Draadloos WiFi

Mijn eigen thuisnetwerk leren configureren en beveiligen

Handleiding-syllabus.

INLEIDING: THEMA, DOELSTELLINGEN en ORGANISATIE

- ***Thema: Een draadloze verbinding met WiFi***
  *In deze handleiding en syllabus richten geven we een korte inleiding op de concepten van datacommunicatie en de verscheidene netwerken. Nu we een **Router** kunnen positioneren gaan we in op de specifieke eigenschappen van een draadloos netwerk, en meer bepaald, deze gebaseerd op de **Wireless Fidelity** standaard.*
  Met deze basiskennis verstaan we nu beter welke parameters dienen ingesteld tijdens de configuratie van een router, en hoe de beveiliging moet gebeuren.

- ***Doelgroep:** 50-plussers met een basiskennis van Computer en Internet, die zelf wel eens draadloos netwerk of thuisnetwerk willen opzetten.*

- ***Doelstellingen:***
  - *50-plussers met een basiskennis PC en Internet **inzicht geven in het versturen van data**:hoe gebeurt dat eigenlijk, wat speelt zich af achter de schermen.*
  - *50-plussers met basiskennis PC en Internet het de functies van de router duidelijk maken: dit is immers de bouwsteen van elk netwerk.*
  - *50-plussers de specifieke kenmerken van draadloze communicatie leren verstaan, en de router leren configureren en beveiligen.*

- ***Organisatie: tijdsduur, lesmateriaal, infrastructuur, apparatuur***

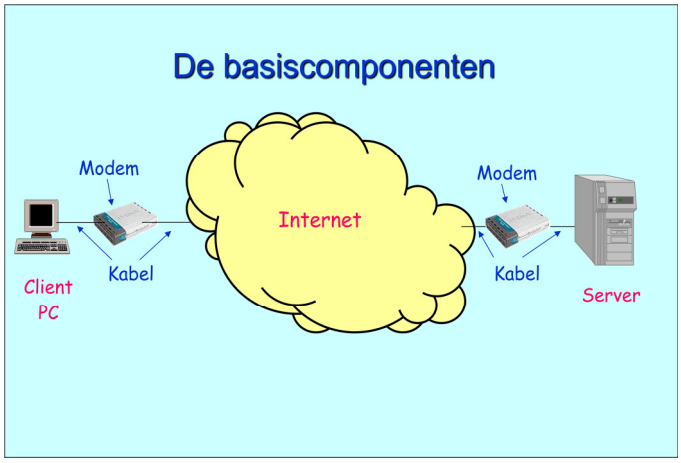
  Deze cursus wordt doorgenomen in een sessies van 2,5 à 3 uur.

  We richten ons op kleine groepen van 8 à 10 personen, te begeleiden door één Seniornet animator. De les wordt gegeven in een daartoe geschikt en uitgerust lokaal, met een opstelling die zoveel mogelijk de U-vorm benadert. De lesgever beschikt over een Computer voorzien van het besturingsprogramma Windows XP of Vista, en een LCD projector. De deelnemers beschikken elk eveneens over een gelijkaardige computer. Er is ook Internetverbinding.

  Indien mogelijk neemt de lesgever zelf een router mee, en indien toegestaan door de IT coordinator van het leslokaal kan hij hiermee een demo geven.

- ***Bemerking:** deze cursus is erg theoretisch en zal waarschijnlijk niet vaak worden gegeven. Het aantal animatoren dat zich geroepen voelt om deze materie te brengen zal ook eerder klein zijn. Toch blijft het interessant om deze curus in onze keuzelijst op te nemen, want draadloze thuisnetwerken zijn erg in trek.*

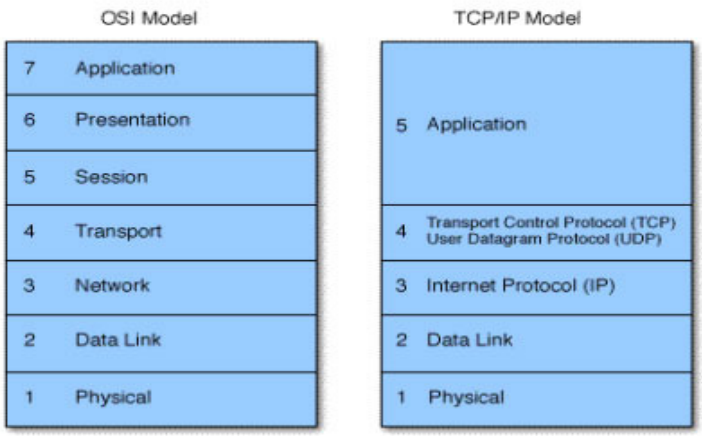
DEEL I: BASIS DATA COMMUNICATIE



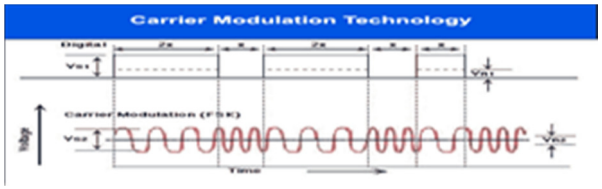
Een standaard data verbinding, verbindt een computer via **kabels** en een **modem** met het internet. Een typische configuratie is dan een PC (de **Client**) die verbonden is met het internet, en een Host (de **Server**), die eveneens verbonden is met het internet. Men spreekt dan van Client-Server communicatie. Bij het surfen is de client de **Webbrowser**, en de server is de **Webserver**.

*Deze communicatie gebeurt in **lagen**, waarbij de hogere laag beroep doet op de diensten van de onderliggende laag.*

Volgens het OSI model zijn er 7 lagen, maar voor internet heeft men zich beperkt tot 5. We overlopen ze kort:



1. **De Physical Layer (L1)**: deze laag zorgt voor het overbrengen van een reeks O en 1 met bijvoorbeeld spanningsniveaus: weinig spanning is een 0, hoge spanning een 1.



2. **De Data Link Layer (L2)**: deze laag zorgt ervoor dat men in de stroom van 0 en 1 een begin en eindpunt kan herkennen zodat men uit de stroom een **Frame** kan selecteren.

In deze stroom is bijvoorbeeld het patroon 0110 de begrenzing van een Frame. Om toestellen die we met deze 2 lagen verbinden te kunnen herkennen, krijgen deze een adres: het **MAC Adres**: elk elektrisch toestel voor datacommunicatie heeft zo een vast Mac Adres. Het wordt vooraan in het Frame meegestuurd. Men noemt laag 2 ook soms de Mac Layer.

3. **De Network Layer (L3)**: dank zij de functies van deze laag kan men niet alleen toestellen rechtstreeks met elkaar verbinden, maar ook over een netwerk: men kan langs verschillende wegen over dit netwerk, de bestemming bereiken. Dit vergt intelligentie: men spreekt van een "weg zoeken", in 't Frans une Route, later in het Engels **Routing**.
In telefoon netwerken gebeurt dit in de telefooncentrale, op basis van het telefoonnummer. Op het internet gebeurt dit in de **Router**, op basis van een **IP Adres**. Je kan dit laatste dus vergelijken met het telefoonnummer, waarmee je aansluit op het netwerk en waarmee men je kan bereiken voor een verbinding.

We kunnen nu al communiceren van punt tot punt , of via een netwerk. Maar wat hebben we te vertellen? En ook , hoe spreken we af: wie spreekt eerst, moet die dan wachten etc…

4. **De Transport Layer (L4)**: die bepaalt de spelregels van het praten, en de toepassingen waar het gepraat naar toe gaat. Er zijn eigenlijk twee communicatie vormen:

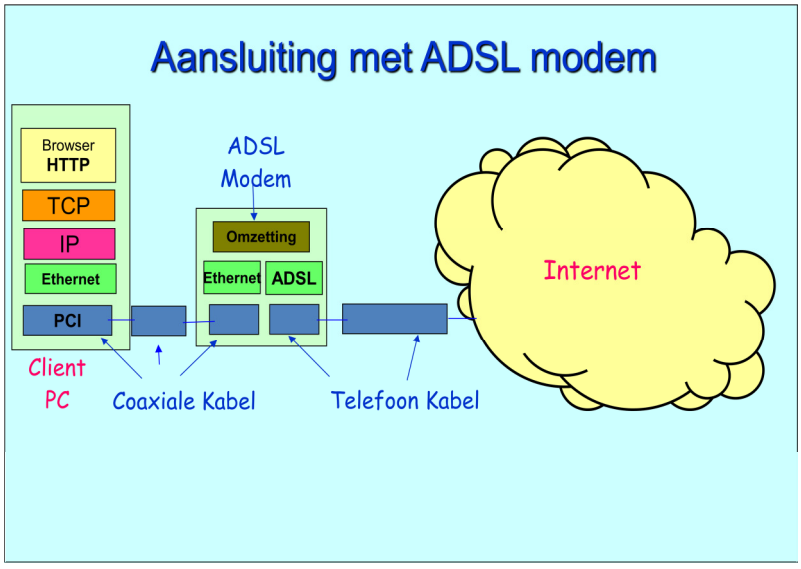
- *met connectie*: dat impliceert dat men eerst een verbinding in beide richtingen opzet, en vervolgens praat. Op het einde moet men de verbinding verbreken. Dit is typisch voor een klassieke telefoonverbinding.
  Hiervoor gebruikt men het protocol **TCP** (Transport Control Protocol).
- *zonder connectie*: hier begint men gewoon te praten, en wat men opstuurt moet dus informatie bevatten om aan de andere kant in de juiste volgorde terug aan elkaar te worden gezet. Dit zou je kunnen vergelijken met het sturen van een reeks SMSjes.
  Hiervoor gebruikt men het protocol **UDP** (User Datagram Protocol).

Het klinkt wel een beetje raar: een connectie maken zonder connectie. Men bedoelt eigenlijk dat de applicaties met elkaar kunnen praten (verbonden zijn), zonder dat daarvoor in de onderliggende lagen permanent een verbinding moet bestaan.

5. **De Application Layer**: hier gaat het uiteindelijk om : applicaties praten tegen elkaar: bijvoorbeeld de WebBrowser praat tegen de WebServer. Het surfen van Browser naar WebServer is gebaseerd op het HTTP protocol: de boodschappen die men mag sturen, en de syntax die men daarbij moet respecteren, zijn voor dit protocol vastgelegd.

Laten we nu eens bekijken wat er gebeurt, als we een verbinding maken met het internet via een klassieke telefoonlijn met een ADSL modem. Een volledige verbinding bestaat uit stukken (segmenten) die elkaar opvolgen, en die telkens werken met hun eigen stapel lagen.

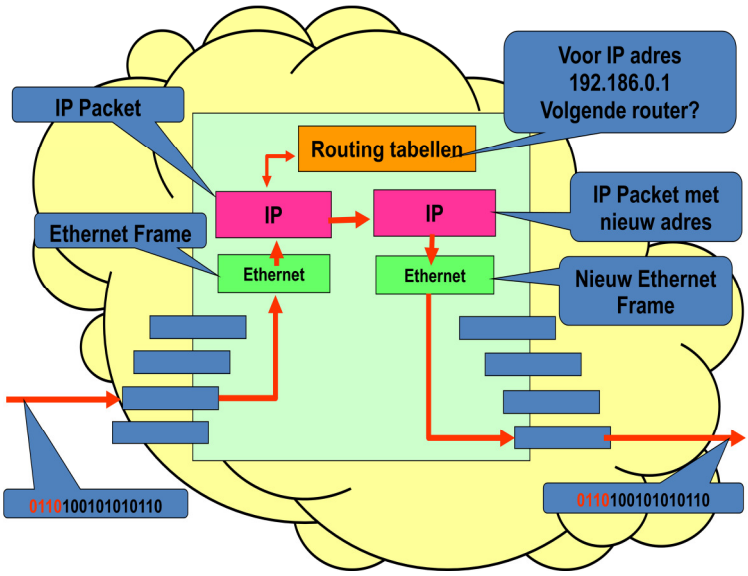
We beginnen bij de gebruiker die in zijn Browser de URL intypt van de webpagina die hij wil krijgen. De Browser maakt een HTTP-Request klaar: dit ziet eruit als een tekst, maar geschreven volgens de regels van het HTTP protocol. De Browser doet beroep op TCP en vraagt een verbinding aan. TCP maakt een verbinding aanvraag klaar en geeft die aan de IP laag. Deze leest het IP adres van de bestemming en steekt alles in een envelop, die het aan de laag 2 geeft. Hier is dat Ethernet, en die steekt de vraag in een Frame. Dit Frame gaat nu als een stroom van 0 en 1 via de PCI connector in de PC langs de coaxiale kabel naar de ADSL modem.



In de modem komt de stroom 0 en 1 toe. Er wordt een Ethernet Frame uitgehaald, en de laag 2 geeft de inhoud van dit Frame aan de netwerklaag: hier is echter geen netwerk: de inhoud gaat gewoon naar de volgende schakel in de ketting: dit wordt de laag2 van de uitgang.

Gezien we nu naar ADSL overstappen steekt deze laag 2 de inhoud in een Frame volgens de ADSL spelregels. De laag 1 is nu een gewoon telefoonpaar dat naar de centrale loopt, en daar klimt de informatie weer de stapel door tot de IP laag, waar de informatie in het internet wordt vertuurd.

Het **internet** is een netwerk opgebouwd uit **Routers** die met elkaar verbonden zijn.
Elke router is een beetje te vergelijken met een postkantoor: er komen briefen en pakjes binnen, we lezen de bestemming, en steken de brief of pakje op een transport in de richting van de bestemming. Ons bestand met de postcodes is de **Routing Tabel**.



De informatie komt links onder binnen als elektrische signalen, en de Ethernet laag 2 maakt er 0 en 1 stroom van en detecteert een Frame. De inhoud gaat naar de IP laag3, en leest op de envelop het IP Adres van de bestemming.

We consulteren de Routing Tabellen en zoeken een transport in de juiste richting. We vullen het IP adres in van de volgende router in. We steken dit alles weer in een envelop die we doorgeven aan laag 2 die er op zijn beurt weer een Frame van maakt en een stroom van 0 en 1 die aan laag 1 wordt gegeven. Die stuurt de gepaste elektrische signalen uit.

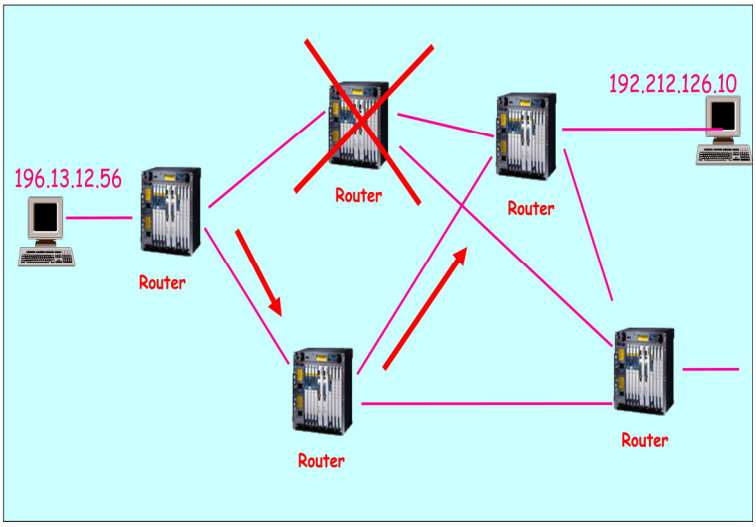
Aan de andere kant van het netwerk gaat alles in de omgekeerde richting: de informatie komt uit het internet, en gaat via de **ADSL modem** naar de **Host** die past bij de domeinnaam in de URL die in de browser werd ingegeven. In deze Host wordt de informatie weer via PCI, Ethernet en IP doorgegeven, en omdat het een HTTP-Request is, wordt het via TCP aan de WebServer afgeleverd. Die haalt de pagina en alles wat erbij hoort op, en stuurt het op een gelijkaardige manier terug (HTTP-Resonse).

Wanneer uiteindelijk deze response aan de browser wordt afgeleverd , leest die de HTML pagina en plaatst alles netjes op het scherm: tekst, prentje, geluid, flash etc…

De cyclus is rond…

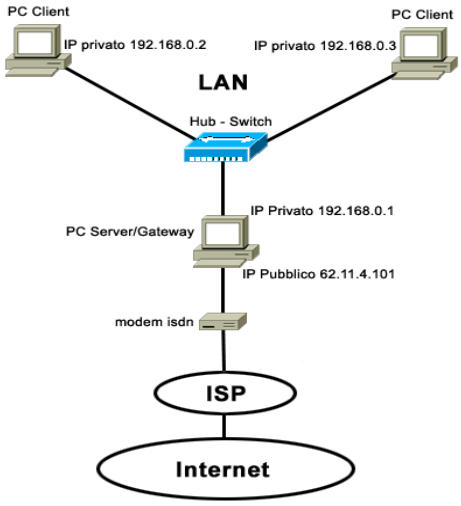
DEEL II: EEN OVERZICHT VAN NETWERKEN

Nu we verstaan wat een router zoal doet, gaan we eens kijken naar een aantal netwerken die we ermee kunnen opbouwen.

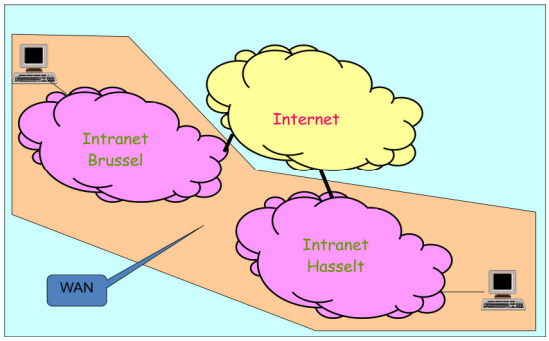


Er is op de eerste plaats het **publieke internet**. Elke router kan een eindbestemming langs meerdere wegen bereiken. Deze informatie staat in de **Routing Tabellen**. Elke router praat voordurend met zijn buren om te weten dat ze nog actief zijn ("Are You There" berichten).
Als er eentje niet meer antwoord, gaat hij uit de routing tabellen en wordt een tijdje niet meer gebruikt. De trafiek voor een bepaalde bestemming, wordt netjes verdeeld over alle mogelijke wegen.

In een bedrijfs- of **lokaal netwerk** (**LAN**) gebeurt hetzelfde, maar men heeft de intelligentie van de router niet altijd nodig: op laag 2 kan men ook een binnenkomend Frame naar alle aansluitingen sturen, en die met het juiste Mac Adres zal het dan wel behandelen. Een "doos" die enkel op laag 2 actief is, noemt men een **Hub ,** en het grotere model, een **Switch.**



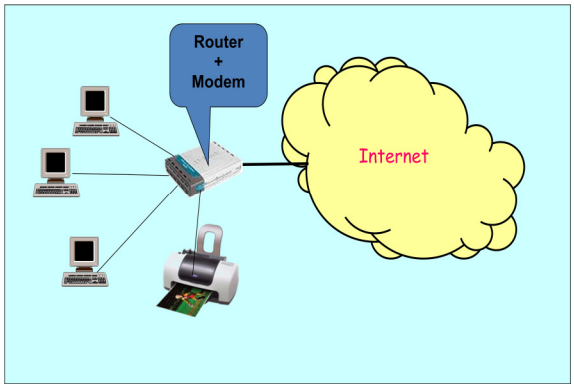
Een LAN heeft meestal ook een speciale toegang tot het publieke internet: dit is een speciale router die ook de functie van **Gateway** erbij neemt en ook een **Firewall** heeft om de LAN van het publieke (gevaar) af te schermen.



Grote bedrijven die op meerder locaties werken zullen vaak hun LAN's via het publieke internet met elkaar verbinden.

Het geheel noemt men dan een **Wide Area Network** of een **WAN**.

Een **Thuisnetwerk** dient om een paar PC's en een printer met elkaar te verbinden, en om toegang te geven tot het publieke internet.
Hiervoor koop je best een doos met **Router en Modem samen**.



In oudere huizen is het vaak moeilijk om kabels te voorzien: daar gaat de voorkeur naar draadloze verbindingen: een **draadloze router** al dan niet met ingebouwde modem, komt nu van pas.

Past men deze technologie toe in het openbaar, dan spreekt men van een **Hotspot**: de antenne heeft een veel hoger zendvermogen, en je kan vanuit je hotelkamer surfen, zonder gesleur met kabels.

Om een draadloze verbinding te kunnen maken volstaat het niet om zomaar signalen in de ether te sturen. Er is een standaard ontwikkeld die netjes beschrijft waaraan antenne en signalen moeten voldoen : dit zijn de **Wireless Fidelity of WiFi** standaarden.

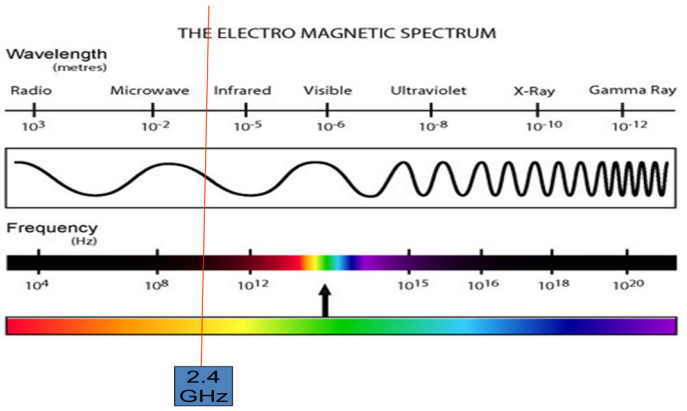
Deze standaarden zijn geschreven door de IEEE organisatie en kregen het nummer 802.11. Vandaar dat men een draadloze router ook wel eens een 802.11 router durft te noemen.

In het volgende hoofdstuk gaan we hier verder op in.

DEEL III: WAT IS WIFI

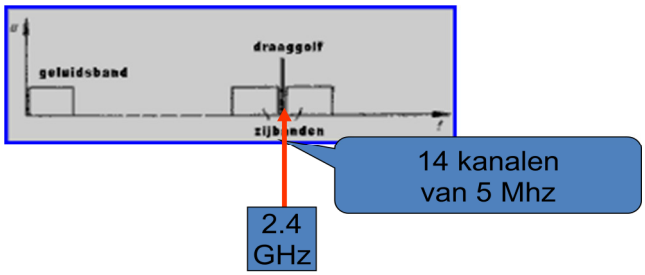
De WiFi situeert zich op laag 1: de fysische laag. De drager van de informatie bij WiFi is geen draad, maar wel **elektromagnetische golven** door de ether.

Om niet in de weg te lopen van andere toepassingen krijgt WiFi netjes zijn plaats toegewezen in het spectrum: op 2,4 of 5,8 GigaHertz.



In de loop der jaren zijn verschillende normen toegevoegd: met f= de draaggolf frequentie en s= de bit rate:

- **a** norm: f = 5.8 GHz en s = 5.4 Mbit/sec
- **b** norm: f = 2.4 GHz en s = 11 Mbit/sec
- **g** norm: f = 2.4 GHz en s = 54 Mbit/sec
- **n** norm: f = 2.4 en 5.8 GHz en s = 100 Mbit/sec



De meeste routers zijn van type g, maar vandaag begint type n de standaard te worden: men geraakt er beter mee door muren…

Op een draaggolf passen 14 kanalen met een bandbreedte van 5 MegaHertz elk.
Je kan dus 14 connecties tegelijkertijd gebruiken.

Er zijn wel een aantal beperkingen:

- Buiten in de tuin, is de draagwijdte ongeveer 100 meter
- Binnen in huis is dat ongeveer 45 meter
- Door baksteen muren of ijzer verlies je meteen 25%
- De WiFi straling is ook erg gevoelig voor storing van:
  - Microgolf
  - Bluetooth
  - Draadloze telefoon
  - Garage-opener

Maar de nadelen wegen niet op tegen de voordelen….

DEEL IV: DE WiFi RADIO

Om WiFi te gebruiken moet je PC hiervoor worden uitgerust. Je hebt een **antenne** nodig en de bijhorende software (**drivers**) om ze aan te sturen. Enkele voorbeelden:

Voor desktop PC's:

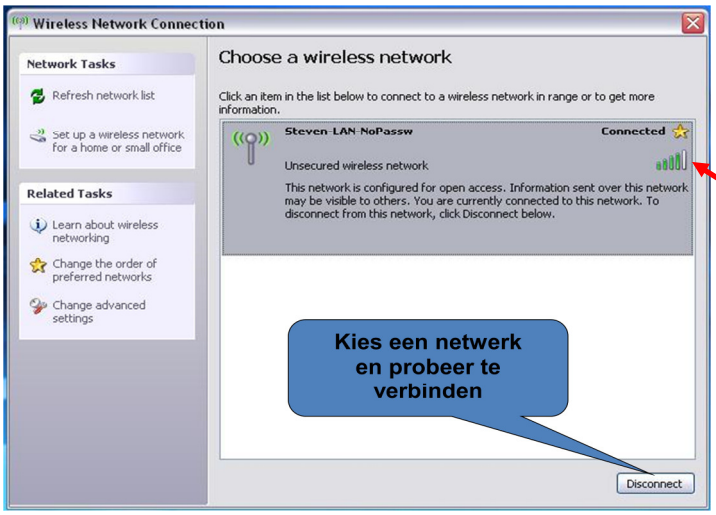
USB met houder

PCI kaartje

USB antenne

Voor draagbare PC's zijn er insteek modules:

Je moet met de bijgeleverde CD de installatie van de driver doen, en als dat gelukt is verschijnt rechts onder in de taakbalk het icoontje van een draadloze verbinding.

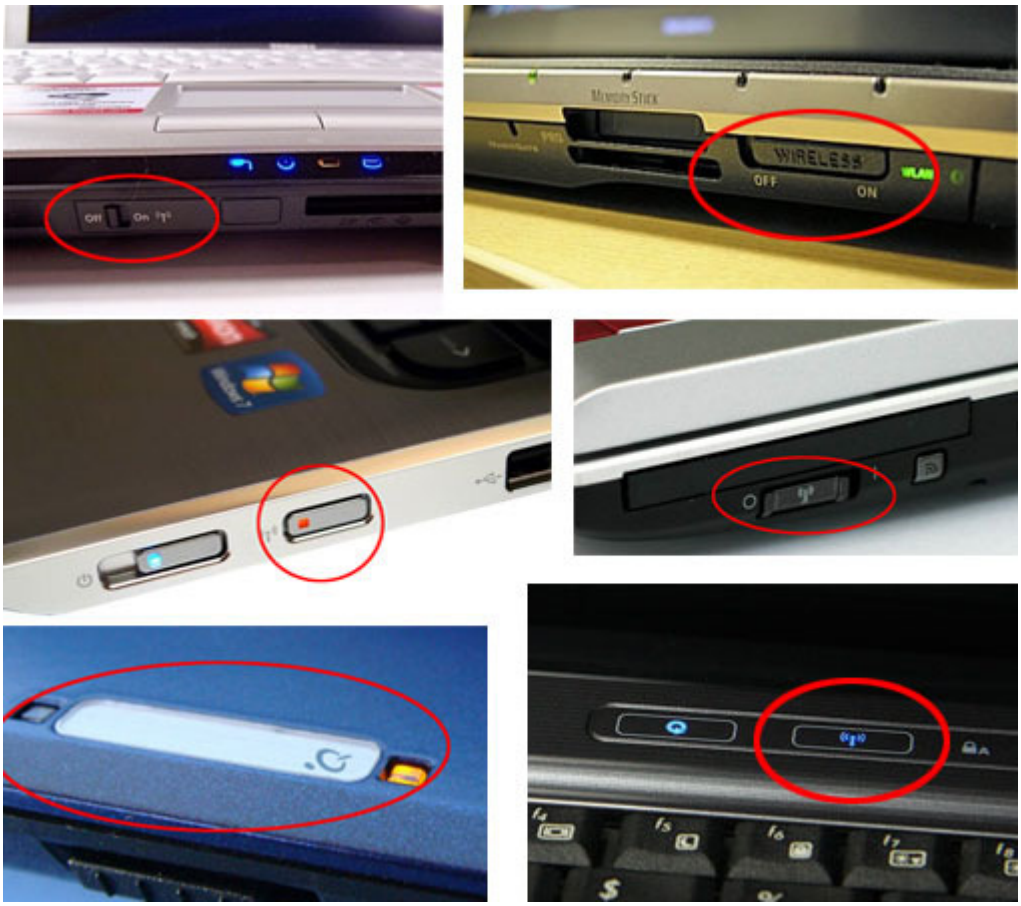


Vervolgens vraag je naar de lijst van netwerken binnen bereik, en probeer je een verbinding te maken. De sterkte van het signaal (de kwaliteit van laag 1) kan je zien aan de groene staafjes.

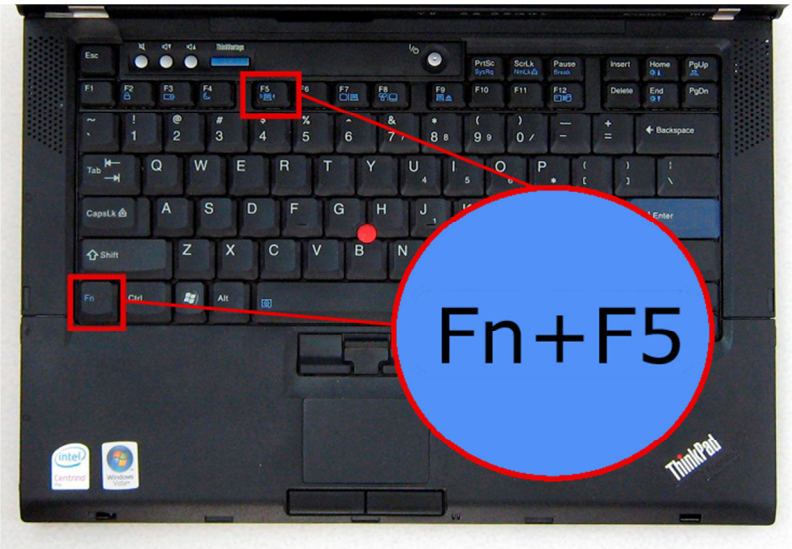
Het gebeurt af en toe dat een WiFi verbinding moeilijk tot stand te brengen is.
Het is dan ook belangrijk na te gaan of de WiFi radio wel degelijk aan staat.

Op draagbare computers die op batterij kunnen werken, wordt de WiFi soms uit gezet omdat die radio toch wel wat energie vraagt.

Kijk eerst na of er eventueel een hardware knop aan het toestel zit, meestal aan de zijkant, soms ook wel bovenaan op het toestel zelf.



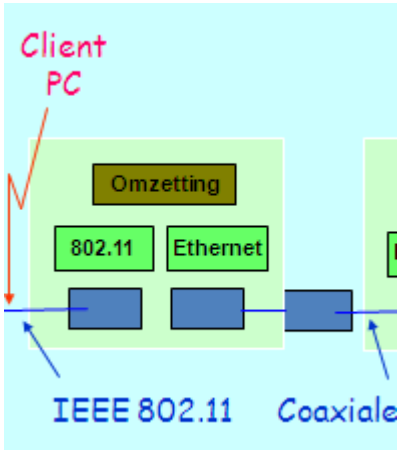
Kijk ook na of de WiFi niet wordt bediend met een toetsencombinatie van het type
Fn + een toets van de bovenste rij, bv. F5: dus Fn + F5.



DEEL V: HET WiFi BASISSTATION CONFIGUREREN

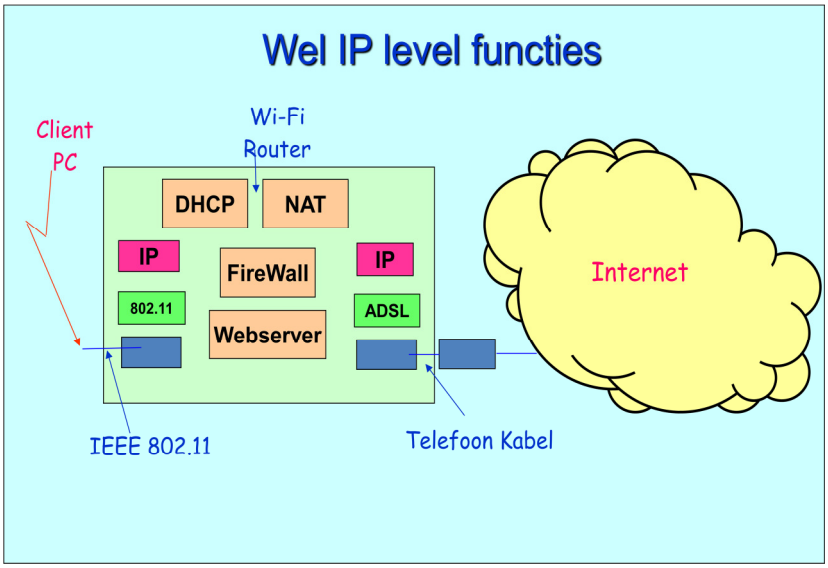
Net als bij draadverbindingen maakt men onderscheid tussen toestellen die werken tot en met laag 2 of tot en met laag 3.

De eerste noemt men een **Access Point**: zeg maar een toegangsdoos. De elektromagnetische golven worden ontvangen en omgezet in een 0 en 1 stroom . De laag 2 (volgens de WiFi standaard 802.11) herkent hierin frames. Deze worden gewoon naar alle uitgangen gestuurd als Ethernet Frames. Met het toestel dat antwoord gaat men verder: er wordt dynamisch een tabel van Mac Adresssen (in plaats van IP Adressen opgebouwd).
Dit toestel moet aan een "intelligente" router worden aangesloten: het groepeert alleen de WiFi traffiek.



Het tweede is dan de **Wireless Router**: die heeft alles in 1 doos. De Frames van laag 2 worden nu doorgegeven aan de IP laag en die gaat nu een aantal functies doen:

- het kent interne IP Adressen toe (DHCP)
- het interne IP Adres wordt vertaalt naar het publieke IP Adres (NAT)
- houdt potentiële schadelijke trafiek buiten (Firewall)
- draait een kleine WebServer om de router te configureren via een browser



Een access point wordt niet veel verkocht maar in de winkel moet je toch even opletten dat je wel degelijk een router aankoopt : anders valt er niets te configureren, en moet je toch nog een extra router in huis halen.

We gaan onze router even installeren: dit gaat in 3 stappen:

- sluit de voeding aan
- verbindt de WAN kant met het internet
- sluit een vaste PC aan op een van de vaste ethernet poorten

Vervolgens gaan we onze router configureren. Daarvoor openen we onze browser en surfen naar het IP Adres van onze router: meestal is die 192.168.0.1.

De ingebouwde WebServer geeft ons nu enkele eenvoudige pagina's: om te beginnen moeten we inloggen met de gebruikersnaam en paswoord die we op de documentatie vinden (meestal admin en 1234). Dan kunnen we eigenschappen van de router instellen:

a) *Eigenschappen van WiFi*:

SS-ID(Service Set Identifier): dit is de naam van de router, zoals hij zal verschijnen in het overzicht bij gebruikers die de lijst opvragen. Hier kies je best iets dat je zelf gemakkelijk onthoudt, maar waarmee buitenstaanders je niet kunnen herkennen.

Kanaal (1-11), standaard is dit 6: wegens interferentie met andere toestellen kan men een ander kanaal kiezen tussen 1 en 11, want er mag geen overlap zijn: er is 5Mhz per kanaal!!!

Beveiliging: er zijn heel wat instellingen hiervoor, gaande van toegang tot het netwerk, tot versleuteling van wat door de ether wordt gestuurd. Dit bespreken we in een apart hoofdstuk.

b) Eigenschappen van de WAN (internet kant):

Heeft mijn router een vast IP Adres of moet hij eentje vragen aan het internet (DHCP)? Afhankelijk van waarmee de router is verbonden, moet men het protocol kiezen dat moet gevolgd om de DHCP en de verbindingen op te zetten (ADSL, telefoon inbel lijn…)

c) Eigenschappen van de LAN (thuisnetwerk kant):

Het **IP Adres** van de router zelf, zoals hij in de LAN moet gekend zijn (dus meestal de 192.168.0.1). Meestal heeft een router een 4 tal vaste aansluitingen en onbeperkt draadloze toegang.

De router zal ook de IP Adressen toekennen aan zijn klanten in de LAN (de DHCP functie): binnen welke **Range** mag dit gebeuren: bvb. 192.168.0.**10** tot 192.168.0.**100**.

We kunnen een lijst opmaken van de Mac Adressen van de toestellen van onze LAN, en alle andere toestellen geen toegang geven. Dit noemt men een **Mac Filter**. Hetzelfde kan ook met de IP Adressen, maar deze laatste kan de gebruiker zelf instellen, en dit biedt dus weinig beveiliging. Dit noemt men een **IP Filter**. Mac Adressen zijn in de hardware van het toestel "gebakken": ze staan meestal aan de onderkant van het toestel op een speciaal plaatje.

Tenslotte is er nog de **Firewall**. We hebben gezien dat laag 4, met TCP of UDP werkt.
De informatie in een TCP of UDP pakket bevat de toepassing en het protocol waarmee moet gepraat worden: een webpagina wordt gevraagd met HTTP.
Zulke toepassing met bijhorend protocol noemt men een **Port**, met een specifiek nummer.

Het is de **Firewall die bepaalt welke deuren open** zijn, en welke gesloten. Om dit te kunnen instellen, moet je natuurlijk verstaan welke poorten bij welke applicatie horen: zo staat poort 80 voor HTTP en die moet openstaan of je kan niet surfen. Andere gekende poorten zijn 110 voor het ophalen van mail (POP3 protocol) en poort 25 voor het verzenden van mail (SMTP). Je kan misschien poort 23 gesloten houden: waarom moet men op je netwerk binnen met het oude Telnet protocol?

DEEL VI: DE WiFi ROUTER BEVEILIGEN

Algemene richtlijnen:

- Vervang het standaard wachtwoord (1234) van je draadloze router door een eigen wachtwoord, en ook de gebruikersnaam (dus niet admin….)
- Gebruik hiervoor een wachtwoord dat niet te raden is, bijvoorbeeld door willekeurige getallen te gebruiken, en geen namen en bestaande woorden.
- Verander de naam van je netwerk (SSID).
  De standaard naam vertelt de buitenwereld wat voor router je gebruikt. Dit is nuttige informatie voor de inbreker.
- Schakel Broadcasten uit. Het netwerk laat zijn aanwezigheid niet aan de buitenwereld merken.
- Gebruik een MAC filter. Hierbij geeft je de Mac Adressen op van de PC's die toegang mogen hebben tot jouw netwerk. Onbekende PC's komen er simpelweg niet op.
- Dit kun je uitbreiden met een IP filter, waarbij alleen PC 's met een bepaald IP-adres toegang krijgen. Je moet dan wel vaste IP Adressen gebruiken.
- Versleutel het dataverkeer tussen je PC 's en de router. Dit vermindert de kans dat het netwerk wordt gekraakt door gebruik te maken van onderschept verkeer.

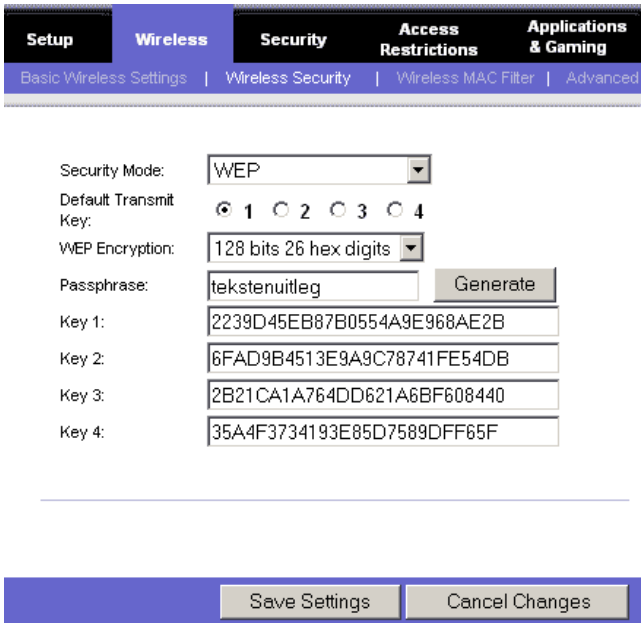
Versleuteling

Het is alsof je de gegevens die je over het draadloos netwerk zal sturen, in een doos steekt, en die doos afsluit met een sleutel. De ontvanger heeft ook een sleutel en kan de doos openen. Hoe complexer de sleutel hoe moeilijker hij is na te maken, lees te kraken.

Voorbeeld 1: WEP: Wired Equivalent Privacy

De sleutel is tegenwoordig 128 tekens groot. Er wordt geen authenticatie met paswoord meegegeven in het bericht. De sleutel wordt aangemaakt op basis van een slagzin, die je moet onthouden.

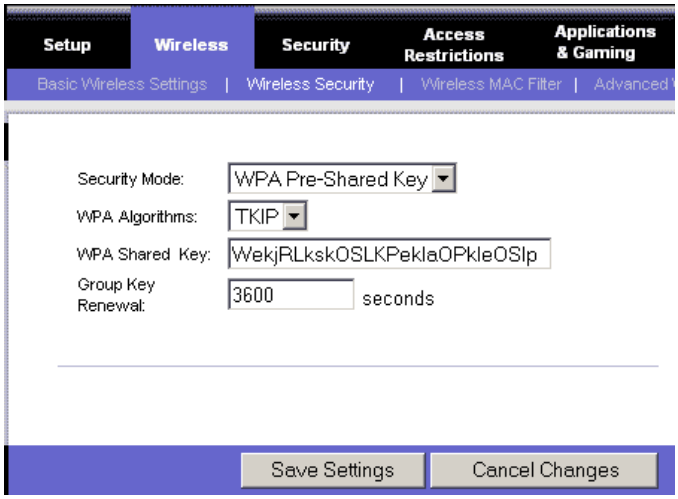
De PC die met de router wil communiceren moet deze slagzin kennen en dit zal dan de juiste sleutel genereren. Of hij moet de sleutel zelf toegestuurd krijgen.



Voorbeeld2: WAP (Wi-Fi Protected Access)

Deze methode is recenter en meer uitgebreid. Er is authenticatie met een paswoord tussen 8-63 tekens, die nog extra worden gemengd (hashed) met de SSID van de router.

Het versleutelen van de gegevens gebeurt met AES, met een 128 bit sleutel en 48 bit initialisatie vector. Ook de headers van de berichten worden mee versleuteld.
Bovendien verandert de sleutel regelmatig in de tijd: dit maakt het kraken des te moeilijker.

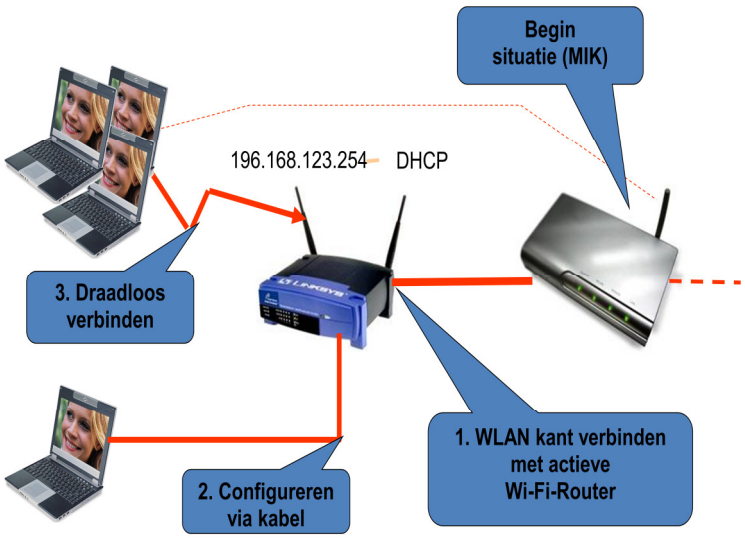


DEEL VII: DE WiFi ROUTER DEMONSTREREN

Als de IT coördinator van het leslokaal dit toestaat, kan de lesgever een eigen router meebrengen en er een demonstratie mee geven.

We doorlopen dan volgende stappen:

1. We sluiten de **WAN kant** van onze router aan, aan de LAN kant van de router van het leslokaal, met een ethernet kabel.
2. We sluiten een PC van het lokaal aan, aan de **LAN kant** van onze router, met een ethernet kabel. Vervolgens surfen we naar onze router en doen een paar **instellingen**.
3. Tot slot bekijken de lesvolgers op hun PC welke instellingen ze moeten doen, om via onze router te kunnen communiceren.



Bijvoorbeeld:

- Verander de SSID, en laat de lesvolgers de lijst van netwerken verversen: staat de nieuwe naam er al tussen???
- Verander eens het kanaal, en kijk of de PC's zich hier zelf aan aanpassen…
- Maak een Mac filter aan, en sluit een aantal PC's hierdoor uit…
- Maak een WEP sleutel, en laat de lesvolgers die op hun PC instellen…