tref je op het tabblad **Geavanceerd** de optie **Roaming aggressiveness**. Ga na wat er gebeurt als je die op een iets hogere waarde instelt. Op een Android-toestel kun je de installatie van de gratis app Wifi Roaming Fixoverwegen, die iets soortgelijks doet.

5 Kanaal

Mijn wifi-verbinding laat het geregeld (even) afweten: de ene keer werkt het, de andere keer niet.

In veel gevallen heeft een wegvallend signaal te maken met interferentie, vooral wanneer je apparaten zich via de 2,4GHz-band verbinden. Dit spectrum wordt namelijk óók gebruikt door andere apparaten, zoals magnetrons, draadloze telefoons en babyfoons. Of misschien word je geplaagd door naburige draadloze netwerken die zich van datzelfde spectrum bedienen. In de meeste gevallen helpt het dan om voor je eigen draadloze netwerk een ander wifi-kanaal in te stellen, dat bij voorkeur minstens vijf kanalen is verwijderd van dat van het (meest) storende netwerk. Tools als NetSpot en WIFI Channel Picker helpen je bij het opsporen van de meest gebruikte kanalen, zodat je op basis daarvan zelf het ideale kanaal kunt instellen.



Vooral binnen de 2,4GHz-band kan de kanaalkeuze wel degelijk een belangrijke rol spelen.

6 Toch wifi

Hoe sluit ik mijn apparaat zonder wifi toch aan op mijn draadloze netwerk?

Als je apparaat over een usb-poort beschikt, kun je een usb-naar-wifi-adapter gebruiken. Zo'n dongle kost je tussen de 10 en de 30 euro, afhankelijk van de specificaties (bijvoorbeeld single band 802.11n versus dual-band 802.11 ac), en kun je bijvoorbeeld gebruiken op een oude laptop of een Raspberry Pi zonder wifi-ondersteuning. Voor deze laatste vind je de nodige instructies hier. Gaat het om een desktop-pc die je van wifi wilt voorzien, dan is een interne wifi-kaart ook een optie (prijzen rond de 20 euro).

Je kunt het natuurlijk ook over een andere boeg gooien en een wireless bridge inzetten. Zo'n apparaat pikt het draadloze signaal van je toegangspunt of router op en voorziet in een switch waarop je bekabelde toestellen kunt aansluiten. Overigens zijn er ook draadloze routers en toegangspunten die zich als wireless bridge laten instellen.

7 Altijd thuis

Ik heb een draadloze printer, maar die is opeens niet meer bereikbaar.

Dat komt wellicht doordat je printer een ip-adres krijgt toebedeeld via de dhcp-service van je router. Het valt niet uit te sluiten dat die op een bepaald moment, bijvoorbeeld na een reset, een ander ip-adres aan je draadloze printer toekent. Je doet er daarom goed aan apparaten die je altijd op hetzelfde ip-adres wilt kunnen bereiken, zoals een printer, nas of ip-cam, een vast ip-adres mee te geven dat buiten de adrespool van je router ligt. Als het ip-bereik bijvoorbeeld tussen 192.168.0.10 en 192.168.0.50 ligt, dan zou je als adres 192.168.0.51 kunnen nemen. Een handig alternatief is dhcp-reservering. Je geeft in je router dan zelf aan welk toestel, op basis van apparaatnaam of mac-adres, altijd hetzelfde ip-adres uit het dhcp-bereik moet krijgen.

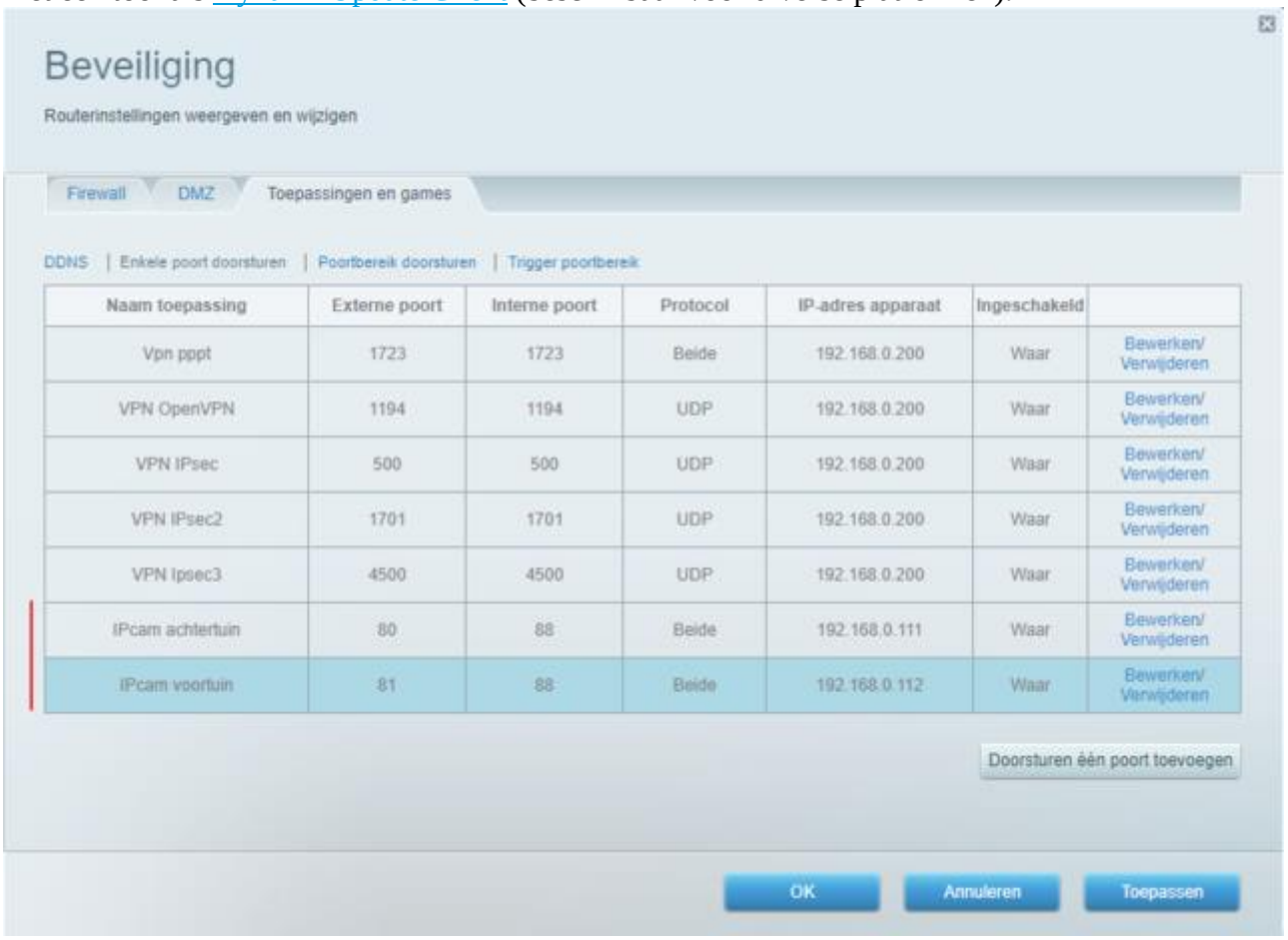
Dhcp-reservering zorgt ervoor dat een toestel altijd hetzelfde ip-adres krijgt toegewezen.

8 Van buitenaf

Ik heb een draadloze ip-camera hangen die ik ook graag via internet wil benaderen.

De kans is reëel dat je dan één of meerdere poorten in je router moet openzetten. Indien je ip-camera luistert op poort 88, dan ga je naar een rubriek als **Port forwarding** in je router en vul je het interne ip-adres van je ip-camera in en geef je zowel bij de externe als de interne poort **88** mee. Het is echter ook mogelijk bij de externe poort bijvoorbeeld 80 in te vullen als

je voor de benadering van je ip-camera liever niet telkens :**88** in de url wilt opnemen. Als protocol kies je dan tcp of udp – of beide (raadpleeg de handleiding bij je ip-cam). Overigens vind je op hier instructies voor tal van routermodellen. Vervelend is wel dat je dan het (actuele) wan-ip-adres van je netwerk moet kennen om je ip-cam te bereiken. Dat kun je oplossen met een dynamische dns-service – zoals het gratis Dynu, eventueel in combinatie met een tool als Dynu IP Update Client (beschikbaar voor diverse platformen).



9 Mobiele hotspot

Hoe maak ik met mijn mobiele apparaat toch een wifi-connectie als er geen draadloos netwerk beschikbaar is?

Stel, je hebt op je hotelkamer wel een bekabelde verbinding voor je laptop, maar geen wifi voor je tablet of smartphone. Of je hebt een 4G-verbinding voor je smartphone, maar er is geen bekabelde of draadloze verbinding voor je laptop. Dan maak je van je laptop of smartphone een mobiele hotspot. Op je laptop met Windows 10 (jubileumupdate) kan dat via **Instellingen / Netwerk en internet / Mobiele hotspot**, waar je de schakelaar op **Aan** zet en de – bekabelde – internetverbinding selecteert die je wilt delen. Via **Bewerken** verzin je dan een eigen ssid en wachtwoord of je zet een tool in als Virtual Router.
Ook je smartphone laat zich echter als mobiele hotspot inzetten: voor Android vind je de nodige instructies hier en voor iOS kun je hier terecht.

10 Verkeerd verbonden

Ik kom niet meer op het draadloze netwerk met mijn wifi-printer.

Het komt wel vaker voor: opeens lukt het niet meer om een wifi-apparaat met je draadloze netwerk te verbinden. Dat kan bijvoorbeeld gebeuren wanneer de netwerkconfiguratie van het

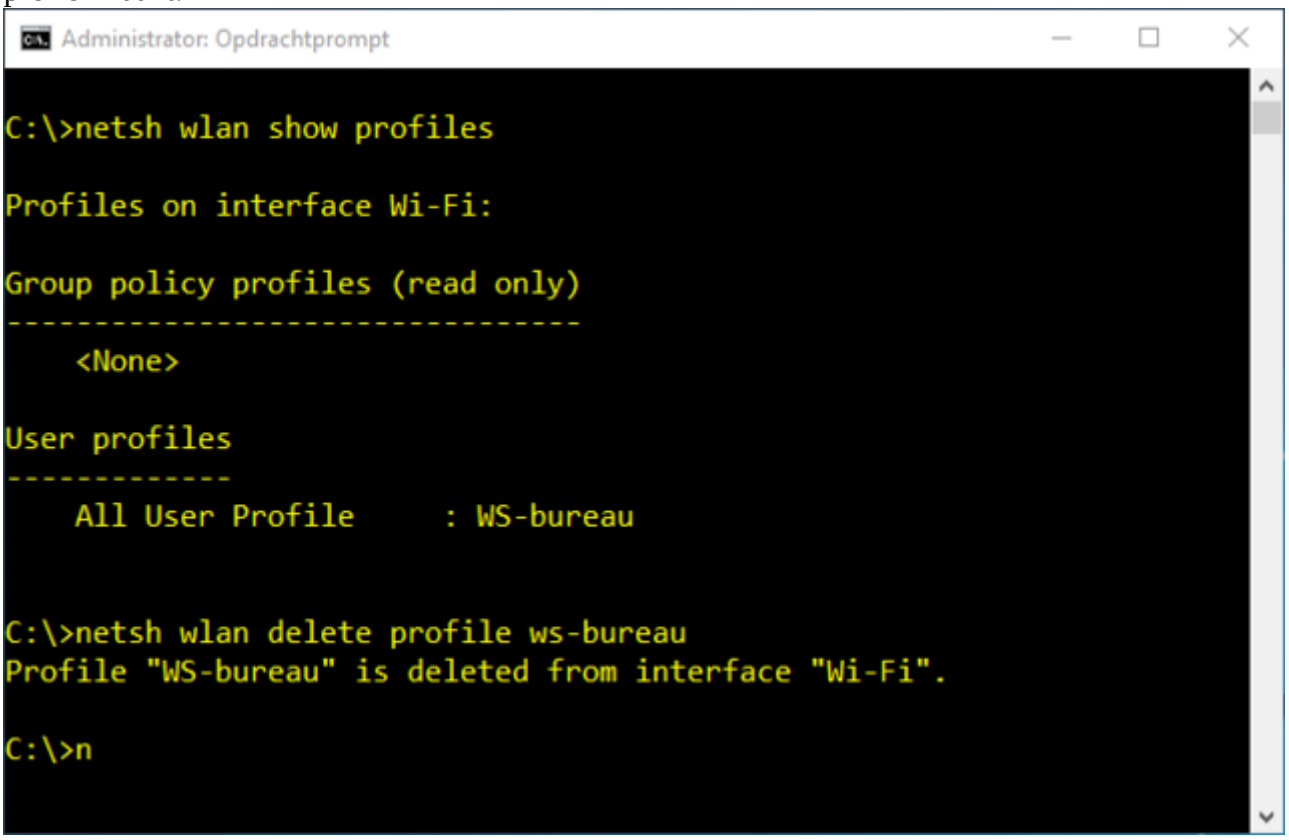
apparaat om een of andere reden opnieuw is geïnitialiseerd. Dat maakt het natuurlijk ook lastig om je draadloze printer te bereiken. In dat geval verbind je die met de usb-poort van je pc, waarna je het apparaat met de tools die de fabrikant beschikbaar heeft gesteld of via je browser alsnog probeert te bereiken. Ga in dat geval na wat het standaard ip-adres van het toestel is of maak gebruik van een gratis tool als Angry IP Scanner (voor Windows, MacOS of Linux) of de mobiele Android-app Fing om het ip-adres van de toestellen binnen je netwerk te achterhalen. Daarna is het slechts een kwestie van opnieuw de juiste netwerkinstellingen vastleggen. Eventueel laat je de printer het wifi-netwerk even tijdelijk vergeten, waarna je het opnieuw probeert.

11 Geen internet (1)

Ik heb blijkbaar wel wifi (of een netwerkverbinding), maar ik kan toch het internet niet op.

Geldt dat voor meerdere apparaten, dan moet je de oorzaak van het euvel centraal zoeken. Je kunt alvast beginnen met het uit- en weer inschakelen van je modem, gevolgd door je router en eventuele switches en toegangspunten. Herstart vervolgens ook je client. De kans is groot dat (een van) deze ingrepen het probleem oplossen.

Laten we er echter even van uitgaan dat het probleem zich bij één toestel voordoet, zoals je laptop. Verbind die dan (tijdelijk) via een utp-kabel met je netwerk. Lukt het nu wel, dan kun je het alvast proberen door het draadloze netwerk-profiel te verwijderen in Windows. Ga als administrator naar de opdrachtprompt en voer het commando **netsh wlan show profiles** uit, gevolgd door **netsh wlan delete profile <naam_van_profiel>**, waar je <naam_van_profiel> vervangt door de naam van het nukkige wifi-profiel (zie ook vraag 20). Vervolgens klik je het netwerkpictogram in het Windows-systeemvak aan, waarna je opnieuw verbinding met dat profiel maakt.



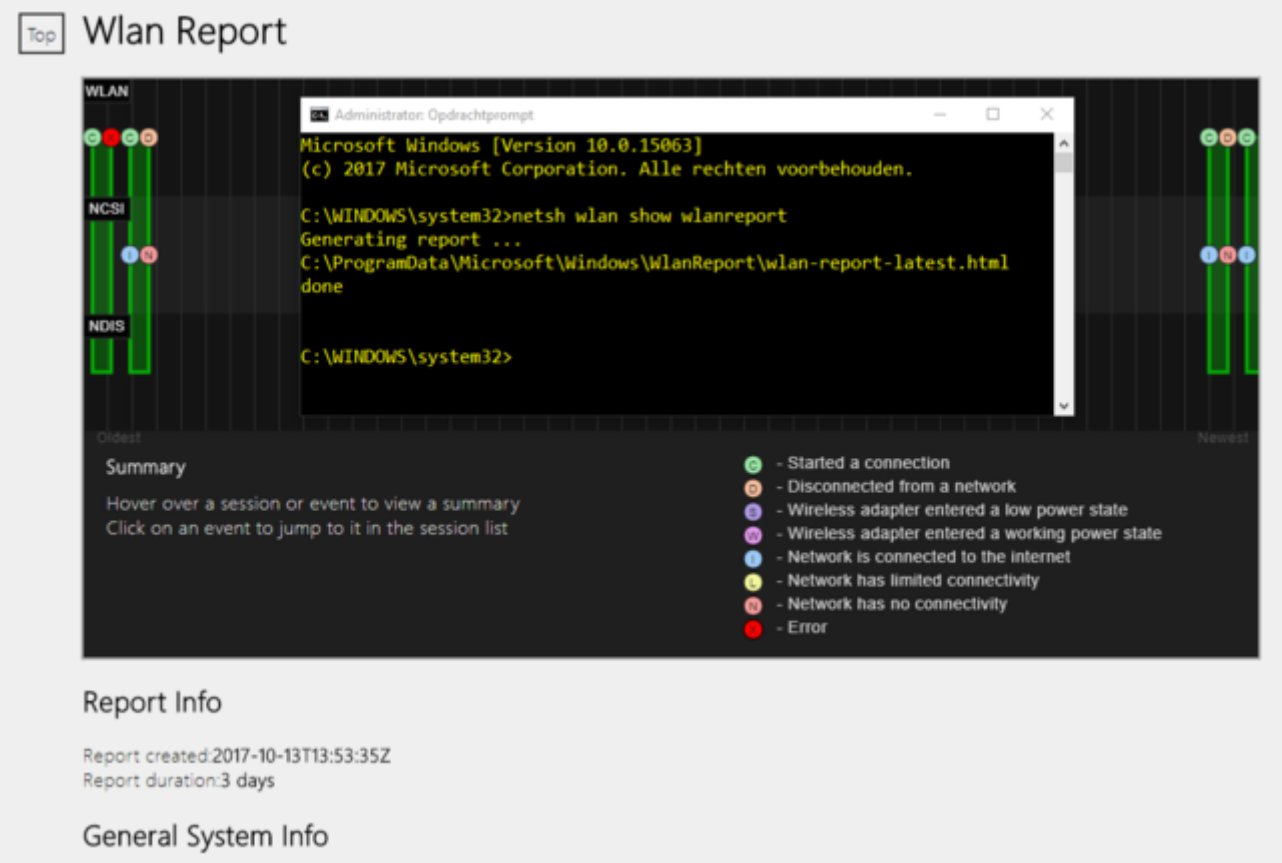
Een (draadloos) netwerkprofiel kan ook corrupt raken. Verwijderen dan maar.

12 Geen internet (2)

Ik heb blijkbaar wel wifi (of een netwerkverbinding), maar ik kan toch het internet niet op.

Er zijn echter nog andere mogelijke oorzaken. Open het **Netwerkcentrum** en kies **Adapterinstellingen wijzigen**. Roep het eigenschappenvenster van je (draadloze) netwerkverbinding op, selecteer **Internet Protocol versie 4**, klik op **Eigenschappen** en ga na of alles correct staat ingesteld, zoals de standaardgateway en dns-servers.

Desnoods haal je er een hersteltool als NetAdapter Repair All-in-One bij, waarmee je eenvoudig enkele netwerkinstellingen kunt resetten.
Nog steeds geen oplossing? Dan zet een grondige studie van het wifi-rapport je wellicht op het spoor. Daar zorgt opdrachtregelcommando **netsh wlan show wlanreport** voor, dat je als administrator uitvoert, waarna je het resulterende html-rapport in je browser opent. Meer informatie over dit en andere nuttige commando's vind je hier.



Windows kan een uitgebreid wifi-rapport genereren, dat je wellicht op het juiste spoor zet.

13 Laptop zonder wifi

Mijn laptop heeft wifi, maar plots weigert het toestel nog een verbinding op te zetten.

Dit probleem zou zomaar eens aan een functietoets of een klein (schuif)knopje te wijten kunnen zijn. Veel laptops hebben namelijk een minuscuul knopje, soms nauwelijks zichtbaar aan de voorzijde, waarmee je de wifi-adapter in- en uitschakelt. Of je schakelt die functie in of uit met behulp van een of andere functietoets of toetscombinatie. Vaak moet je daarbij de Fn-toets samen met een andere toets indrukken.

Het geluk zit soms in een klein knopje …

14 Upgrade

De wifi van mijn oude laptop is te traag voor mijn nieuwe router.

Je hebt een fraaie 802.11ac-router gekocht, maar je oude laptop komt niet verder dan 802.11g of -n. Wil je op het niveau van je router komen, dan zit er weinig anders op dan de wifi-adapter van je laptop te vervangen door een nieuwer model. Ga eerst na of (het bios van) je laptop wel de beoogde wifi-adapter (of specificatie) ondersteunt: de website van je fabrikant geeft je de nodige feedback. Eventueel kan een bios-update soelaas bieden. Het kan echter gebeuren dat het formaat van de nieuwe kaart niet zomaar (lees: niet zonder bracket adapter) in je laptop past. Ga bovendien na of je laptop wel over het benodigde aantal antennes beschikt: voor nieuwere adapters zijn dat er vaak drie, zodat je misschien een derde antenne afzonderlijk moet aanschaffen. Controleer na de installatie of je wel over de up-to-date driver beschikt.

Het vervangen van de wifi-adapter van je laptop vergt enige research en voorbereiding.

15 Firmware

Mijn router ondersteunt bepaalde functies niet. Een nieuwe dan maar?

Dat hangt ervan af. Ga in elk geval eerst na of je router wel is voorzien van de nieuwste firmware. Met wat geluk voegt een firmware-update namelijk net die functie(s) toe die je nodig hebt. Dat gaat van het wegwerken van inmiddels gekende kwetsbaarheden en bugs over het toevoegen van functies als vpn-ondersteuning, wireless bridging en QoS-bandbreedtetoewijzing, tot zelfs de ondersteuning van nieuwere wifi-standaarden.

De aanpak voor een firmware-upgrade kan per router verschillend zijn, maar in grote lijnen komt het hierop neer: roep via je browser de webinterface van je router op en spoor de rubriek voor de firmware-upgrade op (iets als **Firmware Update**, **Maintenance** of **About this Router**). Vervolgens download je het firmware-bestand dat bij jouw routermodel hoort. Vaak kan dat rechtstreeks, maar soms moet je het bestand eerst op je pc bewaren, waarna je het via de webinterface kunt benaderen. Ten slotte kun je de upgrade uitvoeren. Belangrijk is wel dat je dit upgradeproces onder geen beding onderbreekt.

Als je meer van het avontuurlijke type bent, kun je ook de installatie van alternatieve firmware overwegen, zoals dd-wrt of OpenWRT. Ga dan wel eerst goed na of deze firmware wel geheel compatibel is met je router(model).

Misschien voegt een firmware-upgrade van je router wel de gezochte functies toe.

16 Tráááág…

Mijn internetverbinding werkt opvallend traag.

Ga om te beginnen na of de snelheid merkbaar beter is als je de laptop via een utp-kabel rechtstreeks met het modem verbindt. Je kunt hiervoor een online speedtest gebruiken als www.beta.speedtest.net of je gebruikt die van je eigen provider, zoals www.ziggo.nl/speedtest of www.kpn.com/internet/speedtest. Is de snelheid bedraad inderdaad hoger, zie dan ook de antwoorden op vragen 1 tot 5. Wellicht helpt het als je je

laptop dichter bij je router plaatst of een repeater of extra toegangspunt inschakelt, of stel die eens in op een ander kanaal (binnen de 2,4GHz-band).
Blijft het probleem zich voordoen, probeer het dan eerst door je modem/router te herstarten. Is er nog altijd geen verbetering, dan ligt het wellicht bij je provider.

Overigens moet je je er ook van bewust zijn dat de theoretische transfersnelheid van een wifi-standaard in de praktijk nagenoeg nooit haalbaar is. Lees je bijvoorbeeld dat 802.11n 150 Mbit/s haalt, dan zal dat in de praktijk vaak eerder richting de 50 Mbit/s gaan, en bij 802.11ac valt de theoretische doorvoersnelheid (van 433 of zelfs 866 Mbit/s) vaak terug tot circa 30 procent. Deze terugval is vooral te verklaren door de vaak hogere overhead van een draadloze verbinding als gevolg van allerlei storende (omgevings)factoren. Bij een bekabelde verbinding ligt die overhead gewoonlijk rond slechts 10 procent.

Een (online) speedtest vertelt je wat de effectieve up- en downloadsnelheid van je verbinding is.

17 Vergeten wachtwoord

Ik wil een nieuw apparaat toegang geven tot mijn draadloze netwerk, maar ik ben het wachtwoord vergeten.

Als je het wachtwoord van de draadloze router of toegangspunt nog wel weet, kun je in de meeste gevallen via de webinterface van dat toestel alsnog het wachtwoord achterhalen in een rubriek als **Wireless**. Ben je via een (ander) Windows-toestel met dat netwerk verbonden, dan kun je het ook hier aflezen. In Windows 10 zit dat overigens wel diep verstopt. Ga naar het **Netwerkcentrum** en klik, rechts bij **Verbindingen**, het draadloze netwerk aan waarmee je verbonden bent. Kies **Eigenschappen van draadloos netwerk**, open het tabblad **Beveiliging** en plaats een vinkje bij **Tekens weergeven**.

Of je gebruikt een gratis tool als Magical Jelly Bean Wi-Fi password revealer, maar dan wel op een Windows-pc die al eerder verbinding met dat netwerk maakte.

18 Gastnetwerk

Ik wil mijn bezoekers toegang geven tot mijn wifi-netwerk, maar mijn wachtwoord geef ik ze liever niet.

Een mogelijk uitweg – althans voor bezoekers met een Android-toestel – is dat je een QR-code met het login-id (ssid en wachtwoord) voor je draadloze netwerk creëert, bijvoorbeeld met www.zxing.appspot.com/generator, via de optie **Wifi network**. Een veel betere oplossing is echter dat je een gastnetwerk instelt. Voorwaarde is wel dat je router die optie ondersteunt – wellicht na een firmware-update (zie ook vraag 15). In de meeste gevallen volstaat het deze functie (ook wel gasttoegang of guest access geheten) te activeren op je router en die van een ssid en een afzonderlijk wachtwoord te voorzien. Bijkomend voordeel is dat gebruikers die zich met dit netwerk verbinden niet bij de gedeelde mappen van je eigen draadloze netwerk kunnen komen. Sommige routers bieden de mogelijkheid een maximumaantal gebruikers in te stellen dat simultaan het gastnetwerk mag gebruiken. Vaak dienen gebruikers dan eerst hun browser te openen om daar het gastwachtwoord in te vullen voordat ze effectief toegang krijgen.
Interessant is de functie **Wireless Isolation**, ook wel bekend als **AP/Client/Station Isolation**, **Internet access only** of **Access intranet off**. Die zorgt ervoor dat gebruikers van dat netwerk niet met andere apparaten kunnen communiceren; ze kunnen in feite alleen het internet op. Houd er wel rekening mee dat deze functie sommige draadloze applicaties, zoals Google Chromecast, kan hinderen.

Als je router dat allemaal niet ondersteunt, is het echter ook mogelijk zelf een gastnetwerk op te zetten. Dat vereist wel de inzet van twee (of drie) routers op een specifieke manier. Meer uitleg hierover vind je hier.

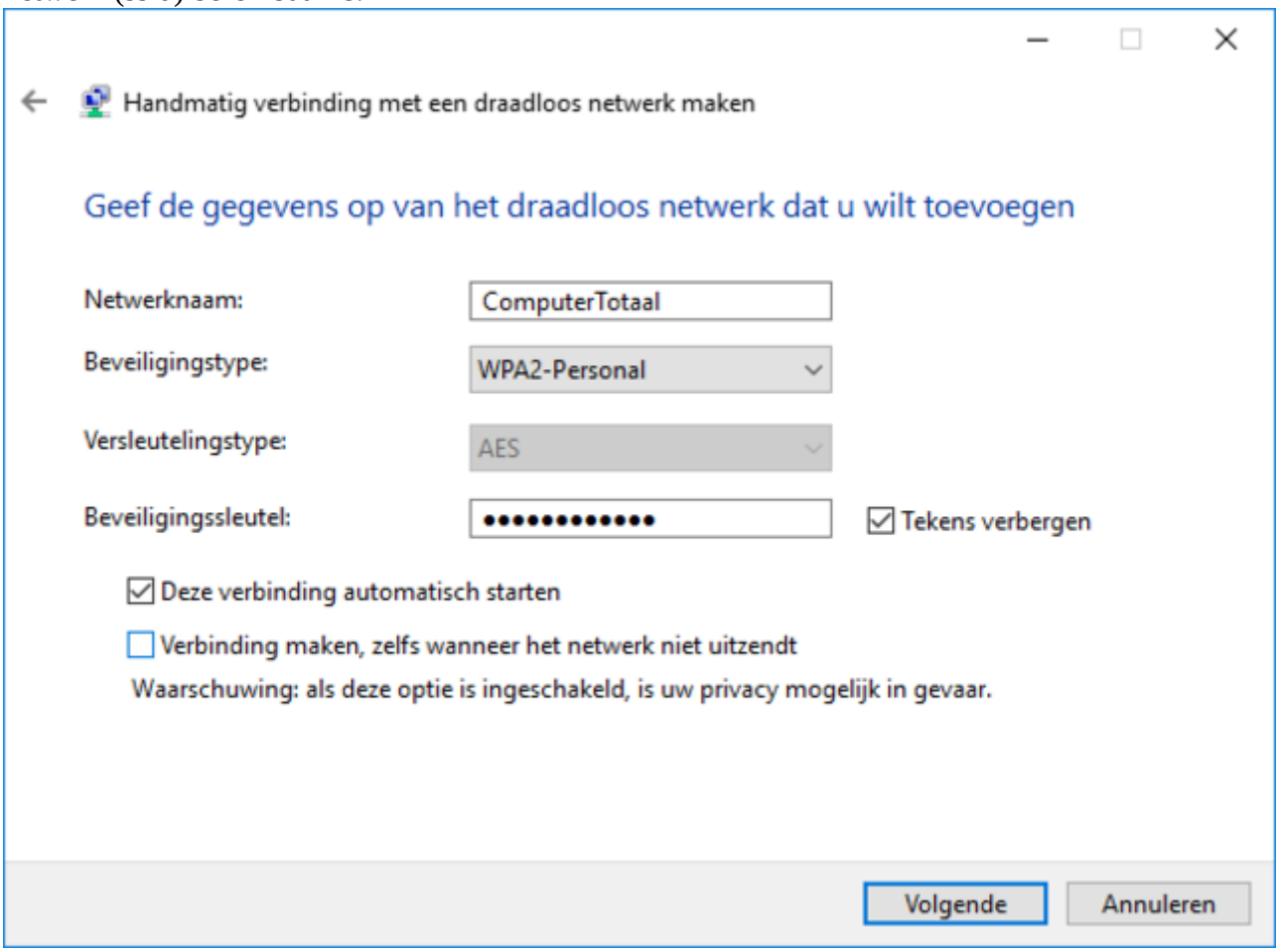
Een afgescheiden netwerk voor je gasten: handig én veilig!

19 Extra beveiliging

Is het nuttig om extra beveiligingen als mac-filtering en het verbergen van het ssid in te schakelen?

Zo'n beetje de enige beveiliging die er écht toe doet, is de wifi-encryptie – bij voorkeur een stevige wpa2-encryptie (op basis van aes) met een stevig wachtwoord. Het inschakelen van mac-filtering en het niet laten broadcasten van het ssid kun je eventueel als bijkomende beveiliging activeren, maar weet dat je het hiermee hooguit de brave buurman of de toevallige voorbijganger wat lastiger zult maken. Een hacker heeft die beveiligingen zo omzeild met behulp van tools als Kismet of Aircrack. Bovendien bemoeilijk je hiermee het toevoegen van een nieuw 'legitiem' apparaat, aangezien je dan zelf het mac-adres aan de whitelist moet toevoegen en ook zelf het ssid en het beveiligingstype moet instellen. Veel te omslachtig dus.

Wat het verbergen van het ssid betreft: dat kan de beveiliging zelfs iets minder sterk maken, vooral als je in Windows de optie **Verbinding maken**, **zelfs wanneer het netwerk niet uitzendt** activeert (ga naar **Netwerkcentrum**, kies **Een nieuwe verbinding of een nieuw netwerk instellen** / **Handmatig verbinding met een draadloos netwerk maken** / **Volgende**). In dit geval zal je laptop, ongeacht waar je toestel zich bevindt, je draadloze netwerk proberen te op te sporen door via 'probe requests' uit te vissen of het netwerk (ssid) bereikbaar is.



Het onzichtbaar maken van je ssid levert nauwelijks iets op (en is soms zelfs onveiliger).

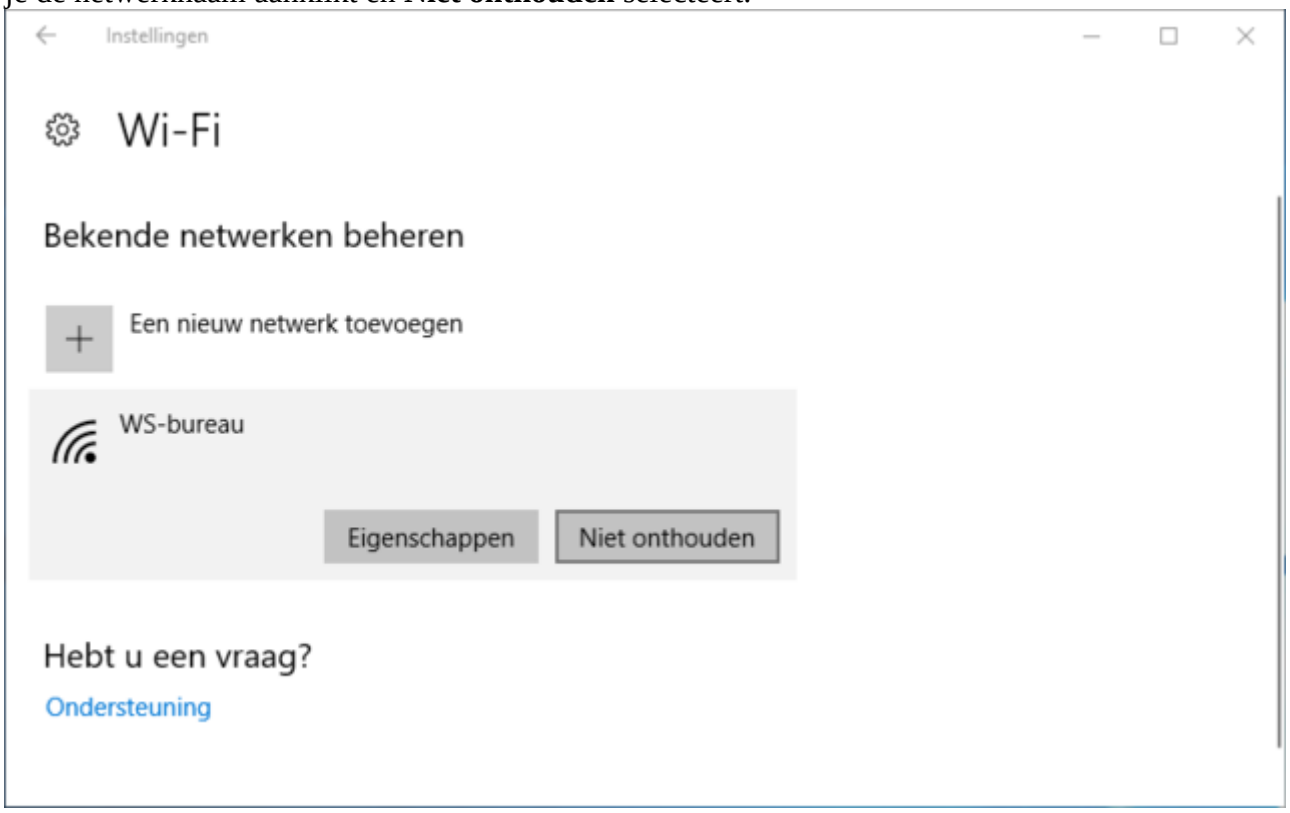
20 Oude netwerken

Hoe vermijd ik dat mijn smartphone, tablet of laptop zich automatisch met oude, bekende netwerken verbindt?

Het is best handig als je mobiele toestel automatisch verbindt met een netwerk waarmee je eerder een connectie hebt gehad, zodat je niet telkens opnieuw hoeft aan te melden. Er kleeft natuurlijk ook een risico aan: hackers kunnen namelijk tools inzetten die de zoekpogingen van je toestel naar een bekend netwerk oppikken, waarna ze zich als het vertrouwde wifi-netwerk kunnen voordoen. Het kan echter ook gewoon vervelend zijn, met name in het geval van openbare hotspots die eerst een autorisatie vereisen. Je bent dan wel verbonden, maar je kunt het netwerk nog niet gebruiken. In deze gevallen kan het handig zijn het netwerk gewoon even te laten 'vergeten'.

In Android doe je dat via **Instellingen / Netwerk en internet / Wifi**, waarna je het gewraakte netwerk selecteert en **Netwerk vergeten** kiest. Op een iOS-toestel doe je dat op nagenoeg dezelfde manier, via **Instellingen / Wi-Fi**, waarna je op de **I**-knop tikt naast de netwerknaam en **Vergeet dit netwerk** kiest.

Op een laptop met Windows 10 kan dat vanaf de opdrachtprompt (zie ook vraag 11), maar ook via **Instellingen / Netwerk en internet / Wi-Fi / Bekende netwerken beheren**, waarna je de netwerknaam aanklikt en **Niet onthouden** selecteert.



Niet langer gewenste wifi-netwerken kun je ook gewoon laten vergeten.

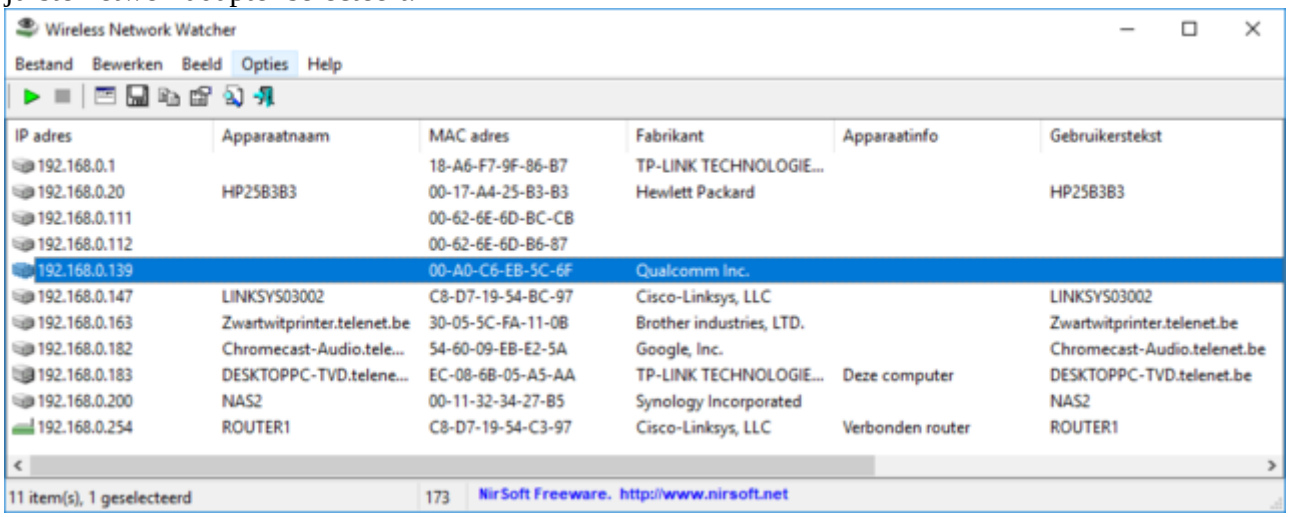
22 Indringer

Hoe ga ik na of iemand stiekem mijn (draadloze) netwerk gebruikt?

Je kunt alvast beginnen met het nakijken van de logs van je router. In de meeste gevallen kun je in een rubriek als **Status** een lijst vinden van de apparaten die met je netwerk verbonden zijn, inclusief ip- en mac-adres, vaak ook de hostnaam en soms zelfs de fabrikant, het model en het besturingssysteem. Op basis van het mac-adres kun je dan eventueel een mac-filter op

je router activeren (zie ook vraag 19). Houd er wel rekening mee dat veel routers hier alleen de apparaten tonen die een adres via dhcp kregen toegewezen.

Verder kun je, in plaats van sporadisch zelf na te gaan of er zich een onbekend of niet-geautoriseerd toestel met je netwerk verbindt, een tool inzetten als Wireless Network Watcher of SoftPerfect WiFi Guard. De eerste tool scant je netwerk continu op de achtergrond en speelt een geluidje af zodra een nieuw toestel een verbinding opzet. De tweede tool is net iets flexibeler: je bepaalt zelf de scanfrequentie en je kunt toestellen ook instellen als 'vertrouwd', zodat die voortaan worden genegeerd. Let er bij beide tools wel op dat je de juiste netwerkadapter selecteert.



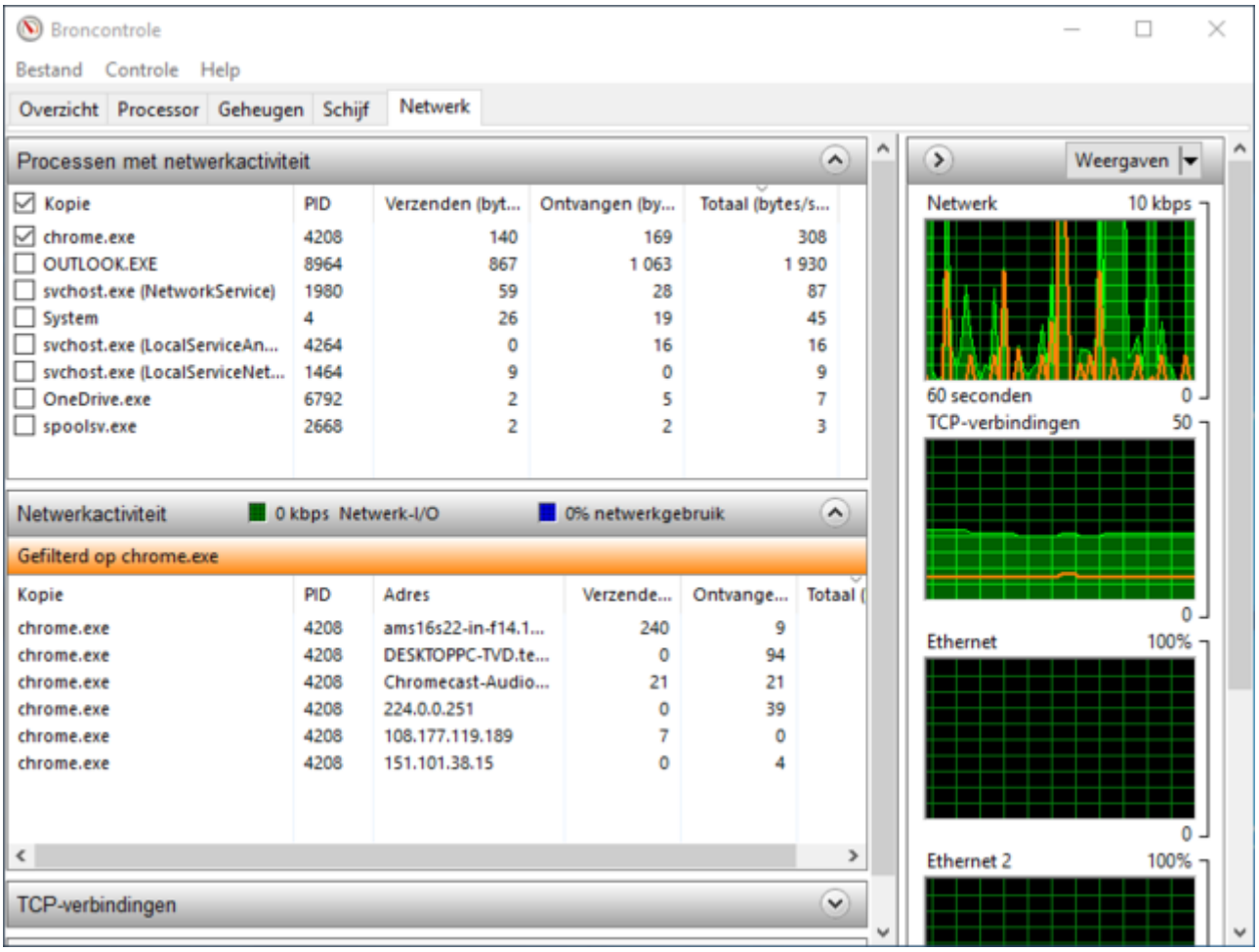
Zodra een nieuw toestel zich met je netwerk verbindt, krijg je een notificatie.

22 Activiteit

De ledjes van mijn (draadloze) router blijven maar knipperen. Moet ik verontrust zijn?

De intensiteit waarmee de ledjes van je router knipperen is natuurlijk niet de meest betrouwbare manier om na te gaan in hoeverre je netwerk(adapter) effectief wordt belast.

Met een Windows-pc krijg je alvast meer duidelijkheid via het ingebouwde taakbeheer (Ctrl+Shift+Esc) op het tabblad **Netwerk**: je leest dan per applicatie of proces de hoeveelheid dataverkeer af. Nog meer details krijg je via de module **Broncontrole** (druk op Windows-toets+R en voer het commando **resmon** uit), onder meer op het tabblad **Netwerk** en met name in de rubriek **Processen met netwerkactiviteit**. Plaats een vinkje bij een item voor nog meer details. Of je zet een tool in als NetLimiter: die laat je niet alleen het dataverkeer van of naar het internet monitoren, je kunt ook verkeer van specifieke apps prioriteren of limiteren naar kwantiteit of tijdsgebruik.
Om na te gaan welk verkeer er precies van of naar draadloze apparaten als een smartphone of tablet gaat, kun je je laptop eventueel tijdelijk instellen als een draadloze hotspot, waarna je je mobiele toestel(len) via die hotspot laat verbinden. Op die laptop installeer je dan een packet sniffer zoals het gratis WireShark, waarna die al het verkeer kan loggen. Dit pakket vergt echter wel een flinke dosis kennis van netwerkprotocollen.



De Broncontrole van Windows geeft ook detailinformatie over het dataverkeer.

23 Publieke hotspot

Is het veilig om me via een openbare hotspot met het internet te verbinden?

Ook als we ervan uitgaan dat het om een legitieme hotspot gaat – en dus geen ‘honey-spot’ opgezet door een hacker met een ssid als ‘Starbucks free’ – is het nooit echt veilig om daarvan gebruik te maken. Met de juiste tools kan een medegebruiker van zo’n netwerk je data immers onderscheppen. Dat geldt in principe ook voor bijvoorbeeld het draadloze netwerk van je hotel, indien ook de hacker (als gast) het bijhorende wachtwoord heeft gekregen.

Om een en ander veilig(er) te maken, maak je zo veel mogelijk gebruik van https-verbindingen en stel je je toestel zo in dat het niet automatisch opnieuw contact maakt met een eerder verbonden draadloos netwerk (zie ook vraag 20).

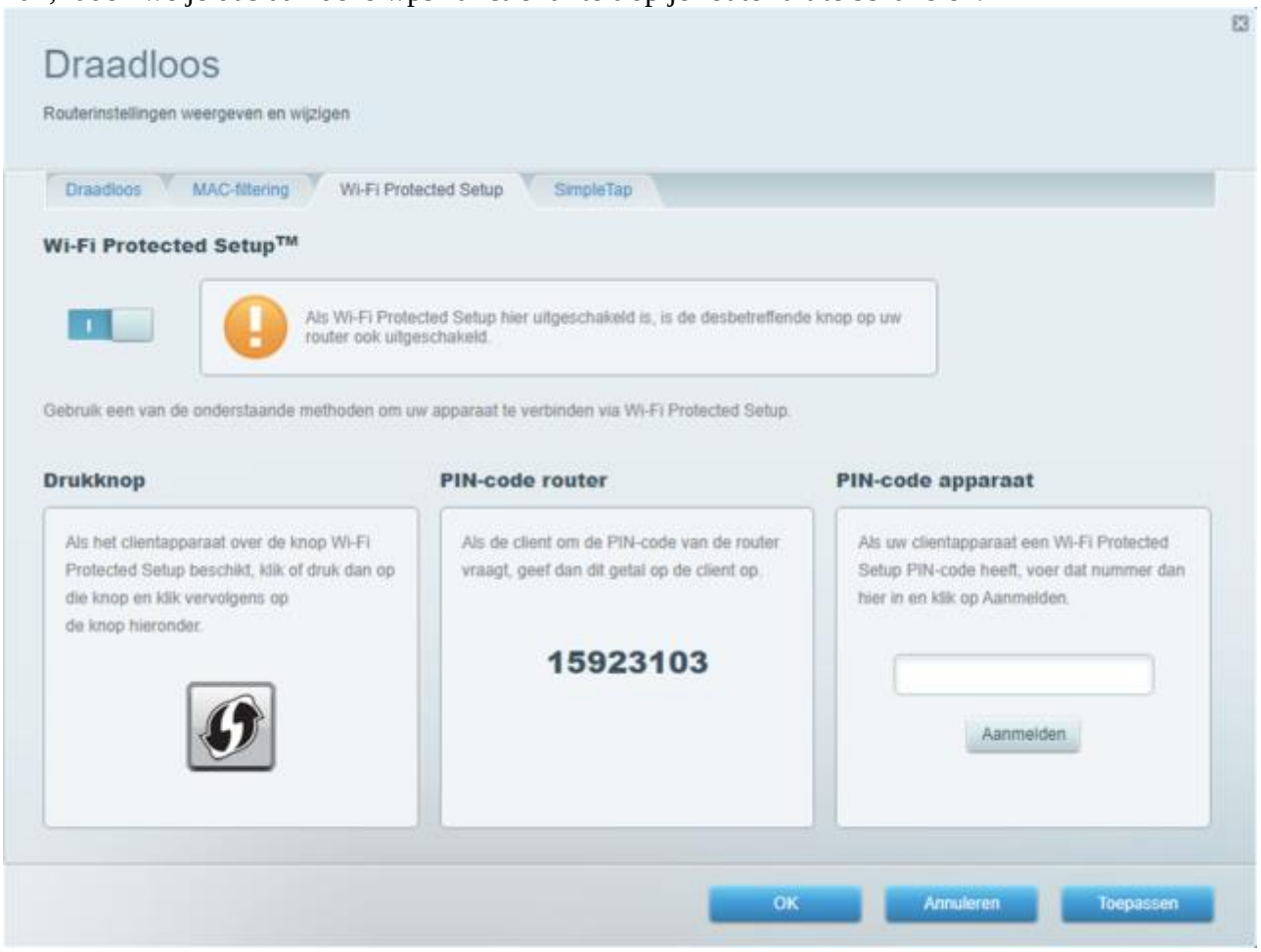
De beste remedie om te vermijden dat iemand data van je draadloze connectie ontfutselt, is een vpn-verbinding (virtual private network). Hiermee creëer je een ‘private tunnel’ naar een vpn-server, waarbinnen alle data stevig worden versleuteld. Een bijkomend voordeel is dat je door zo’n verbinding eventuele siteblokkades en webfilters omzeilt die door het openbare netwerk zijn ingesteld. Er zijn tal van vpn-aanbieders beschikbaar, waaronder CyberGhost (beschikbaar voor zowat alle platformen). Let er wel op dat gratis varianten vaak gelimiteerd zijn, ook op het gebied van transfersnelheid. Een mogelijk alternatief is dat je op je nas zelf een vpn-server opzet, bij voorkeur op basis van OpenVPN of l2tp/ipsec, maar dat is (technisch) weer een ander verhaal.

24 Snel verbinden

Mijn router ondersteunt wps, maar is het veilig om dat te gebruiken?

Wps staat voor wifi protected setup en is een techniek die in het leven is geroepen om makkelijker een draadloze verbinding op te zetten. Gewoonlijk volstaat het een wps-knop in te drukken of een pin-code in te vullen, waarna je client een verbinding met je wifi-netwerk kan opzetten. Onder meer Ziggo levert wifi-modems met deze functionaliteit.

Best makkelijk dus, maar in het verleden zijn er al vaker veiligheidsproblemen geweest: via een eenvoudige ‘brute force’-aanval konden hackers toegang tot zo’n netwerk krijgen. Als het kan, raden we je dus aan deze wps-functionaliteit op je router uit te schakelen.



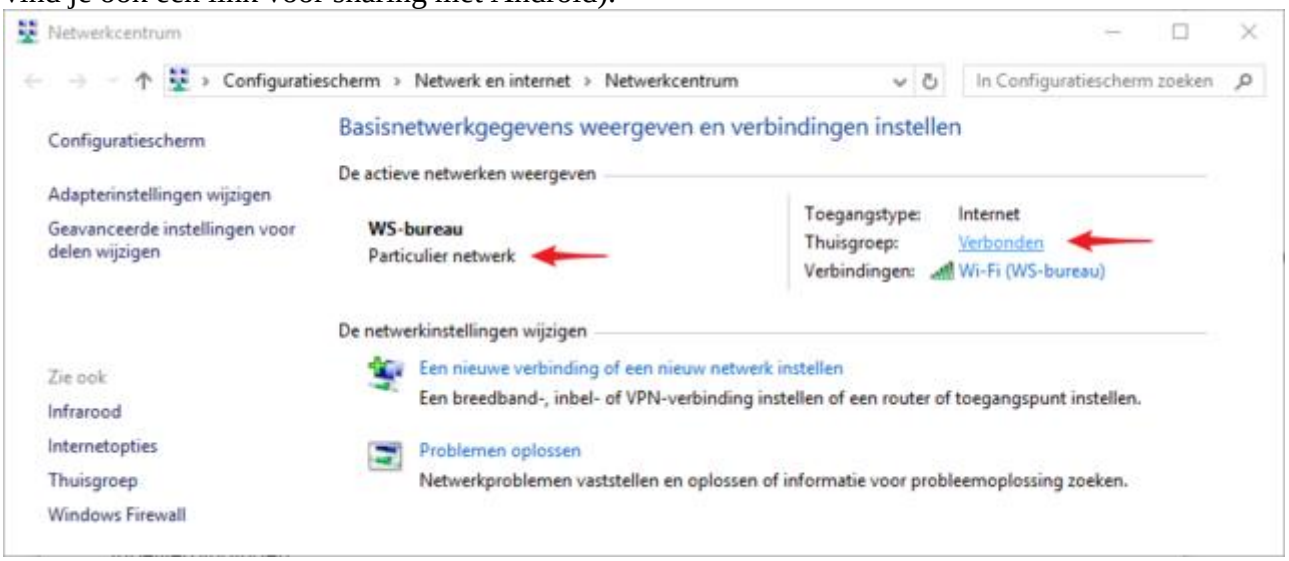
Wps: makkelijk, maar niet altijd even veilig.

25 Data delen

Hoe kan ik bestanden over mijn draadloze netwerk delen?

Zorg er om te beginnen voor dat je toestellen met dezelfde draadloze router verbonden zijn. Vervolgens ga je – we nemen een Windows 10-toestel als voorbeeld – het type netwerk na dat je hebt opgezet: open het **Netwerkcentrum** en ga bij **De actieve netwerken weergeven** na of het wel om een Particulier netwerk gaat. Indien dat niet zo is, ga dan naar **Instellingen**, kies **Netwerk en internet**, klik op **Wi-Fi** en selecteer **Bekende netwerken beheren**, waarna je de netwerknaam aanklikt, **Eigenschappen** kiest en **Deze pc** kan worden gevonden instelt op **Aan**. Ga opnieuw naar het **Netwerkcentrum** waar je nu bij **Thuisgroep** de optie **Kan worden gemaakt** afleest en bevestigt met **Een thuisgroep maken**, waarna je aangeeft wat je

met anderen wilt delen (zoals **Afbeeldingen**, **Muziek**, **Documenten** en **Printers & apparaten**). Even later is je thuisgroep klaar en kun je ook andere Windows-toestellen via het gegeven wachtwoord van deze thuisgroep deel laten uitmaken (zie ook dit artikel).
Om bestanden tussen een Android-apparaat en Windows uit te kunnen wisselen, zijn er verschillende mogelijkheden (afgezien van cloudopslag die je als tussenstation laat fungeren). Zo zijn er apps beschikbaar die je via SMB/CIFS, maar ook via (s)ftp of WebDav bestanden laat uitwisselen, zoals ES File Explorer (met advertenties) of Solid Explorer. Of je maakt gebruik van een tool als Resilio Sync, waarbij het lijkt alsof je je met een cloudopslagserver verbindt, maar dan wel eentje op je eigen pc. Ook voor iOS zijn er apps beschikbaar, waaronder Air Transfer en FileBrowserLite. Instructies hiervoor vind je onder meer hier (daar vind je ook een link voor sharing met Android).



De makkelijkste manier om data te delen (via Windows) is met behulp van een ‘thuisgroep’.