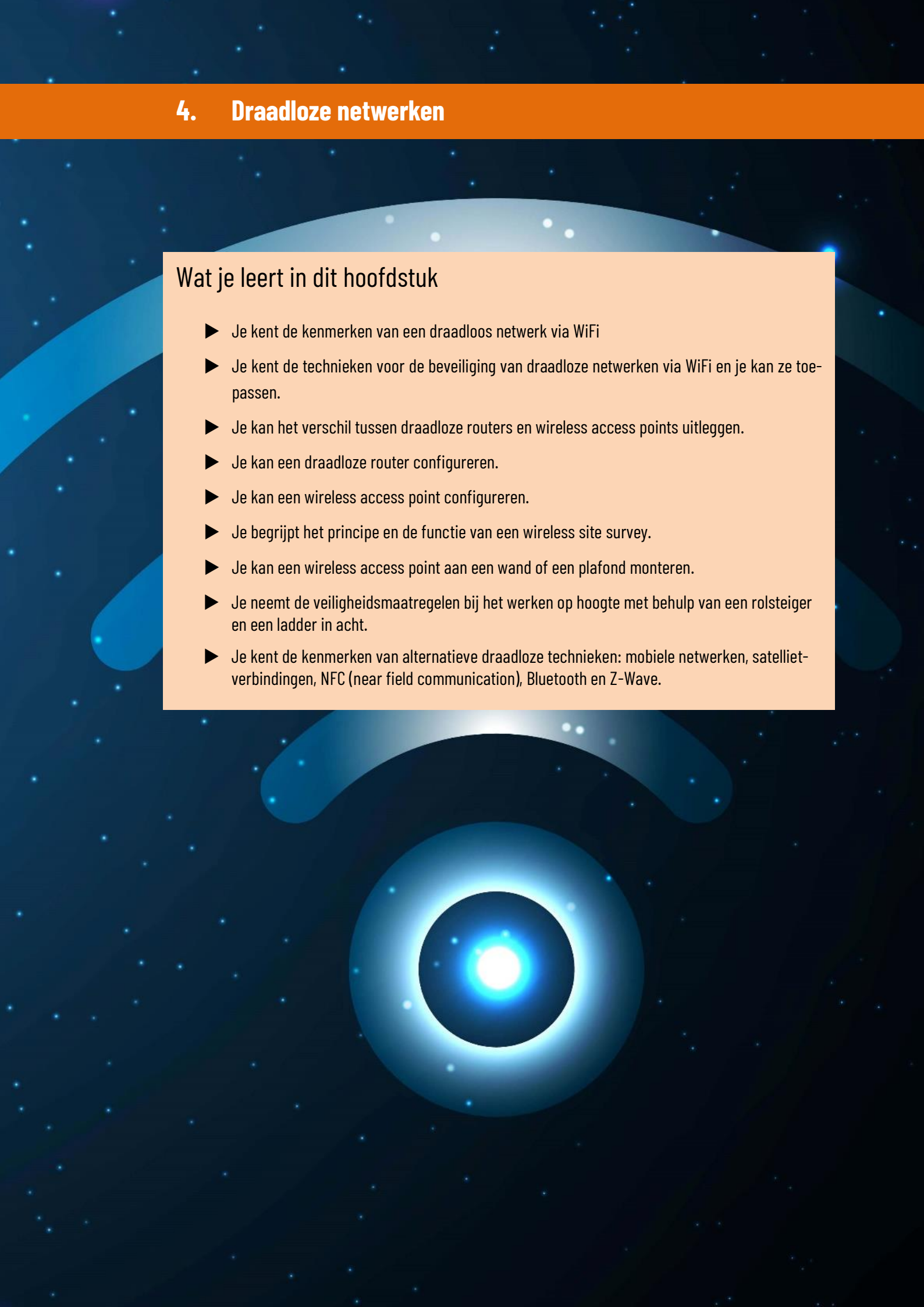
4. Draadloze netwerken



Wat je leert in dit hoofdstuk

- Je kent de kenmerken van een draadloos netwerk via WiFi
- Je kent de technieken voor de beveiliging van draadloze netwerken via WiFi en je kan ze toepassen.
- Je kan het verschil tussen draadloze routers en wireless access points uitleggen.
- Je kan een draadloze router configureren.
- Je kan een wireless access point configureren.
- Je begrijpt het principe en de functie van een wireless site survey.
- Je kan een wireless access point aan een wand of een plafond monteren.
- Je neemt de veiligheidsmaatregelen bij het werken op hoogte met behulp van een rolsteiger en een ladder in acht.
- Je kent de kenmerken van alternatieve draadloze technieken: mobiele netwerken, satellietverbindingen, NFC (near field communication), Bluetooth en Z-Wave.

4.1 WiFi

Radiofrequenties zijn erg bruikbaar voor het opzetten van draadloze netwerken. Ze worden weinig gehinderd door obstakels en afhankelijk van het vermogen van de zender en de gevoeligheid van de ontvanger varieert het bereik van enkele tientallen tot enkele honderden meters. De overdrachtssnelheid komt tegenwoordig in de buurt van bekabelde netwerken maar is wel sterk afhankelijk van de afstand tussen zender en ontvanger. Wireless LAN maakt gebruik van licentievrije radiofrequenties van de 2,4 GHz en de 5 GHz band, en sinds 2020 ook de 6 GHz band.

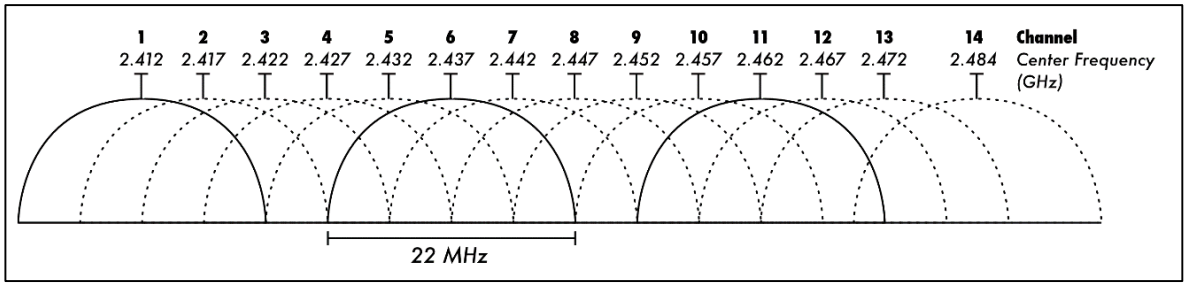
De standaarden voor draadloze communicatie werden internationaal vastgelegd in de IEEE 802.11 norm. Die kennen we beter onder de naam WiFi. Er ontstonden in de loop van de jaren verschillende standaarden. Die zijn gelukkig in grote mate terugwaarts compatibel. Dat wil zeggen dat een mobiel apparaat die een oude standaard hanteert perfect kan samenwerken met een modern access point. De maximale overdrachtssnelheid zal uiteraard die zijn van de traagste component.

802.11	2 Mbit/s	Eerste versie, gestandaardiseerd in 1997.
802.11b	11 Mbit/s	Eind 1999 goedgekeurde standaard op 2,4 GHz en de eerste die algemene verspreiding kende, maar soms werkte de apparatuur van verschillende fabrikanten niet goed met elkaar samen.
802.11a	54 Mbit/s	Deze standaard zag samen met 802.11b het levenslicht maar werkt op 5 GHz. Bovendien wordt het signaal gemakkelijker verstoord door obstakels tussen zender en ontvanger. Wellicht daardoor werd de standaard nooit erg populair.
802.11g	54 Mbit/s	In 2003 de opvolger van de 802.11b standaard voor hogere snelheden en de eerste die echt een commercieel succes was.
802.11n	300 Mbit/s 600 Mbit/s	Opvolger voor 802.11g vanaf 2009, die zowel op 2,4 GHz als 5 GHz werkt.
802.11ac	>1 Gbit/s	Nieuwe standaard in 2013, die enkel werkt op 5 GHz.
802.11ax	tot 7 Gbit/s	Een standaard uit 2018, die tegelijk gebruik maakt van 2,4 GHz en 5 GHz, en sinds 2020 ook van 6 GHz. Het is vooral veel efficiënter wanneer je met meerdere toestellen met eenzelfde access point verbindt.
802.11be	tot 30 Gbit/s	Deze standaard is nog in ontwikkeling en wordt verwacht in de loop van 2024. Ze zal eveneens gebruik maken van zowel 2,4 GHZ, 5 GHZ als 6 GHz.

De snelheden die in de tabel vermeld staan zijn theoretische snelheden: in de praktijk worden ze nooit gehaald. Vaak liggen de reële doorvoersnelheden ver beneden de helft van deze theoretische snelheid omwille van afstand, obstakels en interferentie met andere apparatuur.

Om gebruik te maken van draadloze netwerken, dienen de aangesloten computers uitgerust te zijn met een netwerkkaart met een WiFi-chip. Om het draadloze signaal zo goed mogelijk te kunnen opvangen, is zo'n netwerkkaart doorgaans uitgerust met een antenne. Dat kan een externe antenne zijn zoals bij insteekkaarten voor desktop computers, maar bij draagbare apparatuur zoals laptops, tablets en smartphones is zo'n antenne intern. De draadloze netwerkkaart ontvangt het signaal van een basisstation dat verbonden is met een bekabeld netwerk. Zo'n basisstation wordt een NAP (network access point) genoemd (zie 4.3).

Bij NAP's die gebruik maken van de 2,4 GHz band wordt het frequentiebereik opgesplitst in 14 kanalen, waarvan in Europa alleen het laatste kanaal niet kan gebruikt worden. De kanalen liggen vijf MHz uit elkaar. Een NAP zendt frequentiegolven met een breedte tot 22 MHz uit. Wanneer twee draadloze access points binnen elkaars bereik op eenzelfde of een overlappend kanaal uitzenden, kunnen ze elkaar storen. Daarom worden twee of drie verschillende NAP's die zich binnen elkaars zendbereik bevinden, het best ingesteld op zo ver mogelijk uit elkaar liggende kanalen (gewoonlijk 1, 6 en 11).



Bij NAP's die gebruik maken van de 5 GHz band en de 6 GHz band wordt het frequentiebereik opgesplitst in enkele tientallen kanalen met een frequentiebreedte van 20 MHz die elkaar niet overlappen. NAP's kiezen volledig automatisch het meest optimale kanaal, dus hoef je zelf niets meer in te stellen.

4.2 Beveiliging van draadloze netwerken

De signalen van een draadloos netwerk kunnen opgevangen worden buiten het gebouw waarvoor het bedoeld is en vormen dus een mogelijke toegang voor een hacker. Het enige wat die daarvoor nodig heeft zijn een mobiele computer met een draadloze netwerkkaart en eventueel een extra versterkende antenne. Op zijn laptop bevindt zich de nodige software om vliegensvlug de frequenties te scannen waarop draadloze netwerken actief te zijn. Een NAP (*network access point*) stuurt voortdurend een signaal uit met daarin zijn netwerknaam (SSID). De scanner van een hacker kan dat signaal dus ook oppikken.

Daarom kunnen draadloze netwerken beveiligd worden met encryptie. Dat wil zeggen dat de berichten die over het netwerk verzonden worden, versleuteld worden. Enkel wie het wachtwoord tot het netwerk kent, kan de berichten ontgrendelen. Er bestaan tot nu toe vier verschillende generaties van netwerkbeveiliging:

- **WEP** (wireless equivalent protocol) gebruikt een statische sleutel voor de encryptie. Die sleutel verandert dus nooit, wat de techniek erg kwetsbaar maakt. WEP kan daarom makkelijk gekraakt worden en is volledig voorbijgestreefd.
- **WPA** (WiFi protected access) gebruik een dynamische sleutel, wat wil zeggen dat bij elke nieuwe verbinding, een nieuwe sleutel wordt aangemaakt. Toch werd ook deze beveiligingsmethode al meermaals gekraakt.
- **WPA2** is de opvolger van WPA en gebruikt een nieuwe encryptiemethode, die trouwens in België werd bedacht. Die methode is moeilijker te kraken, maar blijkt voor zeer ervaren hackers toch nog niet veilig genoeg.
- Sinds 2018 bestaat **WPA3**, die gebruik maakt van een geavanceerde encryptiemethode die tot nu toe nog niet werd gekraakt.

Bij het instellen van een NAP stel je best de meest recente standaard in die beschikbaar is. Omdat niet alle toestellen onmiddellijk met WPA3 kunnen omgaan, wordt nieuwe netwerkapparatuur voorzien van zowel WPA2 als WPA3, die broederlijk naast elkaar kunnen werken. Sommige fabrikanten van bijvoorbeeld smartphones voorzien WPA3-ondersteuning via een update, maar heel wat oudere draagbare toestellen zal je moeten vervangen als je van WPA3 gebruik wil maken.

De netwerkbeheerder kan een ACL (access control list) aanleggen in de NAP. Dat is een lijst van alle MAC-adressen van de netwerkinterfaces die toegang krijgen tot het NAP. Komt het MAC-adres van een systeem niet voor in de lijst, dan krijgt die computer geen toegang tot het NAP. Het gebruik van deze techniek wordt **MAC-filtering** genoemd, maar een handige hacker kan die beveiliging vrij makkelijk omzeilen met een techniek die MAC-spoofing heet. Bovendien is deze vorm van beveiliging enkel bruikbaar in relatief kleine netwerken waaraan zelden een nieuw apparaat moet worden toegevoegd.

Bij het instellen van de beveiliging van een NAP volg je best deze aanbevelingen:

- Vul steeds een wachtwoord in voor administratortoegang tot het NAP. De meeste NAP's worden geleverd met een standaard wachtwoord, maar die kunnen zo op het internet gevonden worden. Het gebruik van een zelf gekozen wachtwoord is daarom noodzakelijk als je wil verhinderen dat buitenstaanders de NAP-instellingen kunnen wijzigen.
- Een NAP heeft doorgaans een standaard SSID die bestaat uit de naam van de fabrikant of het type van het NAP. Het best stel je een eigen, uniek SSID in. Meestal kan je het uitzenden van de SSID verbergen voor ongekende computers.
- Beveilig het netwerk met het meest recente beveiligingsprotocol. Betrouw zeker niet op minder veilige methodes als WEP of MAC-filtering.
- Schakel de firewall-functie van het NAP in om openstaande poorten te verbergen, indien die daarover beschikt. Je leert meer over firewalls in hoofdstuk 7.1.

Indien je enkel gebruik maakt van een draadloze router met modem die door een provider werd voorzien, heeft die provider de meeste veiligheidsinstellingen al voor jou gemaakt.

Vergeet ook niet de voor de hand liggende maatregelen om de toegang tot je netwerk moeilijker maken. Plaats een NAP nooit langs een buitenmuur of een raam, maar plaats het op een centraal punt binnen het gebouw. Zo wordt de afstand tussen de NAP en een mogelijke hacker groter en verkleint de kans dat de hacker een succesvolle verbinding maakt.

Wanneer je gebruik maakt van een publieke hotspot mag je niet teveel rekenen op de beveiliging die de beheerder daarvan heeft ingesteld. Een hacker die op dezelfde hotspot aangemeld is, maakt immers gebruik van dezelfde beveiligingstechniek als zijn slachtoffer en kan met de juiste software het gegevensverkeer met het NAP afluisteren. Gebruikers van publieke hotspots zorgen daarom best voor een goede beveiliging van het eigen computersysteem.

4.3 Een draadloos access point installeren

Draadloze access points bestaan in twee soorten:

- Draadloze access points met ingebouwde router voor thuisnetwerken.
- Draadloze access points zonder routerfunctie voor professionele netwerken.

De eerste soort beschikt over een aantal functies om een thuisnetwerk volledig te beheren, zoals een DHCP-server (zie hoofdstuk 6.3) en een firewall (zie hoofdstuk 7.1). De mogelijkheden van die functies zijn voldoende voor een thuisnetwerk, maar onvoldoende voor een professioneel netwerk. Daar worden die functies immers ingevuld door professionele routers of servers, die veel meer mogelijkheden voor het beheer bieden dan routers voor thuisgebruik. Access points voor professionele netwerken hoeven dus niet over dat soort functies te beschikken. Draadloze routers voor thuisnetwerken beschikken meestal ook over een ingebouwde switch met enkele (meestal vier) netwerkpoorten. Die vind je ook niet terug op access points.

De manier waarop je de instellingen in een access point wijzigt, is erg vergelijkbaar met de manier waarop je dat bij een switch doet. Sommige access points kan je via een cloud portal beheren, maar alle access points beschikken over een lokale webinterface. Via de browser van eender welke computer op het netwerk maakt de beheerder dan contact met het IP-adres van het access point. Nadat correct op het access point werd aangemeld via de browser, kan de netwerkbeheerder allerlei instellingen aanpassen.

Wanneer je een nieuw access point installeert, vind je het IP-adres en de standaard aanmeldingsgegevens (een gebruikersnaam en een wachtwoord) in de documentatie die bij het access point geleverd wordt. Oudere access points zet je eerst terug naar de fabrieksinstellingen, net zoals bij switches. Het standaard IP-adres en de standaard aanmeldingsgegevens kan je makkelijk vinden op het internet.

Ook nu weer is het eerste wat je in orde brengt het updaten van de **firmware**. Vervolgens kan je allerlei instellingen wijzigen om het access point zo optimaal mogelijk in te stellen voor je netwerk. Voorbeelden van instellingen die je kan aanpassen in access points zijn:

- De naam van het access point.
- De naam en het wachtwoord van de beheerdersaccount – bij sommige access points kan je extra beheerders aanmaken.
- Het IP-adres en het SSID van het access point.
- De keuze van frequentieband – 2,4 GHz, 5 GHz of 6 GHz.
- De beveiliging van het draadloze netwerk.

- Tijdsinstellingen om het access point automatisch uit te schakelen, bijvoorbeeld 's nachts of in het weekend.
- ...

Eenmaal je alle instellingen van het access point naar je voorkeuren hebt aangepast, moet je soms die instellingen nog definitief bewaren. Net als switches bieden ook access points de mogelijkheid om een **back-up** te nemen van de instellingen. Dat back-up bestand bewaar je dan op een veilige plaats. Als er ooit iets misloopt met het access point en alle instellingen werden gewist, kan je die eenvoudig terugzetten met behulp van het back-up bestand.

Een access point beschikt zelden over een aan/uit-knop. Uitschakelen of herstarten doe je via de webinterface. Zoek naar een optie *shutdown* of *reboot*.

Soms is het signaal van een draadloos netwerk te zwak of is het draadloze netwerk zelfs niet meer te vinden. Dat kan het gevolg zijn van zogenaamde frequentievervuiling die ontstaat door een teveel aan draadloze apparaten in de buurt, die elkaar op dezelfde frequentie in de weg zitten. Ook andere apparaten die met radiogolven werken, kunnen stoorzenders zijn: draadloze deurbellen, draadloze binnenhuistelefoons en zelfs een microgolfoven. Enkele tips om de ontvangst van een draadloze netwerk te optimaliseren:

- Plaats een NAP fysiek zo centraal mogelijk in een ruimte, weg van mogelijke fysieke obstakels.
- Zorg ervoor dat de antennes, indien het access point daarmee uitgerust is, steeds perfect verticaal gericht zijn. Je kan eventueel ook gebruik maken van een externe antenne.
- Bij oudere NAP's kan je eventueel in het instellingenvenster een ander kanaal instellen indien de ontvangst matig is. Bij moderne NAP's (IEEE 802.11n/ac) is dat niet meer nodig, omdat die al automatisch van het meest geschikte kanaal gebruik zullen maken.

Wanneer je draadloze netwerk opgebouwd is uit meerdere access points, is het van belang om de NAP's voldoende ver uit elkaar te zetten zodat ze elkaar niet teveel storen, maar uiteraard ook weer niet zover uit elkaar dat er deadspots ontstaan – dat zijn plekken waar er geen bereik is van het draadloze netwerk. Daarom zal bij een uitgebreid draadloos netwerk altijd een **wireless site survey** worden uitgevoerd. Daarbij wordt met een mobiel toestel doorheen het hele gebouw gegaan. Met de juiste software wordt voortdurend de sterkte van de signalen van de verschillende access points gemeten. Op basis van de resultaten via die scan, kan worden beslist om bepaalde access points te verplaatsen.

Access points worden doorgaans geleverd met een montageset. Dat is dan een metalen of kunststof plaatje, dat je met schroeven in de muur of tegen het plafond bevestigt. Het access point kan dan op dat plaatje vastgeklikt worden. De manier waarop dat moet, is niet gestandaardiseerd. Elke fabrikant heeft z'n eigen systeem. Een montage-handleiding wordt wel meegeleverd en kan je ook steeds terugvinden op de support-website van de fabrikant.

De meeste professionele access points kunnen gevoed worden via Power over Ethernet. Er is dan geen aparte stroomtoevoer meer nodig. Dat is handig omdat er niet altijd een vrij stopcontact in de buurt is en omdat je dan enkel de netwerkkabel naar het access point toe moet leiden. In sommige gevallen kan je die kabel exact op de plaats waar je het access point wil plaatsen, uit de wand of het plafond laten komen. Dat is de meest elegante oplossing om een access point netjes te monteren. Lukt dat niet, dan werk je de kabel het best weg in een kabelgoot die je netjes op de wand of het plafond bevestigt. De kabel gewoon los laten hangen of liggen is uit den boze.

Als alternatief worden access points ook wel eens boven op een vals plafond gelegd. Op die manier is het access point helemaal aan het zicht onttrokken en hoeft er geen bekabeling te worden weggewerkt. Uiteraard kan dit enkel indien het vals plafond niet uit materialen gemaakt is die het WiFi-signaal kan blokkeren.

Veilig op hoogte werken

Wireless access points worden steeds zo hoog mogelijk geplaatst. Op die manier kan het signaal zich optimaal verspreiden. Dat betekent dat we voor het aansluiten van access points vaak op een hoogte moeten werken en dat houdt veiligheidsrisico's in. Heel wat werkongevallen gebeuren door een val van een hoogte.

Bij het werken op een hoogte denk je in de eerste plaats aan het werken op een ladder. Daarbij moet de bedenking worden gemaakt dat ladders niet bedoeld zijn om op te werken. Ze dienen om een hoogteverschil te overbruggen waar geen trap aanwezig is. Wanneer je binnen in een gebouw op een hoogte moet werken, krijgen **rolsteigers** de voorkeur. Dat is een constructie van metalen buizen, voorzien van zwenkwielen, met daarop een platform dat in de hoogte verstelbaar is. Op zo'n rolsteiger is het heel wat veiliger werken dan op een ladder.

Een rolsteiger bestaat uit verschillende onderdelen: de zwenkwielen, ladderframes voor de zijkanten, verankeringsbuizen (schoren) en een of enkele platformen. Afhankelijk van de hoogte kan een rolsteiger immers in niveaus worden opgebouwd. Het opbouwen van een rolsteiger moet aangeleerd worden door ervaren instructeurs en het gebruik ervan hoort te gebeuren onder toezicht van een deskundig persoon. Daarbij moeten de volgende veiligheidsvereisten in acht genomen worden:

- De steiger moet waterpas staan.
- De ondergrond moet stabiel en recht zijn.
- De zwenkwielen moeten ten allen tijde door de rem geblokkeerd staan. Ze worden enkel gedeblokkeerd om de rolsteiger te verplaatsen. Betreed in elk geval nooit een rolsteiger indien de wielen niet geblokkeerd zijn.
- De steiger mag nooit gebruikt worden in de buurt van niet-geïsoleerde elektrische installaties of machines. Het metaal van de steiger is immers geleidend.
- Tijdens de opbouw van en het werken op een rolsteiger, draag je een veiligheidshelm. Voor opbouw en afbraak zijn veiligheidsschoenen en eventueel werkhandschoenen aanbevolen.
- Het opbouwen en afbreken van een rolsteiger doe je nooit alleen, maar steeds met minstens twee personen.

- Controleer na het vastmaken van twee onderdelen goed of ze stevig verankerd zijn, alvorens een volgend onderdeel te plaatsen.
- Betreed het platform nooit vooraleer de leuningen geplaatst zijn.
- Overschrijd nooit de maximaal toegelaten belasting van de steiger. Die wordt vermeld in de documenten die bij de rolsteiger aanwezig moeten zijn.
- Verplaats een rolsteiger nooit terwijl er nog iemand op staat.

Hoewel een **ladder** nooit bedoeld is om effectief op te werken, is het niet erg praktisch als je voor één enkel access point een rolsteiger moet opbouwen en nadien weer demonteren. Dan wordt er doorgaans toch wel gebruik gemaakt van een ladder. Ook daarbij gelden een aantal veiligheidsmaatregelen:

- Plaats een ladder onder een hoek van ongeveer 75 graden op een vlakke, stevige ondergrond.
- Houd de toegang tot de ladder vrij van obstakels.
- Baken de werkzone rond de ladder goed zichtbaar af.
- Gebruik enkel ladders die VCA-gekeurd zijn en tegen schuiven en slippen beveiligd zijn. Op een erg gladde ondergrond kan je gebruik maken van antislipmatten.
- Blokkeer deuren of doorgangen achter de ladder.
- Plaats de ladder zo dicht mogelijk naast de plaats waar het access point moet gehangen worden, links ervan als je rechtshandig bent, rechts ervan als je linkshandig bent.
- Draag schoenen met antislipzolen – bij voorkeur veiligheidsschoenen.
- Beklim een ladder altijd met het gezicht naar de ladder toe.

Moet je niet erg hoog werken, dan kan een dubbele trapladder (1), een huishoudtrap (2) of een reformladder (3) die je open kan zetten een veiliger alternatief zijn dan een ladder die je tegen de muur aan zet.

4.4 Alternatieve draadloze technieken

Voor draadloze netwerken is WiFi de standaard. Er bestaan nog een aantal andere draadloze verbindingstechnieken met elk een verschillend doel.

Al van in de vroege jaren 1980 ontstonden de eerste **mobiele netwerken**. In de loop van de jaren werden telkens nieuwe sprongen genomen in de technologie, die men generaties is gaan noemen. Zo spreken we tegenwoordig over 4G (vierde generatie) en 5G (vijfde generatie) van mobiele telefonie. Aan 6G wordt al volop gewerkt. Aanvankelijk waren mobiele netwerken enkel bedoeld voor telefonie, maar met opkomst van streaming, virtual reality en het Internet of Things is datacommunicatie nu de prioriteit.

Mobiele operatoren beschikken over duizenden zendmasten. Die zenden voortdurend signalen uit om contact te houden met de mobiele apparaten van hun abonnees, die signalen terugzenden. Op die manier weet de operator steeds in welke streek z'n abonnees zich bevinden. Abonnees kunnen zich vrij door het netwerk bewegen en hun toestel maakt automatisch verbinding met de zendmast die het meest optimale signaal aanbiedt. Het schakelen tussen de zendmasten gebeurt ongemerkt. Dat principe heet *roaming*.

Voor dataverbindingen over zeer lange afstanden (zelfs intercontinentaal) kunnen **satellietverbindingen** worden gebruikt. Traditionele satellieten bevinden zich op ongeveer 36 000 km boven de aarde. Dat heeft als voordeel dat een internetverbinding via satelliet zelfs op de meest afgelegen plek op aarde beschikbaar is. De nadelen zijn de lage overdrachtssnelheid en vertragingen in de verbinding omwille van de grote afstanden.

In 2019 begon het Amerikaanse bedrijf SpaceX met de uitbouw van een heel nieuw satellietnetwerk dat Starlink werd gedoopt en de bedoeling heeft om breedband internet mogelijk te maken op de meest afgelegen plaatsen in de wereld. In plaats van enkele satellieten op tienduizenden kilometer boven de aarde te brengen, bouwt SpaceX duizenden satellieten die op slechts enkele honderden kilometer boven het aardoppervlak zweven: sommige op ongeveer 340 km hoogte, andere op ongeveer 550 km en nog een aantal op 1150 km boven de aarde. Door die geringe hoogte wordt het probleem van de vertragingen verholpen.

Om van het Starlink-netwerk gebruik te kunnen maken, neem je een abonnement dat maar een beetje duurder is dan een gewoon breedband-abonnement. Je moet dan wel een Starlink-antenne aanschaffen en plaatsen, met een bijhorende modem. Ook werd een aangepaste antenne ontwikkeld die op grotere voertuigen kan gemonteerd worden, zoals vrachtwagens of mobilhomes.

NFC (near field communication) maakt het mogelijk om gegevens uit te wisselen tussen apparaten die zich op maximaal enkele centimeter afstand van elkaar bevinden. Het wordt vaak toegepast in mobiele apparaten, zoals smartphones en tablets, en wordt gebruikt voor bijvoorbeeld contactloze betalingen, waarbij gebruikers hun mobiele apparaat simpelweg in de buurt van een betaalterminal hoeven te houden om een betaling te voltooien. Andere toepassingen zijn het delen van bestanden tussen twee smartphones, het vervangen van elektronische toegangskaarten in bijvoorbeeld hotels, of het inschakelen van de stille modus wanneer een smartphone op een nachtkastje wordt geplaatst.

NFC vereist twee apparaten: een actief apparaat, zoals een smartphone of een betaalterminal, en een passief apparaat, zoals een kaart met een NFC-tag. Wanneer de apparaten dicht bij elkaar worden gebracht, creëren ze een draadloze verbinding via inductie.

Bluetooth is bedoeld voor goedkope radiolinks tussen draagbare computers, smartphones, draadloze luidsprekers, enz. De technologie maakt gebruik van de 2,4 GHz band om gegevens over een korte afstand (tot 10 meter) en aan een vrij lage snelheid (maximaal 2 Mbit/s) te versturen. Bluetooth creëert een lokaal netwerkje waarvan maximum acht andere apparaten deel kunnen uitmaken. Het eerste apparaat dat een Bluetooth-verbinding aangaat, wordt de beheerder van dat netwerk (master). Alle andere apparaten zijn dan slaven (slaves).

Voor het opzetten van een echt computernetwerk is Bluetooth te beperkt. Daarom wordt Bluetooth voornamelijk gebruikt voor het overbrengen van bestanden tussen mobiele apparaten onderling of als verbinding tussen een mobiel apparaat en een randapparaat, zoals een headset, een printer of het geluidssysteem van een wagen.

Voor domotica is **Z-Wave** de meest gebruikte standaard om schakelaars, camera's en sensoren van een domotica-systeem in een smarthome met elkaar te verbinden. De overdrachtssnelheden zijn erg beperkt, maar voor een domoticasysteem is dat geen bezwaar. Dat communicatie in twee richtingen kan verlopen is wel belangrijk: zo kan niet alleen een commando naar een schakelaar worden gestuurd, maar bijvoorbeeld ook de status ervan opgevraagd. Bovendien is het een voordeel dat Z-Wave erg weinig energie vraagt.

Alle onderdelen van een Z-Wave domoticasysteem – die worden *nodes* genoemd - maken deel uit van een mesh-netwerk dat aangestuurd wordt door de domotica-controller. Maximaal 231 nodes kunnen met die controller maar ook onderling met elkaar communiceren. De nieuwste generatie heet Z-Wave Plus, met een beter bereik, een lager energieverbruik en een hogere overdrachtssnelheid. Beide standaarden zijn wel compatibel en kunnen dus perfect binnen eenzelfde domoticanetwerk draaien. De communicatie tussen de nodes wordt beveiligd door middel van encryptie om te verhinderen dat hackers inbreken op het domoticasysteem.

De grote concurrent van Z-Wave heet Zigbee. Die technologie is helemaal vergelijkbaar met Z-Wave maar maakt gebruik van een andere frequentieband. Daardoor zijn beide concurrenten niet compatibel, al wordt daar wel volop aan gewerkt.