Scriptie

Managed Wi-Fi & Monitoring

Student

Naam:	Stefan van den Heuvel
Studentnummer:	1591945
E-mail:	stefanvandenheuvel@student.hu.nl
Bedrijf:	Lumiad
Telefoon:	06 534 172 39

Eerste examinator

Naam:	Don Dijkstra

Versiebeheer

Versie	Datum	Wijzigingen	Auteur
1.0	27-08-2013	De hoofdstukindeling	Stefan van den Heuvel
1.1	28-11-2013	Oplevering concept versie	Stefan van den Heuvel
1.2	10-12-2013	Feedback in het document verwerkt	Stefan van den Heuvel
2.0	16-12-2013	Definitieve versie	Stefan van den Heuvel

Document Informatie

Document type: Scriptie
Bedrijf: Lumiad
Student: Stefan van den Heuvel

Voorwoord

Geachte lezer,

Voor u ligt de scriptie die ontstaan is uit het Managed Wi-Fi & Monitoring 's project. Deze scriptie is geschreven in het kader van de afstudeeropdracht welke aangeboden is door Lumiad.

Inmiddels is het alweer bijna een half jaar geleden dat ik opzoek was naar een afstudeerproject. Ik heb hiervoor bij diverse bedrijven een sollicitatiegesprek gehad. Eén van deze bedrijven was Lumiad. Het eerste gesprek verliep vlot en het project leek mij vanaf het begin interessanter dan de andere projecten die ik aangeboden heb gekregen. De onderzoeksrichting van het project bood namelijk een goede relatie tussen techniek en management. Ik had dan ook niet veel tijd nodig voor de beslissing om van start te gaan bij Lumiad.

Ik heb de tijd binnen Lumiad als een zeer leerzame en gezellige tijd ervaren. Naast de afstudeeropdracht heb ik Lumiad geholpen andere projecten die leerzaam waren af te ronden. Hiervoor ben ik mee geweest naar diverse klanten. Dit heeft er mede voor gezorgd dat ik de 'grote brei' van informatie die op me afkwam, aan het begin van een project eigen heb kunnen maken.

Een erg leuke ervaring die ik heb opgedaan tijdens het project, was dat ik naarmate ik hier mee bezig was mijn kennis steeds groter werd. Hierdoor raakte ik steeds gemotiveerder om een goed product neer te zetten. Op dit punt heb ik grote plezier beleeft aan het voortzetten van het onderzoek.

Ik wil het voorwoord tevens gebruiken om een aantal personen te bedanken voor de ondersteuning, en hun bijdrage voor de totstandkoming van het project.

Ten eerste wil ik mijn afstudeerbegeleider, Tobias Bakker, bedanken voor de goede ondersteuning tijdens het project.

Ook wil ik Niek Crijns en Alexander Blaauwgeers bedanken voor de hulp die zij hebben geboden door mee te denken over complexe technische vraagstukken.

Tot slot wil ik Wim Bos bedanken voor het vertrouwen en het beschikbaar stellen van de afstudeeropdracht.

De Meern, 16 december 2013

Stefan van den Heuvel

Managementsamenvatting

Het belang van draadloze oplossingen heeft ertoe geleid dat veel kleine en middelgrote bedrijven ook graag een draadloos netwerk geïmplementeerd willen hebben. Lumiad biedt het implementeren en beheren van draadloze netwerken al aan in de vorm van een dienst. Voor deze dienst wordt in de meeste gevallen gebruik gemaakt van een Wireless Lan Controller (WLC) op klantlocatie. Deze controller voorziet de access points in het klantnetwerk van systeemupdates, configuraties en bewaking. Echter is het implementeren van een draadloos netwerk momenteel een prijzige en tijdrovende oplossing omdat de klant een dure controller nodig heeft, en het een tijdrovende klus is om deze te configureren. Ook moet Lumiad het beheer en de monitoring van het draadloze netwerk momenteel op locatie van de klant uitvoeren.

Uit deze aanleiding is het project 'Managed Wi-Fi' ontstaan waarin onderzoek werd gedaan naar de mogelijkheden voor het inzetten van een oplossing waardoor de verschillende klantnetwerken gecentraliseerd vanuit een remote locatie voorzien kunnen worden van configuratie, beheer en bewaking.

Uit de resultaten van het onderzoek ben ik tot de conclusie gekomen dat Managed Wi-Fi kan worden aangeboden aan verschillende de klanten van Lumiad. Uit interviews met klanten blijkt namelijk dat er animo is. Vooral bedrijven met ongeveer vijftien access points zijn geïnteresseerd. Managed Wi-Fi draagt namelijk bij aan een goedkopere implementatie doordat de klant alleen goedkope thin access points aan hoeft te schaffen. Daarnaast zijn de access points sneller te implementeren in het klantnetwerk doordat de controller de access points automatisch configureert. De verschillende klantomgevingen kunnen namelijk door een enkele controller, vanuit Lumiad worden configureert.

Aan de implementatie met alleen thin access points op klantlocatie zit wel een consequentie. De draadloze netwerk omgeving van de klant zal namelijk offline gaan als de verbinding met de controller verbreekt. Lumiad beperkt dit risico door de controller redundant in te zetten m.b.v. een uitwijklocatie. Echter heeft dit geen nut als de netwerkapparatuur of de internetverbinding van de klant niet werkt. Mocht dit het geval zijn kan de klant via het draadloze netwerk niet alleen het internet niet meer bereiken maar ook de apparaten in het interne netwerk niet. Op het interne netwerk kunnen bijvoorbeeld dataservers met gedeelde documenten benaderd worden. Als de klantomgeving wordt voorzien van fat access point of een controller, zal het interne netwerk wel beschikbaar blijven, als de klant geen internetverbinding meer heeft. Daarom raad ik Lumiad ook aan de klant op de hoogte te brengen van deze consequentie, en eventueel te adviseren fat access points of een lokale controller te implementeren.

Managed Wi-Fi kan worden geïmplementeerd met apparatuur van verschillende draadloze merken. In eerste instantie zou Lumiad Managed Wi-Fi met Motorola apparatuur kunnen realiseren. Motorola is namelijk een bekende speler op de Nederlandse markt, bied hoge kortingen, heeft uitgebreide mogelijkheden, is betrouwbaar en verdient de voorkeur van de beheerders van Lumiad. Tevens kan Lumiad in de toekomst ook onderzoek doen naar het realiseren van Managed Wi-Fi met Lancom. Lancom is namelijk een betrouwbaar merk, heeft uitgebreide mogelijkheden, hanteert geen licentiekosten en verdient de voorkeur van de beheerders van Lumiad.

Ik raad Lumiad ook aan om de draadloze Motorola apparatuur te monitoren omdat er dan een product met een hoge beschikbaarheid op de markt gezet kan worden. Monitoring draagt bij aan een hogere beschikbaarheid doordat een incident preventief kan worden voorkomen of sneller kan worden verholpen. De monitoring kan de beheerder van Lumiad namelijk geautomatiseerd inlichten met informatie over een incident, waardoor het incident eerder kan worden verholpen. Een incident kan preventief worden verholpen door proactief te monitoren. Dit betekend dat een incident kan worden gedetecteerd, en verholpen voordat deze optreed. De monitoring kan namelijk 'vreemd' gedrag constateren, bijvoorbeeld een hoge CPU, en de beheerder hierover inlichten voordat er een incident optreed. De beheerder is hierdoor in staat het incident te verhelpen nog voor deze optreed.

Lumiad kan monitoren m.b.v. het systeem Check_MK. Check_MK heeft als voordeel dat de beheerders van Lumiad bekend zijn met dit systeem en apparatuur van andere merken ook met Check_MK wordt gemonitord. Ook gaat Check_MK zuinig om met de bandbreedte, door het bundelen van informatie tot een enkel pakket. Tot slot kan Check_MK naar eigen wensen kan worden ontwikkeld omdat het open source is.

Het ontwikkelen van een goede basis voor de monitoring is met afsluiting van dit project gerealiseerd in Check_MK. Hiervoor is er een uitbesteding gedaan naar een ontwikkelteam in Oekraïne. Lumiad kan hierdoor access points en controllers van Motorola monitoren. Tevens worden de gebruikers, die ingelogd zijn op de access points gemonitord. Ook zijn er functionaliteiten toegevoegd om de gebruikersgemak te verbeteren. Om dit te realiseren is de informatie overzichtelijk weergegeven d.m.v. het toevoegen van filters. Tevens zijn er iconen toegevoegd om sneller te kunnen navigeren, tussen de verschillende plugins en de web interface van een access point of controller.

Voor de implementatie van de monitoring kan Lumiad gebruik maken van distributed monitoring. Bij distributed monitoring wordt er een slave monitoringsserver in een klantnetwerk geïmplementeerd en een centrale monitoringsserver bij Lumiad. Doordat de slave monitoringsservers van de verschillende klanten de monitoringsresultaten verzenden naar de centrale Check_MK server bij Lumiad, kunnen de resultaten van de verschillende klanten gecentraliseerd op een dashboard worden weergeven. Tevens is deze techniek bandbreedte efficiënt omdat het monitoringsverkeer niet constant over het WAN verzonden hoeft te worden, maar eens in de zoveel tijd een update stuurt met informatie over de draadloze klant apparatuur.

Tot slot raad ik Lumiad aan gebruik te maken van een geautomatiseerde implementatiemethode voor de monitoring, waardoor een implementatie minder tijd kost. Om dit te realiseren is er een uitbesteding gedaan voor een geautomatiseerd installatiebestand van het monitoringssysteem. Dit installatiebestand bevat een menu waarin parameters kunnen worden ingegeven, zoals een IP configuratie of mail server, waarna het monitoringssysteem met de benodigde plugins geïnstalleerd wordt. Tevens is het hiermee mogelijk apparatuur automatisch aan Check_MK toe te voegen d.m.v. een scan naar draadloze Motorola apparatuur.

lumiad

Inhoud

1 Inleiding

Deze scriptie is het eindproduct van het afstudeerproject 'Managed Wi-Fi & Monitoring'. Dit project is uitgevoerd in de periode van augustus 2013 tot januari 2014.

Het belang van draadloze oplossingen heeft ertoe geleid dat veel kleine en middelgrote bedrijven graag een draadloos netwerk geïmplementeerd willen hebben. Voorbeelden van draadloze oplossingen zijn:

- Het geautomatiseerd kunnen scannen en schrijven van de informatie naar een database.
- Het gebruik van draadloze beveiligingssystemen.
- Het bellen met VOIP-technologie[1].

Om deze draadloze oplossingen mogelijk te maken en de gebruikers te voorzien van een draadloze internet verbinding wordt er gebruik gemaakt van access points. Lumiad biedt het implementeren en beheren van draadloze netwerken al aan in de vorm van een dienst. Voor deze dienst wordt in de meeste gevallen gebruik gemaakt van een Wireless Lan Controller (WLC)[2]. Deze controller heeft de volgende functionaliteiten:

- Het configureren van configuratieprofielen en de access points hiervan voorzien.
- Het updaten van de besturingssystemen van de access points.
- Het bewaken en uitlezen van de access points.

Het gebruik van een controller heeft de volgende voordelen tegenover het gebruik van alleen access points:

- De access points kunnen gezamenlijk worden configureert en worden geüpdatet.
- Er kunnen goedkopere access points worden aangeschaft.
- De access points kunnen worden gemonitord via de controller en het is mogelijk netwerklogs te verzenden naar een e-mail adres, of alarmen te genereren bij storingen.
- De controller kan als firewall dienen en de access points voorzien van een captive portal[3].

In de huidige situatie worden draadloze netwerken door Lumiad geïmplementeerd met een controller op locatie van de klant. Deze werkwijze heeft de volgende knelpunten:

- Dit is een prijzige en tijdrovende oplossing omdat de klant zelf voor de aanschafsprijs van een controller betaalt, en het personeel van Lumiad de apparatuur op klantlocatie moet implementeren en configureren. Het knelpunt treft vooral de kleinere netwerken omdat de prijs van een controller niet opweegt tegenover enkele access points.
- Het netwerkteam van Lumiad moet het beheer op locatie van de klant uitvoeren. Hiervoor moet het personeel van Lumiad bij de klant langs gaan of gebruik maken van een remote verbinding.
- Het implementeren van een draadloos netwerk kost meer tijd dan nodig omdat de apparatuur handmatig op klantlocatie geconfigureerd dient te worden.
- Bij elke nieuwe klant moet de controller vanaf het nulpunt geconfigureerd worden.

---

[1] VOIP-technologie - Bij Voice over IP(VoIP) wordt het internet of een ander netwerk gebruikt om spraak te transporteren.

[2] Wireless Lan Controller (WLC) - een Wireless Lan Controller (WLC) is een apparaat voor het configureren, updaten en bewaken van access points.

[3] Captive Portal - Een Captive Portal forceert een gebruiker op het netwerk met een webpagina voordat de gebruiker op het netwerk kan. Dit is meestal voor authenticatie of marketing doeleinde.

Hieruit voort is het project ontstaan waarin onderzoek werd gedaan naar de mogelijkheden voor het inzetten van een oplossing waardoor de verschillende klantnetwerken gecentraliseerd vanuit een remote locatie voorzien kunnen worden van configuratie, beheer en bewaking.

Een bijkomend deelonderzoek is het inrichting van de monitoring voor Motorola apparatuur. Omdat Motorola de laatste tijd flinke kortingen biedt op productaankopen is Lumiad draadloze netwerken met Motorola apparatuur gaan implementeren bij klanten. De monitoring van Motorola is hierbij nog niet ingericht. Het is van belang dat dit wordt ingericht omdat monitoring bijdraagt aan de kwaliteit van het draadloos netwerk.

De centrale hoofdvraag die bij dit onderzoek hoort is: ‘Op welke manier kunnen Managed Wi-Fi en de monitoring van Motorola apparatuur door Lumiad worden ingezet?’

De scriptie bestaat uit een omschrijving van de organisatie en een omschrijving van de afstudeeropdracht om de lezer de noodzakelijke voorinformatie te verschaffen. Vervolgens zullen het onderzoek en de onderzoeksresultaten worden beschreven. Hierna worden de conclusies beschreven aan de hand van de onderzoeksvragen uit het plan van aanpak. Tot slot volgt er een advies uit de onderzoeksresultaten en conclusies.

Tevens bevat het document een evaluatie van de procesgang en ondersteunende bijlagen. In de bijlage is het plan van aanpak, een persoonlijke evaluatie, een verklarende woordenlijst, een functioneel en technisch ontwerp en een viertal projectplannen voor de uitbesteding aan het ontwikkelteam in Oekraïne.

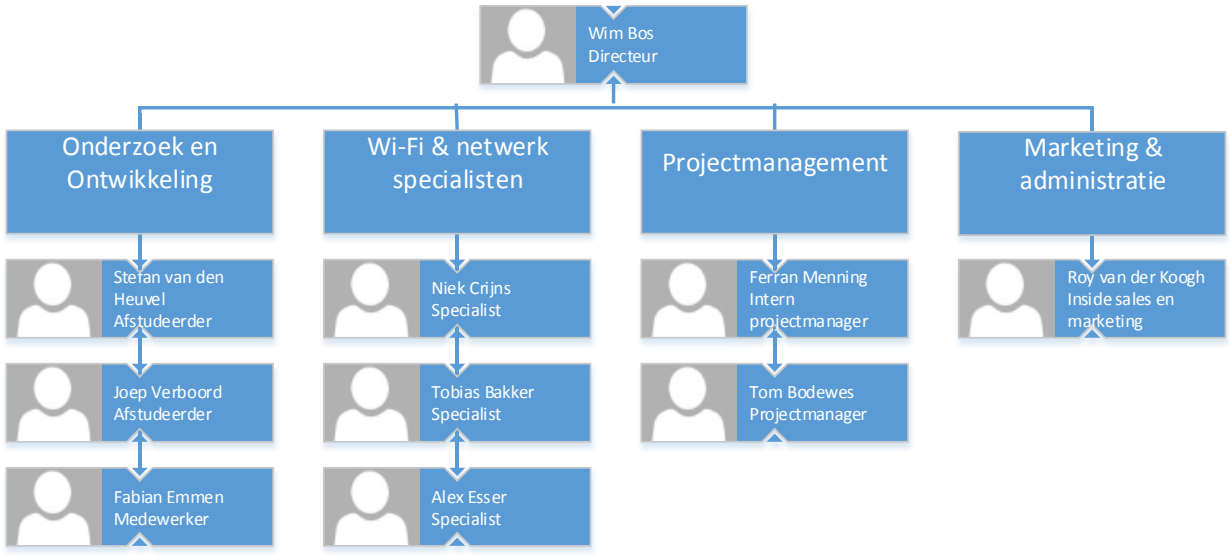
2 Organisatie

De afstudeeropdracht is uitgevoerd bij het bedrijf Lumiad. Lumiad is opgericht in 1999 door Wim Bos als een eenmanszaak in Wi-Fi consultancy. Tussen 2000 en 2002 werkte Wim Bos als intern manager voor bedrijven als Global crossing, Lucent Technologies en Agere Systems. In 2002 is Lumiad gestart met het zelf ontwikkelen van projecten en producten.
Tegenwoordig voorziet Lumiad niet alleen in Wi-Fi consultancy, maar ook in installatie, configuratie en onderhoud van draadloze netwerken. Daarnaast ontwikkelt Lumiad producten onder de naam Aerga. Producten en diensten die Lumiad leveren zijn onder andere op het gebied van:

- Netwerk infrastructuur
- Voice over IP
- Hotspot & Captive Portal
- Locatiebepaling (RTLS)
- Straalverbindingen (P2P)
- Management en Monitoring
- Netwerk beveiliging
- Wi-Fi Cursussen

Deze diensten levert Lumiad aan diverse klanten. Voorbeelden van enkele klanten zijn Schiphol, Creative Valley en Hogeschool Utrecht.

Lumiad bestaat uit elf personeelsleden en vier afdelingen. De afdeling 'Onderzoek en ontwikkeling', (waar ikzelf onderdeel van uitmaak) is met name voor parttimers, stagiaires en afstudeerders. Daarnaast is er een technische afdeling waaronder Wi-Fi en netwerkspecialisten zijn ingedeeld, een afdeling voor marketing & administratie en tot slot een projectmanagement afdeling. Omdat het bedrijf klein is komt het vaak voor dat medewerkers taken van andere afdelingen overnemen.
In figuur 1 is het organogram te vinden die de afdelingen en de indeling van het personeel van Lumiad weergeeft.



Figuur 1- Organogram van Lumiad

De directie van Lumiad bestaat uit Wim Bos. De directie houd zich voornamelijk bezig met het coördineren van het bedrijf en het personeel. Daarnaast houdt de directie zich bezig met het werven van nieuwe klanten en onderhouden van de bestaande contacten.

De afdeling onderzoek en ontwikkeling is een flexibele afdeling die bestaat uit, parttimers, stagiaires en afstudeerders. Omdat de parttimers, stagiaires en afstudeerders verschillende achtergronden hebben worden hier gevarieerde IT gerelateerde projecten uitgevoerd.

Wi-Fi & netwerk specialisten beheren de techniek die Lumiad op de markt zet. Zij configureren en implementeren de producten bij de verschillende klanten. Ook dragen zij zorg voor de technische support die bij de producten word geleverd.

De afdeling projectmanagement bewaakt en organiseert de projecten, waardoor deze beheerst uitgevoerd kunnen worden. Zij zorgen voor de voorbereiding, planning, de uitvoering en de afronding van de projecten.

Marketing & administratie draagt bij aan het werven van nieuwe klanten en het verzorgen van de administratie en financiën. Ook onderhoudt deze afdeling de website en de verschillende sociale media van Lumiad.

3 Afstudeeropdracht

Dit hoofdstuk beschrijft de afstudeeropdracht conform het plan van aanpak.

3.1 Probleemstelling

In de huidige situatie worden draadloze netwerken door Lumiad geïmplementeerd met een controller op locatie van de klant. Deze werkwijze heeft de volgende knelpunten:

- Dit is een prijzige en tijdrovende oplossing omdat de klant zelf voor de aanschafsprijs van een controller betaalt, en het personeel van Lumiad de apparatuur op klantlocatie moet configureren. Het knelpunt treft vooral de kleinere netwerken omdat de prijs van een controller niet opweegt tegenover enkele access points.
- Het netwerkteam van Lumiad moet het beheer op locatie van de klant uitvoeren. Hiervoor moet het personeel van Lumiad bij de klant langs gaan of gebruik maken van een remote verbinding.
- Het implementeren van een draadloos netwerk kost meer tijd dan nodig omdat de apparatuur handmatig op klantlocatie geconfigureerd dient te worden.

Omdat Motorola de laatste tijd flinke kortingen biedt op productaankopen is Lumiad draadloze netwerken met Motorola apparatuur gaan implementeren bij klanten. De monitoring van Motorola is hierbij nog niet ingericht. Het is van belang dat dit wordt ingericht omdat monitoring bijdraagt aan de kwaliteit van het draadloos netwerk.

3.2 Doelstellingen

De doelstellingen waren opgesplitst in doelstellingen voor de student en doelstellingen voor Lumiad.

Doelstellingen van de student:

- Een advies leveren aan Lumiad voor het inzetten van Managed Wi-Fi en monitoring.
- Het inrichten van de monitoring met ondersteuning voor Motorola apparatuur.
- Slagen voor de afstudeeropdracht op HBO niveau, met maximaal resultaat.

Doelstellingen vanuit Lumiad:

- Het beheer en de implementatie van een draadloos netwerk goedkoper aan kunnen bieden.
- Centraliseren van het beheer door het inzetten van Managed Wi-Fi.
- De tijd die het kost om een draadloos netwerk te implementeren terug te dringen.
- Kwaliteit leveren op het draadloze netwerk d.m.v. monitoring

3.3 Projectrelaties

Een project dat van start zou gaan was het automatiseren van de radiusconfiguratie d.m.v. een applicatie. Een relatie tussen deze projecten zou een bundeling van de monitoringsresultaten betreffen. De gegevens die met het monitoringssysteem werden opgevraagd in de individuele projecten zouden namelijk gekoppeld kunnen worden waardoor een completer overzicht zou ontstaan.

De afstudeerder die dit project was gestart heeft Lumiad tijdens het vooronderzoek verlaten. Dit heeft ertoe geleid dat het project nooit gestart is.

3.4 Opdrachtformulering

De opdracht was een onderzoek om de doelstellingen (uit hoofdstuk 3.2) te realiseren. Hiervoor is onderzocht of Managed Wi-Fi door Lumiad zou kunnen worden ingezet. Managed Wi-Fi is een benaming van Motorola om de verschillende klanten gecentraliseerd vanaf een enkele locatie te kunnen voorzien van configuratieprofielen, updates en bewaking. Tevens is er onderzocht hoe de monitoring van Motorola apparatuur ingericht kan worden.

3.5 Afbakening

Om te zorgen dat er duidelijke projectgrenzen waren werd er gebruik gemaakt van een afbakening d.m.v. de MoSCoW methode. Deze methode beschrijft welke eisen er noodzakelijk zijn, welke wensen belangrijk en minder belangrijk zijn en tot slot de aspecten die niet onder het project vallen.

- Must have: Dit geeft aan wat het project absoluut moet bevatten om een succes te zijn, zonder deze eisen is het projectproduct niet bruikbaar.
- Should have: Dit zijn eisen die erg gewenst zijn maar niet noodzakelijk.
- Could have: Deze eisen zijn minder belangrijk maar toch wenselijk.
- Won't have: Deze eisen zullen niet meegenomen worden tijdens dit project.

	Nr.	Onderdeel
Must have	1	Plan van aanpak
	2	Scriptie
	3	Onderzoeksrapport
	4	Functioneel ontwerp
	5	Technisch ontwerp
	6	Proof of concept Managed Wi-Fi met Motorola & Motorola Monitoring
	7	Adviesrapport voor Managed Wi-Fi met Motorola en Motorola monitoring
Should have	8	Toevoeging van Managed Wi-Fi voor Lancom
	9	Adviesrapport voor koppeling tussen monitoring en het AFAS ticketsysteem
	10	Implementatieplan voor Managed Wi-Fi met Motorola
	11	Implementatieplan voor Managed Wi-Fi met Lancom
	12	Procedures voor beheer van Managed Wi-Fi
	13	Procedures voor beheer van de monitoring
Could have	14	Locatiebepaling van clients toevoegen aan Motorola Monitoring
	15	Proof of concept met koppeling tussen monitoring en het AFAS ticketsysteem
	16	Definiëren, uitwerken en documenteren van vervolgprojecten.
	17	Kosten baten analyse voor Managed & Wi-Fi
	19	Kosten baten analyse voor Motorola Monitoring
	20	Medewerkers trainen
Won't have	21	Inrichten van klantomgevingen met Managed Wi-Fi
	22	Managed Wi-Fi voor andere merken als Lancom en Motorola
	23	Monitoring voor andere merken als Motorola
	24	Onderzoek doen naar een nieuw monitoringssysteem

3.6 Methoden en technieken

Het project werd verdeeld in een aantal fasen. De fasen bestonden uit een analyse, architectuur, ontwerp, implementatie en beheerfase. In de analysefase vond het onderzoek plaats. Aan de hand van dit onderzoek kon de architectuur fase van start gaan. Hierna volgde de ontwerpfase waarin een technisch ontwerp is opgesteld. Na deze fase leverde de implementatiefase een proof of concept en een Implementatieplanop. Afsluitend was er de beheerfase die de procedures omschreef voor het verdere beheer.

Per fase zullen werden de onderstaande documenten gemaakt:

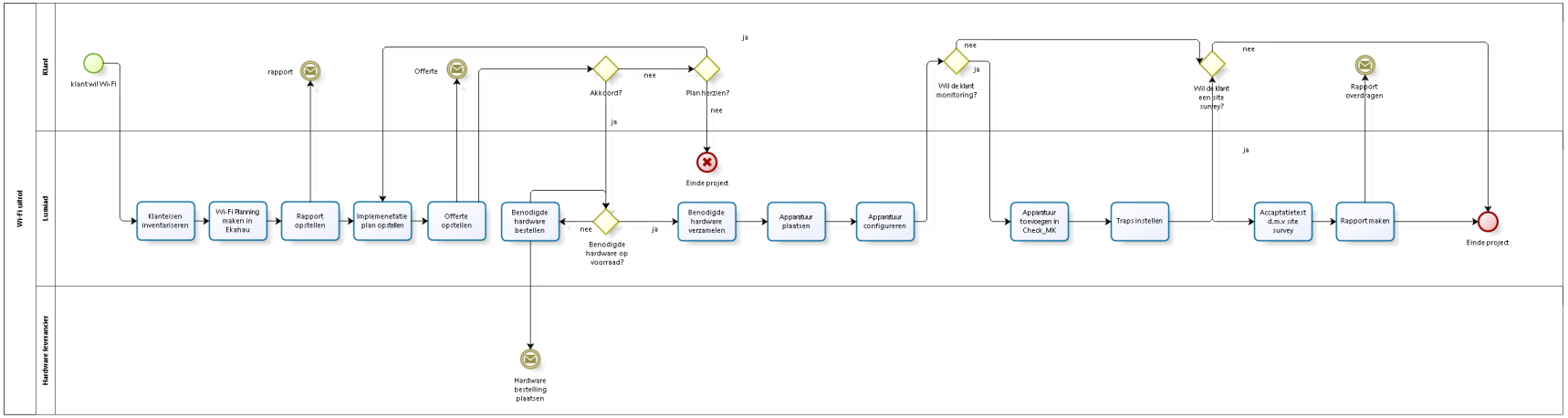
Analyse	Architectuur	Ontwerp	Implementatie	Beheer
Plan van aanpak	Functioneel ontwerp	Technisch ontwerp	Proof of concept Managed Wi-Fi en de monitoring	Procedures voor Managed Wi-Fi en de monitoring
Onderzoeksrapport	Adviesrapport		Implementatie plan (Should have)	

4 Huidige situatie

Dit hoofdstuk beschrijft de huidige werkwijzen voor een implementatie, het beheer van een draadloos netwerk en de monitoring. Ook worden de systemen waarmee het afstudeerproject een raakvlak heeft beschreven.

4.1 Een implementatie van een draadloos netwerk

Een implementatie van een draadloos netwerk bestaat uit diverse stappen. Als een klant mogelijk interesse heeft worden de stappen genomen uit figuur 2.



Figuur 2 - Implementatie van een draadloos netwerk

In veel gevallen wordt er een ‘site survey’ op de klantomgeving gedaan om het huidige netwerk te meten, of om een nieuw draadloos netwerk te plannen. Een site survey wordt gedaan met een softwarepakket en een draadloze netwerk adapter. In het softwarepakket wordt een blauwdruk van de plattegrond ingeladen van de klantomgeving. Tevens wordt hierop aangegeven waar de access points zich bevinden. Vervolgens kan de meting uitgevoerd worden. Een site survey wordt fysiek op locatie van de klant gedaan door een personeelslid van Lumiad. De output van de site survey is een plattegrond die de dekking van het draadloze netwerk weergeeft.

4.2 Het beheer van draadloze netwerken

Momenteel levert Lumiad al beheer op het draadloze netwerk van de klant. De invulling van het beheer verschilt per klant en per contract. Sommige klanten betalen voor een support contract. Hiervoor kan de klant voor een vast bedrag per maand terecht bij Lumiad voor vragen, adviezen of hulp. Andere klanten hebben geen support contract, maar een strippenkaart. Op een strippenkaart staan uren die worden afgeschreven. Als deze uren verbruikt zijn kan de klant een nieuwe strippenkaart tegen een betaling aanschaffen. Als een klant geen contract of strippenkaart heeft, maar toch hulp nodig heeft wordt er een factuur in rekening gebracht.

In de meeste gevallen verloopt het beheer van de access points van het draadloze netwerk van de klant via de controller. De klant heeft dan meestal thin access points [4] . In andere gevallen heeft de klant alleen fat access points [5] en geen controller.

Als Lumiad een netwerk levert met een controller staat deze nu op locatie van de klant. Als er een configuratiewijziging plaatsvindt moet dit via een VPN verbinding, fysiek op locatie bij de klant, of door de klant zelf gedaan worden.

4.3 De monitoring

Lumiad levert monitoring bij de draadloze netwerken die zij zelf geïmplementeerd hebben indien de klant dat wenst. In andere gevallen wordt monitoring geleverd op draadloze netwerken die de klant zelf, of een derde partij heeft geïmplementeerd. Dit wordt gedaan voor diverse merken, bijvoorbeeld voor Lancom en Juniper. De monitoring wordt gedaan m.b.v het systeem Check_MK (hoofdstuk 4.3.1)

4.3.1 Check_MK

Check_MK is een collectie van uitbreidingen op de IT-monitoring-Kernel van Nagios. Na een onderzoek is er voor dit systeem gekozen omdat Check_MK SNMP pakketten kan bundelen tot een enkel pakket, waardoor er minder bandbreedte wordt verbruikt dan bij vele andere monitoringspakketten. Ook is Check_MK open-source[6], dit maakt het pakket flexibel. Als er een functie aan Check_MK moet worden toegevoegd, of als een klant maatwerk nodig heeft wordt hier een project van gemaakt en uitbesteed aan een ontwikkelteam in Oekraïne.

4.3.2 NagVis

NagVis is een gratis uitbreiding op Nagios. In deze tool kan een netwerktekening worden gemaakt van de hardware in een netwerk. Dit dient wel handmatig te worden gedaan. Aan de verschillende componenten in de tekening kan een IP adres worden toegewezen, waarna kan worden gemonitord. Hierdoor wordt een netwerk tekening en monitoring in één overzicht gecreëerd.

4.3.3 PNP4Nagios

PNP4Nagios is een uitbreiding op Nagios die performance data verzameld, analyseert en opslaat in een database. PNP4Nagios zorgt ervoor dat er snel en eenvoudig grafieken kunnen worden gecreëerd van de geanalyseerde data.

---

[4] Thin access point - Een thin access point kan zonder controller niet geconfigureerd worden, en stopt met het uitzenden van het draadloze netwerk als de verbinding met de controller verbreekt. Als een thin access point een verbinding heeft met een controller, beschikt het access point over dezelfde functionaliteiten als een fat access point.

[5] Fat access point - Een fat access point kan geconfigureerd worden, en blijft het draadloos netwerk uitzenden, zonder dat er een controller benodigd is.

[6] Open source - Open source betekend dat de broncode openbaar is. Dit geeft de eindgebruiker vrije toegang geeft tot de bronmaterialen van het eindproduct, de bron kan hierdoor aangepast worden.

5 Onderzoek en resultaten

Dit hoofdstuk beschrijft het onderzoek. Eerst zullen de onderzoeksvragen uit het PVA herhaald worden. Daarna zal de onderzoeksmethodiek worden beschreven. Hierin wordt toegelicht hoe het onderzoek werd gerealiseerd en welke middelen er zijn gebruikt. Vervolgens wordt het onderzoek met de resultaten beschreven.

5.1 Onderzoeksvragen

De hoofdvraag luidt: 'Op welke manier kunnen Managed Wi-Fi en de monitoring van Motorola apparatuur door Lumiad worden ingezet?'

De bijhorende deelvragen luidden:

- Hoe word de remote verbinding tussen de access points en controller opgezet?
- Hoe worden verschillende klanten op een enkele controller beheert?
- Hoe kan Managed Wi-Fi bijdragen aan het sneller uitrollen van een Wi-Fi netwerk voor de klant?
- Hoe kan Managed Wi-Fi bijdragen aan het goedkoper aanbieden van het beheer van een Wi-Fi netwerk?
- Hoe kan Managed Wi-Fi zorgen voor gecentraliseerd beheer van een Wi-Fi netwerk?
- Hoe kan Managed Wi-Fi schaalbaar worden ingezet door Lumiad?
- Hoe kan de monitoring van Motorola apparatuur worden ingericht?
- Hoe kan de monitoring efficiënter ingericht worden?

5.2 Onderzoekmethodiek

Het onderzoek voor het realiseren van de doelstellingen door het inzetten van Managed Wi-Fi en monitoring heeft de volgende doelstellingen:

- Het beheer en de implementatie van een draadloos netwerk goedkoper aan kunnen bieden.
- Centraliseren van het beheer door het inzetten van Managed Wi-Fi.
- De tijd die het kost om een draadloos netwerk te implementeren terug te dringen.
- Kwaliteit leveren op het draadloze netwerk d.m.v. monitoring.

Dit onderzoek is vormgegeven door literatuuronderzoek, interviews, experimenten en praktijkervaring.

Half gestructureerde en ongestructureerde interviews vonden plaats om de wensen en eisen van belanghebbende te achterhalen. Ook hebben er experimenten plaatsvinden in een testomgeving met de middelen die Lumiad hiervoor beschikbaar heeft gesteld. Tot slot heb ik een cursus gevolgd en diverse project uitgevoerd om praktijkervaring op te doen voor de implementatie en het beheer van een draadloos netwerk.

Voor het creëren van een overzichtelijk onderzoek is het onderzoek opgedeeld in:

- Een vooronderzoek waarin onderzocht wordt met welke merken Managed Wi-Fi kan worden gerealiseerd. Hiervoor zijn aan de verschillende merken een aantal kwaliteitscriteria gekoppeld. Er is gebruik gemaakt van literatuur en interviews om een conclusie te trekken.

- Een marktonderzoek waarin de wensen van de klant worden geïnventariseerd. De output van dit onderzoek is een business case. De business case is doorslaggevend voor het inzetten van Managed Wi-Fi. Tevens geeft dit onderzoek antwoord op de vraag hoeveel klanten er geïnteresseerde zijn in Managed Wi-Fi, uit hoeveel access points een gemiddelde klantnetwerk bestaat en wat de wensen van de klant zijn. Voor dit onderzoekdeel is gebruik gemaakt van interviews.

- Een onderzoek naar Managed Wi-Fi waarin onderzocht is hoe Managed Wi-Fi schaalbaar kan worden ingezet door Lumiad. Hiervoor is gebruik gemaakt van brainstormen, literatuur en experimenten in een testomgeving.

- Een onderzoek naar het inzetten van de monitoring met als output projectplannen voor een uitbesteding aan een extern ontwikkelteam. Voor dit onderzoekdeel is gebruik gemaakt van literatuur en experimenten. Meer over de uitbesteding is te lezen in hoofdstuk 5.2.1.

5.2.1 De uitbesteding

In verband met de duur van het project was de uitbesteding van de monitoring aan het ontwikkelteam in Oekraïne opgesplitst in meerdere delen. Hierdoor kon de ontwikkeling al de tweede projectweek van start gaan. De ontwikkeling van de monitoring bestond uit de delen:

1. Access point & WLC checks
2. Client historie & Gebruikersgemak

Hiervoor werden diverse projectplannen gemaakt. Deze projectplannen beschreven de functionaliteiten die geprogrammeerd moesten worden in Check_MK. Alle projectplannen zijn toegevoegd in bijlage F (projectplannen voor Oekraïne) . Alvorens de projectplannen gemaakt konden worden is er onderzoek verricht. Dit is uitgewerkt in hoofdstuk 5.4 (Monitoring).

Met het ontwikkelteam zijn van te voren duidelijk afspraken gemaakt, voor een goede aansturing. Er is afgesproken dat het ontwikkelteam een planning oplevert voordat zij beginnen met het realiseren van een projectplan. Ook is er afgesproken dat het ontwikkelteam documentatie oplevert d.m.v. quoten in de code. Hierdoor kan een andere programmeur in de toekomst eventueel het werk voorzetten. Tevens werd er na elk projectplan een Skype sessie ingepland. Het nut hiervan was het ophelderen van onduidelijkheden aan beide kanten. De Engelse vaardigheid van de ontwikkelaars in Oekraïne is erg beperkt. Een gevolg hiervan is dat er uitgebreide projectplannen nodig zijn met veel toelichting en ondersteuning.

Na de oplevering van een deel van de monitoring, of het afronden van een projectplan werd er een demo ingepland. De demo werd gegeven door het ontwikkelteam over Skype. Na de demo werden de nieuwe functionaliteiten getest. De tests werden door de student uitgevoerd conform de functionaliteiten uit het bijbehorende projectplan. Hieruit ontstonden uitbreidingen op de projectplannen, waarin wijzigingen of nieuwe functionaliteiten werden beschreven. De afstudeerbegeleider (Tobias Bakker) controleerde de projectplannen, voordat deze naar het ontwikkelteam werden verstuurd.

5.3 Managed Wi-Fi

Dit hoofdstuk beschrijft het onderzoek en de resultaten. Het hoofdstuk bevat uit een vooronderzoek om te beslissen welk merk als eerst onderzocht werd voor Managed Wi-Fi. Vervolgens vond er een marktonderzoek plaats om op te helderen wat de klant wenste en welke klanten geïnteresseerd zijn in Managed Wi-Fi. Na het marktonderzoek is onderzoek verricht naar Managed Wi-Fi en de monitoring van Motorola apparatuur. Tot slot vond er een praktijktest plaats.

5.3.1 Vooronderzoek

Er is onderzocht met welke merken Lumiad Managed Wi-Fi kan realiseren. De kwaliteitscriteria waren:

1. Het merk moet al in het assortiment van Lumiad zitten
2. Technisch mogelijkheden voor Managed Wi-Fi en de monitoring van de apparatuur
3. Prijstechnisch voordelig
4. De voorkeur van de klant

Er zijn een aantal merken vergeleken. Deze merken zijn gekozen omdat het een bekend merk is of omdat Lumiad veel met deze merken te werk gaat. De belangrijkste voor- en nadelen tussen de verschillende merken zijn vastgelegd in een tabel.

De voordelen:

Motorola	Lancom	Cisco
Goedkope hardware	Uitgebreide mogelijkheden	Naamsbekendheid
Naamsbekendheid	Betrouwbaar merk	Uitgebreide mogelijkheden
Uitgebreide mogelijkheden	Heeft de voorkeur van beheerders van Lumiad	Betrouwbaar merk
Betrouwbaar merk	Goede supportmogelijkheden	Al lang op de markt
Al lang op de markt		Voorkeur van de klant
Voorkeur van de klant		
Heeft de voorkeur van beheerders van Lumiad		

De Nadelen:

Motorola	Lancom	Cisco
Hanteert licentiekosten	Onbekend in Nederland	Duurdere hardware
	Nieuw in de markt	niet in het assortiment van Lumiad

Motorola komt het beste overeen met de kwaliteitscriteria. Daarom is er besloten het eerste onderzoek te richten op Motorola. Motorola biedt momenteel flinke kortingen op apparatuur. Daarnaast ligt Motorola goed in de markt. Klanten kiezen liever voor zekerheid en durven het vaak nog niet aan om voor een onbekender merk te kiezen.

5.3.2 Marktonderzoek

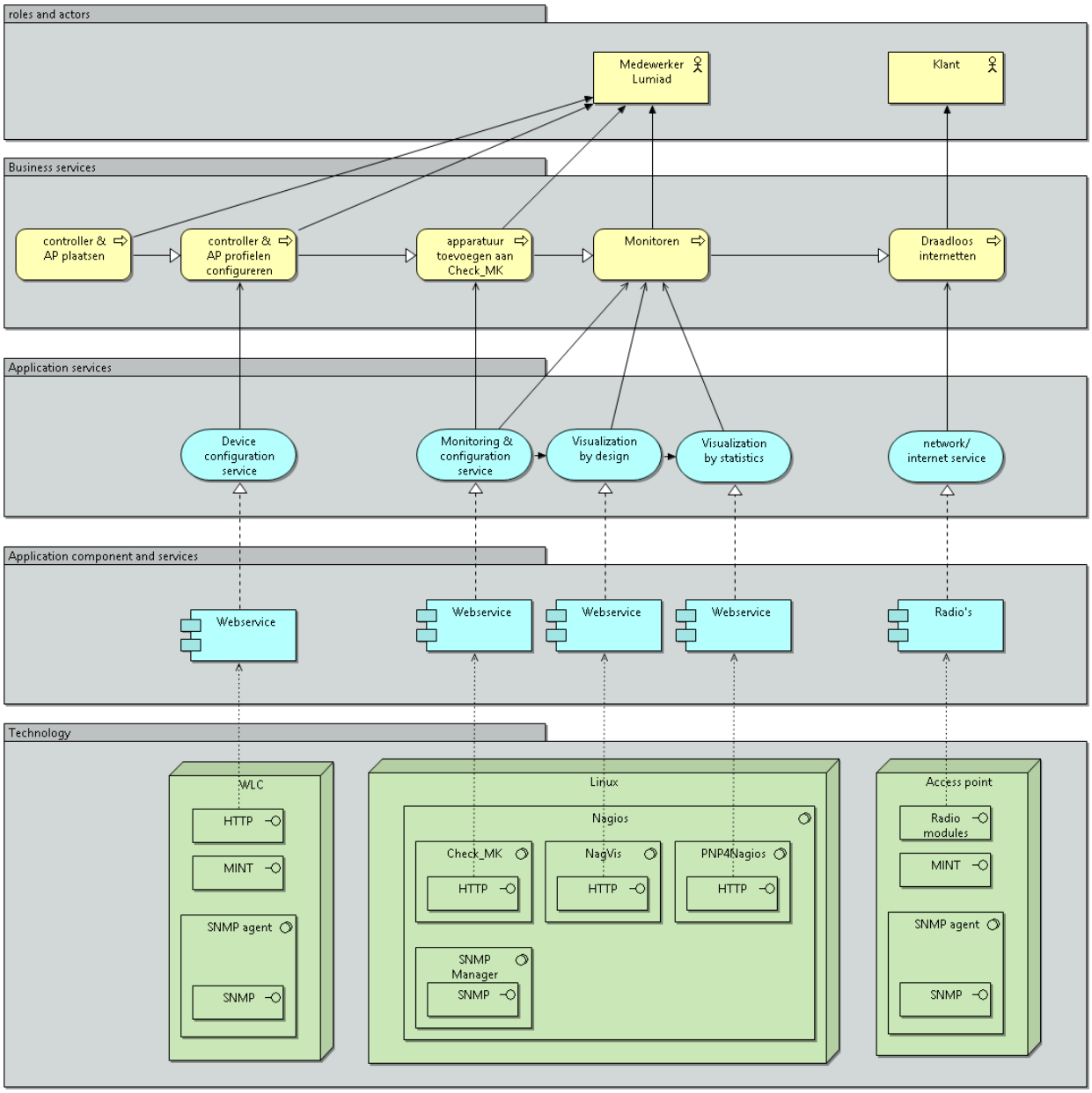
Er is een markonderzoek uitgevoerd om te achterhalen hoeveel klanten geïnteresseerde zijn in Managed Wi-Fi, en wat voor soort klant dit betreft. Deze informatie is relevant om twee redenen. Ten eerste draagt het bij aan de vraag waar de controller(s) worden geïmplementeerd, omdat het aantal klanten een impact heeft op de bandbreedte en de kosten. De controller komt in een extern datecenter, of intern in het netwerk van Lumiad. Ten tweede kon er een schatting worden gemaakt van de grote, en de middelen die het klantnetwerk bevat.

Na overleg is besloten dat het marktonderzoek werd uitgevoerd door Wim Bos omdat hij de contactpersoon is voor de klantcontacten. Hiervoor heeft hij gesproken met klanten en een schets gemaakt van de klantomgeving. Naar verwachting zijn er 50 klanten die gebruik willen maken van Managed Wi-Fi. Een draadloze netwerkomgeving van een klant bestaat gemiddeld uit vijftien access points.

De verwachting is dat vooral klanten met een kleiner netwerk gebruik zullen maken van Managed Wi-Fi, omdat het aanschaffen van een controller niet opweegt tegenover het aanschaffen van enkele thin access points. Bovendien hebben veel bedrijven met enkele medewerkers vaak niet de expertise in huis om zelf een draadloze omgeving te beheren.

5.3.3 De architectuur

In figuur 3 is de architectuur weergegeven die de relaties tussen de apparatuur, de functionaliteiten en de eindgebruiker toelicht.



Figuur 3 - Architectuur

Op de technologie laag is de hardware weergegeven met de belangrijkste modules, die nodig zijn om de functionaliteiten van de apparaten aan de gebruiker aan te bieden.

De applicatie, component en service laag geeft de belangrijkste services weer waarover de apparatuur ten behoeve van de gebruiker beschikt. Deze componenten zijn nodig om functionaliteiten mogelijk te maken.

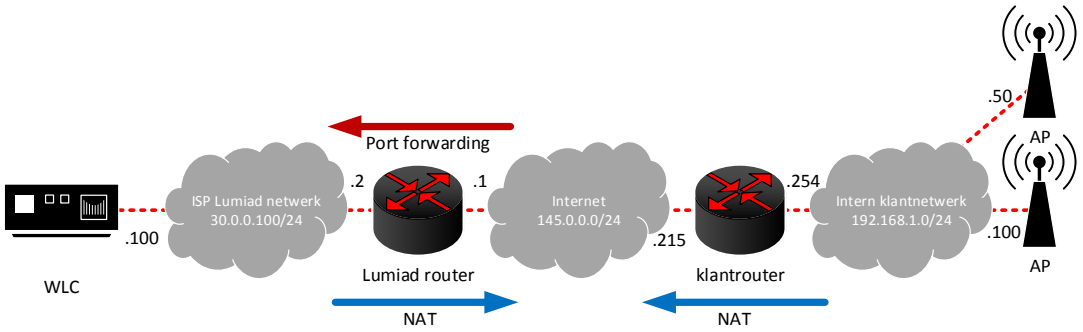
De applicatie service laag geeft de functionaliteiten weer van de verschillende applicatie componenten.

De business service laag geeft de menselijke handelingen weer die nodig zijn om gebruik te maken van de functies. Tevens geeft dit een tijdlijn weer van de technische handelingen die plaatsvinden bij een implementatie en monitoring van een draadloos netwerk.

De bovenste laag geeft de relatie weer tussen de services en de eindgebruikers.

5.3.4 De techniek Managed Wi-Fi

Om de techniek achter Managed Wi-Fi te onderzoeken is Managed Wi-Fi over een gesimuleerde internet verbinding opgebouwd (figuur 4). Door gebruik te maken van NAT kon de klantomgeving het interne netwerk van Lumiad niet bereiken, zoals in de praktijk het geval is. Tevens is er een port forwarding ingesteld op de Lumiad router om het publiekelijke adres met UDP poort 24576 te vertalen naar het interne adres van de controller. De sessie tussen een controller en access point wordt altijd geïnitieerd vanaf het access point. Om deze reden is het voldoende om alleen een port forwarding [7]aan de Lumiad zijde in te stellen.



Figuur 4 - Managed Wi-Fi testomgeving

Op het access point werd het publieke adres van de controller opgegeven in het daarvoor bestemde 'adoptie' veld. Tevens werd MINT geconfigureerd op de access points om op laag drie van het OSI model te kunnen communiceren en werd er een nul-route ingesteld naar de klantrouter. De access points konden nu een tunnel naar de controller opbouwen. Om te onderzoeken hoe de sessie werd opgebouwd is er gemonitord met Wireshark.

Deze sessie wordt opgezet d.m.v. het Medium Independent Network Transport[8] (MINT) protocol. Dit is een protocol die lijkt op het protocol CAPWAP, die Cisco access points en controllers gebruiken. MINT is een Motorola specifiek protocol die word gebruikt door controllers en access points om apparaten op het netwerk te ontdekken en hiermee te communiceren. Dit protocol wordt gebruikt voor zowel het configureren, updaten en bewaken van de access points. MINT kan over zowel laag twee als laag drie van het OSI model [9]communiceren. MINT kent hiervoor twee levels:

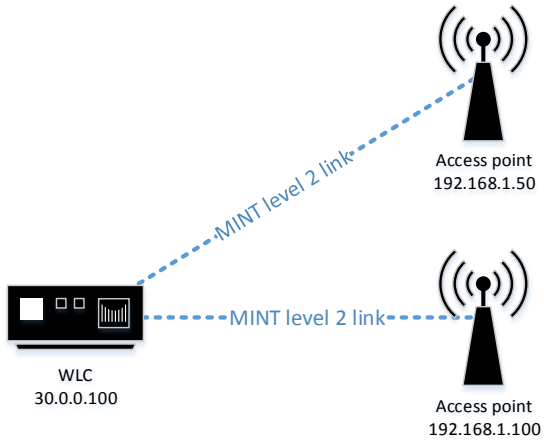
- MINT level 1 communiceert over de data link laag
- MINT level 2 communiceert over de netwerk laag

[7] Port forwarding - Port forwarding is het doorsturen van TCP-of UDP-pakketten door een NAT-gateway door middel van poortnummers.
[8] Medium Independent Network Transport (MINT) - Medium Independent Network Transport (MINT) is een protocol die door Motorola controllers en access points word gebruikt om een link voor datacommunicatie op te bouwen.
[9] OSI-model - Het OSI-model is een gestandaardiseerd referentiemodel voor datacommunicatiestandaarden.

Het was vast te stellen dat er een MINT link opgezet was tussen de controller en de access points door de gateway van het klantnetwerk te monitoren (192.168.1.254 in figuur 4). De access points waren aangesloten op een switch. MINT is te herkennen aan UDP pakketten met source en destination port (24576). Te zien was dat beide access points een eigen level twee MINT link opbouwde met de controller(figuur 4 en 5). Tevens was op de controller te zien dat beide access points geadopteerd waren (figuur 7) Toen de MINT link was opgezet kregen de access points de configuratie.

```
 98 16.896685  192.168.1.100      30.0.0.100          UDP      106 Source port: 24576  Destination port: 24576
429 80.882800  192.168.1.50       30.0.0.100          UDP      128 Source port: 24576  Destination port: 24576
```

Figuur 5 - MINT over het WAN

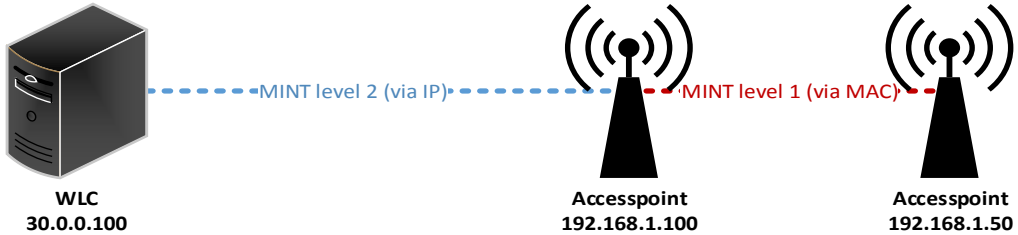


Figuur 6 - MINT level 2 link

	Adopted Device	Type	RF Domain Name	Model Number	Config Status	Config Errors	Adoptor Hostname	Adoption Time	Startup Time
	AP1	AP6522	default	AP-6522-66030-	version-mismatcl		WLC	Wed Nov 20 2013	Wed Nov 20 2013 0
	AP2	AP6522	default	AP-6522-66030-	version-mismatcl		WLC	Wed Nov 20 2013	Wed Nov 20 2013 0

Figuur 7 - adoptie op de controller

Nadat de acces points van een configuratie zijn voorzien, creëren de access points onderling over het LAN een level één MINT link. Deze link werkt op laag twee van het OSI model. Zodra de access points onderling een MINT link op laag 2 hebben opgezet communiceert er maar één access point met de controller. Deze wordt de RF domain manager genoemd. Dit was terug te zien op de router doordat er enkel MINT pakketten vanaf de access point met IP adres 192.168.1.100 kwamen. Dit bewees dat de situatie nu als volgt werkte(figuur 8).



Figuur 8 - MINT levels

Voor het testen van de techniek zijn er twee fat access points gebruikt van hetzelfde model (twee keer Motorola AP6522). De techniek is tevens getest met twee thin access points(Motorola AP622). Ook deze bleken zowel een level twee MINT link over het WAN te kunnen opzetten als een onderlinge level één MINT link. Via MINT level één wordt een RF domain manager geselecteerd. Nadat de RF domain manager is vastgesteld zullen de overige access points hun level twee MINT link opheffen en communiceren over de enkele tunnel van de RF domain manager. Hetzelfde scenario is ook getest met twee verschillende modellen fat access points (Motorola AP6522 en AP6532). deze bleken beide een aparte MINT level twee link op te bouwen, en geen onderlinge MINT level één link. Twee verschillende typen access point kunnen dus niet als RF domain manager dienen voor elkaar. Dit is geen probleem, alleen word er meer bandbreedte verbruikt omdat er twee RF-domain managers zullen ontstaan, waardoor de controller een configuratie of update twee keer moet verzenden.

Om de verbinding te beveiligen via het Internet Protocol Security (IPsec) protocol[10], kon IPsec Secure op de access points en controller worden geconfigureerd. De UDP pakketten waren nu beveiligd op laag drie van het OSI-model[11] (figuur 9).

```
AP1>show mint link
1 mint links on 1A.26.07.78:
link ip-30.0.0.100:24576 at level 2, 0 adjacencies, (used), (secured by ipsec)
AP1>
```

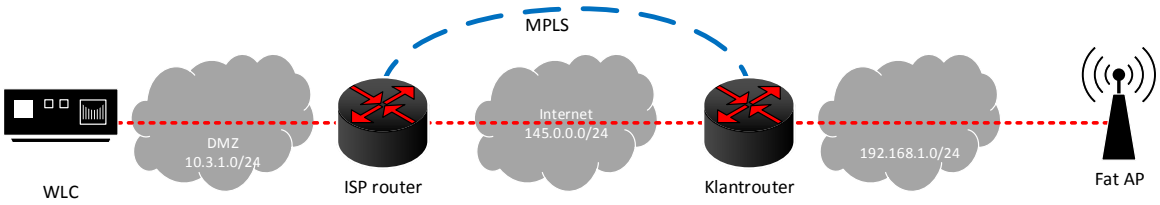
Figuur 9 - het Internet Protocol Security (IPsec)

5.3.5 Managed Wi-Fi scenario's

Managed Wi-Fi kan over het WAN communiceren in verschillende scenario's. De volgende scenario's zijn hierbij onderzocht.

- MPLS scenario
- WLC achter NAT

5.3.5.1 MPLS scenario



Figuur 10 - MPLS

In dit scenario (figuur 10) worden de verschillende klanten aan Lumiad gekoppeld via hardware die Multi Protocol Label Switching (MPLS) ondersteund. Deze oplossing creëert een private WAN.

[10] Internet Protocol Security (IPsec) - Internet Protocol Security (IPsec) is een standaard voor het beveiligen van het internetprotocol (IP) door middel van encrypties op de IP-pakketten.
[11] OSI-model - Het OSI-model is een door ISO gestandaardiseerd referentiemodel voor datacommunicatiestandaarden.

MPLS zorgt ervoor dat het access point en de controller met elkaar kunnen praten als over een LAN. Bij MPLS wordt gebruik gemaakt van een gehuurde lijn, waarin via labels aan de pakketten geswitcht wordt. Om gebruik te maken van MPLS moeten zowel Lumiad als de klant een contract afsluiten met een serviceprovider. Ook wordt er betaald voor de implementatie, bandbreedte en managementkosten. Wanneer er MPLS wordt gebruikt is er op klantlocatie wel hardware nodig die MPLS ondersteund.

Voordelen:

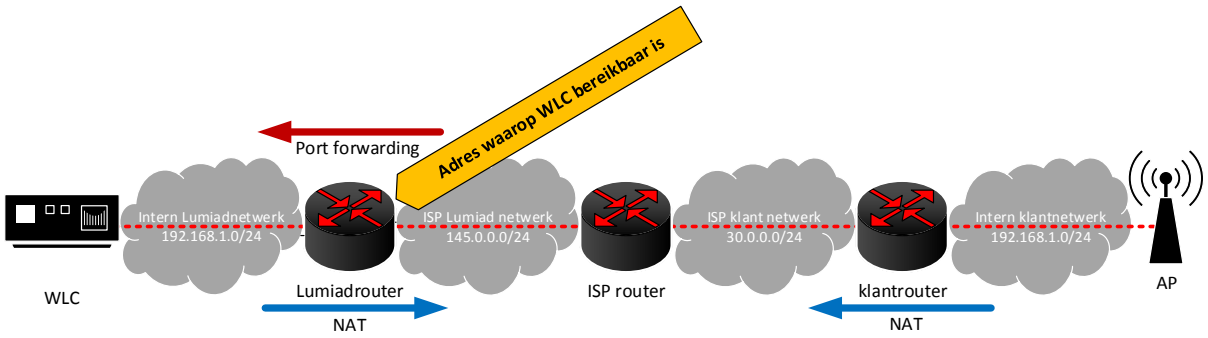
- QoS, CoS of de pakketfiltering kunnen in de cloud kunnen plaatsvinden waardoor de performance van het netwerk toeneemt.

Nadelen:

- Extra kosten voor de MPLS dienst. Dit betreft kosten voor de implementatie, bandbreedte en managementkosten.
- Er MPLS ondersteunende hardware benodigd.
- Afhankelijkheid van de serviceprovider.

5.3.5.2 De WLC achter een NAT

De controller kan d.m.v. een Network Address Translation (NAT) met het internet communiceren(figuur 11). Hiervoor moest er een poort forwarden worden ingesteld vanaf het publieke internet adres met UDP poort 24576 naar het interne adres van de controller. Dit zorgt ervoor verkeer vanaf het publieke internet adres met de betreffende poort werd vertaald naar het IP adres de controller.



Figuur 11 - controller achter NAT

Als de access points nu willen communiceren met de controller bij Lumiad moet hierin het publieke IP adres van de Lumiad router worden opgegeven in plaats van het interne adres van de controller. Zodra het verzoek voor de MINT link op de WAN interface van de Lumiadrouter aankomt wordt deze via de port forwarding omgezet naar het interne adres van de controller.

Omdat een port forwarding maar naar één IP adres kan vertalen per poort moet er wel een tweede publiekelijk IP adres beschikbaar zijn om een eventuele tweede controller in te zetten binnen Lumiad. Voor het access point betekent dit dat er een tweede regel, met het publieke IP adres van de tweede controller moet worden ingesteld in het adoptieveld.

Voordelen:

- Flexibele oplossing (access points kunnen de controller overal vanuit het internet bereiken)
- Goedkope oplossing

Nadelen:

- De apparatuur van Lumiad is over het publieke internet bereikbaar
- Er is een firewall nodig om onbevoegde access point te weren
- Meerdere publieke IP adressen nodig bij meerdere controllers

5.3.6 Managed Wi-Fi bij Lumiad

Er vond een onderzoek plaats om te onderzoeken hoe Managed Wi-Fi schaalbaar binnen Lumiad kan worden ingezet. Concreet is het onderstaande hier onderzocht:

- Hoe de omgeving redundant kan opgezet kan worden, en in hoeverre dit van belang is.
- Wat de eisen zijn voor Managed Wi-Fi, en of Lumiad aan deze eisen voldoet.
- Wat de mogelijkheden zijn tot clustering[12].

Als Managed Wi-Fi wordt geïmplementeerd bij Lumiad met een enkele controller en een enkele internetverbinding krijgt Lumiad te maken met de volgende single point of failure 's:

- De controller bij Lumiad.
- De netwerkapparatuur van Lumiad.
- De Internet Service Provider (ISP) van Lumiad.

Het grootste gedeelte van de single points of failure kunnen worden voorkomen. Hiervoor zijn de volgende oplossingen beschikbaar:

- Gebruik maken van een tweede internetlijn / internetprovider.
- De controllers zouden redundant uitgevoerd kunnen worden.
- De controller(s) zouden extern gehost kunnen worden.

5.3.6.1 Het netwerk

Het netwerk van Lumiad kent twee routes naar het internet. De eerste is een glasverbinding, de tweede lijn is een ADSL verbinding. Managed Wi-Fi kan eventueel gebruik maken van beide verbindingen om een single point of failure van de media over het internet te vermijden. Hieraan zitten wel een aantal eisen:

- Er is op elke verbinding een extra publiekelijk IP adres nodig (indien er twee controllers worden ingezet)
- De verbinding moet snel genoeg zijn voor Managed Wi-Fi

Managed Wi-Fi verbruikt een constante verbinding van 4 Kbps per access point volgens Motorola. Bij het updaten van een access point loopt het dataverbruik op. Dit is ook het geval als er een RF-domain manager is voor de overige access points met de controller communiceert. Dit komt omdat de RF-domain manager statusinformatie, van de overige access points aan de controller over het internet door communiceert.

Vanwege firmware, en configuratie updates raadt Motorola een verbinding van minimaal 256 Kbps aan. Echter bleek dat Motorola tot nu toe maar maximaal twee keer per jaar een firmware update uitbracht. De laatste twee firmware versies waren ongeveer 125 MB. Indien het updaten s 'nachts plaatsvind, en per RF-domein zou Lumiad is slechts 256 Kbps + de constante verbinding per klant voldoende bandbreedte hebben.

[12] Cluster - Een cluster bestaat uit meerdere apparaten die met elkaar verbonden zijn voor een betere prestatie of hogere beschikbaarheid.

Met 50 klanten en 15 access points per klant betekent dit dat er in totaal een constante verbinding van 3 Mbps (50*15*4 Kbps = 3000 Kbps) nodig is. Voor 50 klanten zou dit in theorie betekenen dat Lumiad een 15,8 Mbps (50*256 Kbps + 3000 Kbps = 15800 Kbps) verbinding nodig heeft.

De glasverbinding van Lumiad kan 20 Mbps uploaden en downloaden waardoor er zelfs in het extreemste geval ruim voldoende bandbreedte zou zijn. Er kan dus gesteld worden dat de glasverbinding ruimschoots voldoende is voor de business case van Lumiad.

De ADSL verbinding van Lumiad heeft momenteel een zeer lage snelheid van ongeveer 1,65 Mbps. Er is een prijsaanvraag gedaan bij Unet om de ADSL verbinding van Lumiad te verhogen met minimaal 3 Mbps. De reactie was dat het geen nut had deze lijn te verhogen in verband met de maximaal mogelijke snelheid. Deze kon niet hoger door de afstand tussen de wijkcentrale en Lumiad. De huidige snelheid is al onvoldoende voor enkel de constante verbinding die de access points vereisen. Er kan dus gesteld worden dat de ADSL verbinding van Lumiad ongeschikt is. De ADSL verbinding als tweede lijn is dus geen optie. Een andere optie om de afhankelijkheid van het netwerk en de provider van Lumiad toch terug te dringen is door de controllers, of één van de controller bij een hostingprovider te laten hosten. Meer hierover is beschreven in hoofdstuk 5.3.8 (interne of externe hosting).

5.3.6.2 Clustering

Motorola apparatuur kan geclusterd worden. Een cluster bestaat uit meerdere apparaten die met elkaar verbonden zijn voor een betere prestatie of hogere beschikbaarheid. Aan een cluster van Motorola zitten wel een aantal beperkingen:

- Het cluster kan uit maximaal twee controllers bestaan.
- De controllers moeten hetzelfde model zijn (bijvoorbeeld twee keer de RFS-4000).
- De apparaten moeten beschikken over dezelfde firmware versie.

Het cluster bestaat uit een clustermaster en een clustermember. De clustermaster synchroniseert zijn configuratie naar de clustermember. Hiervoor wordt gebruik gemaakt van MINT op level 2. Er kan gekozen worden tussen een active-active of een active-standby cluster.

Bij een active-standby cluster voorziet de clustermaster alle access points alle access points van systeemupdates en configuraties. De clustermember wordt de stand-by controller. Deze neemt de taken van de clustermaster over zodra deze te kampen heeft met een probleem of storing. Dit kan bijvoorbeeld gebeuren door een stroomstoring, systeemcrash of een probleem met het netwerk. De access points moeten hiervoor wel beschikken over het adres van de stand-by controller in de configuratie. Bij een storing zullen de access points, nadat de controller een bepaalde tijd niet reageert het initiatief nemen om een MINT link op te bouwen naar de tweede controller. De clustermember kan de access points overnemen zonder dat de access points opnieuw hoeven te worden voorzien van een update of configuratie, door de synchronisatie van de clustermaster.

Bij een active-active cluster kunnen beide controllers de access points voorzien van systeemupdates en configuraties. Een loadbalancer zorgt ervoor dat de access points verdeeld worden over beide controllers. Om dit mogelijk te maken synchroniseren de controllers de configuratie via MINT level 2. De access points moeten hiervoor beschikken over de adressen van beide controllers. Als één van de twee controllers faalt zal de andere controller alle access points voorzien van updates en configuraties totdat de andere controller weer online is.

5.3.7 Externe of interne hosting

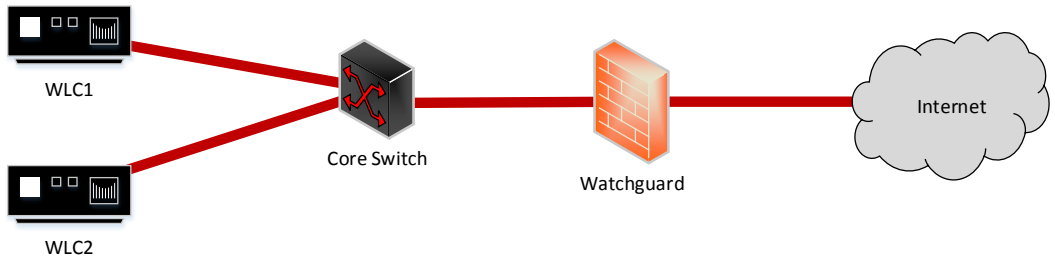
Een vraagstuk was of de controller intern bij Lumiad of extern in een data center zou worden gehost. In dit hoofdstuk wordt onderzocht hoe de controllers intern zouden kunnen worden gehost. Tevens wordt hier onderzocht hoe de controllers extern gehost zouden kunnen worden.

5.3.7.1 Interne hosting

Uit de business case van het vooronderzoek bleek dat er in eerste instantie uitgegaan wordt van 50 klanten met vijftien thin access points.

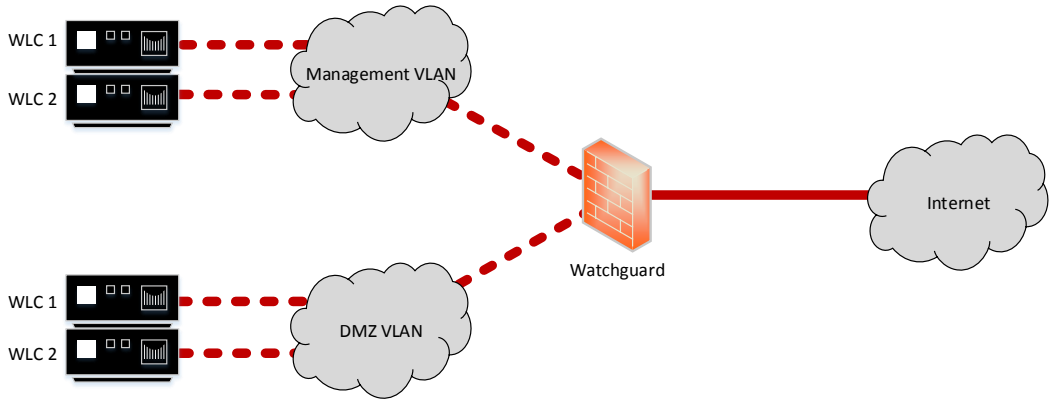
Lumiad heeft een glasverbinding met een upload en download van 20Mb met acht publiekelijke IP adressen, waarvan meer dan twee beschikbaar. Het grootste deel van de bandbreedte is onbenut waardoor er ruim voldoende snelheid overblijft voor Managed Wi-Fi. Ook zijn er voldoende publieke IP adressen beschikbaar voor een tweede controller. De ADSL verbinding bleek helaas niet geschikt vanwege onvoldoende snelheid en geen mogelijkheid tot verhogen hiervan.

Ook heeft Lumiad een eigen data center in het kantoorpand met voldoende rackspace. Het is mogelijk hier één of twee controllers fysiek in op te nemen. Lumiad zou de controllers kunnen aansluiten op de Watchguard. De Watchguard is de firewall voor het internet. (figuur 12).



Figuur 12 - Fysieke hosting van controllers bij Lumiad

Om het internet verkeer logisch te scheiden van het interne netwerk kan gebruik gemaakt worden van een demilitarized zone (DMZ). Tevens kan er een management VLAN worden gekoppeld aan de controllers om het beheren mogelijk te maken (figuur 13).



Figuur 13 Logische hosting van controllers bij Lumiad

Het resultaat is dat Lumiad de controllers wel intern kan hosten, maar momenteel over een enkele internetverbinding. Hierdoor blijft de single point of failure een risico. Echter is het netwerk wel geschikt doordat er voldoende bandbreedte, publieke IP adressen en ruimte in het data center beschikbaar is. Een ander voordeel is dat er geen extra kosten nodig zijn voor een externe hosting. Deze kosten zijn beschreven in hoofdstuk 5.3.7.2.

5.3.7.2 Externe hosting

De controller(s) zouden als infrastructure as a service (IaaS)[13] kunnen worden gehost in een extern datacenter, omdat het hier om fysieke hardware gaat.

De controllers zouden beide extern gehost kunnen worden. Om de prijs te achterhalen zijn er een aantal offertes opgevraagd. De goedkoopste hostingprovider bood een redundante uplink met 10Mbit, stroomvoorziening en rackspace aan voor ongeveer 200 euro per maand. Via een VPN verbinding zouden de medewerkers van Lumiad kunnen inloggen op de controllers voor het beheer. Als nu één van de twee verbindingen (de glasvezel en ADSL verbinding) van Lumiad offline gaat kan de tweede verbinding alsnog gebruikt worden om de klant te beheren. De beschikbaarheid wordt hiermee aanzienlijk verhoogd. Het enige risico is dat de controllers op een enkele locatie staan. Echter is het data center van Nedzone voorzien van brandbeveiliging en noodstroomvoorziening, waardoor dit geen risico beperkt is.

Een andere optie is het extern laten hosten van één van de twee controllers, waarbij één controller intern bij Lumiad gehost wordt en de tweede bij Nedzone. Dit is mogelijk voor ongeveer 80 euro, inclusief een 10 Mbit verbinding, redundante uplink, stroomvoorziening en rackspace. Hoewel één controller bij Lumiad gevestigd is en de andere controller bij Nedzone, vormt dit geen probleem voor het cluster. De controllers kunnen namelijk op IP basis (MINT level 2) communiceren over het internet. De klantomgevingen kunnen beheerd worden vanaf de controller bij Lumiad, deze synchroniseert zijn configuratie naar de tweede controller in de cloud. Als de omgeving bij Lumiad problemen ondervind kan de tweede internet lijn gebruikt worden om vanuit de controller in de cloud het beheer te raadplegen. Zodra de apparaten weer met elkaar kunnen communiceren zullen deze weer synchroniseren.

Er zijn dus drie opties mogelijk voor het hosten van de controllers, deze zijn hieronder beschreven.

1. Lumiad host de controllers intern over de glasverbinding en accepteert het feit dat de klantomgeving niet beheert kan worden zodra de verbinding tussen klant en Lumiad offline gaat.
2. De controllers worden extern gehost, voor ongeveer 200 euro per maand, met redundante uplink. Door de twee internetverbindingen die Lumiad beschikbaar zijn de controllers, en daarmee het beheer altijd beschikbaar.
3. één van de controllers wordt extern gehost, de andere intern, voor ongeveer 80 euro per maand. De klantomgevingen kunnen hierdoor vanuit het interne netwerk beheerd worden. De extern gehoste controller kan gebruikt worden in geval van storing, de controllers, en daarmee het beheer zijn hierdoor altijd beschikbaar.

5.3.8 Managed Wi-Fi bij de klant

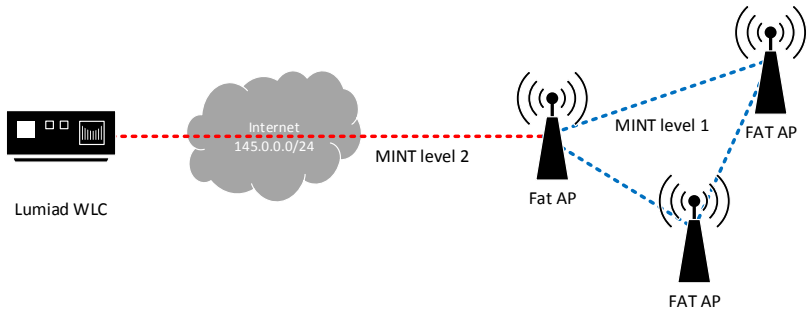
Er is onderzocht hoe de access point bij de klant kunnen worden geïmplementeerd.

5.3.8.1 Fat access points

Als er fat access points worden geïmplementeerd in de klantomgeving zullen deze een MINT level 2 link opbouwen naar de controller. Nadat deze is opgebouwd zullen ze intern een MINT level 1 opbouwen met de overige access points, en een RF-domainmanager selecteren. Deze communiceert namens de overige access points met de controller, de overige access points verbreken de MINT level 2 link met de controller bij Lumiad. Als de RF-domainmanager te maken krijgt met een storing wordt er een nieuwe RF-domain manager geselecteerd. Als de verbinding met de controller offline gaat blijven de access points standalone werken met de huidige configuratie. Het wijzigen van de configuratie dient dan per

[13]Infrastructure as a Service (IaaS) - Infrastructure as a Service (IaaS) betekent dat de infrastructuur wordt aangeboden aan de eindgebruiker via een hardware-integratie. De eindgebruiker heeft bij deze oplossing alle vrijheid over de hardware.

individuele access point gedaan te worden. Dit scenario is weergegeven in figuur 14.

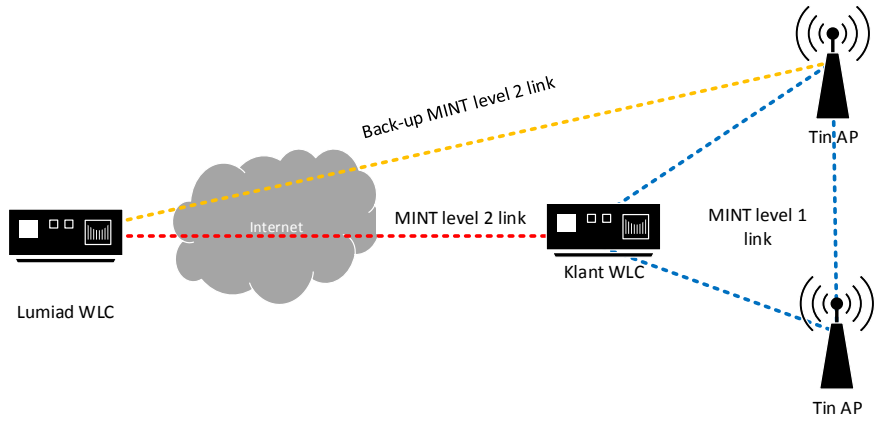


Figuur 14 - Fat AP scenario

5.3.8.2 Thin access points

Als er Thin access points worden geïmplementeerd bij de klant zullen deze net als bij fat access points een MINT level 2 link naar de controller, een onderlinge MINT level 1 link opbouwen en een RF-domainmanager selecteren. Ook wordt er een nieuwe domain manager geselecteerd als de huidige RF-domainmanager offline gaat. Het verschil is dat het draadloze klantnetwerk offline gaat zodra de access points de controller niet meer kunnen benaderen. Hierdoor kan de klant geen gebruik meer maken van het draadloze netwerk. De verbinding moet bij het inzetten van thin access points dus altijd stand houden. Dit scenario is afhankelijk van het netwerk en de apparatuur van Lumiad, de apparatuur en het netwerk van de klant en de ISP. Dit scenario is daarom niet altijd aan te raden.

Om toch thin access points te kunnen implementeren bij de klant kan er eventueel een controller op locatie van de klant worden gevestigd (figuur 15). Hiervoor zou de goedkoopste WLC van 600 euro aangeschaft kunnen worden. Ook kan Lumiad de controller in bruikleen aanbieden bij de klant.



Figuur 15 - WLC op klantlocatie

Door een controller op klantlocatie te implementeren blijft de omgeving standalone werken als de verbinding met Lumiad wegvalt. Ook kunnen de thin access points blijven functioneren als de controller op klant locatie offline gaat, doordat deze een MINT level 2 link kunnen opbouwen met de Lumiad controller(de oranje lijn). Hiervoor is een extra regel in de configuratie van de access points nodig waardoor zowel het adres van de interne controller als de controller bij Lumiad bekend is.

In dit scenario kan de controller tevens dienen als RF-domain manager voor verschillende modellen access points zonder dat er meerdere RF-domain managers worden gedefinieerd. Hierdoor blijft de omgeving makkelijker te beheren en is het bandbreedte efficiënt.

5.3.8.3 De prijzen

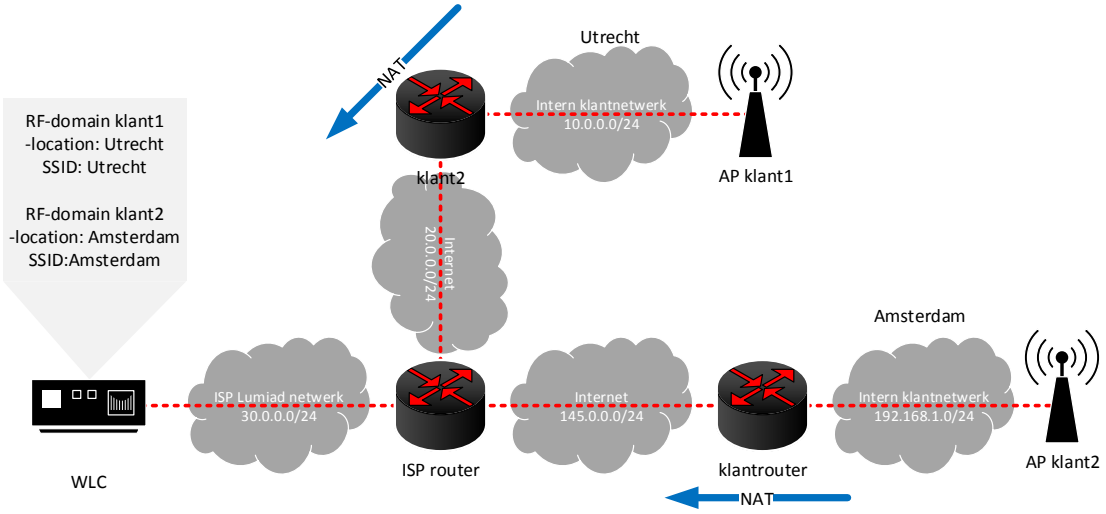
Er is onderzocht wat de prijzen ongeveer zijn voor de hardware voor het scenario met enkel thin access points, fat access points en het scenario met een controller en thin access points. Hierbij is uitgegaan van de goedkoopste hardware omdat dit voldoende is voor de meeste klanten met 15 access points. Er zijn gevallen waarbij duurdere hardware benodigd is. Bijvoorbeeld voor access points die outdoor worden geïmplementeerd, of in omgevingen met extreem veel gebruikers(bijvoorbeeld een theater).

Aantal access points	Thin access points	Thin access points + controller	Fat access points
1	€200	€800	€400
2	€400	€1000	€800
3	€600	€1200	€1200
4	€800	€1400	€1600
5	€1000	€1600	€2000
6	€1200	€1800	€2400
7	€1400	€2000	€2800
8	€1600	€2200	€3200
9	€1800	€2400	€3600
10	€2000	€2600	€4000
11	€2200	€2800	€4400
12	€2400	€3000	€4800
13	€2600	€3200	€5200
14	€2800	€3400	€5600
15	€3000	€3600	€6000

In de bovenstaande tabel is te zien dat een omgeving met enkel tin access points prijstechnisch het voordeligst is. Hoe meer access points er benodigd zijn hoe minder de controller kost in verhouding. Tegenover het scenario met een controller op de klantlocatie heeft het scenario met fat access points een prijstechnisch voordeel voor een klant die gebruikt maakt van twee access points of minder. In beide scenario’s komen er tevens kosten bij voor licenties en software. Deze zijn hierbij niet meegenomen. Echter zijn deze kosten in beide scenario’s hetzelfde.

5.3.9 Beheren van meerdere klanten

Om met Managed Wi-Fi meerdere locaties te beheren kunnen er per klant één of meerdere RF-domeinen geconfigureerd worden. Om dit te illustreren is dit in een testomgeving opgezet (figuur 16). Vervolgens zijn er RF-domeinen geconfigureerd en toegewezen aan een access point.

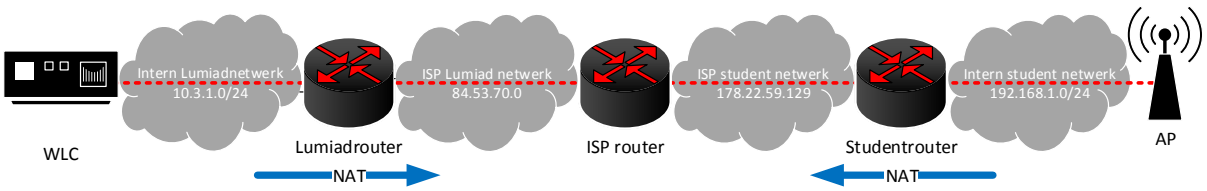


Figuur 16 - Managed Wi-Fi locaties

De access points worden toegewezen aan een bepaald RF-domein. Dit RF-domein overschrijft de configuratie van het access point. Met RF-domeinen kunnen de administrators per geografische locatie configuraties instellen. Zo kunnen er contact -en locatiegegevens, of draadloze netwerken worden geconfigureerd. Een RF-domain kan automatisch worden toegewezen aan een omgeving via een auto-provisioning policy. Op de controller kan hiervoor een filter, bijvoorbeeld per IP adres, VLAN, of apparaat naam worden ingesteld. Als de access points overeenkomen met de gegevens uit het filter worden ze verwezen naar een bepaald RF-domein.

5.3.10 De praktijk

Om te toetsen of Managed Wi-Fi uit de testopstelling in de praktijk toegepast kon worden is de controller geïmplementeerd in het testnetwerk van Lumiad (zie ook figuur 17). In de router die met het internet communiceert is vervolgens een port forwarding geconfigureerd naar het interne IP adres van de controller. Vervolgens is er een access point geconfigureerd en bij de student thuis in het netwerk gehangen.



Figuur 17

Het access point had bij Lumiad een basisconfiguratie gekregen. Dit betrof:

1. Het IP adres van de controller bij Lumiad
2. MINT level twee configureren
3. Routing naar de gateway van de router van de student

Door het access point een minuut in het testnetwerk te implementeren, en aan het default RF-domein het adoptieveld en MINT te configureren konden de eerste twee punten automatisch via de controller geconfigureerd worden. De gateway van de student router diende handmatig te worden geconfigureerd in het routing veld van het access point.

Vervolgens is het access point bij de student thuis in het netwerk geïmplementeerd. Hierdoor ging het access points het draadloze netwerk uitzenden die in de controller geconfigureerd was. Ook was het access point terug te zien in de statistieken op de controller bij Lumiad.

5.4 Monitoring

Er dit hoofdstuk is het onderzoek naar de monitoring beschreven. Het geeft antwoord op de vraag waarom monitoring van belang is, wat de voordelen en nadelen zijn van de verschillende monitoringssystemen, wat er van de Motorola apparatuur gemonitord zou kunnen worden en hoe de monitoring kan worden ingezet.

5.4.1 Het belang van monitoring

Lumiad zou een monitoringsysteem kunnen implementeren om de Motorola apparatuur te kunnen monitoren. Dit zorgt ervoor dat er sneller gereageerd kan worden op een incident, doordat een gebruiker het incident niet eerst hoeft te constateren en te melden. de monitoring kan namelijk zo ingericht worden dat het systeem de beheerder met informatie over het incident informeert per e-mail. Doordat de monitoring de beheerder eerder informeert, en voorziet van uitgebreide informatie kan het incident eerder worden verholpen, wat resulteert in een hogere beschikbaarheid. Tevens werkt monitoring pro-actief. Dit betekend dat een incident kan worden gedetecteerd, en verholpen voordat deze optreed. De monitoring kan namelijk ‘vreemd’ gedrag constateren, bijvoorbeeld een CPU die bijna 100% capaciteit verbruikt.

5.4.2 De verschillende systemen

De controller van Motorola beschikt over de optie om de access points in het klantnetwerk te monitoren. Ook kan de controller ‘traps’ versturen naar de controller. De controller kan weer een alert afgeven naar een e-mailadres. Bij een ‘trap’ stuurt een access point informatie over een belangrijke gebeurtenis naar de controller. Zo kan het access point de controller, met daarbij de systeembeheer inlichten (over bijvoorbeeld een defecte radio). Hieraan zitten een aantal voor- en nadelen:

- Een voordeel is dat dit systeem al kant en klaar is voor gebruik. De controller heeft een web interface waarin de monitoring geconfigureerd kan worden.
- Een nadeel is dat de monitoring enigszins beperkt is. Informatie over de ingelogde gebruikers is bijvoorbeeld nauwelijks te zien. Ook kunnen er geen grafieken worden gegenereerd. Statistieken en informatie over ingelogde gebruikers zijn juist van belang voor de monitoring. Deze uitgebreidere informatie kan de beheerder juist helpen een oplossing van een probleem eerder te verhelpen.

Een andere optie is het laten ontwikkelen van de monitoring in het huidige gebruikte monitoringspakket Check_MK. Hier zitten een aantal voordelen en nadelen aan:

- Een nadeel aan Check_MK is dat de monitoring geprogrammeerd moet worden. Dit is een prijzige en tijdsintensieve oplossing.
- Een ander nadeel is dat de monitoring op de controller kan niet worden uitgeschakeld. Als er dus gebruik wordt gemaakt van een tweede monitoringsysteem zullen de access points tweemaal worden gemonitord. Dit gaat ten koste van performance en bandbreedte
- Een voordeel is dat de monitoring hierbij helemaal op maat kan worden geprogrammeerd. Het eindproduct bevat hierdoor geen overbodige functionaliteiten.
- Een ander voordeel is dat de monitoring gecentraliseerd wordt met de monitoring van andere systemen. De monitoring van draadloze apparatuur van Lancom en Juniper zijn namelijk ook geprogrammeerd in Check_MK.
- Check_MK open source en gratis. Er hoeft dus eenmalig te worden geïnvesteerd in de ontwikkeling.
- Check_MK maakt efficiënt gebruik van de bandbreedte door losse SNMP pakketten te bundelen tot één pakket en deze naar het te monitoren systeem te versturen

Een derde optie is het aanschaffen van een nieuw monitoringsysteem. Deze optie heeft ook een aantal voor en nadelen:

- Een voordeel is dat er een monitoringsysteem kan worden aangeschaft die al kant en klaar is voor gebruik.
- Een nadeel is dat beheerders van Lumiad niet bekend zijn met dit nieuwe systeem. Dit levert mogelijk resistance op van de beheerders. Tevens moet het personeel leren werken met het systeem alvorens dit gebruikt kan worden.
- Bij het aanschaffen van een nieuw monitoringssysteem voor Motorola zou de monitoring gedaan worden met een ander systeem als de monitoring van draadloze Lancom of Juniper apparatuur. Voor de beheerders is het onhandig als er twee verschillende monitoringsystemen worden gebruikt. Hierdoor is Lumiad bijna genoodzaakt de monitoring van de andere merken ook in dit nieuwe systeem te implementeren. Dit vergt veel uitzoekwerk en is een tijdsintensieve oplossing.
- Monitoringspakketten vergen vaak aanschaf en licentie -kosten.

5.4.3 De uitbesteding

Nadat er uit de conclusie (hoofdstuk 6) was besloten om de monitoring is het systeem Check_MK te programmeren zijn er diverse projectplannen geschreven. Deze projectplannen zijn uitbesteed aan het ontwikkelteam in Oekraïne. De projectplannen zijn toegevoegd in (bijlage F). De uitbesteding is verdeeld drie delen, waardoor het ontwikkelteam snel kon beginnen met ontwikkelen en de uitbesteding overzichtelijk bleef. De uitbesteding is verdeeld in:

1. Het monitoren van de access points en controller
2. Client historie en features
3. Toepassen van de monitoring

5.4.3.1 Monitoren van access points en controller

Voor het eerste deel, het monitoren van de controller en access points is onderzocht welke data er van de controller en access points gemonitord moest worden. Om deze informatie te vergaren is er gebruik gemaakt van:

- De gemonitorde omgeving van Juniper
- De beschikbare Object Identifiers (OIDs) [14] van motorola.
- De eisen en wensen van collega's

De gemonitorde Check_MK omgeving van Juniper is gebruikt om inzicht te krijgen in de informatie die met apparatuur van andere merken word gemonitord. Uit deze informatie is een eerste opzet ontstaan. Bij Motorola bleek het tevens mogelijk via de controller informatie over de access points uit te lezen. Toch is er besloten zoveel mogelijk informatie van de access points uit te lezen i.p.v. uit de controller. Dit ten eerste omdat de CPU van de controller hierdoor minder belast wordt. Ten tweede omdat hier bandbreedte op bespaard word doordat het verkeer dan niet over het internet hoeft aangezien de Check_MK server momenteel bij de klant gevestigd is.

Nadat er besloten was wat er gemonitord moest worden zijn de juiste OIDs hierbij gezocht m.b.v. het programma MibBrowser. De MIB bestanden werden aangeleverd door Motorola. Een MIB bestand is een database met de verschillende OIDs. Tevens is er in de MIB bestanden gezocht naar andere interessante informatie. Deze zijn meegenomen in het eerste projectplan. Dit projectplan is doorgenomen met het netwerkteam (Tobias Bakker en Niek Crijns). In het eerste projectplan (zie bijlage projectplan v1) werd de onderstaande informatie verwerkt voor de uitbesteding.

Monitoring van de WLC:

- De naam van het apparaat, het type apparaat, de locatie, contactinformatie en de software versie van de WLC
- De tijd in dagen, uren en minuten die de WLC online is
- De CPU utilisatie in procenten van de afgelopen vijf minuten
- Het aantal inactieve access points van de WLC
    - Inactieve access points zijn de access points die ooit geadopteerd zijn maar momenteel offline zijn
- Het aantal active access points van de WLC
    - Actieve access points zijn de access points die geadopteerd en online zijn
- Het aantal verwachte access points van de WLC
    - Dit zijn zowel de online als offline access points die ooit geadopteerd zijn
- Het aantal online access points die succesvol een configuratie hebben gehad
- Het aantal adapted access points die door de controller geadopteerd zijn
    - Adapted access points zijn de geadopteerde access points die een andere configuratie hebben dan het profiel die de controller distribueert naar de access point. Een afwijkende configuratie ontstaat door een access point een aparte configuratie te geven die de configuratie overschrijft.

Monitoring van het access point:

- De naam, het type apparaat, de locatie, contactinformatie en de software versie van het access point
- De tijd in dagen, uren en minuten dat het access point online is
- Aantal clients per radio van het access point
- De CPU utilisatie in procenten van de afgelopen vijf minuten
- De uitgezonden SSIDs door het access point

[14] OID - Een Object Identifier (OID)identificeert de unieke objecten in de MIB hiërarchie. Een OID object bevat informatie over een systeem.

- De radio modus van de radio's van het access point
    - Dit is of 2.4 GHz of 5 GHz
- De transmit power per radio

5.4.3.2 Client historie en features

De tweede stap was het toevoegen van de cliënt historie en het verbeteren of toevoegen van functionaliteiten in de monitoring. De cliënt historie wordt gebruik voor troubleshooting. Dit is een log waarin alle clients (laptops, computers, telefoons etc.) die ooit verbonden waren met de infrastructuur worden weergegeven. Elke 30 seconden wordt er een controlecheck uitgevoerd om te controleren op wijziging. Indien dit het geval is worden de wijzigingen toegevoegd aan de lijst.

Voor het vergaren van de informatie voor cliënt historie is overleg gepleegd met het netwerkteam omdat zij degene zijn die hiermee gaan werken. Ook is er gebruik gemaakt van de monitoring van de Juniper omgeving. besloten is om de volgende informatie weer te geven in de cliënt historie:

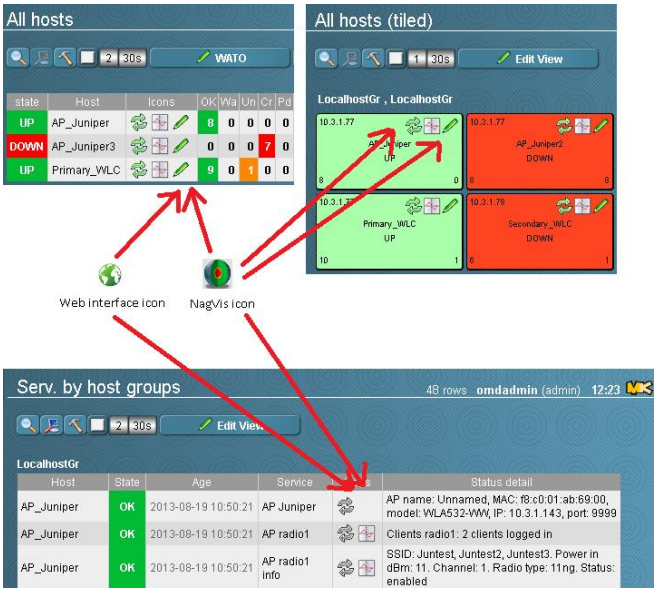
- Computernaam van de cliënt die verbonden is met het access point
- IP adres van de cliënt die verbonden is met het access point
- MAC adres van de cliënt die verbonden is met het access point
- Naam van het access point waarmee de betreffende cliënt verbonden is
- De locatie van het access point
- Virtueel LAN (VLAN) waarmee de cliënt verbonden is
- Het SSID waarmee de cliënt verbonden is
- Signal to Noise (SNR) van de client
    - Dit is het verschil in decibel tussen de sterke van het signaal en de ruisvloer in de omgeving
- De ruisvloer waarmee de cliënt te maken heeft
    - De ruisvloer wordt veroorzaakt door ongewenste storing
- Received signal strength Indication (RSSI) van de client
    - Dit is het signaal in decibel dat de cliënt ontvangt
- De tijd in dagen, uren en minuten dat het access point waarmee de cliënt verbonden is online is
- Het IP adres van de WLC waarmee het access point van de cliënt verbonden is

Omdat de cliënt historie er bij Juniper erg onoverzichtelijk uitzag is er ook besloten betere filters te laten ontwikkelen. Hierdoor wordt de informatie overzichtelijker weergegeven. De cliënt historie kreeg hiervoor twee extra items in het menu. Het eerste item liet de online cliënts zien, het tweede item de offline cliënts.

Ook zijn er een aantal hyperlinks toegevoegd om sneller naar NagVis, en de web interface van het betreffende apparaat te kunnen navigeren. Deze hyperlinks zijn verwerkt in iconen die zijn toegevoegd onder de menu items die de access points en controllers weergeven(figuur 18).

Tevens is er besloten een check aan de monitoring van de access points toe te voegen waarin weergegeven word met welke controller het access point verbonden is. Deze is toegevoegd omdat het access point in de controller moet worden geconfigureerd.

De cliënt historie en de nieuwe functionaliteiten zijn verwerkt in een

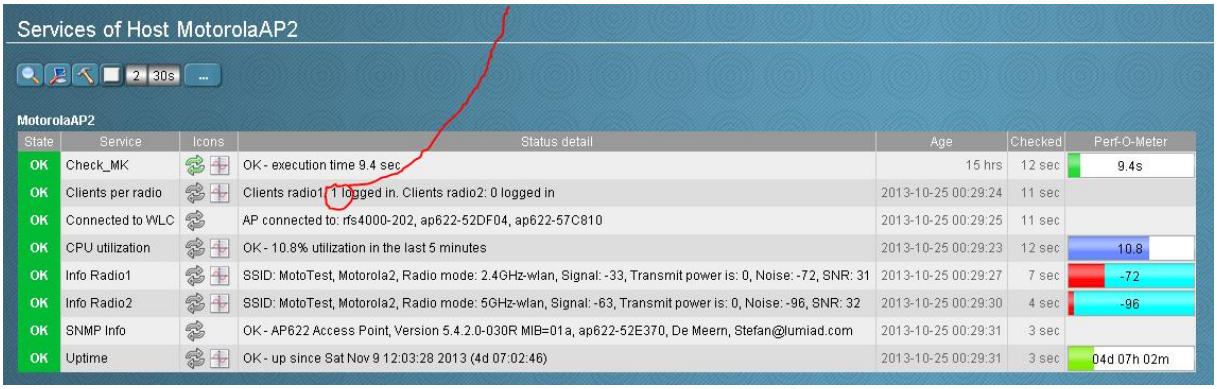


Figuur 18 - Toegevoegde functionaliteiten

uitbreiding op het projectplan. Deze is toegevoegd in de bijlage F Projectplannen. (projectplan v2)

Na de oplevering van de eerste gebouwde versie heeft er een test plaatsgevonden, door het systeem te toetsen aan de hand van het projectplan. De eerste gebouwde versie was de monitoring van de access points en controllers.

Na het testen is er een uitbreiding gemaakt op het projectplan. Hierin zijn oplossingen bedacht en verwerkt voor het oplossen van fouten. De fouten hadden voornamelijk te maken met verkeerde OIDs, of het incorrect weergeven van bepaalde checks. Tevens zijn er twee functionaliteiten aan dit projectplan toegevoegd voor het filteren op een MAC adres in de cliënt historie. Bij het selecteren van een MAC adres, van een laptop, desktop, telefoon of ander apparaat wordt nu alleen het betreffende apparaat weergegeven. Tevens is er een functionaliteit toegevoegd waarbij er een hyperlink is vanaf 'cliënts per radio' naar de cliënt historie(figuur 19). Hierdoor kunnen de gebruikers op het betreffende access point geïdentificeerd worden. Het bijhorende projectplan is toegevoegd in de bijlage(extended projectplan v3).



Figuur 19 - Hyperlink naar cliënt historie

5.4.3.3 Automatisering

Er is ook onderzoek verricht om het proces voor het inzetten van de monitoring te automatiseren. Voor het inzetten van de monitoring moet in de huidige situatie eerst een Linux variant geïnstalleerd worden, vervolgens moeten Nagios en Check_MK via OMD [15]geïnstalleerd worden. Tot slot moet alle apparatuur handmatig d.m.v. het IP adres worden toegevoegd aan Check_MK.

Om dit te automatiseren zou er van een compleet geïnstalleerde Linuxsysteem(CentOS), inclusief Check_MK met bijbehorende plugins een ISO [16]bestand worden gemaakt. Aan het ISO bestand kan een kleine configuratie worden toegevoegd aan de installatiesetup waarin configuratie kan worden meegegeven. Hiervoor zou de opgesomde informatie van belang zijn:

- IP configuratie van de machine zelf
- Hostname van de machine zelf
- ingeven van een domeinnaam en wachtwoord
- De SMTP server voor traps en informatie per mail

Als deze informatie is toegevoegd is de Check_MK server klaar voor gebruik. Ook zou het handmatig toevoegen van de apparatuur aan de monitoring geautomatiseerd kunnen worden. Dit kan gedaan

[15] OMD - Open Monitoring Distribution(OMD) is een bundeling van Nagios inclusief de belangrijkste plugins in een enkele installatie.
[16] ISO – Een ISO bestand is een digitale copy van een CD of DVD

worden door een functie in te bouwen in Check_MK waarbij een IP scan wordt gedaan door een SNMP request te verzenden. Als een apparaat reageert kan deze worden toegevoegd aan Check_MK. Om andere apparatuur als een controller of access point te scheiden kan hiervoor een Motorola specifiek SNMP request worden gebruikt. Het is wel van belang dat de scan wordt uitgevoerd in het VLAN van de access points en controllers, omdat de apparatuur anders bereikbaar is.

In het onderstaande tabel zijn de voordelen van de geautomatiseerde oplossingen tegenover de huidige situatie weergegeven.

Huidige situatie	Nieuwe situatie
Handmatig installeren van Nagios en plugins	Geautomatiseerde ISO uitrollen inclusief configuratie
Configureren van naam, ip adres etc.	Geautomatiseerd configuratiemenu voor het ingeven van deze configuratie
één voor één de apparatuur handmatig toevoegen aan Check_MK	Geautomatiseerde scan die de apparatuur toevoegt aan Check_MK.
-	ISO bestand kan zowel op in een virtuele als fysieke omgeving worden geïmplementeerd.

5.4.4 Implementatie van de monitoring

Om de monitoringsresultaten van de access points en de controllers van de klant te monitoren, kan het monitoringsverkeer over een VPN verzonden worden tussen Lumiad en de klant. Hierdoor kunnen de monitoringresultaten van de verschillende klantomgevingen worden weergegeven op een dashboard. Een nadeel is dat het opvragen van SNMP verkeer over het internet vaak resulteert in time-outs omdat doordat het internet, of de klantomgeving teveel vertraging oplevert.

Andere techniek is het implementeren van een Check_MK server in de klantomgeving. De Check_MK server kan de beheerder informeren per e-mail zodra er een incident plaatsvind. Een nadeel van deze techniek is dat elke klantomgeving een eigen Check_MK server nodig heeft. Een ander nadeel is dat de monitoringsresultaten van de verschillende klanten niet op een gecentraliseerd dashboard bij Lumiad kunnen worden weergegeven. Tot slot is het een nadeel dat de beheerder een VPN verbinding opbouwen naar de klant als het monitoringsysteem bereikt moet worden. Een voordeel is dat er geen monitoringsverkeer over het internet verzonden hoeft te worden, waardoor er geen time-outs ontstaan.

Een andere methode is het implementeren van een slave monitoringsserver bij de klant en een master monitoringserver bij Lumiad. De slave monitoringsserver bij de klant zou de access points en controllers aan de klantzijde kunnen monitoren. Vervolgens kan de Check_MK server bij de klant zijn configuratie eens in de zoveel tijd synchroniseren naar de Check_MK server bij Lumiad. Hierdoor kan de monitoring van de verschillende klantomgevingen worden weergegeven op een dashboard op de centrale monitoringsserver bij Lumiad. Een ander voordeel van deze oplossing is dat het bandbreedte efficiënt is en daarnaast time-outs voorkomt. Als een SNMP request over het internet verzonden moet worden en daar teveel vertraging oploopt ontstaat er een time-out. Check_MK geeft in dat geval weer dat de hele klantomgeving offline is. Een nadeel van deze methode is wel dat iedere klantomgeving een eigen monitoringserver vereist.

Om distributed monitoring te configureren kan OMD gebruikt worden. OMD is een bundeling van meerdere software versies en plugins van Nagios. Tijdens de installatie, of in het OMD menu kan distributed monitoring aangezet worden. Hierin dient dan het IP adres van de centrale Check_MK server bij Lumiad te worden opgegeven. Als de Check_MK achter NAT hangt dient het NAT adres te worden opgegeven. Tevens moet er een port forwarding worden ingesteld op de router bij Lumiad die het adres van de betreffende poort vertaald naar de interne Check_MK server.

6 Conclusies

Dit hoofdstuk beschrijft de conclusies aan de hand van het onderzoek.

6.1 Managed Wi-Fi

De conclusie is dat Managed Wi-Fi kan bijdragen aan de het goedkoper implementeren van een draadloos netwerk doordat de klant de keuze heeft alleen goedkope thin access points aan te schaffen. in de huidige situatie moet de klant namelijk fat access points of een dure controller aanschaffen. Ook draagt Managed Wi-Fi bij aan een snellere implementatie doordat de controller het configureren van de access points heeft geautomatiseerd. De verschillende klanten kunnen namelijk door een enkele controller, of cluster van controllers worden geconfigureerd en voorzien van updates.

Managed Wi-Fi kan worden gerealiseerd met verschillende merken draadloze netwerk apparatuur. Bijvoorbeeld met Cisco, Aerohives, Lancom of Motorola. Cisco zit niet in het assortiment van Lumiad en verkrijgt niet de voorkeur van de beheerders van Lumiad. Aerohives is onbetrouwbaar, niet zo bekend in de markt en beheerders van Lumiad hebben afkeer van dit merk. Lancom is betrouwbaar en heeft uitgebreidere mogelijkheden maar is onbekend in de Nederlandse markt. Motorola is bekend in de Nederlandse markt, heeft goedkopere hardware, krijgt de voorkeur van de beheerders van Lumiad en is bekend in de markt. De conclusie is dat Motorola voor Lumiad geschikt is om Managed Wi-Fi mee te realiseren.

6.2 Het marktaanbod

Uit interviews met diverse klanten bleek dat bedrijven met enkele medewerkers baat hebben bij een betrouwbaar draadloos netwerk maar vaak geen expertise in huis hebben om een betrouwbaar en stabiel draadloos netwerk te realiseren. Uit deze informatie kan geconcludeerd worden dat er vraag is naar een implementatie en overname van het beheer voor een betrouwbaar draadloos netwerk. Managed Wi-Fi biedt hier uitkomst omdat dit bijdraagt aan een prijsvriendelijke en snelle implementatie. De klant hoeft immers niet perse een controller aan te schaffen, hoeft geen tijd te steken in onderzoek en de implementatie is tijdsvriendelijk.

6.3 Beschikbaarheid

Het is belangrijk voor Lumiad om Managed Wi-Fi op de markt te zetten met een hoge beschikbaarheid van het draadloze netwerk. Een enkele controller is een single point of failure, dus verlaagt de beschikbaarheid. Beschikbaarheid is belangrijk voor de implementatie van Managed Wi-Fi omdat dit bijdraagt aan het verkopen, en het leveren van een professioneel en betrouwbaar product.

Hieruit kan geconcludeerd worden dat een tweede controller van belang is. De twee controllers kunnen als een cluster worden geconfigureerd. Configuraties van de verschillende klantomgevingen zullen hierbij gesynchroniseerd worden tussen de twee controllers waardoor beide controllers de klantomgeving individueel kunnen beheren in geval van een storing.

Als beide controllers gehost worden bij Lumiad en met het internet communiceren via een enkele uplink betreft dit ook een single point of failure. Beide controllers, of één van de twee zouden extern gehost kunnen worden. Het hosten van beide controllers met een dubbele uplink levert een hogere beschikbaarheid als het hosten bij Lumiad omdat er twee internetlijnen beschikbaar zijn. Deze oplossing is wel 200 euro duurder per maand als het intern hosten bij Lumiad. Een ander voordeel zou kunnen zijn dat Lumiad zelf geen bandbreedte verbruikt aan Managed Wi-Fi. Echter is er ruim voldoende bandbreedte beschikbaar waardoor dit geen grote rol speelt bij de keuze. Het extern laten hosten van een enkele controller, waarbij de andere bij Lumiad gehost wordt bespaard ongeveer 100 euro per maand. Hierdoor blijft er 100 euro bespaard in vergelijking met het laten hosten van twee controllers. Een voordeel is dat de klanten beheert kunnen worden vanaf de controller bij Lumiad. Dit is een voordeel omdat er nu geen verbinding naar de externe hostingprovider hoeft te worden opgebouwd. De controller bij Lumiad kan hierbij de configuraties van de verschillende klantomgevingen

synchroniseren over het internet naar de tweede controller. Als Lumiad problemen ondervind met de primaire internet verbinding kan de secundaire ADSL verbinding dienen als back-up om de controller in het externe data center te bereiken. Deze maatregelen om beschikbaarheid te garanderen treft alleen Lumiad. De klantomgeving is in veel gevallen nog steeds voorzien van een enkele internetverbinding. Als deze met storing kampt, werkt de draadloze omgeving van de klant niet meer.

De klant wil ten allen tijden gebruik kunnen maken van zijn draadloze netwerk. Sommige klanten maken bijvoorbeeld gebruik van draadloze pin apparatuur, als het draadloze netwerk te kampen heeft met een storing en de schuld is van Lumiad zijn de gevolgen niet te overzien. Om deze reden is het van belang dat de draadloze netwerk omgeving van de klant een zo hoog mogelijke beschikbaarheid krijgt. De conclusie is dat er veel verschillende manieren zijn om een hoge beschikbaarheid te realiseren. Wel is dit mede afhankelijk van het scenario die Lumiad gebruikt voor het hosten van de controllers. Als Lumiad de controllers namelijk intern gaat hosten en de internetverbinding ondervind een storing, zal een klantomgeving met enkel thin access points offline gaan, deze kunnen immers niet standalone functioneren. Als Lumiad één controller bij een externe provider host, en de andere controller intern is de kans dat beide controllers onbereikbaar zijn vrijwel nihil, waardoor het inzetten van enkel thin access points een optie kan zijn. Managed Wi-Fi zou als volgt bij de klant geïmplementeerd kunnen worden:

- Thin access points op de klantlocatie
- Thin access points met een controller op klantlocatie
- Fat access points of klantlocatie

6.3.1 Thin access points in de klantomgeving

In de klantomgeving kunnen enkel thin access points worden geïmplementeerd. Deze oplossing heeft een prijstechnisch voordeel. Dit scenario heeft de volgende voor- en nadelen:

- Deze oplossing is prijstechnisch het voordeligst. Thin access points zijn namelijk twee keer zo goedkoop als fat access points, de functionaliteiten zijn afgezien van het standalone kunnen functioneren hetzelfde.

- De beschikbaarheid is lager dan het inzetten van fat access points of een controller op klantlocatie. Als de verbinding tussen de controller(s) van Lumiad en de thin access points van de klant verbreekt, zullen de thin access points zichzelf uitschakelen. Hierdoor is het draadloze netwerk niet meer te gebruiken. Het risico op het verliezen van de verbinding kan teruggedrongen worden tot bijna nihil door de controllers redundant uit te voeren waarvan één of twee controllers bij een externe hostingprovider gehost worden. Het netwerk en de netwerkapparatuur van de klant blijven hier wel een risico. Echter blijft dit ook een risico bij het inzetten van een controller of fat access points op klantlocatie. Lumiad zou aan de hand van een analyse de klant kunnen adviseren het netwerk, en de netwerkapparatuur redundant uit te voeren.

6.3.2 Access points met een controller in klantomgeving

Een andere optie is het inzetten van access points bij de klant in combinatie met een controller. De klant zou de controller zelf kunnen aanschaffen of Lumiad zou deze in bruikleen kunnen aanbieden waardoor de klant geen aanschafskosten betaald. Het scenario met een controller op klantlocatie heeft de volgende voor- en nadelen:

- De draadloze omgeving van de klant blijft ten alle tijden online. Als de controller bij de klant offline gaat zullen de access points automatisch geadopteerd worden door de controllers van Lumiad. Als de controllers van Lumiad niet te bereiken zijn blijven de thin access points standalone functioneren m.b.v. de controller op klantlocatie.

- Zero touch configuratie en goedkope thin access points. Dit betekent dat het access point zonder enige configuratie in het klantnetwerk kan worden geïmplementeerd. Hiervoor heeft de klant alleen een DHCP server nodig. Het access points verkrijgt een IP adres en zal vervolgens een MINT link opbouwen met de klantcontroller. Vervolgens krijgt hij de juiste configuratie inclusief de configuratie om de WLC bij Lumiad te bereiken in geval van storing aan de klantcontroller.

- Dit scenario biedt vanaf drie of meer access points een prijstechnisch voordeel tegenover het scenario met fat access points. Thin access points kosten 200 euro per stuk. Daarentegen is een fat access point minimaal 400 euro en een controller 600 euro.

- Alle modellen access points kunnen worden ingezet bij de klant in dit scenario zonder dat er meer bandbreedte verbruikt wordt. De controller op klantlocatie kan namelijk alle modellen access points van Motorola adopteren. Als er geen controller op klantlocatie is zal elk model access points een RF-domain manager selecteren, die een tunnel opbouwt naar de Lumiad controller. Als er twee verschillende modellen gebruikt worden ontstaan er dus twee tunnels.

- Een nadeel is dat de controller prijzig vrij prijzig is, terwijl de doelstelling was om de kosten te reduceren. Het implementeren van enkel thin access points bij de klant doet het op dit gebied beter. Echter, heeft het scenario met controller op klantlocatie wel een hogere beschikbaarheid.

6.3.3 Fat access points in de klantomgeving

Een ander scenario is het implementeren van enkel fat access points op klantlocatie. Ook dit scenario heeft voor en nadelen. Deze zijn hieronder beschreven.

- De draadloze omgeving van de klant blijft ten alle tijden online. Als de controller(s) van Lumiad niet te bereiken zijn blijven de fat access points standalone functioneren. Als de RF domain manager offline gaat, door bijvoorbeeld een storing, zal een andere fat access point de taak als RF domain manager automatisch over nemen.

- Dit scenario biedt in omgeving met twee of minder access points een prijstechnisch voordeel tegenover het scenario met thin access points en een controller. twee fat access points kosten ongeveer 800 euro, twee thin access point met een controller ongeveer 1000 euro.

- Als er verschillende modellen access points gebruikt worden zullen er meerdere RF domain managers en tunnels ontstaan. Het gevolg hiervoor is een verhoging in het bandbreedte verbruik doordat elke RF domain manager zijn configuratie of update apart toegezonden krijgt van de controller. Verschillende merken communiceren niet onderling op MINT level 1.

6.4 Monitoring

Lumiad wil de klant een draadloos netwerk met een hoge beschikbaar kunnen garanderen. Hiervoor zou een monitoringsysteem geïmplementeerd kunnen worden, waarmee de Motorola apparatuur kan worden gemonitord. Dit draagt bij aan het sneller verhelpen van een incident, omdat het systeem een incident automatisch detecteert en de beheerder hierover inlicht. De beheerder is hierdoor voorzien van informatie en in staat eerder te reageren op het incident, waardoor de beschikbaarheid en daarmee de kwaliteit van het draadloze netwerk verbeterd wordt. Tevens kan de monitoring worden gebruikt om incident proactief te constateren. Dit betekent dat een incident kan worden gedetecteerd, en voorkomen voordat deze optreed. De monitoring kan namelijk ‘vreemd’ gedrag constateren en de beheerder hierover inlichten. De beheerder is hierdoor in staat het incident te verhelpen nog voor deze optreed.

6.5 Monitoringssystemen

De monitoring voor Motorola kan worden gerealiseerd op verschillende systemen. De monitoring is mogelijk d.m.v. de controller, in een nieuw monitoringssysteem of in Check_MK.

Check_MK is bekend onder de beheerders van Lumiad. Monitoring d.m.v. controller of een nieuw monitoringssysteem brengt met zich mee dat het personeel hiervoor getraind moet worden. Een nadeel van Check_MK is dat de monitoring nog moet worden ontwikkeld, terwijl monitoring d.m.v. de controller al kant er klaar is, en veel nieuwe systemen ook kant en klaar zijn. Een voordeel van het laten ontwikkelen in Check_MK is dat de monitoring op maat kan worden ingericht, naar de wensen en eisen van Lumiad. Dit kan niet gedaan worden in de controller, omdat de software geen open source is. Bovendien is de monitoring in de controller erg beperkt. Als er wordt gekozen voor een nieuw monitoringsysteem word Motorola afzonderlijk gemonitord, de monitoring van de merken Lancom en Juniper wordt immers gedaan in Check_MK.

6.6 Implementatie van de monitoring

De monitoringsserver kan geïmplementeerd worden in het netwerk bij Lumiad of in het netwerk van de klant. Een andere optie is het implementeren van distributed monitoring.

Als de monitoringserver bij Lumiad geïmplementeerd wordt kan Check_MK de draadloze klantapparatuur via een VPN verbinding monitoren. Een nadeel is dat het opvragen van SNMP verkeer over het internet vaak resulteert in time-outs omdat doordat het internet, of de klantomgeving teveel vertraging oplevert. Als de Check_MK server in het klantnetwerk wordt geïmplementeerd, of er wordt gebruik gemaakt van distributed monitoring is dit niet het geval. Een voordeel is dat de monitoringresultaten van alle klanten op hetzelfde dashboard kan worden weergegeven. Dit is niet het geval als de monitoringsserver in het klantnetwerk wordt geïmplementeerd. De beheerder moet dan een VPN verbinding opbouwen naar de klant om de monitoring per omgeving in te kunnen zien.

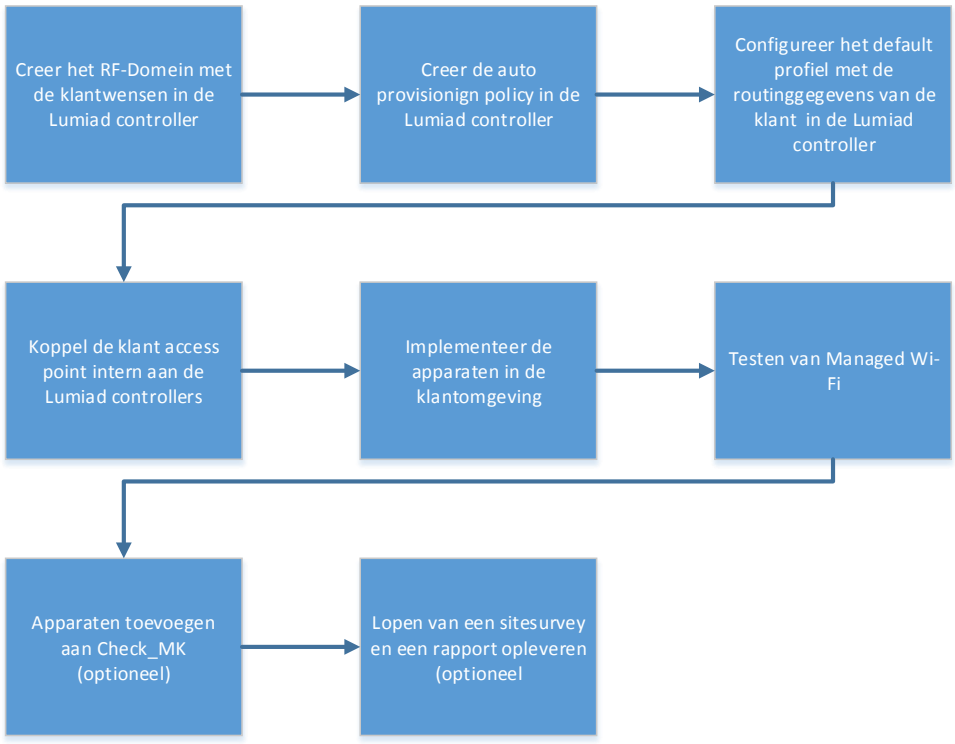
Als er gebruik gemaakt wordt van distributed monitoring zijn deze nadelen er niet, omdat de monitoring van alle klantomgevingen op de centrale Check_MK server bij Lumiad kunnen worden weergegeven. De draadloze apparatuur wordt hierbij op de klantomgeving gemonitord door de slave monitoringserver. Hierdoor ontstaan er geen time-outs door vertraging in het internet. Het enige nadeel is dat iedere klantomgeving wel een eigen monitoringsserver vereist.

7 Nieuwe situatie

Dit hoofdstuk beschrijft de een implementatie als Lumiad mijn advies voor het inzetten van Managed Wi-Fi en de monitoring toepast.

7.1 Managed Wi-Fi

In de nieuwe situatie kan Managed Wi-Fi in een paar stappen (figuur 20) worden geïmplementeerd bij de klant. Voorafgaande aan deze stappen dient de klant een vragenlijst in te vullen. Aan de hand hiervan, en in sommige gevallen een site survey kan het personeel van Lumiad een aanbeveling uitbrengen. Managed Wi-Fi behoort nu tot één van de aanbevelingen. Bij een site survey wordt het draadloze netwerk gemeten. hieruit kan een rapport worden opgesteld met plattegronden en statistieken over het draadloze netwerk.



Figuur 20 - Managed Wi-Fi klant implementatie

Het RF-domein bepaalt de configuratie die op de klant access points geconfigureerd zal worden.

De auto provisioning policy zorgt ervoor dat de klant access points automatisch in het juiste RF-domein komen na implementatie.

Het default profiel wordt geconfigureerd met de benodigde gegevens van de klant, die nodig zijn om met de Lumiad controller te communiceren. Hang de access points nu een minuut aan de controller en controleer in de controller statistieken of het access points default configuratie heeft gehad.

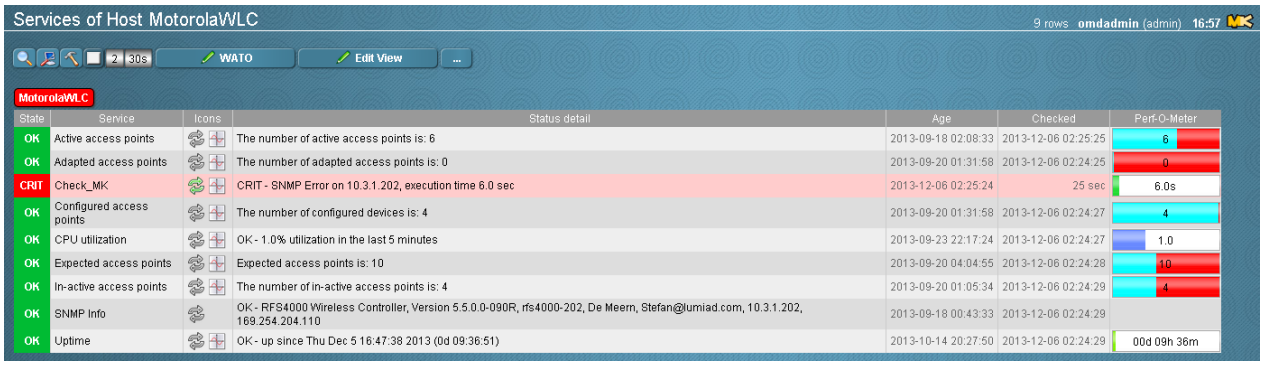
Implementeer nu de access points in het klantnetwerk, deze zullen een verbinding opbouwen met Managed Wi-Fi. Controller of de groene en rode ledjes van het access points knipperen. Als dit het geval is heeft het access point de configuratie van de controller verkregen.

Indien de klant monitoring nodig heeft kunnend de apparaten worden toegevoegd aan Check_MK. Ook kan er op wens van de klant een rapport worden opgeleverd als output van een site survey.

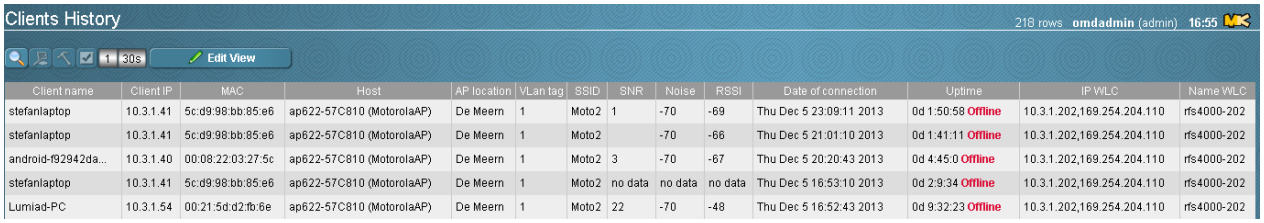
7.2 Monitoring

In de nieuwe situatie kunnen de controllers en access points gemonitord worden(figuur 21 en 2). Tevens is er een client historie beschikbaar die een informatielog van de clients weergeeft (figuur 23).

Figuur 21- Access point monitoring



Figuur 22 - Controller monitoring



Figuur 23 - Clients history

8 Aanbeveling

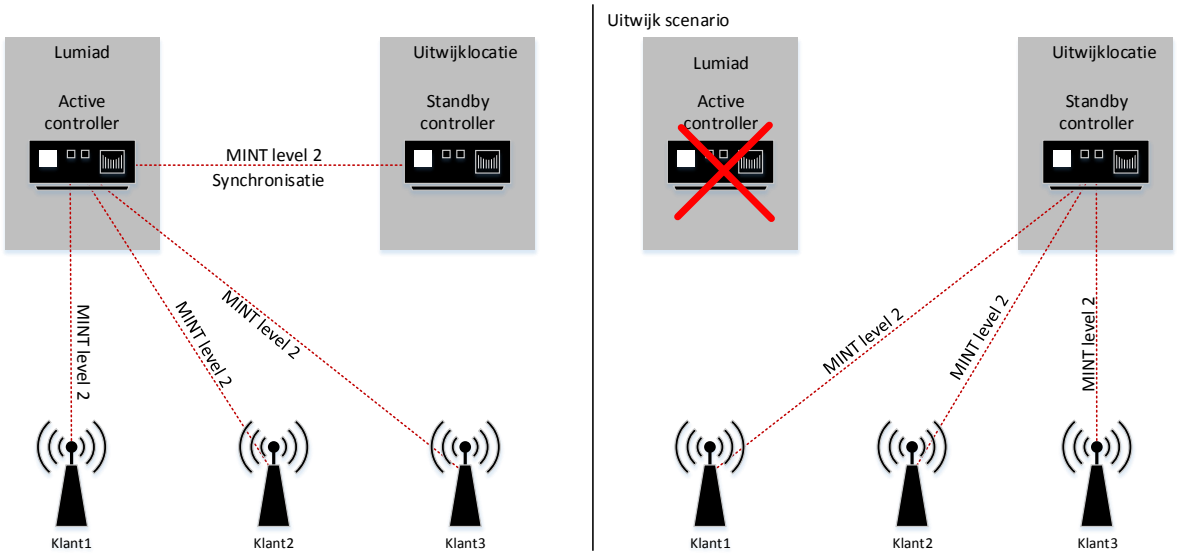
Dit hoofdstuk beschrijft de aanbeveling geschreven door de student op basis van de conclusies.

8.1 Managed Wi-Fi

Zoals eerder beschreven ben ik tot de conclusie gekomen dat Managed Wi-Fi kan worden aangeboden aan verschillende klanten. Uit interviews met klanten blijkt namelijk dat er animo is. Vooral bedrijven met ongeveer vijftien access points zijn geïnteresseerd. Managed Wi-Fi draagt namelijk bij aan een goedkopere implementatie doordat de klant alleen goedkope thin access points aan hoeft te schaffen. Daarnaast zijn de access points sneller te implementeren in het klantnetwerk doordat de controller de access points automatisch configureert. De verschillende klantomgevingen kunnen namelijk door een enkele controller, of cluster van controllers worden geconfigureerd en voorzien van systeemupdates.

8.1.1 Implementatie van Managed Wi-Fi

Het inzetten van alleen thin access points op de klantlocatie heeft wel het risico dat de draadloze netwerkomgeving offline gaat als de verbinding met de controller van Lumiad verbreekt. Daarom raad ik Lumiad aan een cluster van twee controllers te configureren, waarbij één controller in een extern data center gehost wordt als uitwijklocatie en de andere bij Lumiad zelf (zie ook figuur 24). Dit is te realiseren voor ongeveer 100 euro per maand bij Nedzone. Bovendien garandeert Nedzone een hoge beschikbaarheid. De controller wordt namelijk voorzien van een redundante uplink, brandbeveiliging en noodstroom.



Figuur 24 - Uitwijk scenario

De controller bij Lumiad wordt geconfigureerd als de actieve controller in een active-standby cluster. De controller bij de uitwijklocatie wordt geconfigureerd als de standby controller. De controllers zullen onderling synchroniseren. Als de controller bij Lumiad nu onbereikbaar is zullen de access points van de klant automatisch migreren naar de controller in de uitwijklocatie. Zodra de controller bij Lumiad weer bereikbaar is zullen de access points weer migreren naar de eerste controller. Het risico dat beide controllers niet meer bereikbaar zijn is door de redundante uitvoering met uitwijk locatie zeer beperkt.

8.1.2 De klant

De beschikbaarheid van de draadloze netwerk omgeving van de klant is ook afhankelijk van de bedrade netwerkapparatuur en de internetprovider. Daarom raad ik Lumiad aan een analyse te doen van de netwerkinfrastructuur en de doeleinden van het draadloze netwerk. Aan de hand van deze informatie kan de klant geïnformeerd worden over de risico's die de beschikbaarheid van het draadloze netwerk kunnen beperken. Tevens kan Lumiad hier een advies over uitbrengen om de beschikbaarheid te verhogen. Lumiad kan bijvoorbeeld een advies uitbrengen om de netwerkinfrastructuur redundant uit te laten voeren.

8.1.3 Consequenties

Het inzetten van Managed Wi-Fi met alleen thin access points op klantlocatie heeft als risico dat het draadloze netwerk offline gaat als de verbinding met de controller verbreekt. Lumiad beperkt dit risico door de controller redundant in te zetten met een uitwijklocatie. Echter heeft dit geen nut als de netwerkapparatuur of de internetverbinding van de klant niet werkt. In dit geval kan de klant niet alleen het internet niet meer bereiken maar ook de apparaten in het interne netwerk niet. Op het interne netwerk kunnen bijvoorbeeld dataservers benaderd worden. Als er fat access points geïmplementeerd worden, of een controller op locatie zal het interne netwerk wel beschikbaar blijven als de klant geen internetverbinding meer heeft. Daarom raad ik Lumiad ook aan de klant op de hoogte te brengen van deze consequentie, en eventueel te adviseren fat access points of een lokale controller te implementeren.

8.1.4 De verschillende merken

Managed Wi-Fi kan worden geïmplementeerd met verschillende merken. Ik raad Lumiad aan om in eerste instantie Managed Wi-Fi met Motorola apparatuur te realiseren. Motorola is namelijk een bekende speler op de Nederlandse markt, biedt hoge kortingen, heeft uitgebreide mogelijkheden, is betrouwbaar en verdient de voorkeur van de beheerders van Lumiad. Tevens raad ik aan om onderzoek te doen naar het realiseren van Managed Wi-Fi met Lancom. Lancom is namelijk een betrouwbaar merk, heeft uitgebreide mogelijkheden, hanteert geen licentiekosten en verdient de voorkeur van de beheerders van Lumiad.

8.2 Monitoring

Ik raad Lumiad ook aan om de draadloze Motorola apparatuur te monitoren omdat er dan een product met een hoge beschikbaarheid op de markt gezet kan worden. Monitoring draagt bij aan een hogere beschikbaarheid doordat een incident preventief kan worden voorkomen of sneller kan worden verholpen. De monitoring kan de beheerder van Lumiad namelijk geautomatiseerd inlichten met informatie over een incident, waardoor het incident eerder kan worden verholpen. Een incident kan preventief worden verholpen door proactief te monitoren. Dit betekend dat een incident kan worden gedetecteerd, en verholpen voordat deze optreed. De monitoring kan namelijk 'vreemd' gedrag constateren en de beheerder hierover inlichten. De beheerder is hierdoor in staat het incident te verhelpen nog voor deze optreed.

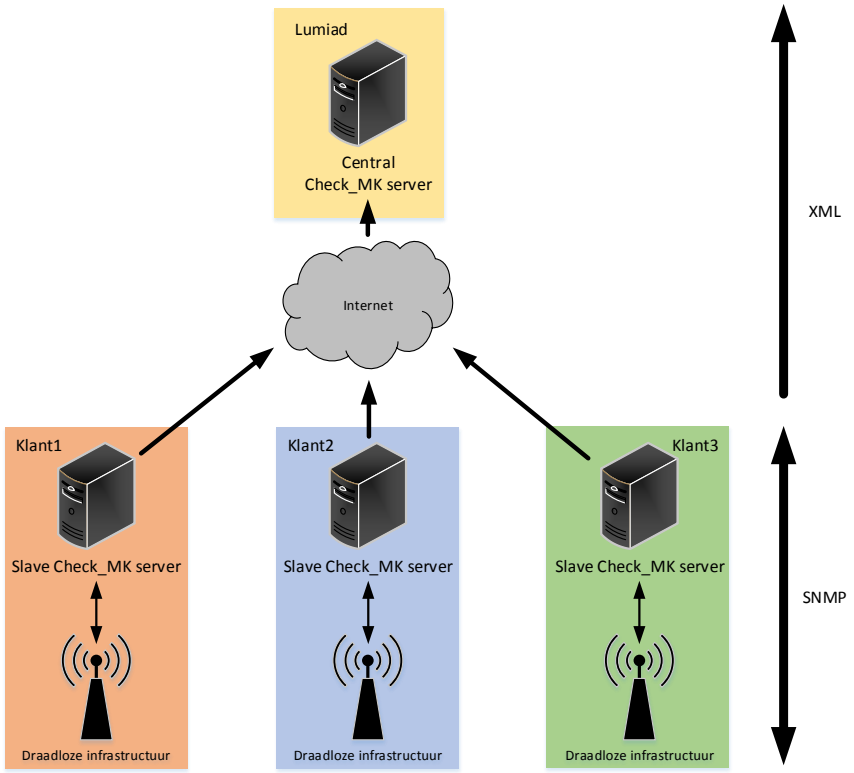
8.2.1 Het monitoringssysteem

Lumiad kan de monitoring doen m.b.v. het systeem Check_MK. Check_MK heeft als voordeel dat de beheerders van Lumiad bekend zijn met dit systeem, andere merken ook met Check_MK worden gemonitord, Check_MK zuinig om gaat met de bandbreedte en Check_MK naar eigen wensen kan worden ontwikkeld.

Het ontwikkelen van een goede basis voor de monitoring is al gerealiseerd met Check_MK. Hiervoor is een uitbesteding gedaan naar een ontwikkelteam in Oekraïne. Lumiad kan hierdoor access points en controllers van Motorola monitoren. Tevens worden de gebruikers, die ingelogd zijn op de access points gemonitord. Ook is de gebruikersgemak verbeterd, door de informatie overzichtelijk weer te geven. het toevoegen van filters en iconen om sneller te kunnen navigeren tussen de verschillende plugins en de web-interface van een controller of access point hebben hieraan bijgedragen.

8.2.2 Implementatie van het monitoringssysteem

Ik raad Lumiad aan gebruik te maken van distributed monitoring. Bij distributed monitoring wordt er een slave monitoringsserver in het klantnetwerk geïmplementeerd, en een centrale monitoringsserver bij Lumiad (zie ook figuur 25). Doordat de slave monitoringsservers van de verschillende klanten de monitoringsresultaten verzenden naar de centrale Check_MK server bij Lumiad, kunnen de resultaten van de verschillende klanten gecentraliseerd op een dashboard worden weergeven. Tevens is deze techniek bandbreedte efficiënt omdat het monitoringsverkeer niet constant over het WAN verzonden hoeft te worden, maar eens in de zoveel tijd een update stuurt met informatie over de draadloze klant apparatuur.



Figuur 25 - Distributed monitoring

De slave Check_MK servers monitoren de draadloze klanten infrastructuur over het interne netwerk via het SNMP protocol. Na een bepaalde interval sturen de slave Check_MK servers een XML pakket naar de centrale Check_MK server, waardoor de informatie van de verschillende klantomgeving hier beschikbaar is.

Tot slot zou Lumiad gebruik kunnen maken van een geautomatiseerde implementatiemethode voor de monitoring, waardoor een implementatie minder tijd kost. Om dit te realiseren is er een uitbesteding gedaan voor een geautomatiseerd installatiebestand van het monitoringssysteem. Dit installatiebestand bevat een menu waarin parameters kunnen worden ingegeven, zoals een IP configuratie of mail server, waarna Nagios met de addons Check_MK, PNP4Nagios en NagVis geïnstalleerd wordt. Tevens is het hiermee mogelijk apparatuur automatisch aan Check_MK toe te voegen d.m.v. een scan op SNMP basis.

9 Evaluatie van de procesgang

Het project bestond uit een analyse, architectuur, ontwerp, implementatie en beheerfase. Per fase is een evaluatie van de procesgang beschreven. Daarnaast zijn de projectresultaten vergeleken met het plan van aanpak.

9.1 Analysefase

In de analysefase is het plan van aanpak beschreven en vond het onderzoek plaats. Om kennis op te doen voor het beschrijven van de documenten uit deze fase zijn er interviews gehouden en is er een literatuuronderzoek gedaan. Daarnaast zijn er experimenten uitgevoerd in een testomgeving.

Deze fase duurde langer dan gepland. Het technische onderzoekdeel bleek lastig omdat ik niet bekend was met de technieken van Motorola en Lancom. Ook bleek de support van Motorola erg beperkt en technische documenten waren nauwelijks voorhanden. Ook het aanschaffen van nieuwe software versies en hardware, die nodig waren om Managed Wi-Fi in een testomgeving op te bouwen was een tijdrovende klus. Hiervoor hebben ik en de directie (Wim Bos) veel moeten mailen en bellen met Motorola. Daarnaast werkt het netwerkteam veel buiten de deur, waardoor hulp bij het beantwoorden van vragen vaak even duurde. Ook bleek de uitbesteding voor het ontwikkelen van de monitoring een tijdrovende klus, omdat de Engelse vaardigheid van het ontwikkelteam beperkt is. Hierdoor moesten de projectplannen erg uitgebreid beschreven worden inclusief een beschrijving van de techniek. Tot slot kwam het ontwikkelteam de planning niet altijd na, door problemen als een stroomstoring of problemen met een server.

Het wachten op reacties betekent niet dat het project niet vorderde. De tijd is nuttig besteed door in tussentijd andere vraagstukken alvast te realiseren. Zo konden het marktonderzoek, de monitoring, het plan van aanpak en de inrichting van het beheer en de implementatie alvast gerealiseerd worden.

Het onderzoeksrapport is gedurende het project vaak bijgewerkt doordat sommige onderzoeksvragen onbeantwoord bleven door het wachten op personen of een organisatie. Bijvoorbeeld een hostingprovider, Motorola support of een collega. Ook lokte sommige resultaten nieuwe vraagstukken op die ook onderzocht moesten worden en gedurende het project werken toegevoegd.

9.2 Architectuurfase

In de architectuurfase werden het functioneel ontwerp en het adviesrapport beschreven. Om de benodigde informatie voor deze documenten te vergaren is er gebruik gemaakt van de onderzoekresultaten. Ook is er overleg geweest met collega's voor het reviewen en beantwoorden van vragen. De concepten zijn door aanpassingen in het onderzoeksrapport gedurende het project bijgewerkt om uiteindelijk tot een definitieve versie te komen.

9.3 Ontwerpfase

In de ontwerpfase is het technisch ontwerp beschreven. Het technisch ontwerp is beschreven en net als het functioneel ontwerp gedurende het project bijgewerkt door wijzigingen in het onderzoek, of nieuwe vraagstukken.

9.4 Implementatiefase

De implementatiefase leverde een proof of concept van Managed Wi-Fi en (indien genoeg tijd) een Implementatieplan op. Een proof of concept is inmiddels opgeleverd. Om dit te realiseren is Managed Wi-Fi eerst in een omgeving opgebouwd, die bestond uit drie Lancom routers een controller en een aantal access points. Nadat het onderzoek voltooid was zijn de controllers verplaatst naar de testomgeving voor de proof of concept. hier zijn diverse tests op uitgevoerd, zoals een praktijktest. Het Implementatieplan is nog niet gerealiseerd omdat het onderzoek meer tijd koste dan gepland. Het Implementatieplan zal naar waarschijnlijkheid alsnog worden uitgewerkt, na het inleveren van de scriptie, en voordat de eindpresentatie plaatsvind.

9.5 Beheerfase

In de beheerfase zijn procedures en documenten opgeleverd voor de nazorg. Hiervoor zijn handleidingen en configuraties beschreven. Tevens heb ik collega's betrokken bij het project, zodat ook zij met het product kunnen werken na afsluiting van het project. Het overdragen zal een vervolg krijgen na het inleveren van de scriptie door het Implementatieplan, de procedures en handleidingen uit te breiden.

9.6 Plan van aanpak

Als het project vergeleken wordt met de eisen uit het plan van aanpak komt dit overeen. De deelvragen zijn door de scriptie heen beantwoord en alle punten uit de 'must have' van de scope zijn gerealiseerd. Daarnaast is het merendeel van de 'should have' afgrond. Ook zullen de punten die nog missen uit de 'should' have grotendeels worden gerealiseerd na het opleveren van de scriptie.

10 Bibliografie

Boeken.

Roel Grit, M. J. (2009). *Zo doe je een Onderzoek*. Groningen: Noordhoff Uitgevers.

Steehouder, M. (2006). *Leren Communiceren*. Enschede: Noordhoof Uitgevers.

Websites.

How To Motorola centralized Deployements. (2013). Opgehaald van Motorola Centralized Deployements: https://docs.symbol.com/manuals/WING5X_How_To_Centralized_Deployments_Rev_D.pdf

kettner, M. (2013, 11 26). *Check_MK*. Opgehaald van Mathias-kettner.de: http://mathias-kettner.de/check_mk.html

Nagios. (sd). Opgehaald van Nagios: http://www.nagios.org/

Linge, J. (sd). Opgehaald van NagVis: http://www.nagvis.org

Linge, J. (sd). Opgehaald van PNP4Nagios: http://www.pnp4nagios.org

Wensink, M. (2013, 7 1). *Afstudeerleidraad*. Opgehaald van Sharepoint: https://onderwijsteams.sharepoint.hu.nl/fnt/Cluster_ICT/afstuderen/Gedeelde%20documenten/Afstudeerleidraad%20Instituut%20voor%20ICT%20cursus%202013-2014.pdf

lumiad

Bijlagen

A. PVA

Plan van aanpak

Managed Wi-Fi & Monitoring

Naam:	Stefan van den Heuvel
Studentnummer:	1591945
E-mail:	stefanvandenheuvel@student.hu.nl
Bedrijf:	Lumiad
Telefoon:	06 534 172 39

Document status

Version	Datum	Wijzigingen	Auteur
1.0	19-08-2013	Eerste opzet document	Stefan van den Heuvel
2.0	13-10-2013	wijziging in formulering	Stefan van den Heuvel
3.0	17-10-2013	Definitieve versie	Stefan van den Heuvel

Document Informatie

Document type: Plan van aanpak
Bedrijf: Lumiad
Hoofdauteur: Stefan van den Heuvel

Inhoud

1 Inleiding

Lumiad plaatst bij het implementeren van een Wi-Fi netwerk de Wireless Lan Controller (WLC) altijd op locatie van de klant. Deze wordt gebruikt voor het gecentraliseerd beheren en bewaken van de verschillende access points. In deze situatie betaalt de klant zelf voor de WLC, en vindt het beheer plaats bij de klant.
Voor het project is er voorgesteld te onderzoeken wat de mogelijkheden zijn voor het fysiek verplaatsen van de WLC naar het interne netwerk van Lumiad, of naar een data center. Hierdoor kunnen er meerdere klanten door een enkele WLC beheert worden. Ook worden de kosten van de klant teruggedrongen doordat er niet meer betaalt hoeft te worden voor een eigen WLC. Daarnaast kan het beheer gecentraliseerd plaatsvinden bij Lumiad. Een bijkomend deelproject omvat het onderzoeken en inrichten van de monitoring voor Motorola apparatuur. Omdat Motorola flinke korting biedt op draadloze apparatuur is het voor Lumiad interessant geworden Motorola aan de monitoring toe te voegen.

De centrale hoofdvraag die bij dit onderzoek hoort is: ‘Op welke manier kunnen Managed Wi-Fi en de monitoring van Motorola door Lumiad worden ingezet?’

In dit plan staat beschreven waarom het project wordt uitgevoerd en welke werkzaamheden hiervoor nodig zijn. Daarnaast wordt beschreven met welke methoden en technieken het project uitgevoerd wordt en wat er opgeleverd gaat worden. Dit plan dient door mij, hogeschool Utrecht en Lumiad goedgekeurd te worden alvorens het project van start zal gaan. Het plan van aanpak zal gebruikt worden als naslag gedurende het traject. Mocht er een wijziging optreden zal het plan van aanpak worden geüpdatet, indien de docent-begeleider hier toestemming voor geeft. Tevens zullen de wijzigingen in het versiebeheer (te vinden op de eerste pagina) worden vermeld.

2 De context

In dit hoofdstuk volgt een beknopte omschrijving van het bedrijf. Daarnaast beschrijft het de relatie van het project met Lumiad, en de relaties met andere projecten.

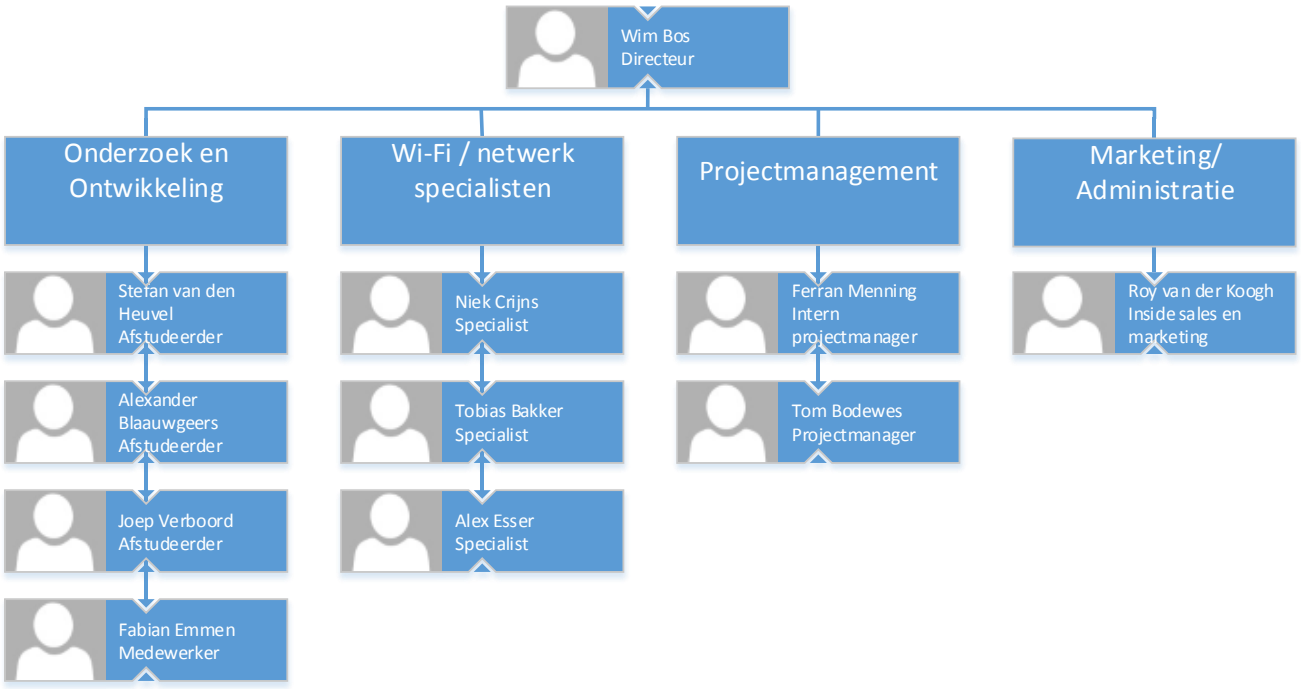
2.1 Het bedrijf Lumiad

Lumiad is een bedrijf dat gespecialiseerd is in draadloze oplossingen. Producten en diensten die zij leveren zijn onder andere in de richting:

- Netwerk infrastructuur
- Voice over IP
- Hotspot & Captive Portal
- Locatiebepaling (RTLS)
- Straalverbindingen (P2P)
- Management en Monitoring
- Netwerk beveiliging
- Wi-Fi Cursussen

Deze diensten levert Lumiad aan diverse klanten. Voorbeelden van enkele klanten zijn Schiphol, Creative Valley en Hogeschool Utrecht.

Lumiad bestaat uit elf personeelsleden en vier afdelingen. De afdeling 'Onderzoek en ontwikkeling', waar ikzelf onderdeel van uit maak, is voor parttimers, stagiaires en afstudeerders. Daarnaast is er een afdeling voor Wi-Fi en netwerkspecialisten, marketing en administratie, en een projectmanagement afdeling. Omdat het bedrijf klein is komt het vaak voor dat medewerkers taken van andere afdelingen overnemen.
In figuur 1 is weergegeven welke afdelingen Lumiad heeft en waar het personeel in onder verdeeld is.



Figuur 26- Organogram van Lumiad

2.2 De opdrachtgever

Het project kan worden beschouwt als een intern project omdat het wordt uitgevoerd in opdracht van Lumiad zelf. De verwachting van de opdrachtgever (Wim Bos) is het verkrijgen van een advies. Aan de hand van dit advies kan beslist worden of Managed Wi-Fi wordt ingezet, en of de monitoring aan het assortiment wordt toegevoegd.

2.3 Relatie tussen project en afdeling/organisatie

De opdracht wordt uitgevoerd onder de afdeling onderzoek en ontwikkeling. De uitkomst van dit project kan leiden tot een uitbreiding op de huidige productreeks van Lumiad.

2.4 Relaties met andere projecten

Een project welke binnenkort van start zal gaan is voor het automatiseren van de radiusconfiguratie d.m.v. een applicatie. Een relatie tussen deze projecten is dat beide te maken hebben met monitoring. Hiervoor is overleg en afstemming nodig.

3 Positie, taken en verantwoordelijkheden van de student

Mijn rol in dit project is adviseur. Ik zal het onderzoek zelfstandig uitvoeren en hier een advies over uit brengen. Daarnaast zal er een demo gegeven worden door middel van een proof of concept (POC).

Voor technische vragen en sturing kan ik terecht bij mijn afstudeerbegeleider en de andere specialisten binnen Lumiad. Voor vragen over financiën kan ik terecht bij projectmanagement en marketing/administratie.

4 De opdracht

In dit hoofdstuk wordt de opdracht beschreven.

4.1 Probleembeschrijving

Momenteel worden Wi-Fi netwerken door Lumiad geïmplementeerd met een WLC op locatie van de klant. Deze WLC zorgt voor het beheer en de bewaking van de draadloze apparatuur voor dat netwerk. Voor de klant is het aanschaffen en goed configureren van de WLC een tijdrovende en prijzige oplossing. Zeker als het klantnetwerk maar over enkele access points beschikt. Daarnaast moet het beheer op locatie van de klant gedaan worden, en kost het implementeren van een Wi-Fi netwerk meer tijd dan nodig.

Omdat Motorola de laatste tijd flinke kortingen biedt op productaankopen is Lumiad netwerken van Motorola gaan implementeren bij klanten. De monitoring van Motorola is hierbij nog niet ingericht. Het is van belang dat dit wordt ingericht omdat monitoring bijdraagt aan de kwaliteit van het Wi-Fi netwerk. Lumiad heeft ook geen werkwijzen en procedures, waardoor er niet altijd tijdig gereageerd wordt op een incident.

4.2 Doelstellingen

De doelstellingen zijn opgesplitst in doelstellingen voor mij als student en doelstellingen voor Lumiad.

Doelstelling als student:

- Een advies leveren aan Lumiad voor het inzetten van Managed Wi-Fi en monitoring.
- Het inrichten van de monitoring met ondersteuning voor Motorola apparatuur.
- Slagen voor de afstudeeropdracht op HBO niveau.

Doelstelling vanuit Lumiad:

- Het beheer van een Wi-Fi netwerk goedkoper aan kunnen bieden door te zorgen dat de klant geen WLC hoeft aan te schaffen.
- Centraliseren van het beheer en verminderen van de kosten voor Lumiad door meerdere klanten op een enkele WLC te laten draaien.
- Een Wi-Fi netwerk sneller kunnen uitrollen.
- Kwaliteit leveren voor Wi-Fi netwerken door middel van monitoring.

4.3 Projectomschrijving

Voor de afstudeeropdracht worden de mogelijkheden voor het inzetten van Managed Wi-Fi onderzocht. Managed Wi-Fi houdt in dat de klant niet per se een WLC meer hoeft aan te schaffen maar alleen access points. De WLC draait dan intern in het netwerk bij Lumiad, of in een data center. Hierdoor kan de klantomgeving gecentraliseerd vanuit Lumiad beheert worden, en kunnen de diverse klanten van configuraties worden voorzien. Daarnaast wordt voor Motorola de monitoring ingericht. Er zal hierbij een onderzoek plaatsvinden om erachter te komen hoe de monitoring ingericht kan worden. Hierbij zullen ook procedures worden opgesteld om te zorgen dat het personeel kan werken met de nieuwe situatie.

4.4 Hoofd en deelvragen

In dit hoofdstuk zijn de hoofd en deelvragen van het project beschreven. De hoofdvraag is opgedeeld in een aantal deelvragen welke bijdragen aan het beantwoorden van de hoofdvraag.

De hoofdvraag luidt: ‘Op welke manier kunnen Managed Wi-Fi en de monitoring van Motorola door Lumiad worden ingezet?’

De bijhorende deelvragen luiden:

- Hoe wordt de remote verbinding tussen de access points en controller opgezet?
- Hoe worden verschillende klanten op een enkele controller beheert?
- Hoe kan Managed Wi-Fi bijdragen aan het sneller uitrollen van een Wi-Fi netwerk voor de klant?
- Hoe kan Managed Wi-Fi bijdragen aan het goedkoper aanbieden van het beheer van een Wi-Fi netwerk?
- Hoe kan Managed Wi-Fi zorgen voor gecentraliseerd beheer van een Wi-Fi netwerk?
- Hoe kan Managed Wi-Fi schaalbaar worden ingezet door Lumiad?
- Hoe kan de monitoring van Motorola worden ingericht?
- Hoe kan de monitoring efficiënter ingericht worden?

4.5 Afbakening

De afbakening zal gedaan worden m.b.v. MoSCoW. Deze methode beschrijft welke eisen er absoluut vereist zijn en welke aspecten juist niet onder het project vallen. Daarnaast laat deze methode ruimte over voor eventuele gewenste eisen.

- Must have: Dit geeft aan wat het project absoluut moet bevatten om een succes te zijn, zonder is het projectproduct niet bruikbaar.
- Should have: Dit zijn eisen die erg gewenst zijn maar niet noodzakelijk.
- Could have: Deze eisen zijn minder belangrijk maar toch wenselijk.
- Won't have: Deze eisen zullen niet meegenomen worden tijdens dit project.

	Nr.	Onderdeel
Must have	1	Plan van aanpak
	2	Scriptie
	3	Onderzoeksrapport
	4	Functioneel ontwerp
	5	Technisch ontwerp
	6	Proof of concept Managed Wi-Fi met Motorola & Motorola Monitoring
	7	Adviesrapport voor Managed Wi-Fi met Motorola en Motorola monitoring
Should have	8	Toevoeging van Managed Wi-Fi voor Lancom
	9	Adviesrapport voor koppeling tussen monitoring en het AFAS ticketsysteem
	10	Implementatieplan voor Managed Wi-Fi met Motorola
	11	Implementatieplan voor Managed Wi-Fi met Lancom
	12	Procedures voor beheer van Managed Wi-Fi
	13	Procedures voor beheer van de monitoring
Could have	14	Locatiebepaling van cliënts toevoegen aan Motorola Monitoring
	15	Proof of concept met koppeling tussen monitoring en het AFAS ticketsysteem
	16	Definiëren, uitwerken en documenteren van vervolgprojecten.
	17	Kosten baten analyse voor Managed & Wi-Fi
	19	Kosten baten analyse voor Motorola Monitoring
	20	Medewerkers trainen
Won't have	21	Inrichten van klantomgevingen met Managed Wi-Fi
	22	Managed Wi-Fi voor andere merken als Lancom en Motorola
	23	Monitoring voor andere merken als Motorola
	24	Onderzoek doen naar een nieuw monitoringssysteem

4.6 Projectproducten

De onderstaande opsommingen geven weer welke producten worden opgeleverd, tijdens of na het project. De eerste tabel geeft weer welke producten er aan Lumiad worden opgeleverd. De tweede tabel welke producten er aan school worden opgeleverd. Wanneer welk product wordt opgeleverd is te vinden in de planning en deadlines (H12.1).

Lumiad na oplevering van het project de onderstaande producten in ontvangst nemen.

- Plan van aanpak
- Onderzoeksrapport
- Functioneel ontwerp
- Technisch ontwerp
- Proof of concept Managed Wi-Fi
- Proof of concept monitoring met Motorola
- Adviesrapport
- Implementatieplan (Should have)
- Procedures voor managed Wi-Fi en monitoring

Projectproducten voor school:

- Plan van aanpak
- Scriptie

Bovenstaande documenten zullen als bijlage worden meegenomen in de scriptie.

4.7 Projectaanpak

Het project wordt verdeelt in een aantal fasen. De fasen bestaan uit een analyse, architectuur, ontwerp, implementatie en beheerfase. In de analysefase zal het onderzoek gedaan worden. Aan de hand van dit onderzoek kan de architectuur fase van start gaan. Hierna volgt de ontwerpfase waarin een technisch ontwerp wordt opgesteld. Na deze fase zal de implementatiefase een proof of concept en een implementatieplan opleveren. Afsluitend is er de beheerfase welke de procedures zal omschrijven voor het verdere beheer.

Per fase zullen de volgende documenten worden gemaakt:

Analyse

- Plan van aanpak
- Onderzoeksrapport

Architectuur

- Functioneel ontwerp
- Adviesrapport

Ontwerp

- Technisch ontwerp

Implementatie

- Proof of concept managed Wi-Fi
- Proof of concept monitoring via Motorola
- Implementatie plan (Should have)

Beheer

- Procedures voor managed Wi-Fi en monitoring

4.7.1 Middelen

Dit project vereist middelen voor het onderzoeken, testen en bouwen van een Proof of concept. Deze zijn door Lumiad al beschikbaar gesteld in een testomgeving. Dit project heeft geen budget nodig omdat de middelen die nodig zijn voor onderzoek en testen al beschikbaar zijn. Eventuele onverwachte kosten zullen in overleg met Wim Bos besproken worden. Hieronder is een inventarisatie van de benodigde middelen te vinden.

Hardware			
Nr.	**Voorwerp**	**Onderdeel**	**Doel**
1	Motorola WLC	1a	Opzetten en testen van Managed Wi-Fi. Hierbij communiceert de WLC met de access points over het internet.
		1b	Opzetten en testen van de monitoring.
2	Lancom WLC	2a	Opzetten van Managed Wi-Fi. Hierbij communiceert de WLC met de access points over het internet.
3	Motorola Access points	3a	Opzetten van Managed Wi-Fi. Hierbij communiceert de WLC met de access points over het internet.
		3b	Opzetten en testen van de monitoring.
4	Lancom Access points	4a	Opzetten van Managed Wi-Fi. Hierbij communiceert de WLC met de access points over het internet.
Hardware			
Nr.	**Voorwerp**	**Onderdeel**	**Doel**
5	Check_MK	5a	Toevoegen van Motorola monitoring aan Check_MK
		6b	Toevoegen van features
6	Wireshark	7a	Bekijken van het Managed Wi-Fi & Monitoringsverkeer

5 Planning en deadlines

In de onderstaande tabel is de planning te vinden die per week laat zien welke activiteiten er uitgewerkt zullen worden.

		Weeknummer																							
Inleverdata	Activiteit	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	1	2	3	4
18-10-2013	PVA																							
25-10-2013	onderzoeksrapport																							
27-09-2013	PVA voor Oekraïne opstellen																							
24-11-2013	implementeren POC monitoringsdeel																							
08-11-2013	Functioneel ontwerp																							
08-11-2013	Technisch ontwerp																							
24-11-2013	POC Managed Wi-Fi opstellen en uitvoeren																							
08-12-2013	Adviesrapport																							
01-11-2013	Scriptie deel analyse																							
17-12-2013	Scriptie compleet																							
17-01-2013	Presentatie voorbereiden																							
13 / 24-01-2013	Afstudeerzitting																							

5.1 Deadlines

In dit hoofdstuk is een opsomming vinden van de door de afstudeercommissie opgestelde deadlines en de deadlines binnen Lumiad.

School		
Datum/tijd	**Product**	**Distributie**
18-10-2013	Plan van aanpak met contract	• Afstudeeradministratie • Bedrijfsbegeleider • Docent-begeleider • Student
17-12-2013 12:00	Scriptie met bewijs van upload en beoordeling Inclusief alle documenten voor Lumiad als bijlage	• Afstudeercommissie • HBO Kennisbank • Student
13-01-2014 t/m 24-01-2014	Afstudeerzitting	• Eerste examinator • Tweede examinator • Bedrijfsbegeleider • Lid van CvT Student
Lumiad		
18-10-2013	Plan van aanpak met contract	• Bedrijfsbegeleider • Student
27-10-2013	Onderzoeksrapport	• Bedrijfsbegeleider • Student
08-11-2013	Functioneel ontwerp	• Bedrijfsbegeleider • Student
08-11-2013	Technisch ontwerp	• Bedrijfsbegeleider • Student
24-11-2013	Proof of concept	• Bedrijfsbegeleider • Student
08-12-2013	Adviesrapport	• Bedrijfsbegeleider • Student

6 Project risico's

Onderstaand tabel geeft de risico's weer samen met de maatregelen.

Risico nr.	Risico	Maatregel nr.	Maatregel
1	Een te grote projectomvang zorgt ervoor dat het onderzoek niet succesvol afgerond kan worden.	1A	Een scope opstellen met de minimale eisen, de wensen en wat niet wordt meegenomen in het project.
		1B	Voortgang bewaken met planning en bijsturen indien nodig.
2	Lumiad biedt mij onvoldoende tijd om mijn onderzoek succesvol uit te voeren.	2A	Aangeven wat er moet gebeuren en niet teveel andere taken aannemen.
		2B	Projecttaken prioriteit geven zodat ik binnen de planning blijf.
3	Opdrachtgever komt met nieuwe doelstellingen of doelstellingen die er tijdens het project bijkomen.	3A	Nieuwe doelstellingen voordragen als vervolgprojecten.
		3B	Eventuele nieuwe doelstellingen aan de scope toevoegen als wens (could of should have).

7 Bedrijf/persoonsgegevens

Lumiad
Plaats: De Meern
Adres: Veldzigt 24
Tel: 030-7670670
E-mail: info@lumiad.nl

Hogeschool Utrecht
Plaats: Utrecht
Adres: Nijenoord 1
Tel: 088-4818283
E-mail: info@hu.nl

Afstudeerbegeleider
Naam: Tobias Bakker
Mobiel: 06 81 412 284
Tel: 030-7670634
E-mail: tbakker@lumiad.nl

Schoolbegeleider
Naam: Don Dijkstra
Mobiel: 06 23 345 099
E-mail: don.dijkstra@hu.nl

Student
Naam: Stefan van den Heuvel
Mobiel: 06 53 417 239
E-mail: stefan.vandenheuvel@student.hu.nl

8 Bibliografie

How To Motorola centralized Deployements. (2013). Opgehaald van Motorola Centralized Deployements: https://docs.symbol.com/manuals/WING5X_How_To_Centralized_Deployments_Rev_D.pdf

kettner, M. (sd). *Check_MK*. Opgehaald van Check_MK: http://mathias-kettner.de/check_mk.html

McCabe. (2012). *SYNA Systeem en netwerk architectuur*. Opgehaald van Sharepoint: https://cursussen.sharepoint.hu.nl/fnt/46/TCSB-V2DSM1-12/default.aspx?RootFolder=%2Ffnt%2F46%2FTCSB-V2DSM1-12%2FStudiemateriaal%2FSYNA%20%28SYSTEEM%20EN%20NETWERKARCHITECTUUR%29&FolderCTID=0x0120004833E130AB299C409F801E7A10A61934&View={EB34723D-6B12-4E20-

Nagios. (sd). Opgehaald van Nagios: http://www.nagios.org/

Wensink, M. (2013, 7 1). *Afstudeerleidraad*. Opgehaald van Sharepoint: https://onderwijsteams.sharepoint.hu.nl/fnt/Cluster_ICT/afstuderen/Gedeelde%20documenten/Afstudeerleidraad%20Instituut%20voor%20ICT%20cursus%202013-2014.pdf

B. Evaluatie eigen functioneren

Mijn eigen functioneren gedurende dit project kent positieve en negatieve eigenschappen. Ik vond mezelf in dit project communicatief sterk. Ik heb namelijk veel belanghebbende bij dit project betrokken om de bedrijfsbelangen en knelpunten duidelijk te krijgen. Daarnaast heb ik partijen bij dit project betrokken om advies te krijgen op vraagstukken, zoals hostingproviders en supportafdelingen.

Ook heb ik een uitbesteding voor het ontwikkelen van de monitoring moeten aansturen. Hiervoor heb ik functionele eisen moeten vertalen naar een concrete plannen, die overgedragen moesten worden aan het ontwikkelteam in Oekraïne. Deze uitbesteding heb ik in fasen verdeeld en goed gepland, waardoor er nu een goede basis ontwikkeld is voor de monitoring. De aansturing is naar mijn mening erg goed gegaan.

Wat voor mijn gevoel ook goed ging was het organiseren van het onderzoek. Voor de analyse heb ik voorgesteld mee te helpen met projecten, die betrekking hadden op het afstudeerproject. Zo heb ik onder andere praktijkervaring opgedaan in het beheren van een klantomgeving, door het lopen van een site survey. Ook heb ik meegeholpen aan een implementatie van een draadloos netwerk met Lancom in een ziekenhuis. Deze kennis heb ik kunnen gebruiken om de huidige situatie in het onderzoek te kunnen beschrijven en conclusies uit te halen.

Waar ik aan het begin van dit project moeite mee had was het proces denken. Ik had in het begin erg de neiging om de technische kant op te gaan en direct de infrastructuur te gaan bouwen. Nadat ik dit geconstateerd had heb ik een stapje terug gedaan en ben begonnen aan een analyse van de huidige werkwijzen. Na deze analyse ben ik breder na gaan denken over oplossingen. In plaats van enkel onderzoeken hoe de apparatuur technisch in elkaar zit ben ik gaan nadenken over hoe de oplossing kan bijdragen aan de processen voor het beheer, de monitoring en de implementatie van een draadloos netwerk. Hiermee het ik voor mijn gevoel het project naar een hoger niveau getild.

Daarnaast had ik in het begin van het project ook veel moeite om ‘nee’ te zeggen tegen niet-project gerelateerde werkzaamheden. Sommige weken was ik meer dagen met andere werkzaamheden bezig als met het afstudeerproject. Om dit op te lossen heb ik mensen ingelicht over mijn situatie, het doel van het afstudeerproject en de deadlines, waarna ik gelukkig meer tijd kreeg voor de opdracht.

Wat ik heb geleerd tijdens het afstudeertraject is om in het vervolg voorafgaande een project start meer tijd te steken in het uitdenken van het doel en de verschillende oplossingen. Nu had ik erg de neiging om snel aan het bouwen van een product te beginnen.

Al om al vind ik dat het project georganiseerd is uitgevoerd en dat ik tot een goede aanbeveling heb gedaan. Het bedrijf is ook blij met de aanbeveling en zij zullen dit ook zeker in acht nemen. Het project heeft nog uitbreidingsmogelijkheden. Zo kan Managed Wi-Fi nog worden opgezet met andere merken. Ook kan er de monitoring nog uitgebreid worden.

C. Verklarende woordenlijst

Term	Definitie
Access point	een access points is een apparaat die andere apparaten (bijvoorbeeld een laptop of telefoon) verbinding laat maken met een draadloos netwerk.
Captive portal	Een Captive Portal forceert een gebruiker op het netwerk met een webpagina voordat de gebruiker op het netwerk kan. Dit is meestal voor authenticatie of marketing doeleinde.
Check_MK	Check_MK is een op Nagios gebaseerde plug-in voor het monitoren van systemen.
Cluster	Een cluster bestaat uit meerdere apparaten die met elkaar verbonden zijn voor een betere prestatie of hogere beschikbaarheid.
Demilitarized Zone (DMZ)	Een demilitarized zone is een netwerksegment dat zich tussen het interne en externe netwerk bevindt (internet) en voor de buitenwereld volledig toegankelijk is.
fat access point	Een fat access point kan geconfigureerd worden, en blijft het draadloos netwerk uitzenden zonder dat er een controller benodigd is.
Internet Protocol Security (IPsec)	Internet Protocol Security (IPsec) is een standaard voor het beveiligen van het internetprotocol (IP) door middel van encrypties op de IP-pakketten.
ISO	Een digitale copy van een CD of DVD
Management Information Base (MIB)	Een Management Information Base (MIB) is een collectie van hiërarchie informatie over systemen die kan worden benaderd via SNMP.
Medium Independent Network Transport (MINT)	Medium Independent Network Transport (MINT) is een protocol die door Motorola controllers en access points word gebruikt om een link voor datacommunicatie op te bouwen.
Multi Protocol Label Switching (MPLS)	Multi Protocol Label Switching (MPLS) is een protocol om om data over een computernetwerk te transporteren
Nagios	Nagios is een opensourcecomputersysteem en netwerksurveillance-applicatie. Het houdt servers en services in de gaten die men specificeert en stuurt berichten als er dingen stuk gaan en wanneer services of servers die stuk waren weer beter gaan functioneren.
NagVis	NagVis is een op Nagios gebaseerde visualisatie plugin.
Object Identifiers (OID)	Een Object Identifier (OID) identificeert de objecten in de MIB hiërarchie.
Open Monitoring Distribution (OMD)	Open Monitoring Distribution is een bundeling van Nagios inclusief de belangrijkste plugins in een enkele installatie.
Open source	Open source code geeft de eindgebruiker vrije toegang geeft tot de bronmaterialen van het eindproduct, de bron kan hierdoor aangepast worden.
OSI-model	Het OSI-model is een gestandaardiseerd referentiemodel voor datacommunicatiestandaarden.
PNP4Nagios	PNP4Nagios is een op Nagios gebaseerde plugin die performance data opslaat in een database.
Port forwarding	Port forwarding is het doorsturen van TCP-of UDP-pakketten door een NAT-gateway door middel van poortnummers.
RF-domain	Een RF-domain is een geografische locatie die uit een één of meerdere access points bestaat. Administrators kunnen hierdoor

	per locatie een gezamenlijke configuratie instellen.
RF-domainmanager	Een RF-domainmanager is het access point die namens een geografische locatie, bestaande uit één of meerdere access points met de controller communiceert.
Simple Network Management Protocol (SNMP)	protocol voor netwerkbeheer en het beheer van de randapparaten in een netwerk. Hiermee kan de netwerkbeheerder informatie naar een systeem schrijven of van een systeem aflezen.
Site survey	Bij een site survey worden de specificaties van een draadloze netwerk gemeten m.b.v. een softwareprogramma en een draadloze netwerkadaptor.
STMP	Simple Mail Transfer Protocol (SMTP) is een standaard protocol voor het versturen van e-mail over het internet.
Thin access point	Thin access point - Een thin access point kan zonder controller niet geconfigureerd worden, en stopt met het uitzenden van het draadloze netwerk als de verbinding met de controller verbreekt. Als een thin access point een verbinding heeft met een controller, beschikt het access point over dezelfde functionaliteiten als een fat access point.
Virtual LAN (VLAN)	Een VLAN bestaat uit één of meerdere apparaten die zich in een gemeenschappelijk LAN bevinden, terwijl deze apparaten zich fysiek op meerdere locaties kunnen bevinden.
Virtueel Particulier Netwerk (VPN)	VPN creëert een vertrouwelijke Wide Area Netwerk verbinding tussen apparaten of locaties
VOIP	Bij Voice over IP(VoIP) wordt het internet of een ander netwerk gebruikt om spraak te transporteren.
Wireless Lan Controller (WLC)	Een Wireless Lan Controller (WLC) is een apparaat voor het configureren, updaten en bewaken van access points.

Functioneel ontwerp
Managed Wi-Fi & Monitoring

Naam:	Stefan van den Heuvel
Studentnummer:	1591945
E-mail:	stefanvandenheuvel@student.hu.nl
Bedrijf:	Lumiad
Telefoon:	06 534 172 39

Document status

Version	Datum	Wijzigingen	Auteur
1.0	15-10-2013	Eerste opzet document	Stefan van den Heuvel

Document Informatie

Document type: Plan van aanpak
Bedrijf: Lumiad
Hoofdauteur: Stefan van den Heuvel

lumiad

Inhoud

1 Inleiding

Dit document is het functioneel ontwerp voor Managed Wi-Fi. De eisen en wensen van Managed Wi-Fi worden hier beschreven. Tevens worden de middelen en kosten hier geïnventariseerd. Ook worden handelswijzen beschreven voor het implementeren van een draadloze netwerk omgeving ingericht met Managed Wi-Fi. Hiervoor is onder andere een vragenlijst en acceptatietest gemaakt. Tot slot zijn er handelswijzen voor het reageren op een incident of wijzigingsverzoek vastgelegd.

2 Wensen, eisen

In het onderstaande schema zijn de eisen om Managed Wi-Fi schaalbaar voor Lumiad te implementeren vastgelegd.

- De klanten moeten centraal beheerd kunnen worden vanuit Lumiad
- De Managed Wi-Fi omgeving moet gemonitord kunnen worden
- Er moet een vellige verbinding tot stand komen over het internet
- Managed Wi-Fi moet toepasbaar zijn voor 50 klanten met gemiddeld 15 access points

Wensen

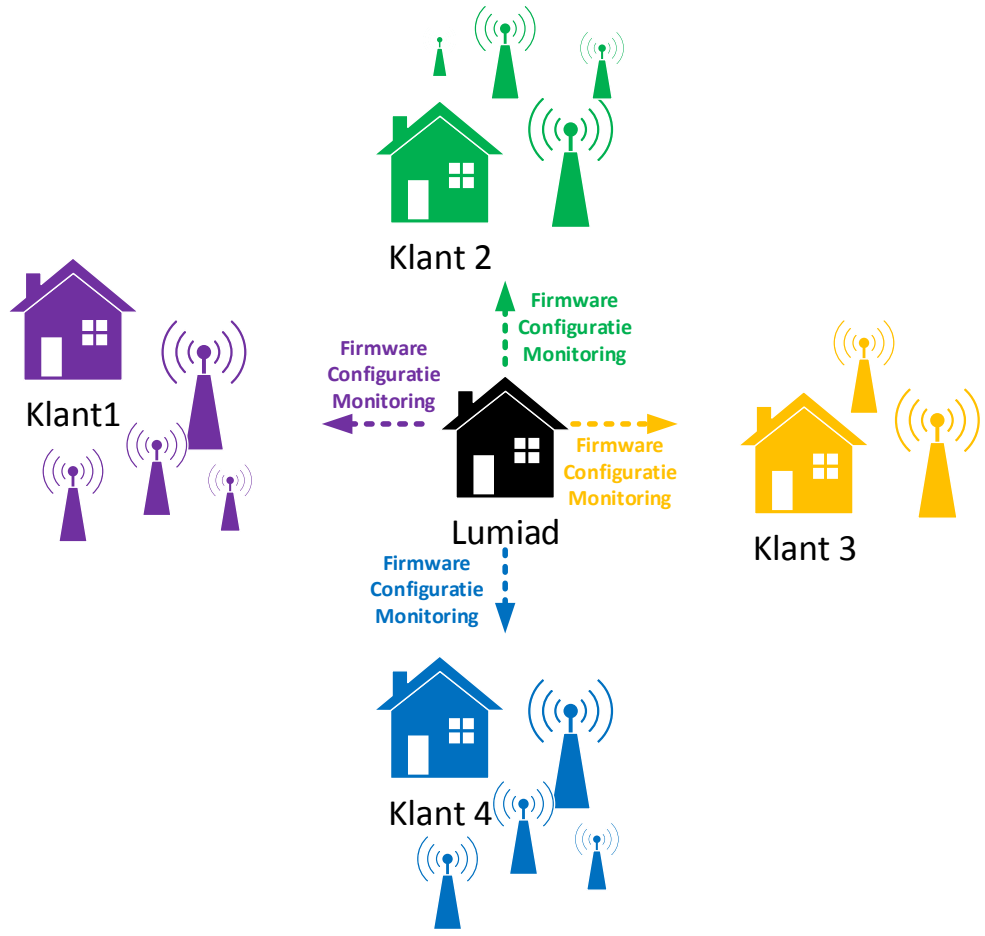
- Managed Wi-Fi zou toepasbaar kunnen worden gemaakt voor diverse soorten klantomgevingen
    - Omgevingen met veel draadloze clients (Bijvoorbeeld een theater, horeca, of school)
    - Omgevingen met weinig draadloze clients (Bijvoorbeeld een kantoor of winkeltje met enkele draadloze scanners)
- Als het mogelijk is zou de klantomgeving door kunnen draaien zonder verbinding met Lumiad
- Configuratiedocumentatie is gewenst
- Stappenplannen voor de implementatie is gewenst
- Stappenplannen voor het beheer is gewenst
- Stappenplannen voor de monitoring is gewenst

3 Managed Wi-Fi

Managed Wi-Fi is het kunnen beheren van de access points op een remote locatie vanuit een centraal punt Door dit schaalbaar in te zetten kan Lumiad de verschillende klanten gecentraliseerd beheren. Tevens kan hier monitoring op worden toegepast. Figuur 1 geeft Managed Wi-Fi weer. Voor de klant kan Managed Wi-Fi meerdere voordelen hebben.

Voordelen voor de klant:

- Goedkoper een draadloos netwerk kunnen implementeren
- Een snellere implementatie
- De klant heeft zelf geen kennis nodig van draadloze netwerken
- Monitoring op het draadloze netwerk
- Support bij storing of vragen



Figuur 27- Managed Wi-Fi

4 Middelen en kosten

Voor het opzetten van Managed Wi-Fi zijn bij Lumiad de volgende middelen benodigd:

Aantal	Middel	Doel
2	Controllers	• Diverse klanten voorzien van configuratie en firmware • Clusteren
1	Internet verbinding	• De klanten te bereiken over het internet
2	Publieke IP adressen	• Om beide controllers over het internet te laten communiceren
1	Datacenter	• Ruimte in een data center voor de controller
1	Hostingprovider	• Uitwijklocatie

Bij de klant zijn de volgende middelen benodigd:

Aantal	Middel	Doel
1	Access points	• Minimaal 1 access point om een tunnel naar de Lumiad controller te kunnen opbouwen
1	Internet verbinding	• Lumiad te kunnen bereiken over het internet

De kosten voor Lumiad voor de implementatie en het beheer van Managed Wi-Fi zijn:

- Aanschafskosten voor twee controllers
- Aanschafskosten voor apparatuur in bruikleen
- Aanschafskosten voor firmware
- Licentiekosten per access point

Voor de klant zijn de kosten voor implementatie als volgt:

- Aanschafskosten voor hardware of maandelijkse kosten voor bruikleen
- Maandelijkse kosten voor het beheer
- Eventueel maandelijkse kosten voor de monitoring

5 Implementatie

De eenmalige implementatie bij Lumiad

1. Controllers vestigen in het data center
2. Controllers vestigen in het uitwijklocatie
3. Controllers configureren met de basis voor Managed Wi-Fi
4. Switch configureren met VLANs voor Managed Wi-Fi
5. Internet router configureren met een IP masquerating
6. RF-domeinen en provisioning policy 's aanmaken voor klanten

5.1 Een klant toevoegen aan Managed Wi-Fi

1. Vragenlijst laten invullen (hoofdstuk 5.1.1)
2. een advies uitbrengen
    a. Welke type access points
    b. Welke scenario Managed Wi-Fi
    c. Locaties voor de access points
3. Factuur opstellen

Indien de klant akkoord gaat:

4. Klant access points of controller configureren
5. RF-domein en auto provisioning policy configureren in de Lumiad controller
6. Implementatie bij de klant
    a. Apparatuur scannen
    b. Apparatuur stickeren
7. Acceptatietest doorlopen (hoofdstuk 5.1.2)

5.1.1 Vragenlijst voor de klant implementatie

De vragenlijst draagt bij aan het adviseren van een klant. Bijvoorbeeld het typen access points.

Gegevens	
Klant:	
Contactpersoon:	
Adres:	
Tel. Nr	

Gebouw		
Naam gebouw:		
Openingstijden:		
Is er andere radiografische apparatuur aanwezig (zowel WiFi als niet-WiFi)?		☐ Nee
	* svp op plattegrond(en) aangeven	

Dekking			
Type:	☐ Data	☐ Spraak	☐ Video
Waar is dekking gewenst:			
	* svp op plattegrond(en) aangeven		
Zijn er speciale ruimtes welke van dekking moeten worden voorzien? (met speciale ruimtes worden bedoeld: koel/vriesruimtes, kluizen, gevaarlijke ruimtes, technische ruimtes)		☐ Nee	
	* svp op plattegrond(en) aangeven		
Dienen transportgebieden (trappenhuizen/liften) van dekking te worden voorzien? *(belangrijk voor voice)*		☐ Nee	
	* svp op plattegrond(en) aangeven		

Gebruik			
Hoeveel gebruikers worden er verwacht?	Minimaal:	Maximaal:	Gemiddeld:
Wat voor type apparaten worden er gebruik en in welke verhouding?	☐ Laptop ☐ Tablet/Smartphone ☐ WiFi Telefoon	% van totaal % van totaal % van totaal	
In welke ruimte(s) wordt bovengemiddeld gebruik verwacht? (denk aan vergader- en presentatieruimtes)*			
	* svp op plattegrond(en) aangeven		

5.1.2 Acceptatietest

Deze acceptatietest kan gebruikt worden bij de implementatie van een klant.

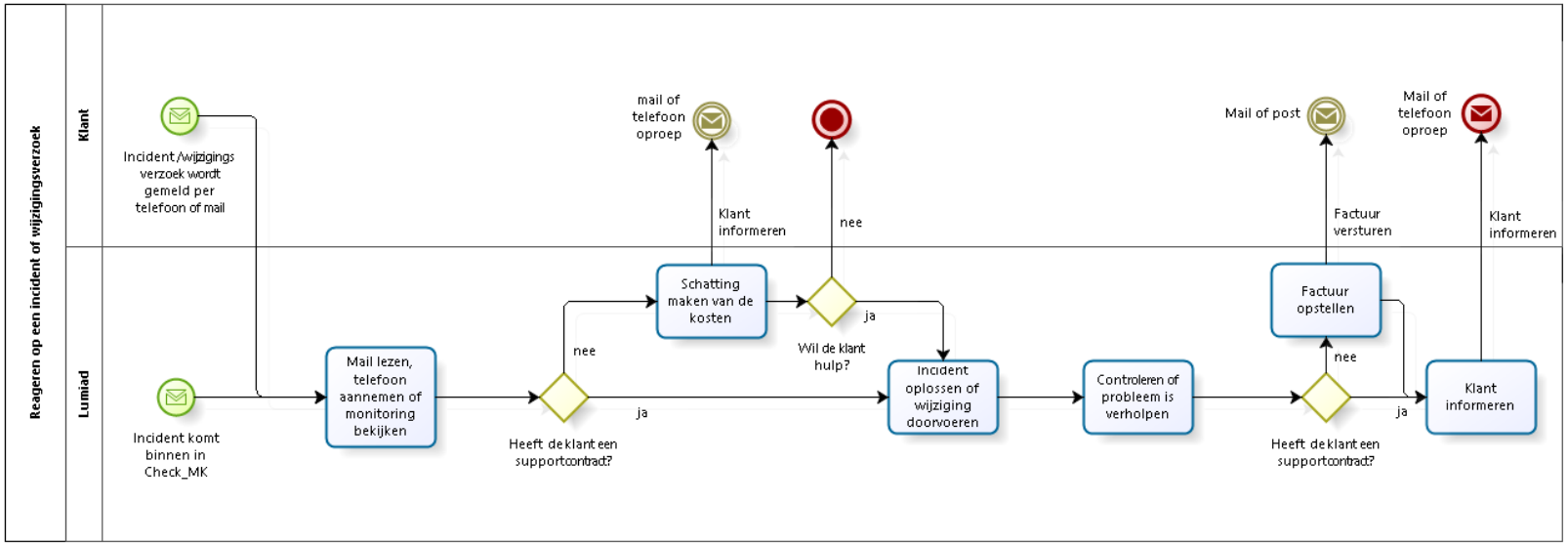
Test Nr.	Test	testmethode	Test door	Datum	✓	Remark
1	Adoptie	1. Log in op de web interface van het access points en controleer onder 'adoption' in de statistieken of het access point geadopteerd is. 2. Log in op de web interface van het access points en controleer onder 'health' in de statistieken of het access point de juiste firmware (huidige versie, WING 5.5) heeft. 3. Controller of de SSIDs worden uitgezonden zoals voorheen geconfigureerd op het RF-domein in de Lumiad controller				
1	Site survey (optioneel)	1. Doe een site survey met Ekahau om eventuele stoorbronnen te vinden, en statistieken als dekking per access point en access points locaties te rapporteren aan de klant				

6 Het beheer

Het beheer wordt gedaan vanuit de controllers bij Lumiad door het netwerkteam. Het netwerkteam bestaat uit:

- Niek Crijns
- Tobias Bakker
- Alex Esser (parttime)

De handelwijze is afhankelijk van het contract met de klant. De handelswijze is weergegeven in figuur 2 – beheer.



Figuur 28 - Beheer

Technisch ontwerp
Managed Wi-Fi & Monitoring

Naam:	Stefan van den Heuvel
Studentnummer:	1591945
E-mail:	stefanvandenheuvel@student.hu.nl
Bedrijf:	Lumiad
Telefoon:	06 534 172 39

Document status

Version	Datum	Wijzigingen	Auteur
1.0	15-10-2013	Eerste opzet document	Stefan van den Heuvel

Document Informatie

Document type: Plan van aanpak
Bedrijf: Lumiad
Hoofdauteur: Stefan van den Heuvel

Inhoud

1 Inleiding

Dit document is het technisch ontwerp voor het project Managed Wi-Fi. De technische specificaties zijn hierin uitgewerkt. De techniek achter Managed Wi-Fi wordt in dit document toegelicht. Vervolgens worden de benodigde elementen van Managed Wi-Fi toegelicht. Tevens wordt de topologie waarin Managed Wi-Fi wordt geïmplementeerd toegelicht d.m.v. een logisch en technisch ontwerp. Vervolgens wordt de applicatie architectuur weergegeven om de relatie tussen de verschillende componenten en belanghebbende weer te geven. Tot slot volgen er stappenplannen voor het implementeren van Managed Wi-Fi bij Lumiad en de klant samen met de gebruikte configuraties.

2 Managed Wi-Fi

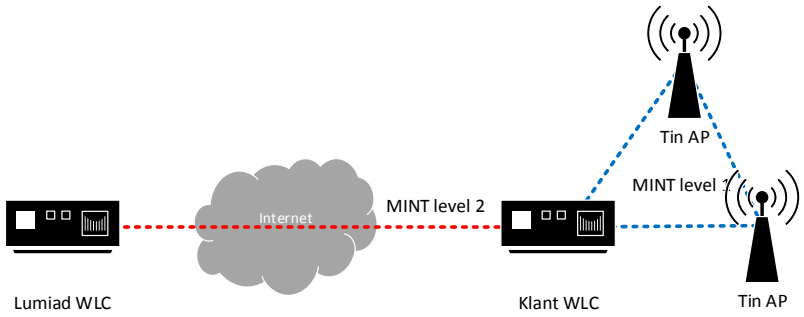
Managed Wi-Fi is het kunnen beheren van de access points op een remote locatie vanuit een centraal punt.

2.1 MINT

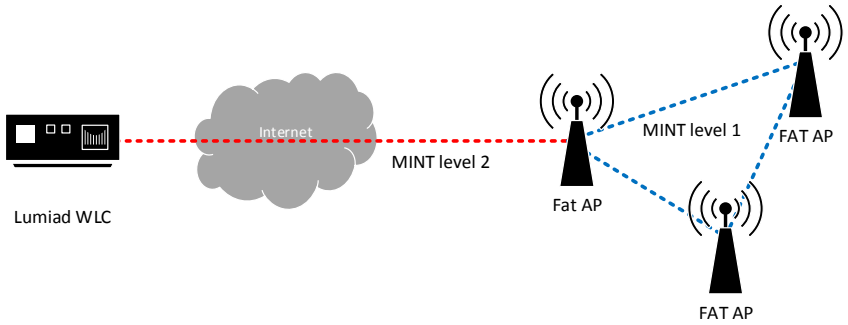
De adoptie en de data verbinding verlopen met het protocol MINT. MINT communiceert zowel op layer 2 als layer 3 van het OSI model.

MINT level 1 werkt op layer 2 van het OSI model. Dit protocol gebruikt ether-type 0x8783. Via het MAC adres communiceren de access points met elkaar in een LAN.
MINT level 2 werkt op layer 3 van het OSI model. Dit protocol gebruikt UDP port 24576. Op IP basis kan dit protocol communiceren over het internet.

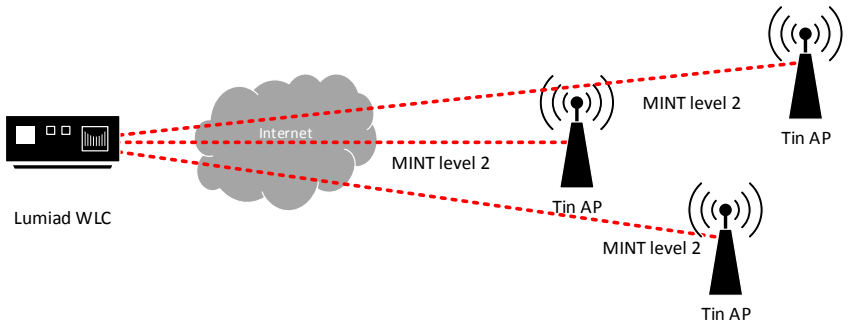
Deze techniek maakt het mogelijk meerdere access points uit een remote site te beheren via een enkele tunnel. Er is hierbij één controller of access point die via MINT level 2 communiceert met de controller bij Lumiad. De rest van de access points communiceren onderling op level 1. Hierdoor hoeft een configuratie of een firmwareversie maar naar een enkele access point gedistribueerd te worden. dit access point distribueert dit naar de access points in het LAN.



De klantcontroller communiceert op MINT level 2 met de controller bij Lumiad. De klantcontroller voorziet de tin access points op MINT level 1 van configuraties en firmware.



Een fat access point communiceert op MINT level 2 met de controller bij Lumiad. Het fat access point voorziet de overige fat access points op MINT level 1 van configuraties en firmware.

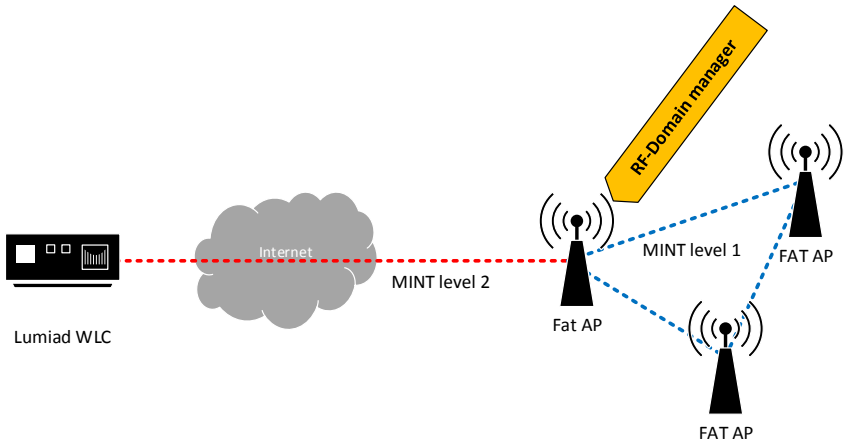


Een tin access point communiceert zonder controller op klantlocatie individueel met de controller bij Lumiad. Hierdoor zullen er meerdere tunnels ontstaan.

2.2 RF domain manager

Het access point die vanuit de remote site met de controller bij Lumiad communiceert wordt de RF domain manager genoemd. Taken van de RF-Domain manager zijn:

- De tunnel met de Lumiad controller tot stand te houden
- Het RF-Domain voorzien van configuraties
- Het RF-Domain voorzien van firmware
- Status informatie via SNMP door communiceren



De RF-domain manager wordt automatisch geselecteerd door een smart-RF calculatie. Tevens kan handmatig worden gekozen voor een specifieke RF-domain manager. In de configuratie kan een access point een bepaalde waarde krijgen. Degene met de hoogste waarde wordt de RF-domain manager.

3 Ontwerp

In dit hoofdstuk worden de middelen die nodig zijn voor Managed Wi-Fi beschreven. Eveneens worden de elementen beschreven die van belang zijn bij Managed Wi-Fi

3.1 Middelen

Aantal	Middel	Doel
2	Controllers	• Diverse klanten voorzien van configuratie en firmware • Clusteren
1	Internet verbinding	• De klanten te bereiken over het internet
2	Publieke IP adressen	• Om beide controllers over het internet te laten communiceren
1	Datacenter	• Ruimte in een data center voor twee controller

Bij de klant zijn de volgende middelen benodigd:

Aantal	Middel	Doel
1	Fat Access points Of Controller en tin access points	• Minimaal 1 access point om een tunnel naar de Lumiad controller te kunnen opbouwen • Minimaal 1 controller en 1 access points om een tunnel naar de Lumiad controller te kunnen opbouwen
1	Internet verbinding	• Lumiad te kunnen bereiken over het internet

3.2 Elementen

De onderstaande sub-hoofdstukken zijn elementen uit de controller die van belang zijn voor Managed Wi-Fi.

3.2.1 Profielen

Een profiel is een configuratie voor een specifiek model access point. Bijvoorbeeld voor het instellen van een radio op het profiel van de AP6522. Deze configuratie wordt nu toegepast op alle access points van het model AP6522.

3.2.2 RF-domeinen

Een RF-domein kan gebruikt worden voor een overschrijvende configuratie van een profiel. Een klant kan hierdoor bijvoorbeeld een specifieke configuratie krijgen per locatie, co-locatie of verdieping. In het RF-domein kan bijvoorbeeld een specifieke SSID en wachtwoord worden ingesteld als overschrijving op het profiel.

3.2.3 Device overrides

Tot slot zijn er configuraties voor een specifieke access point. Dit overschrijft zowel de configuratie van het profiel als de configuratie van het RF-domein. Hierdoor is het mogelijk om een access point een afzonderlijke configuratie te geven.

3.2.4 Auto provisioning policy

Een auto provisioning policy zorgt ervoor dat een access point in het juiste RF-domein terecht komt. Er kan hiervoor een regel worden geconfigureerd waarin staat: als het access point voldoet aan X dan moet deze naar het RF-domein X. De filter kan worden ingesteld op bijvoorbeeld een IP adres, een VLAN of een MAC Address. Het instellen hiervan is te vergelijken met een ACL.

3.2.5 Cluster

Er kan een cluster worden ingesteld tussen twee controllers of twee access points, van eenzelfde model. Het cluster kan bestaan uit maximaal twee controllers/access points. Het cluster kan active-active of active-standby zijn. Bij active-active worden de access points geloadbalanced tussen de twee controllers/access points. Bij active-standby neemt de clustermaster alle access points tot zich. Bij storing neemt de tweede controller/access point deze over. De configuratie tussen beide controllers wordt gesynchroniseerd. De synchronisatie vind plaats op MINT level 2.

3.2.6 Operations

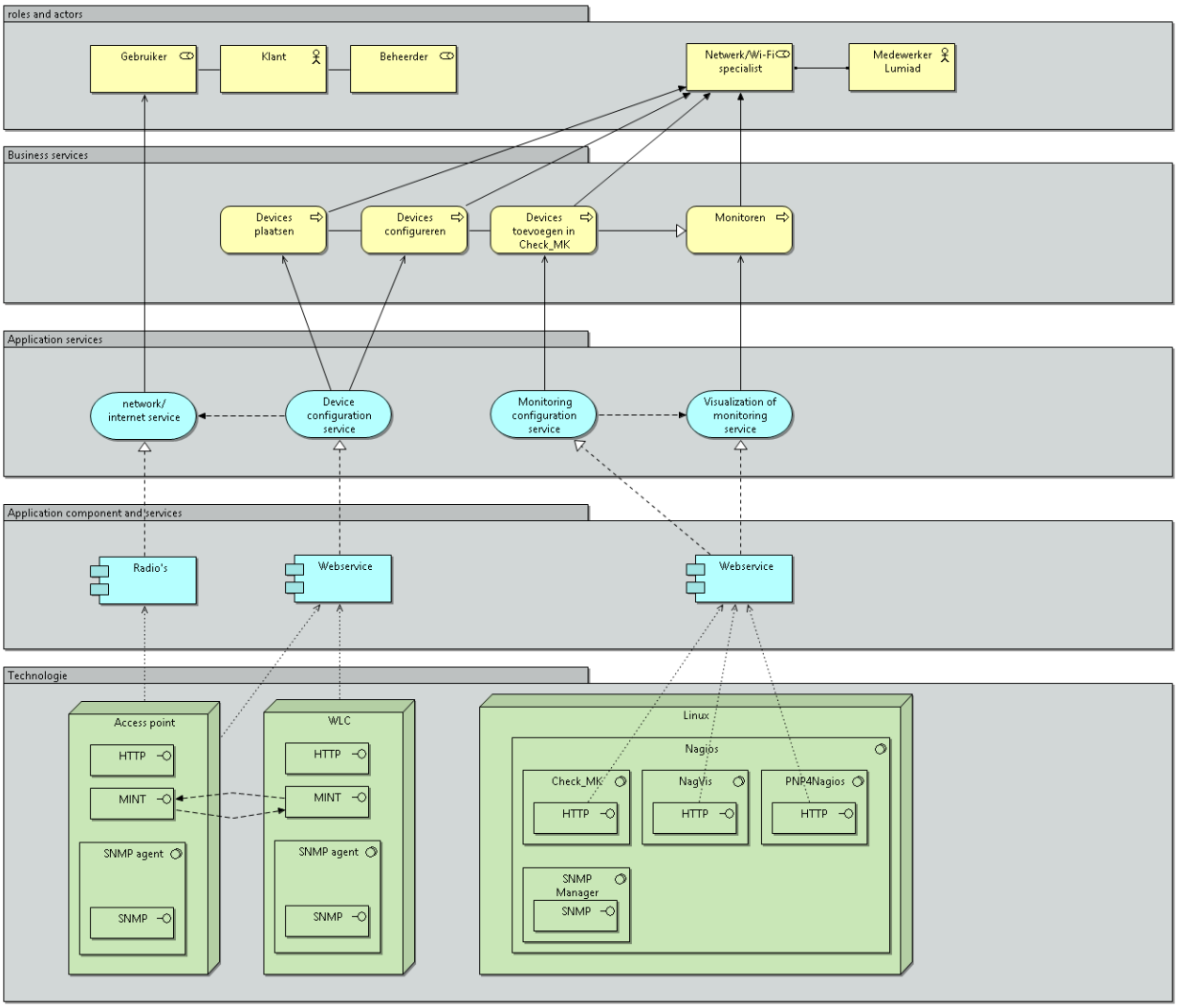
Operations is een functie in de controller waarmee firmware kan worden verstrekt. Ook kan de bestandmanagement van de verschillende access points vanaf hier worden benaderd.

3.2.7 Statistieken

De statistieken in de controller bieden een grafisch overzicht van de functionaliteiten op de controller. Hier kunnen bijvoorbeeld de geadopteerde access points worden bekeken. Welke radio's deze uitzenden, wat de namen zijn en welke clients er op ingelogd zijn is hier onder andere terug te vinden. Dit werkt op basis van het SNMP protocol tussen de controller is access points.

4 Applicatie architectuur

In de ontstaande tekening is de architectuur van Managed Wi-Fi en de monitoring weergegeven. Het doel hiervan is de relatie aan te geven tussen zowel de systemen als de rollen van de belanghebbende.



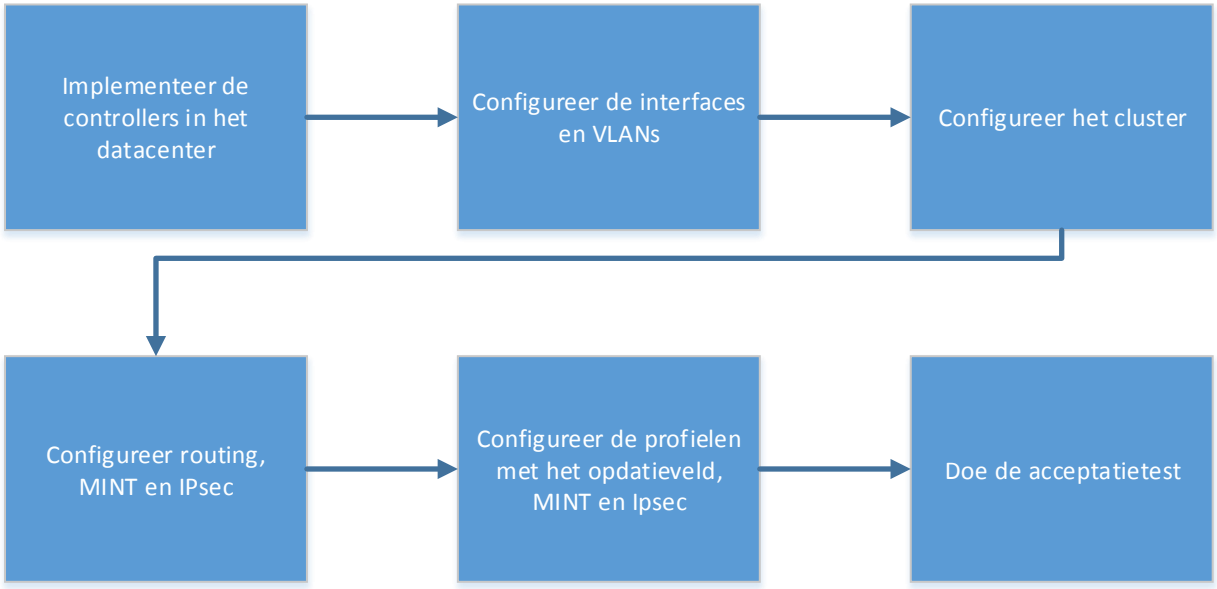
De access points zijn voorzien gebruikers van draadloos netwerk. De controller voorziet de access points van configuratie om te zorgen dat de gebruiker krijgt wat hij/zij wenst. De netwerkbeheerders van Lumiad implementeren het netwerk bij de klant. Tevens voegen zij de apparaten toe in Check_MK voor de monitoring en statistieken.

5 Stappenplannen

Dit hoofdstuk beschrijft de stappenplannen voor het configureren van de controllers en het toevoegen van een klant

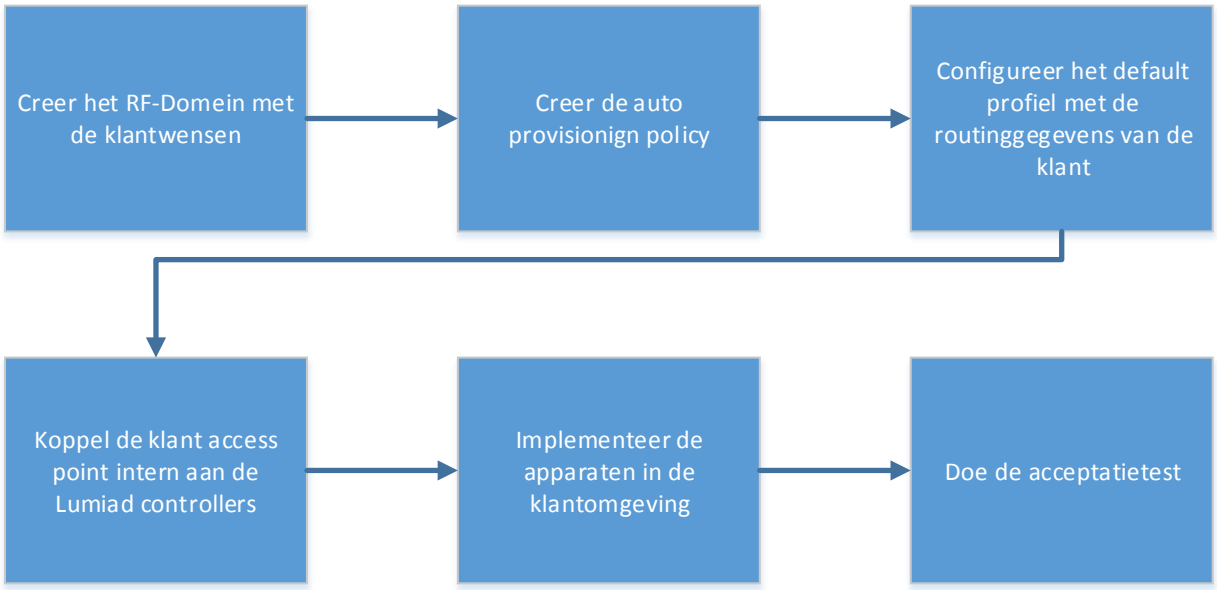
5.1 Configureren van de Lumiad omgeving

De onderstaande stappen dienen gevolgd te worden voor het implementeren van Managed Wi-Fi bij Lumiad.



5.2 Toevoegen van een klant

Voor het toevoegen van een klant dient het onderstaande stappenplan te worden gevolgd.



F. Projectplannen aan Oekraïne

Projectplan Monitoring v1

Naam:	Stefan van den Heuvel
Studentnummer:	1591945
E-mail:	stefanvandenheuvel@student.hu.nl
Bedrijf:	Lumiad
Telefoon:	06 534 172 39

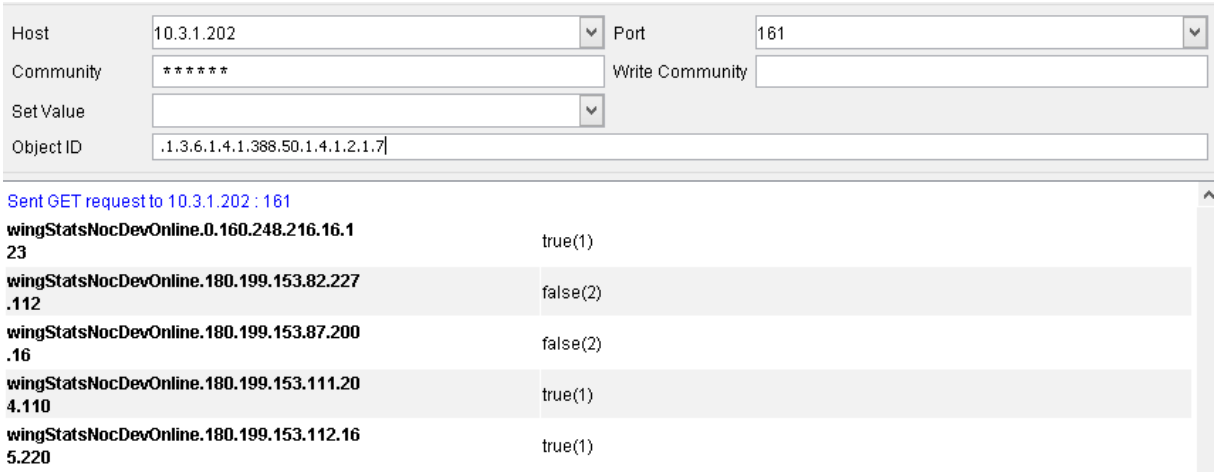
6 Motorola WLC checks

Check	OID	Example
Device information	.1.3.6.1.2.1.1.1	RFS4000 Wireless Controller, Version 5.4.2.0-030R MIB=01a
Device uptime	.1.3.6.1.2.1.25.1.1.0	14 days, 17 hours, 29 minutes, 29 seconds
WLC CPU utilization	.1.3.6.1.4.1.388.50.1.4.1.2.1.12 (it list the % CPU used over 10 minutes for the WLC and the AP's)	OK - 12.0% utilization in the last 5 minutes

In-active access points	.1.3.6.1.4.1.388.50.1.4.1.2.1.7 (false is in-active)	The number of in-active access points is 2
Active access points	.1.3.6.1.4.1.388.50.1.4.1.2.1.7 (true is in-active)	The number of active access points is 3
Expected access points	.1.3.6.1.4.1.388.50.1.4.1.2.1.7 (true and false are expected)	Expected access points is 5

The output of 'Active, in-active and expected access points' should be rebuilt to a number. True is active, false is in-active and true and false are the expected access points. For example, according to figure 1.

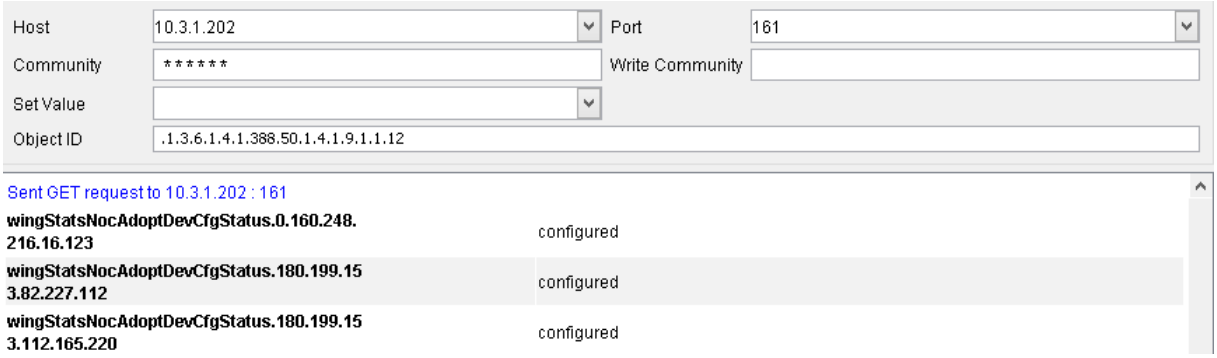
- Active access points = 3
- In-active access points = 2
- Expected access points = 5



Fugure 29. Active access points

Configured access points	.1.3.6.1.4.1.388.50.1.4.1.9.1.1.12	The number of configured devices is 3
Adapted access points	.1.3.6.1.4.1.388.50.1.4.1.9.1.1.12	The number of adapted access points is 0

Configured and Adapted access points should also be rebuilt to a number. Configured access point is the number shown in this list. For example see figure 2, which has a number of 3 configured access points.



7 Acces point checks

Check	OID	Example
Device uptime (historical)	.1.3.6.1.2.1.1.3	OK - up since Tue Aug 20 13:48:06 2013 (14d 00:05:15)
Clients per radio (one check per radio)	.1.3.6.1.4.1.388.50.1.4.3.2.8.1.1 .15	Clients radio1: 1 clients logged in Clients radio2: 1 clients logged in
Device information (type/version)	.1.3.6.1.2.1.1.1	AP622 Access Point, Version 5.4.2.0-030R
System name	.1.3.6.1.2.1.1.5	System name: ap622-52370E
System location	.1.3.6.1.2.1.1.6	The physical location of this node is: 3rd floor
Device CPU load (historical)	-- .1.3.6.1.4.1.388.50.1.4.2.2.1.1.8 (measured over 5min) -- .1.3.6.1.4.1.388.50.1.4.2.2.1.1.9 (measured over 10min) -- .1.3.6.1.4.1.388.50.1.4.2.2.1.1.1 0 (measured over 15min)	OK - 12.0% utilization in the last 5 minutes
Used SSIDs	.10.3.1.49	SSIDs: Moto, Moto2
Radio mode	.1.3.6.1.4.1.388.50.1.3.16.2.6.1. 1	2.4, 5GHz-wlan
Transmit power of radio's	.1.3.6.1.4.1.388.50.1.3.16.2.6.1. 3	Transmit power is 0
Radio's Signal	.1.3.6.1.4.1.388.50.1.4.2.25.10.1 .1.15	Radio1: Signal: -47
Raidio's Noise	.10.3.1.52	Radio1 Noise: -95

Combined in one check
Combined in one check

Projectplan Monitoring v2

Naam:	Stefan van den Heuvel
Studentnummer:	1591945
E-mail:	stefanvandenheuvel@student.hu.nl
Bedrijf:	Lumiad
Telefoon:	06 534 172 39

Inhoud

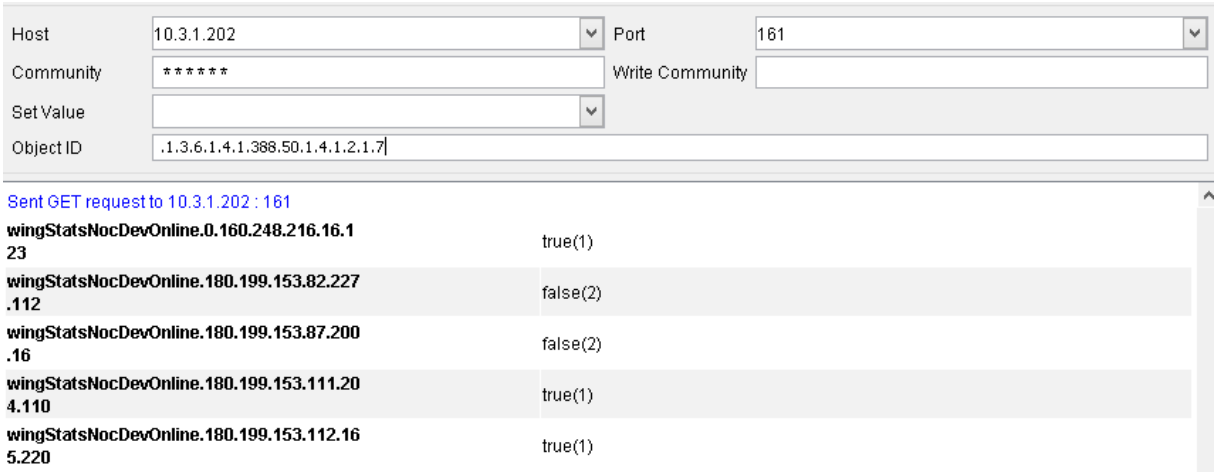
1 Motorola WLC checks

Check	OID	Example
Device information	.1.3.6.1.2.1.1.1	RFS4000 Wireless Controller, Version 5.4.2.0-030R MIB=01a
Device uptime	.1.3.6.1.2.1.25.1.1.0	14 days, 17 hours, 29 minutes, 29 seconds
WLC CPU utilization	.1.3.6.1.4.1.388.50.1.4.1.2.1.12 (it list the % CPU used over 10 minutes for the WLC and the AP's)	OK - 12.0% utilization in the last 5 minutes

In-active access points	.1.3.6.1.4.1.388.50.1.4.1.2.1.7 (false is in-active)	The number of in-active access points is 2
Active access points	.1.3.6.1.4.1.388.50.1.4.1.2.1.7 (true is in-active)	The number of active access points is 3
Expected access points	.1.3.6.1.4.1.388.50.1.4.1.2.1.7 (true and false are expected)	Expected access points is 5

The output of 'Active, in-active and expected access points' should be rebuilt to a number. True is active, false is in-active and true and false are the expected access points. For example, according to figure 1.

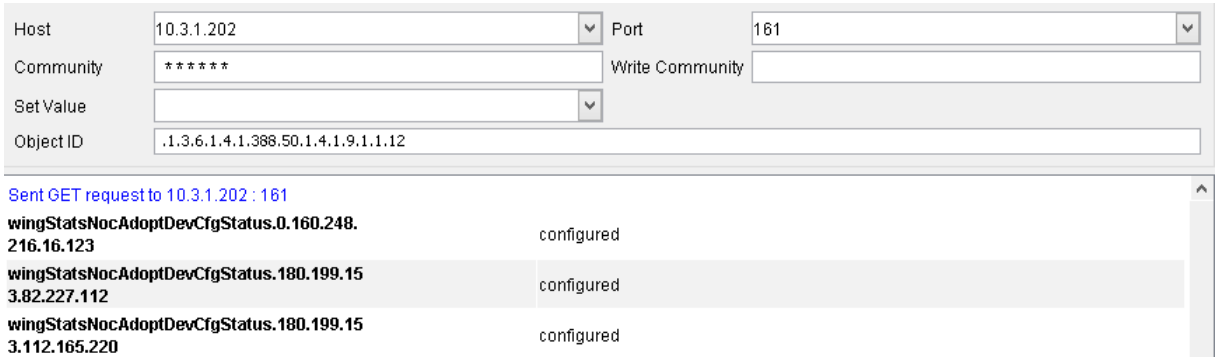
- Active access points = 3
- In-active access points = 2
- Expected access points = 5



Fugure 30. Active access points

Configured access points	.1.3.6.1.4.1.388.50.1.4.1.9.1.1.12	The number of configured devices is 3
Adapted access points	.1.3.6.1.4.1.388.50.1.4.1.9.1.1.12	The number of adapted access points is 0

Configured and Adapted access points should also be rebuilt to a number. Configured access point is the number shown in this list. For example see figure 2, which has a number of 3 configured access points.



2 Acces point checks

Check	OID	Example
Device uptime (historical)	.1.3.6.1.2.1.1.3	OK - up since Tue Aug 20 13:48:06 2013 (14d 00:05:15)
Clients per radio (one check per radio)	.1.3.6.1.4.1.388.50.1.4.3.2.8.1.1.15	Clients radio1: 1 clients logged in Clients radio2: 1 clients logged in
Device information (type/version)	.1.3.6.1.2.1.1.1	AP622 Access Point, Version 5.4.2.0-030R
System name	.1.3.6.1.2.1.1.5	System name: ap622-52370E
System location	.1.3.6.1.2.1.1.6	The physical location of this node is: 3rd floor
Device CPU load (historical)	-- .1.3.6.1.4.1.388.50.1.4.2.2.1.1.8 (measured over 5min) -- .1.3.6.1.4.1.388.50.1.4.2.2.1.1.9 (measured over 10min) -- .1.3.6.1.4.1.388.50.1.4.2.2.1.1.10 (measured over 15min)	OK - 12.0% utilization in the last 5 minutes
Used SSIDs	.10.3.1.49	SSIDs: Moto, Moto2
Radio mode	.1.3.6.1.4.1.388.50.1.3.16.2.6.1.1	2.4, 5GHz-wlan
Transmit power of radio's	.1.3.6.1.4.1.388.50.1.3.16.2.6.1.3	Transmit power is 0
Radio's Signal	.1.3.6.1.4.1.388.50.1.4.2.25.10.1.1.15	Radio1: Signal: -47
Raidio's Noise	.10.3.1.52	Radio1 Noise: -95

Combined in one check
Combined in one check

3 Features

Check_MK need the following features for Motorola:

- Client history
- Icon button to NagVis and AP/WLC web interface

The next chapters will explain the new features

3.1 Client history

Client history for Motorola should contain the following information:

Check	OID
Client name	.1.3.6.1.4.1.388.50.1.4.2.25.5.1.1.2
Client IP	.1.3.6.1.4.1.388.50.1.4.2.25.3.1.1.15
Mac	.1.3.6.1.4.1.388.50.1.4.2.25.3.1.1.1
Host	.1.3.6.1.4.1.388.50.1.4.2.4.1.1.1
AP location	.1.3.6.1.4.1.388.50.1.4.2.25.3.1.1.18
Vlan tag	.1.3.6.1.4.1.388.50.1.4.2.25.3.1.1.13
SSID	.1.3.6.1.4.1.388.50.1.4.2.25.3.1.1.10
SNR	.1.3.6.1.4.1.388.50.1.4.2.25.5.1.1.16
Noise	.1.3.6.1.4.1.388.50.1.4.2.25.5.1.1.15
RSSI	.1.3.6.1.4.1.388.50.1.4.2.25.5.1.1.14
Date of connection	-
Uptime	.1.3.6.1.2.1.25.1.1.0
IP WLC	.1.3.6.1.4.1.388.50.1.4.2.17.1.1.2 (obtain address via WLC name?)

An example of how the information should appear is shown in figure 2.

Client name	Client IP	Mac	Host	AP location	Vlan tag	SSID	SNR	Noise	RSSI	Date of connection	Uptime	Name WLC	IP WLC
Stefan_notebook	10.3.1.43	5c d9 98 bb 85 e6	ap622	De meern	1	Moto2	17	-68	-67	Mon Sep 9 09:53:55 2013	0d 0:11:59 Online	rfs4000	10.3.1.202
Tobias_notebook	10.3.1.42	5c d9 98 bb 85 e7	ap622	De meern	1	Moto2	17	-68	-67	Mon Sep 9 09:53:55 2013	0d 0:11:59 Online	rfs4000	10.3.1.202

Figure 31 – display client history

Also we need a filter to separate online and offline access points in the client history from Check_MK. This should be done in two extra buttons in the client history tab, as shown in figure 3.
This feature should be built under the 'client history tab' in client history. This new option allows us to have a beter view in long client history lists. The device state refers to the state of the AP, which the client is connected to. 'all' includes both, online and offline Aps. 'Online devices' includes online AP's and 'offline 'the offline AP's

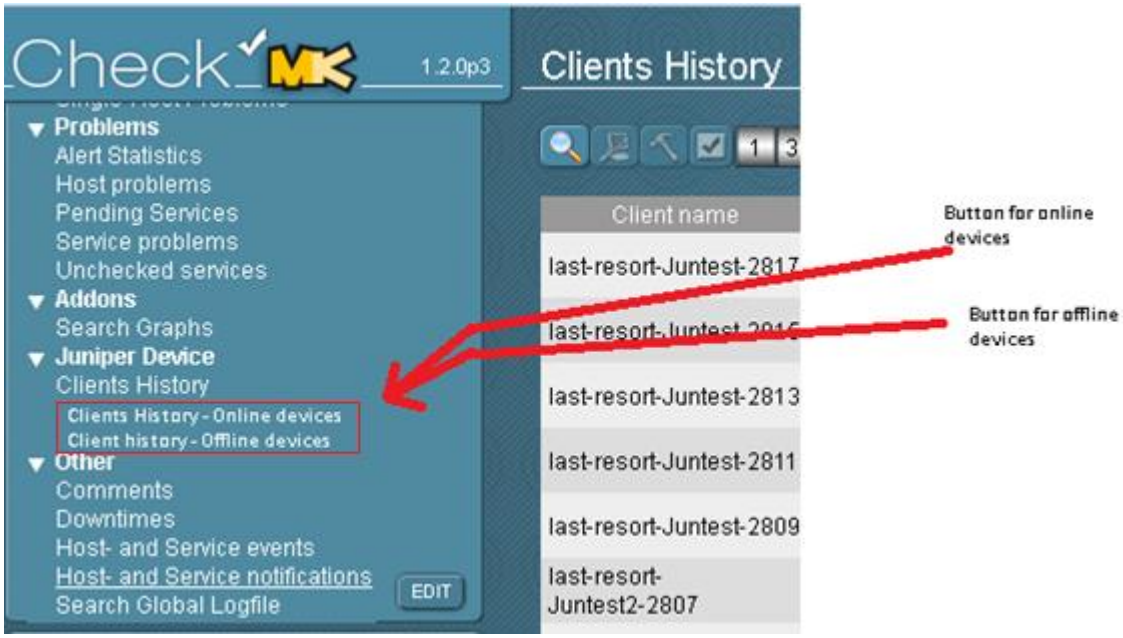


Figure 3 – device state

3.2 Icon button to NagVis and AP/WLC web interface

Check_MK needs two additional buttons for WLCs and APs. The first one for Nagvis should be a link to NagVis so we have a direct link to the drawing and can instantly see if the device is online/offline and to which devices the device is connected.
The second button should be a link to the web interface of the device. Preferably to HTTPS and if not available to HTTP. For example: AP_juniper needs an icon button to open the browser and the following URL ' https://10.3.1.77/'.
These two buttons should be placed under 'Icons' in every view. For example under 'all hosts' and under 'all services'. See (figure 4 – icons) for an example.

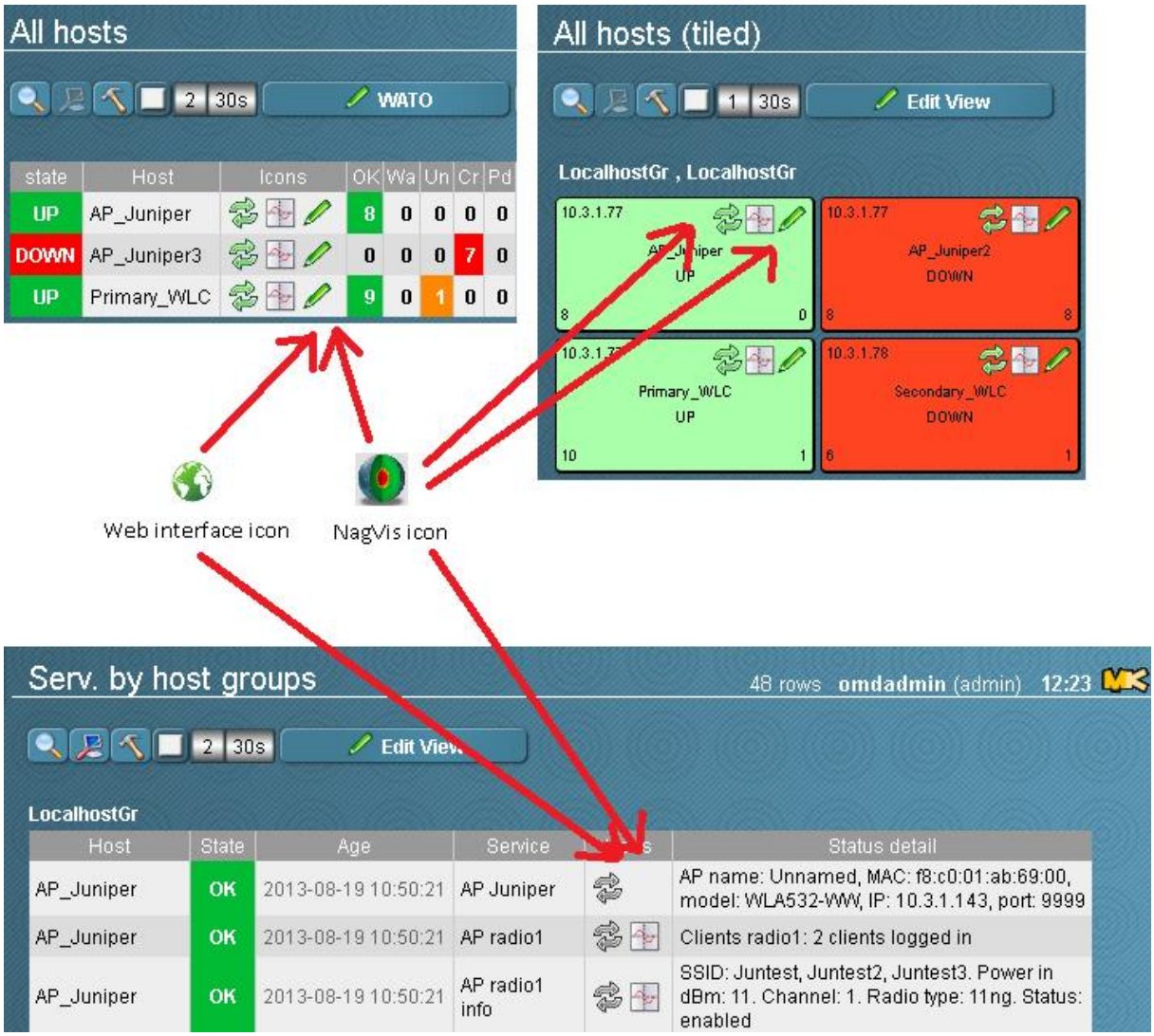


Figure 32 - icons

4 Additional checks

The following additional checks should be implemented to Check_MK:

4.1 Additional Access point checks

Check	OID	Example
Connected to WLC	.1.3.6.1.4.1.388.50.1.4.2.17.1.1.2	AP connected to WLC: rfs4000

Projectplan Monitoring v3

Naam:	Stefan van den Heuvel
Studentnummer:	1591945
E-mail:	stefanvandenheuvel@student.hu.nl
Bedrijf:	Lumiad
Telefoon:	06 534 172 39

Index

1 Checks bug list

This chapter contains the bugs in the WLC and AP checks.

1.1 Transmit power AP check

Transmit power has the wrong OID. Please use: .1.3.6.1.4.1.388.50.1.3.4.1.1.9 The OID used right now shows the transmit power that is manually configured, instead of the value that is actually sending.

1.2 Connected to WLC AP check

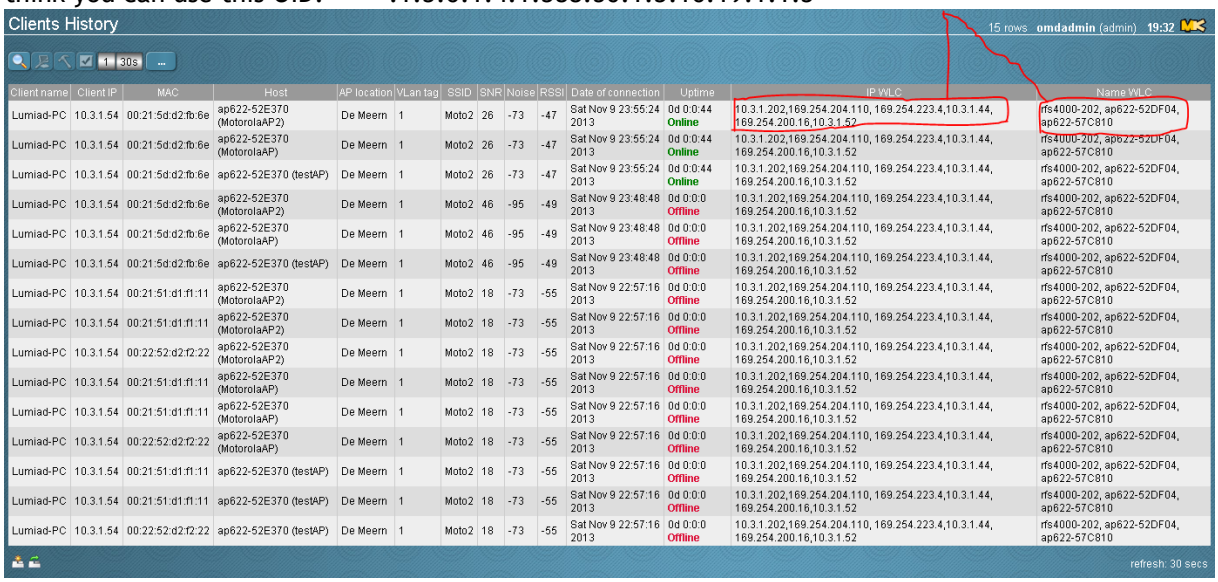
The AP check need to show the WLC, not a list of all devices. Maybe you can use this OID: .1.3.6.1.4.1.388.50.1.3.16.19.1.1.3 It shows the IP address of the WLC that has done the adoption of the AP.

2 Client history bug list

This chapter contains the bugs in the client history

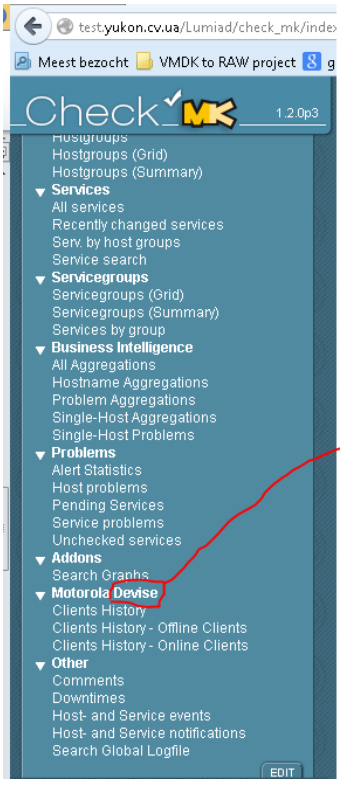
2.1 Name and IP WLC

The field IP WLC and name WLC Shows the access points as well, but it should only display the WLC. I think you can use this OID: .1.3.6.1.4.1.388.50.1.3.16.19.1.1.3



Client name	Client IP	MAC	Host	AP location	VLan tag	SSID	SNR	Noise	RSSI	Date of connection	Uptime	IP WLC	Name WLC
Lumiad-PC	10.3.1.54	00:21:5d:d2:fb:6e	ap622-52E370 (MotorolaAP2)	De Meern	1	Moto2	26	-73	-47	Sat Nov 9 23:55:24 2013	0d 0:0:44 Online	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:5d:d2:fb:6e	ap622-52E370 (MotorolaAP)	De Meern	1	Moto2	26	-73	-47	Sat Nov 9 23:55:24 2013	0d 0:0:44 Online	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:5d:d2:fb:6e	ap622-52E370 (testAP)	De Meern	1	Moto2	26	-73	-47	Sat Nov 9 23:55:24 2013	0d 0:0:44 Online	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:5d:d2:fb:6e	ap622-52E370 (MotorolaAP2)	De Meern	1	Moto2	46	-95	-49	Sat Nov 9 23:48:48 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:5d:d2:fb:6e	ap622-52E370 (MotorolaAP)	De Meern	1	Moto2	46	-95	-49	Sat Nov 9 23:48:48 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:5d:d2:fb:6e	ap622-52E370 (testAP)	De Meern	1	Moto2	46	-95	-49	Sat Nov 9 23:48:48 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:51:d1:f1:11	ap622-52E370 (MotorolaAP2)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:51:d1:f1:11	ap622-52E370 (MotorolaAP2)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:22:52:d2:f2:22	ap622-52E370 (MotorolaAP2)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:51:d1:f1:11	ap622-52E370 (MotorolaAP)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:51:d1:f1:11	ap622-52E370 (MotorolaAP)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:22:52:d2:f2:22	ap622-52E370 (MotorolaAP)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:51:d1:f1:11	ap622-52E370 (testAP)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:51:d1:f1:11	ap622-52E370 (testAP)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:22:52:d2:f2:22	ap622-52E370 (testAP)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810

2.2 Not ‘Devise’ but ‘Device’



In the menu of check_MK the tab ‘Motorola Devise’ is spelled incorrectly. Please change this to ‘Motorola Devices’.

3 AP/WLC check Features

3.1 Link to client history

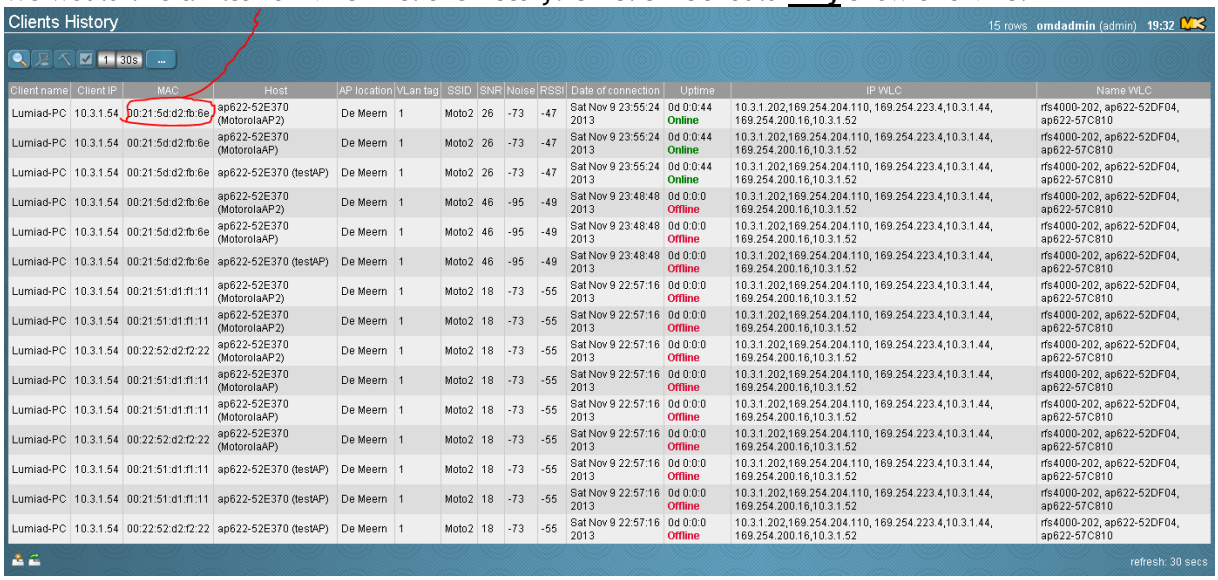
If you click on the number of logged in clients in AP check, it should hyperlink to the client history page.

4 Client history features

This chapter describes new features in client history

4.1 Mac filter

We would like a filter on MAC in client history. On click it should **only** show this MAC.



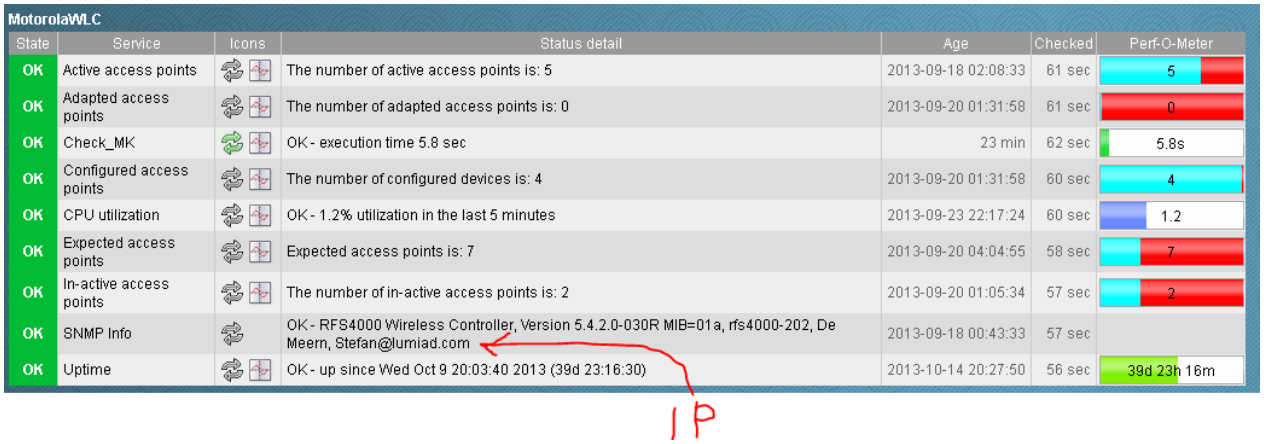
Client name	Client IP	MAC	Host	AP location	VLan tag	SSID	SNR	Noise	RSSI	Date of connection	Uptime	IP WLC	Name WLC
Lumiad-PC	10.3.1.54	00:21:5d:d2:fb:6e	ap622-52E370 (MotorolaAP2)	De Meern	1	Moto2	26	-73	-47	Sat Nov 9 23:55:24 2013	0d 0:0:44 Online	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:5d:d2:fb:6e	ap622-52E370 (MotorolaAP)	De Meern	1	Moto2	26	-73	-47	Sat Nov 9 23:55:24 2013	0d 0:0:44 Online	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:5d:d2:fb:6e	ap622-52E370 (testAP)	De Meern	1	Moto2	26	-73	-47	Sat Nov 9 23:55:24 2013	0d 0:0:44 Online	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:5d:d2:fb:6e	ap622-52E370 (MotorolaAP2)	De Meern	1	Moto2	46	-95	-49	Sat Nov 9 23:48:48 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:5d:d2:fb:6e	ap622-52E370 (MotorolaAP)	De Meern	1	Moto2	46	-95	-49	Sat Nov 9 23:48:48 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:5d:d2:fb:6e	ap622-52E370 (testAP)	De Meern	1	Moto2	46	-95	-49	Sat Nov 9 23:48:48 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:51:d1:f1:11	ap622-52E370 (MotorolaAP2)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:51:d1:f1:11	ap622-52E370 (MotorolaAP2)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:22:52:d2:f2:22	ap622-52E370 (MotorolaAP2)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:51:d1:f1:11	ap622-52E370 (MotorolaAP)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:51:d1:f1:11	ap622-52E370 (MotorolaAP)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:22:52:d2:f2:22	ap622-52E370 (MotorolaAP)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:51:d1:f1:11	ap622-52E370 (testAP)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:21:51:d1:f1:11	ap622-52E370 (testAP)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810
Lumiad-PC	10.3.1.54	00:22:52:d2:f2:22	ap622-52E370 (testAP)	De Meern	1	Moto2	18	-73	-55	Sat Nov 9 22:57:16 2013	0d 0:0:0 Offline	10.3.1.202,169.254.204.110, 169.254.223.4,10.3.1.44, 169.254.200.16,10.3.1.52	rfs4000-202, ap622-52DF04, ap622-57C810

5 check Features

This chapter describes new features in the checks.

5.1 IP address in checks

We would like to add IP address of the device in the SNMP info, so we can identify the AP or WLC. This need to be built in the AP checks and in the WLC checks.



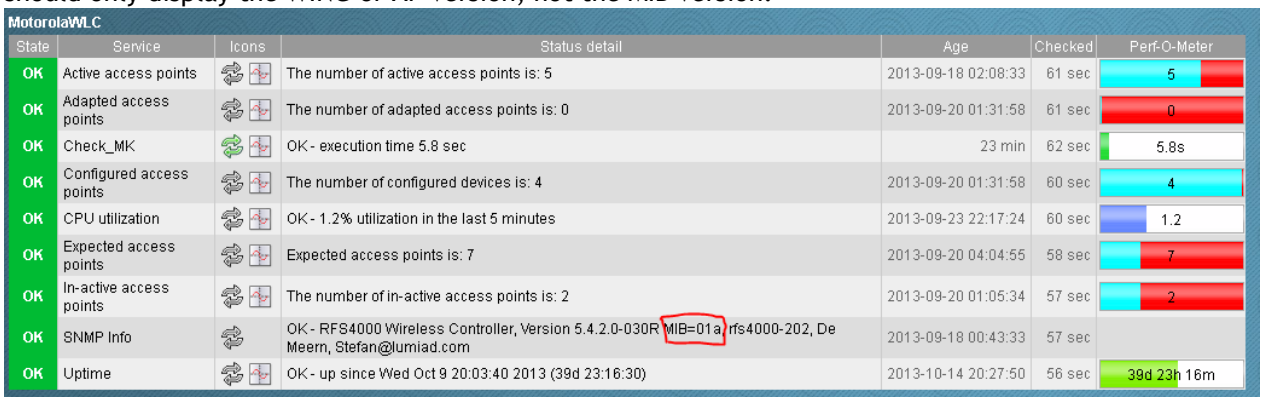
MotorolaWLC

State	Service	Icons	Status detail	Age	Checked	Perf-O-Meter
OK	Active access points		The number of active access points is: 5	2013-09-18 02:08:33	61 sec	5
OK	Adapted access points		The number of adapted access points is: 0	2013-09-20 01:31:58	61 sec	0
OK	Check_MK		OK - execution time 5.8 sec	23 min	62 sec	5.8s
OK	Configured access points		The number of configured devices is: 4	2013-09-20 01:31:58	60 sec	4
OK	CPU utilization		OK - 1.2% utilization in the last 5 minutes	2013-09-23 22:17:24	60 sec	1.2
OK	Expected access points		Expected access points is: 7	2013-09-20 04:04:55	58 sec	7
OK	In-active access points		The number of in-active access points is: 2	2013-09-20 01:05:34	57 sec	2
OK	SNMP Info		OK - RFS4000 Wireless Controller, Version 5.4.2.0-030R MIB=01a, rfs4000-202, De Meern, Stefan@lumiad.com	2013-09-18 00:43:33	57 sec	
OK	Uptime		OK - up since Wed Oct 9 20:03:40 2013 (39d 23:16:30)	2013-10-14 20:27:50	56 sec	39d 23h 16m

IP

5.2 Remove MIB=01a

Please remove the MIB information in SNMP info. This need to be built in both the AP and WLC check. It should only display the WING or AP version, not the MIB version.



MotorolaWLC

State	Service	Icons	Status detail	Age	Checked	Perf-O-Meter
OK	Active access points		The number of active access points is: 5	2013-09-18 02:08:33	61 sec	5
OK	Adapted access points		The number of adapted access points is: 0	2013-09-20 01:31:58	61 sec	0
OK	Check_MK		OK - execution time 5.8 sec	23 min	62 sec	5.8s
OK	Configured access points		The number of configured devices is: 4	2013-09-20 01:31:58	60 sec	4
OK	CPU utilization		OK - 1.2% utilization in the last 5 minutes	2013-09-23 22:17:24	60 sec	1.2
OK	Expected access points		Expected access points is: 7	2013-09-20 04:04:55	58 sec	7
OK	In-active access points		The number of in-active access points is: 2	2013-09-20 01:05:34	57 sec	2
OK	SNMP Info		OK - RFS4000 Wireless Controller, Version 5.4.2.0-030R MIB=01a, rfs4000-202, De Meern, Stefan@lumiad.com	2013-09-18 00:43:33	57 sec	
OK	Uptime		OK - up since Wed Oct 9 20:03:40 2013 (39d 23:16:30)	2013-10-14 20:27:50	56 sec	39d 23h 16m

Projectplan Monitoring v4

Naam:	Stefan van den Heuvel
Studentnummer:	1591945
E-mail:	stefanvandenheuvel@student.hu.nl
Bedrijf:	Lumiad
Telefoon:	06 534 172 39

Content

1 Introduction

This document contain new functions we would like to add in Check_MK.

Please start building with the function from heading 1, then 2, then 3 etc. We made this order because some functions are more important as other functions.

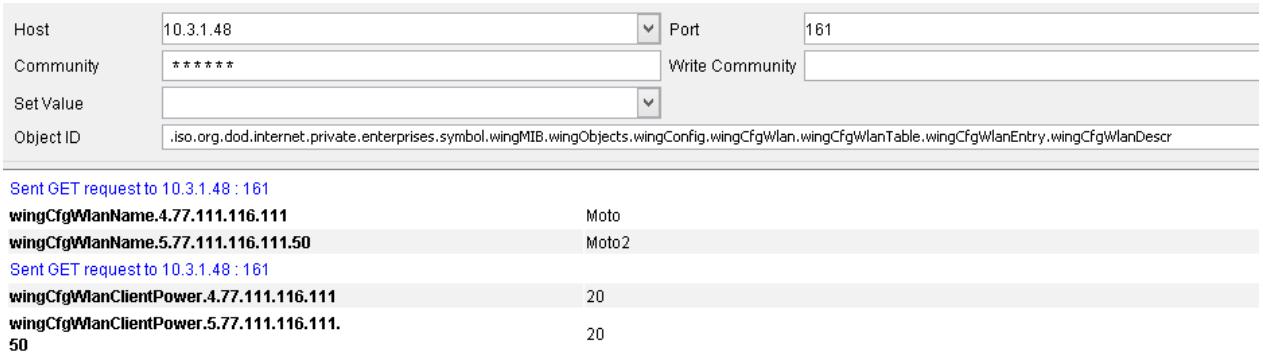
2 Transmit power AP check

I found the solution to know which transmit power is for which radio.

Use OID: .1.3.6.1.4.1.388.50.1.3.4.1.1.9

wingCfgWlanClientPower.4.77.111.116.111 = radio1

wingCfgWlanClientPower.**5**.77.111.116.111.**50** = radio2



The number for each radio is the same on all types of Motorola access points.

3 ‘Motorola Device’ to ‘Clients History’

Please rename ‘Motorola Device’ to ‘Clients history’ . Because the menu-name doesn’t say much about the sub-items.

4 Scan IP addresses to add devices in Check_MK

Currently we have to add all devices manually. In environment with many access points this job takes time.

For this reason we would like an option in Check_MK to add devices by an IP scan. It should look like something as in figure 1. The scan should send a SNMP request on which only Motorola APs and WLCs respond (OID .1.3.6.1.2.1.47.1.1.1.1.12) to every IP address in the specified IP range. If the device respond, it should be added in the list of devices and does a full check.

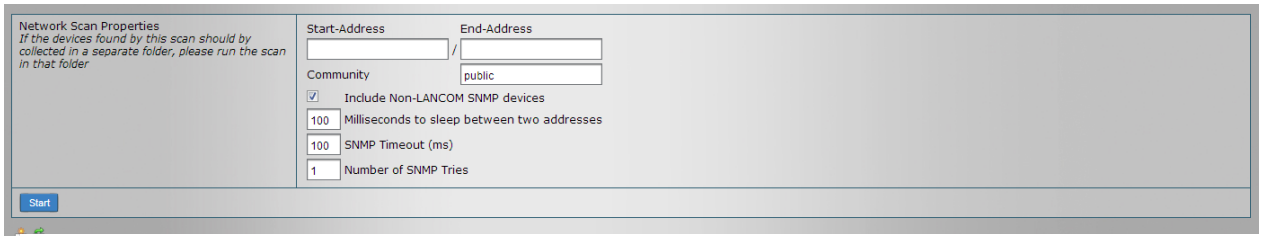


Figure 1 - scan for IP adres

I will example step by step how to do this. For example I use:

- start-address 192.168.1.20
- End-address 192.168.1.25

The network has two access points:

- AP1 192.168.1.22
- AP2 192.168.1.25

1. The user press ‘start’
2. Check_MK sends OID .1.3.6.1.2.1.47.1.1.1.1.12 to 192.168.1.20
3. No response
4. Check_MK sends OID .1.3.6.1.2.1.47.1.1.1.1.12 to 192.168.1.21
5. No response
6. Check_MK sends OID .1.3.6.1.2.1.47.1.1.1.1.12 to 192.168.1.22
7. Response from 192.168.1.22
8. Check_MK sends the rest of the AP checks and adds 192.168.1.22 to Check_MK hosts
9. Check_MK sends OID .1.3.6.1.2.1.47.1.1.1.1.12 to 192.168.1.23
10. No response
11. Check_MK sends OID .1.3.6.1.2.1.47.1.1.1.1.12 to 192.168.1.24
12. No response
13. Check_MK sends OID .1.3.6.1.2.1.47.1.1.1.1.12 to 192.168.1.25
14. Check_MK sends the rest of the AP checks and adds 192.168.1.25 to Check_MK hosts
15. Check_MK stops scanning

This option should be added under ‘Hosts & Folders’ in the WATO configuration menu (figure 2). The option ‘New host scan’ should appear as a button (figure 3).

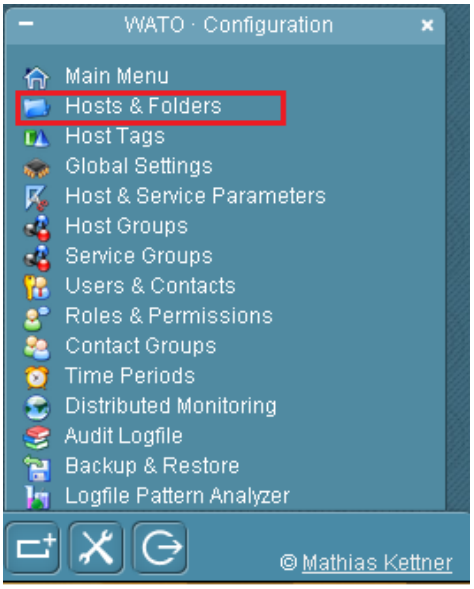


Figure 2- WATO menu

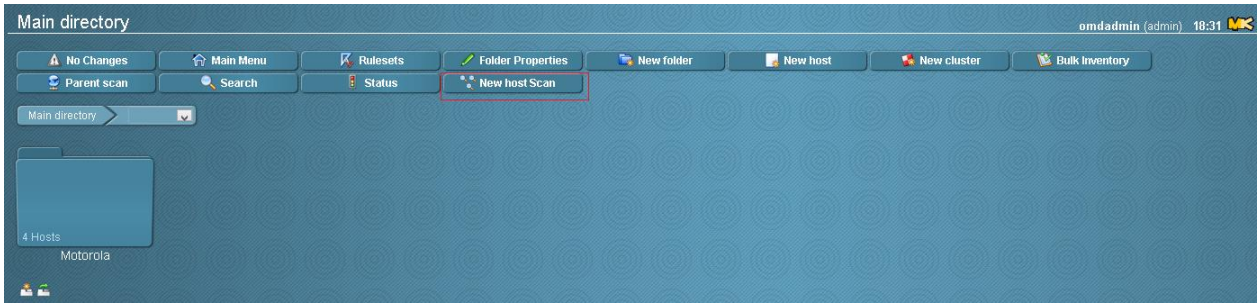


Figure 3 New host scan button

5 Layout

For marketing purposes we would like a new design for Check_MK. A new background with the Lumiad blue or green colors would be nice. And maybe add the Lumiad logo somewhere in the webpage.
An example background I think would be nice:

6 Complete ISO Check_MK installation file

Currently we have to manually install/configure CentOS and OMD. We can reduce the time for this by making an ISO file which has everything pre-installed and configured. Also, in the installation we would like to add a little menu which has the following options:

- Hostname of the machine
- IP configuration for the machine
- Add domain option
- Specify a SNMP server

In Windows this is possible with Sysprep and answer file scripts. I think Linux has something like that as well. Do you think it is possible to realize this?