

Een thuisnetwerk aanleggen

FSGG LaMaMa van januari 2020

Index:

Wat is een thuisnetwerk	1
Wat heb minimaal je nodig	1
De Router	2
Functies van de router	2
Configureren van de router	3
Uitbreidingsmogelijkheden	8

Wat is een thuisnetwerk

[index:](#)

De reden om een thuisnetwerk aan te leggen is omdat je met één of meerdere computers, tablet of smartpone wil surfen op het Internet en/of wil e-mailen.

Wat heb je minimaal nodig

[index:](#)

- Een Service provider:

Om verbinding te kunnen maken met het Internet heb je een service provider nodig, iemand die de toegang tot het Internet aan jou beschikbaar stelt. Er zijn maar een paar serviceproviders met een eigen netwerk, bv. KPN, Ziggo. Die serviceproviders hebben verschillende typen netwerken in de straat liggen. (TV)kabel voor Ziggo en de telefoonlijn (DSL) en glasvezel voor KPN.

In Nederland zijn 31 service providers actief die allemaal gebruik maken van deze netwerken.

De keuze voor een serviceprovider hangt af van de netwerken die bij jou in de straat liggen. De meeste serviceproviders leveren ook TV, Radio en Telefoon maar daar gaat deze handleiding niet over.

Hardware:

Als je een keuze hebt gemaakt stelt de service provider een minimale set hardware ter beschikking die je zelf kunt aanleggen maar je kunt dat ook door de provider laten doen.

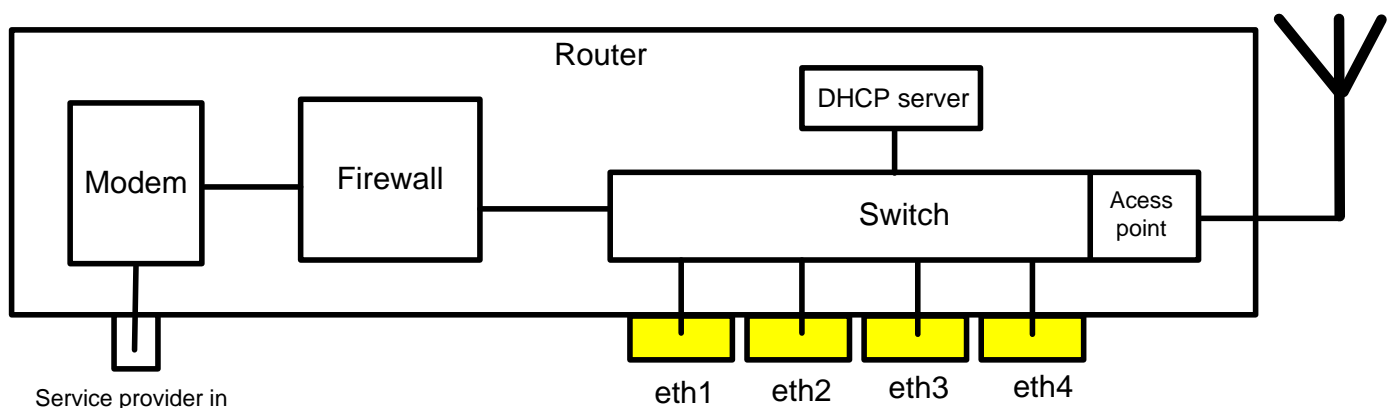
De minimale set hardware bestaat uit:

- Een filter (om het Internetsignaal uit het totaalaanbod te filteren)
- Een modem (om het Internetsignaal om te zetten naar het IP protocol)
- Een router (regelt het verkeer tussen de aangesloten netwerken)
- Een firewall (bepaalt welk verkeer door mag naar het andere netwerk)
- Een DHCP server (geeft IP adressen uit op je thuisnetwerk)
- Een switch (schakelt het verkeer door naar de juiste Ethernetpoort)
- Een WiFi-accesspoint (vervangt een ethernetkabel)

Gelukkig zitten al die onderdelen in één kastje, die we "router" noemen.

De router wordt geleverd en geplaatst bij het punt waar het serviceprovider netwerk het huis binnenkomt. Dit is vaak de meterkast.

Hieronder het blokschema van een "router"



De router:

[index:](#)

Het signaal dat je huis binnenkomt via één van de genoemde mogelijkheden komt via een splitter en een (speciaal)kabeltje op je router aan. Dit deel van het netwerk en het plaatsen van de router wordt gedaan door de service-provider. Hiermee is de aanleg van je thuisnetwerk eigenlijk klaar. Als je meer wilt, zul je dat zelf moeten aanleggen.



Functies van de router:

[index:](#)

Functioneel wordt de router geplaatst tussen het netwerk van de serviceprovider en je eigen thuisnetwerk.

De router zorgt ervoor dat het ethernetverkeer van je thuisnetwerk niet op "het Internet" beland, maar ook dat het Internetverkeer op jouw thuisnetwerk terecht komt.

Je kunt de router vergelijken met een douanepost aan de grens tussen twee landen. De slagboom staat altijd naar beneden, maar als er verkeer met de juiste papieren komt laat de douanier, lees de **Firewall**, het verkeer passeren en mag het verder reizen op het andere netwerk.

Alleen moet de lading ter plekke overgeladen worden in een andere auto met een andere chauffeur die de weg kent in het land van bestemming.

Dit wordt **NAT** (Network Address Translation) genoemd.

Om de apparaten op je thuisnetwerk met elkaar te laten communiceren hebben ze een IP adres nodig. De uitgifte van IP-adressen wordt gedaan door de **DHCP** server van de router. Dit is een programma dat luistert naar aanvragen van apparaten om een IP-adres te krijgen.

De **switch** die in de router zit "weet" welke apparaten zijn aangesloten op de (gele) ethernet poorten. De switch zorgt dat het verkeer bij het juiste apparaat wordt aangeboden.

Het **WiFi-accesspoint** is een vervanger voor een ethernetkabel.
Er kunnen meerdere apparaten connectie maken met het WiFi-accesspoint.

Het configureren van de router:

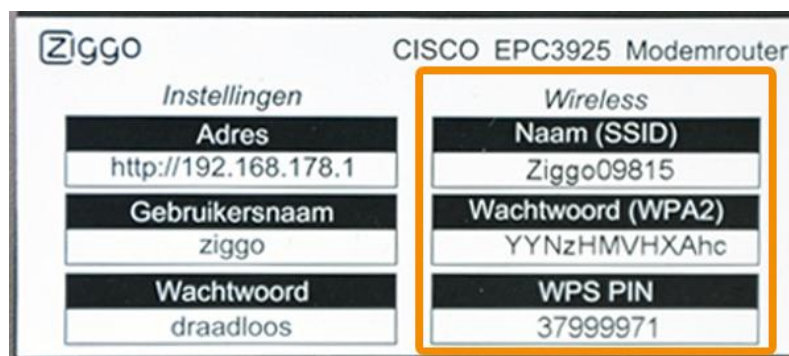
Als de router is geplaatst kun je aan de slag om je apparaten aan te sluiten.
Maar sommige instellingen van de router kun je aanpassen naar je eigen wensen.

- Het wachtwoord om in te loggen op de router
- Het WiFi-accesspoint
- De DHCP server
- De Firewall
- UPnP

Inloggen op de router

[index:](#)

Omdat er veel verschillende routers zijn is het ondoenlijk om de inlogprocedure in detail te behandelen maar meestal staan de inloggegevens op een sticker op de router.



Om ongewenste toegang te voorkomen is het verstandig om het inlog-wachtwoord te wijzigen.

Wijzig wachtwoord

Op deze pagina kun je de gebruikersnaam en wachtwoord wijzigen om de instellingen van je Connect Box te wijzigen. Wij adviseren je het standaard wachtwoord aan te passen.

Huidig wachtwoord

Voer een nieuw wachtwoord in

Minimale eisen:
- 8 karakters lang
- Minimaal 1 hoofdletter
- Minimaal 1 kleine letter
- Minimaal 1 cijfer

Instellingen opslaan

Sla het nieuwe wachtwoord goed op, zodat je later nog eens kunt inloggen op je router.

Het WiFi-accesspoint

Ook de naam van het WiFi-accesspoint en het toegangswachtwoord staan op de sticker op de achterkant.

Je kunt dat zo laten maar ook hier is het verstandig om het WiFi-wachtwoord te wijzigen.

The screenshot shows the 'Draadloze Beveiliging' (Wireless Security) settings page. On the left is a navigation menu with 'Home', 'Verbonden apparaten', 'Geavanceerde instellingen', 'Draadloos', 'Beveiliging', and 'DHCP'. The main content area is titled '2,4 GHz wifi-configuratie'. At the top, a green box indicates 'De instellingen zijn opgeslagen.' Below this, the settings are: 'Wifi-naam (SSID)' is '9728z'; 'Wifi-naam zichtbaar?' is set to 'Ja'; 'Beveiliging' is set to 'WPA-PSK/WPA2-PSK'; and 'Wifi-wachtwoord' is 'Pietje#puk#Was#hier!'. A password strength indicator shows a green bar labeled 'Goed'. A tooltip on the right states: 'De netwerknnaam moet beginnen en eindigen met een letter, een speciaal teken of een nummer. Maximaal 32 karakters.'

Om je WiFi accesspoint wat beter te herkennen kun je de Wifi-naam (SSID) wijzigen.

5GHz band

De meeste moderne routers hebben ook een WiFi accesspoint in de 5GHz band. Als je apparaten hebt die ook gebruik kunnen maken van de 5GHz band kun je ook deze instellingen aanpassen.

Gebruik je het 5GHz accesspoint niet, dan kun je die beter uitzetten.

5 GHz frequentieband

Schakel 5 GHz in Schakel 5 GHz uit

Gastnetwerk

Heeft jouw router de mogelijkheid voor een Gastnetwerk, is het aan te bevelen om deze aan te zetten. Dit netwerk staat los van je "eigen" WiFi netwerk en je gasten kunnen wel het Internet op maar kunnen ze geen connectie maken met de apparaten op de "eigen" netwerk, zoals de printer, de gedeelde mappen van de NAS, de Chromecast, PC, enz.

Wifi-gastnetwerk

Inschakelen Uitschakelen

Wifi-naam (SSID) ⓘ

Wifi-naam zichtbaar? Ja Nee

Beveiliging ⓘ

Wifi-wachtwoord ⓘ

Minimale eisen:
- 8 karakters lang
- Minimaal 1 hoofdletter
- Minimaal 1 kleine letter
- Minimaal 1 cijfer


Goed

De DHCP server

De DHCP server in je router geeft IP-adressen uit aan de aangesloten apparaten zodra ze zich "op het netwerk bekend maken".

Zonder IP adres kan een apparaat geen gebruik maken van het thuisnetwerk of het Internet. Ook hier is er wat te configureren als je dat wilt.

De DHCP server kan nog maximaal 252 IP-adressen uitgeven maar als je dat aantal in de hand wil houden, kun je dat aanpassen.

Hieronder zie je dat er 30 IP-adressen uitgegeven kunnen worden: van 192.168.178.100 t/m 192.168.178.129

DHCP-instellingen

DHCPv4-server

Op deze pagina kun je instellen hoe IPv4 adressen worden toegewezen. Standaard is de Connect Box ingesteld als DHCP (Dynamic Host Configuration Protocol) server.

Ingeschakeld Uitgeschakeld

Begin lokaal adres .

Aantal apparaten

Lease tijd seconden

Je kunt apparaten, bv een Desktop PC die altijd op het netwerk blijft zitten, een vast IP adres geven. Je moet de PC dan wel een IP_adres geven die buiten de bovenstaande range valt, bv. 192.168.178.140 , anders heb je de kans dat 2 apparaten hetzelfde IP-adres krijgt en daardoor allebei niet werken.

Dan is er nog de mogelijkheid om een apparaat een "gereserveerd IP-adres" te geven. Voordeel hiervan is dat het IP-adres op je thuisnetwerk altijd hetzelfde is maar daar buiten, op een ander netwerk, je een adres krijgt van de DHCP server van het betreffende netwerk.

Lijst gereserveerde IPv4-adressen

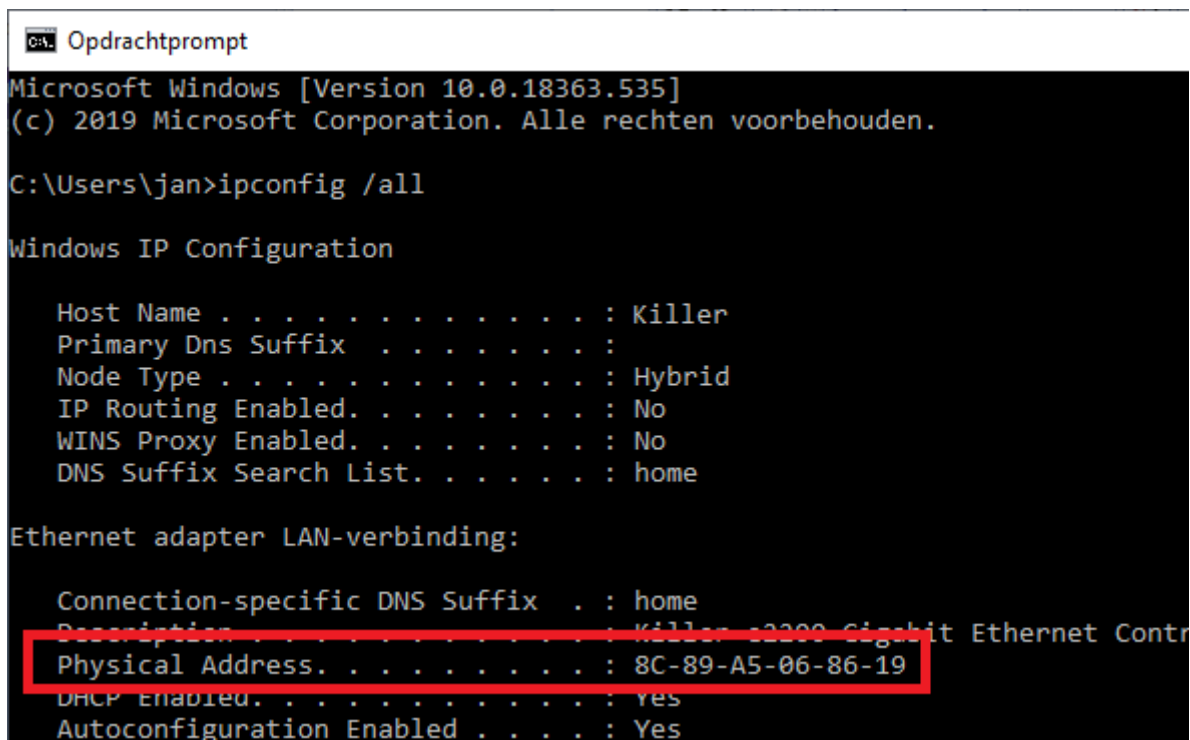
MAC-adres	IP-adres	Wis
8C:89:A5:06:86:19	192.168.178.111	<input type="checkbox"/>
C4:4E:AC:80:7A:8B	192.168.178.253	<input type="checkbox"/>

Wil je dit toepassen, dan heb je het MAC of physical-adres van het apparaat nodig. Dit is een uniek "ingebakken" adres. Ieder apparaat heeft een ander MAC-adres meegekregen van de fabrikant .

Er zijn twee mogelijkheden om achter het MAC -adres van een apparaat te komen:

- Tik in het zoekscherm van Windows in "cmd". Er opent zich een zwart scherm. Tik hier in "ipconfig /all" (let op de spatie)

Het zwarte scherm vult zich met allerlei data. Zoek naar het Physical Address van de netwerkkaart. Maar Let op: de WiFi netwerkkaart heeft een ander physical adres dan de LAN netwerkkaart.



```
Opdrachtprompt
Microsoft Windows [Version 10.0.18363.535]
(c) 2019 Microsoft Corporation. Alle rechten voorbehouden.

C:\Users\jan>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Killer
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : home

Ethernet adapter LAN-verbinding:

Connection-specific DNS Suffix . : home
Description . . . . . : Killer 12200 Gigabit Ethernet Contr
Physical Address. . . . . : 8C-89-A5-06-86-19
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
```

Vul het gevonden Physical Address in op het lijstje en kies een IP-adres die buiten de DHCP range valt. Vergeet niet te saven.

De Firewall

De router heeft een eenvoudige firewall. De firewall doet dienst als politieagent en regelt alleen het verkeer tussen het Internet en je thuisnetwerk. De firewall doet niets aan het verkeer van je thuisnetwerk naar het Internet. Met andere woorden: in de default configuratie laat de firewall geen verkeer passeren vanaf het Internet en laat al het verkeer passeren vanaf je thuisnetwerk dat bestemd is voor het Internet. Verkeer dat niet thuishoort op het Internet, wordt natuurlijk wel tegengehouden. Voor aanvallen vanaf het Internet ben je dus redelijk beschermd. Als je wilt dat bepaalt verkeer niet naar het Internet mag, moet je dat zelf regelen in de firewall van Windows.

Poort-forwarding

Als je op de thuisnetwerk een Webserver, FTP server, of een Teamspeakserver hebt draaien die wél bereikbaar moet zijn vanaf het Internet moet de firewall toestemming krijgen om dat specifieke verkeer wél door te laten naar de betreffende server. Dit stel je in bij "Poort-forwarding".

Hieronder een voorbeeld van het bereikbaar maken van een webserver op je thuisnetwerk met het IP-adres 192.168.178.130 (dit is een vast IP-adres buiten de DHCP range)

Poort-forwarding

Hier zet je poorten statisch open voor specifieke diensten en software.

Indien uPnP staat ingeschakeld, kunnen apparaten of applicaties ook zelf automatisch poort-forwarding regels instellen. Die worden hieronder ook weergegeven.

Lokaal IP	<input type="text" value="192.168.178."/> <input type="text" value="130"/>	IP adres van de webserver
Lokale beginpoort	<input type="text" value="80"/>	het poortnummer van de webserver http://
Lokale eindpoort	<input type="text" value="80"/>	
Externe beginpoort	<input type="text" value="80"/>	
Externe eindpoort	<input type="text" value="80"/>	
Protocol	<input type="text" value="TCP"/>	
Ingeschakeld	<input type="text" value="Actief"/>	

De firewall stuurt nu alle verzoeken voor de website (poort 80) door naar de webserver die draait op de pc met het IP-adres 192.168.178.130

Als je meer wilt weten over poortnummers, klik dan [hier](#).

UPnP

Als je dit inschakelt kunnen apparaten op je thuisnetwerk zelf Poort-forwarding configureren, als ze dat (denken) nodig te hebben. Er worden poorten in de firewall open gezet zonder dat je het weet. Dit is een ernstig veiligheidslek. Hackers maken hier gebruik van. **Uitzetten dus.**

UPnP

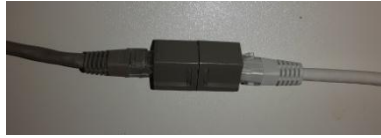
Hier zet je uPnP aan of uit. UPnP zorgt ervoor dat apparaten en applicaties in je thuisnetwerk zonder speciale poort-forwarding instellingen, met het internet kunnen communiceren.

De automatisch ingestelde poort-forwarding regels kan je vinden op de Poort-forwarding pagina, onder de Beveiliging categorie in het menu aan de linkerkant van het scherm. Op die pagina kan je ook handmatig poort-forwarding regels toevoegen indien uPnP is uitgeschakeld.

Ingeschakeld Uitgeschakeld

Switch

De gele switchpoorten op de router zijn van het type RJ45. Ze worden "ethernet poorten" genoemd, naar het ethernet protocol waarmee het netwerk werkt. Je kunt met behulp van een "ethernet kabel" verbinding maken met je computer of printer, mits die computer een ook een ethernet poort heeft. Mocht de (gekochte) kabel te kort zijn kun je 2 kabels koppelen met een koppelblokje



Uitbreidingsmogelijkheden:

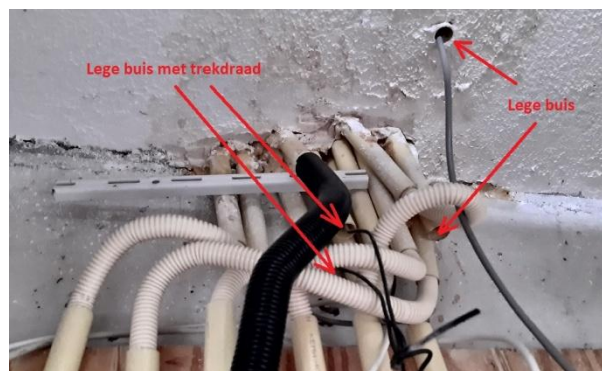
[index:](#)

Als je aan 4 ethernetpoorten te weinig hebt, of de switch staat niet op de goede plaats, kun je 1 poort gebruiken als "uplink" naar een andere switch.

Klik [HIER](#) voor de verschillende uitbreidingsmogelijkheden in een handleiding op de FSGG site.

UTP ethernet bekabeling aanleggen

Als je router in de meterkast is afgewerkt en je computerwerkplek is op de 1^e verdieping moet er een ethernetkabel naartoe. Aanleg van zo'n kabel kan lastig zijn maar misschien kun je gebruik maken van een lege buis vanuit de meterkast naar een punt ergens in huis. Kijk in de grootste slaapkamer of er een lege doos in de muur zit die is aangelegd voor een extra TV of telefoonaansluiting. Kijk ook bij de wasmachine of bij de verwarmingsketel of daar het andere eind van een lege buis uitkomt.



Vaak is er ook een lege buis aangelegd naar de keuken, in de buurt van de gas aansluiting

Mocht je zo'n buis kunnen gebruiken kun je de verder met de kabel naar je werkplek.

Kijk voor de het monteren van een RJ45 connector aan het einde van de kabel in [deze](#) handleiding.