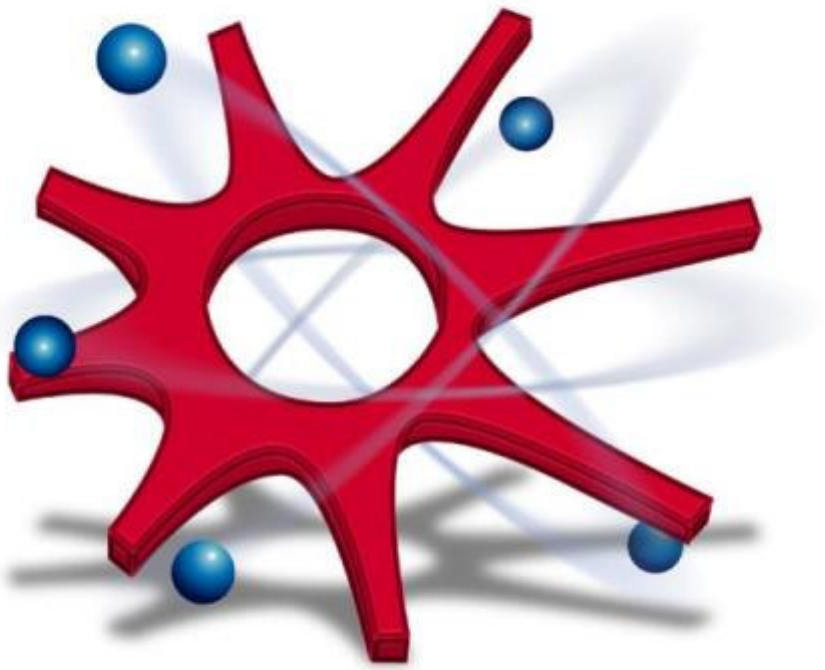
Afstudeerverslag

Netwerkbeveiliging ten behoeve van netwerkgebruikers op de Haagse Hogeschool



Afstudeerder:
Remko Sikkema (20008983)

Examinatoren:
L.C.M. van Koppen
J.W. Witkamp

Organisatie:
Haagse Hogeschool (Dienst ICT)

Afstudeerrichting:
IVIT-MBIT

Plaats , Datum:
Den Haag, 14 januari 2005

Referaat

Sikkema, R., Eindverslag afstuderen, HHS Dienst ICT, Den Haag, januari 2004

In dit verslag is het proces beschreven dat de afstudeerder heeft doorlopen en welke stappen zijn ondernomen gedurende het uitvoeren van de afstudeeropdracht voor de Dienst ICT (Informatie en Communicatie Technologie) van de Haagse Hogeschool.

Gedurende de opleiding Informatica en Informatiekunde dienen studenten een afstudeeropdracht uit te voeren bij een organisatie om zo hun bekwaamheid te bewijzen. Deze afstudeeropdracht is uitgevoerd door Remko Sikkema in opdracht van de Haagse Hogeschool, Dienst ICT. Het afstuderen is op 30 augustus 2004 begonnen en op 14 januari beëindigd.

Descriptoren:

- Afstudeerverslag
- Authenticatie
- Autorisatie
- 802.1x
- EAP
- LDAP
- Firewall
- Radius
- Supplicant
- TTLS
- VLAN
- WLAN

Voorwoord

Dit is het afstudeerverslag van Remko Sikkema, een student van de Haagse Hogeschool, studerende aan de sector Informatica en Informatiekunde (I&I). Het verslag is opgesteld naar aanleiding van het afstudeerproject dat studenten aan het einde van hun opleiding dienen te doorlopen.
De opdracht bestond uit een onderzoek naar authenticatie mogelijkheden van netwerkgebruikers. De mogelijkheden zijn vervolgens in verschillende pilots tot oplossingen uitgewerkt.
In dit verslag wordt beschreven hoe dit onderzoek en deze pilots tot stand zijn gekomen, welke aanpak ik daarbij heb gehanteerd en welke problemen ik ben tegengekomen. Het was mij niet gelukt dit allemaal te voltooien zonder de hulp van een aantal personen die ik graag wil bedanken.

Mijn examinatoren Leo van Koppen en Hans Witkamp hebben mij in eerste instantie geholpen met het formuleren van een duidelijke opdrachtomschrijving en daarnaast hebben zij advies gegeven hoe ik het best aan het afstuderen kon beginnen. In een later stadium hebben zij mij geholpen bij het tot stand komen van dit afstudeerverslag en stonden ze altijd klaar om advies te geven.
Mijn bedrijfsmentor Jos Schutte wil ik bedanken voor het aanbieden van een afstudeerproject, het ondersteunen van werkzaamheden en motivatie om hard te werken aan zowel het verslag als het product.
Ik wil John van Boxtel bedanken voor het aanbieden van een vaste werkplek, Frits Sikkema voor informatievoorziening, mijn kamergenoten voor de gezelligheid en de rest van de Haagse Hogeschool medewerkers die altijd vriendelijk waren.

Ik dank allen voor hun positieve inzet en waardevolle adviezen.

Den Haag, 26 november 2004

Remko Sikkema

Inhoudsopgave

1 ◦ Inleiding 1

2 ◦ Organisatie 2
2.1 ▫ Beschrijving organisatie 2
2.2 ▫ Veranderingen 4

3 ◦ De opdracht 5
3.1 ▫ Details opdracht 5
3.2 ▫ Het project 6

4 ◦ Huidige Situatie 9
4.1 ▫ Gebruikersgroepen 9
4.2 ▫ Overzicht netwerk 14
4.3 ▫ Databases 16

5 ◦ Eisen en wensen 17
5.1 ▫ Technische eisen en wensen 17
5.2 ▫ Gebruikers platform eisen en wensen 18
5.3 ▫ Eisen en wensen ten aanzien van beveiliging 20
5.4 ▫ Eisen en wensen ten aanzien van beheer 21

6 ◦ Onderzoek oplossingsmogelijkheden 22
6.1 ▫ Opzet onderzoek 22
6.2 ▫ Resultaten onderzoek 22

7 ◦ De pilots 27
7.1 ▫ Pilot 1: 802.1x Authenticatie 27
7.2 ▫ Pilot 2: Accounting/logging van gebruikers 31
7.3 ▫ Pilot 3: Authenticatie via Firewall 33
7.4 ▫ Pilot 4: Gebruik van VLAN's 34
7.5 ▫ Pilot 5: Website voor quarantainenetwerk 39

8 ◦ Evaluatie 43
8.1 ▫ Proces evaluatie 43
8.2 ▫ Product evaluatie 44

9 ◦ Conclusie 45

Literatuurlijst 46

Interne Bijlagen 47
Bijlage I: Glossarium 47
Bijlage II: Lijst van figuren 50

Externe Bijlagen:

- Bijlage A: Plan van aanpak
- Bijlage B: Onderzoeksrapport
- Bijlage C: Adviesrapport
- Bijlage D: Uitkomst van de pilots
- Bijlage E: Informatievoorziening voor de gebruiker met de maatregelen

1 ◦ Inleiding

Het verslag dat u nu aan het lezen bent is het resultaat van het afstudeertraject dat ik heb doorlopen gedurende mijn studie. Het afstuderen is een verplicht onderdeel van de studie Informatica en Informatiekunde die ik heb gevolgd aan de Haagse Hogeschool. Het afstuderen is een proef van bekwaamheid en alleen bij een positieve beoordeling van het afstuderen kan de studie worden afgerond. Tijdens de studie heb ik voor de studierichting Management en Beheer van Informatietechnologie (MBIT) gekozen.
Ik heb voor een afstudeeropdracht gekozen die een sterk raakvlak heeft met mijn studierichting. De opdracht betrof het onderzoeken en testen van oplossingen om de netwerkbeveiliging van netwerkgebruikers te bevorderen. Deze opdracht werd uitgevoerd voor hetzelfde instituut als ik studeerde, namelijk de Haagse Hogeschool. Bij de Haagse Hogeschool was ik tijdens het afstuderen werkzaam voor Dienst ICT, een ondersteunde afdeling. De opdracht is ontstaan door het probleem van het groeiende aantal netwerkgebruikers met computers in eigen beheer en de huidige problemen betreffende identificatie en authenticatie van gebruikers.
Dit verslag is geschreven met als doel het afstudeertraject dat ik heb doorlopen beoordeelbaar te maken voor mijn examinatoren en de gecommitteerde, die allen bij de afstudeerzitting aanwezig zullen zijn.

Het verslag is in *drie delen* opgedeeld.

Het *eerste deel* bestaat uit het hoofdstuk 'organisatie' waarin een beschrijving wordt gegeven van de organisatie waar ik werkzaam was en de rol die ik daar vervulde en het hoofdstuk 'de opdracht' waar een toelichting wordt gegeven op de opdrachtomschrijving en ook een deel van plan het van aanpak wordt toegelicht.

Het *tweede deel* zal de werkzaamheden beschrijven die ik heb verricht tijdens het afstuderen. Dit is in vijf verschillende hoofdstukken vastgelegd. In het hoofdstuk 'huidige situatie' zal een beeld worden geschetst van de situatie zoals die bij aanvang van de opdracht was. Hoofdstuk 'eisen en wensen' beschrijft de eisen en wensen die in overleg met de opdrachtgever zijn besproken waaraan de oplossingsmogelijkheden moeten voldoen. Vervolgens wordt in het hoofdstuk 'onderzoek oplossingsmogelijkheden' duidelijk gemaakt welke mogelijkheden aanwezig waren, welke keuzes zijn gemaakt en waarom.
In het hoofdstuk 'de pilots' beschrijf ik hoe ik vijf verschillende pilots heb opgezet en wat de resultaten daarvan zijn.

In het *derde deel* zal in het hoofdstuk 'evaluatie' een persoonlijke beoordeling worden gegeven over het verloop van het afstuderen en het opgeleverde product. Ten slot wordt in het hoofdstuk 'conclusie' een eindoordeel gegeven over het onderwerp netwerkbeveiligingen.

2 ◦ Organisatie

In dit hoofdstuk staat beschreven bij welke organisatie de afstudeerder werkzaam was, de Haagse Hogeschool. Dit met het doel de lezer een duidelijk beeld te geven van de organisatie en de plaats die ik had in de organisatie. Binnen de Haagse Hogeschool had ik een functie bij Dienst ICT als stagiair. Na de beschrijving van de organisatie, is een paragraaf gewijd aan de veranderingen die de Haagse Hogeschool de laatste jaren heeft ondergaan. Deze veranderingen zijn deels de oorzaak van het noodzakelijk maken van deze afstudeeropdracht.

2.1 ▫ Beschrijving organisatie

Informatie over de organisatie was vrij beschikbaar op het intranet van de Haagse Hogeschool. Deze was verspreid over verscheidene webpagina's en PDF bestanden (Adobe Portable Document Format). Door het gebruik van de zoekfunctie van het intranet is deze informatie ingewonnen.

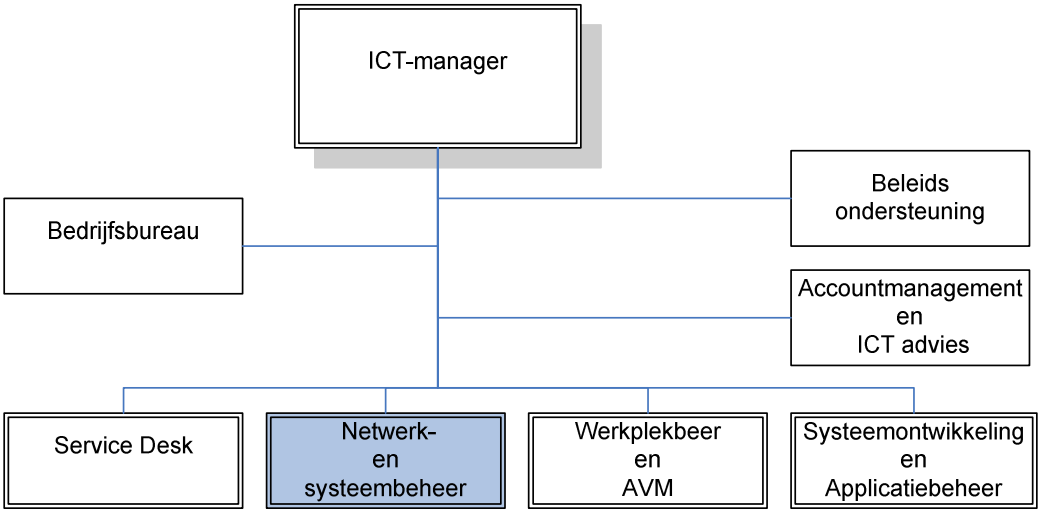
Haagse Hogeschool
De Haagse Hogeschool is een onderwijsinstelling die een scala aan opleidingsmogelijkheden aanbiedt in de vorm van hoger beroepsonderwijs.
Er is een keuze uit negenendertig opleidingen die verdeeld zijn in zeven aandachtsgebieden: economie, gezondheidszorg, gedrag en maatschappij, informatica, internationaal, techniek, onderwijs en sport. Opleidingen worden in verschillende vormen aangeboden: voltijd, duaal of deeltijd. Daarnaast is het ook voor bedrijven en particulieren mogelijk om aan de Haagse Hogeschool te studeren, denk hierbij aan na- en bijscholing door middel van masters, (post-hbo-) opleidingen, cursussen en trainingen.

Naast deze opleidingen zijn ook een aantal ondersteunende diensten aanwezig, zoals de Hogeschoolbibliotheek, Facilitaire Dienst, Dienst Personeel & Organisatie en Dienst ICT. Deze diensten ondersteunen de Haagse Hogeschool in haar primaire proces: verzorgen van onderwijs. Het gehele overzicht van afdelingen en diensten van de Haagse Hogeschool is terug te vinden in het organogram in bijlage A (Plan van aanpak). De afstudeeropdracht zal worden uitgevoerd voor Dienst ICT.

Dienst ICT
Dienst ICT bestaat globaal gezien uit vier onderdelen, genaamd service-units. Daarnaast bestaat Dienst ICT ook uit een aantal interne stafdiensten. In het organogram van Dienst ICT (figuur 2.1) zijn de service-units en stafdiensten terug te vinden.
De manager van Dienst ICT is Kees van Loon.
Service-unit "Werkplekbeheer / Audio- en Visuele Middelen" draagt zorg voor computers en randapparatuur op de werkplekken, les- en practicalokalen. Deze computers kunnen zowel voor gebruik van studenten en/of docenten worden ingericht. Ook is de service-unit verantwoordelijk voor het onderhouden van de software die op de computer hoort. Software die door gebruikers zelf wordt geïnstalleerd, wordt niet ondersteund.
Computers die door studenten en medewerkers zelf worden aangeschaft zijn computers in het beheer van de eigenaar en worden dus ook niet beheerd door werkplekbeheer. Daarnaast bestaat de service-unit ook uit het onderdeel audio- en visuele middelen die apparatuur beheert zoals videocamera's en beamers.

Service-unit "Service Desk" zorgt voor communicatie tussen de gebruikers en de andere service-units. Gebruikers met computer gerelateerde problemen of verzoeken kunnen terecht bij de Service desk. Afhankelijk van de omvang en aard van het verzoek/probleem zal een "call" worden aangemaakt voor de gebruiker. Deze call is voor iedere gebruiker uniek en koppelt de gebruiker aan een bepaald probleem/verzoek. De Service desk stuurt deze calls vervolgens door naar de juiste service-unit, die op zijn beurt de call afhandelt.
Netwerk- en systeembeheer is verantwoordelijk voor de informatie-infrastructuur. Dit houdt in dat de diverse netwerken (studenten/bedrijf/financieel) naar behoren moeten werken en dat het Internet goed bereikbaar is. Deze netwerken zijn ook deels beveiligd tegen misbruik door middel van bijvoorbeeld firewalls en een domain controller. Ook is netwerk- en systeembeheer voor een groot deel verantwoordelijk voor server beheer en back-up/restore van data.
Als laatste is er nog de service-unit "Systeemontwikkeling en applicatiebeheer", die zoals de naam al doet vermoeden, de applicaties van de Haagse Hogeschool beheert en ontwikkelt.

Organogram van de Dienst ICT zoals deze momenteel is:



Figuur 2.1: Organogram Dienst ICT

Plaats in organisatie
Ik was werkzaam bij de Dienst ICT, service-unit "Netwerk- en systeembeheer". Mijn directe leidinggevende en tevens opdrachtgever was Jos Schutte, 1e medewerker netwerk- en systeembeheer.
Hoofd netwerk- en systeembeheer was mijn uiteindelijke manager, al had ik niet veel met hem te maken. Jos Schutte was de aangewezen persoon om mij aan te sturen.
Er was niet genoeg kamerruimte aanwezig bij de afdeling op de 2de verdieping en hierdoor was ik genoodzaakt om een alternatieve ruimte te zoeken. Via John van Boxtel kwam ik uiteindelijk terecht op de afdeling Informatica op een flexplek en deelde de kamer met "Unit Organisatie Ondersteuning" en een andere informatica student die ook aan het afstuderen was. Er werd op de afdeling niet anders omgegaan met stagiaires dan met vaste werknemers. Dit had als positief gevolg dat ik me gelijk voelde met de rest van de werknemers.

2.2 ▫ Veranderingen

De Haagse Hogeschool is enkele jaren geleden overgestapt van decentraal naar centraal beheer. De opleidingen die de Haagse Hogeschool aanboden waren onderverdeeld in sectoren die individueel te werk gingen, waardoor weinig communicatie tussen de onderlinge sectoren plaats vond. De sectoren waren hierdoor een school op zich met al hun eigen regels en voorzieningen.
Om een betere samenwerking en aansluiting te bieden tussen de verschillende opleidingen was het beleid van de afgelopen jaren gericht om de sectoren samen te voegen tot één groot geheel. Dit had als gevolg dat er met afdelingen gewerkt zou worden in plaats van sectoren. Deze veranderingen hebben ervoor gezorgd door ook alle ICT diensten samengevoegd werden en de decentrale helpdesks werden vervangen door één centrale ICT-servicedesk.
Dienst ICT is sindsdien ook volgens het ITIL (Information Technology Infrastructure Library) model gaan werken. ITIL wordt in een organisatie gebruikt om de kwaliteit van de dienstverlening van de ICT dienst te verbeteren en er een structuur in aan te brengen.
Het werken met ITIL leverde vooral in het begin een hoop problemen, maar daar wordt momenteel hard aan gewerkt om de service naar gebruikers toe te verbeteren. Ook worden duidelijkere SLA's (Service Level Agreements) opgesteld. Deze SLA’s zullen ervoor zorgen dat een bepaald niveau van dienstverlening wordt gehandhaafd.

Het ICT beleid is ook dat studenten overal op school kunnen inloggen op een studentencomputer om daar hun werk te kunnen verrichten. Momenteel is het (nog) zo dat studenten alleen gebruik kunnen maken van lokalen die speciaal ingericht zijn voor hun opleiding. Het draadloze netwerk is wel te gebruiken door alle studenten, onafhankelijk van hun opleiding.
Er is nog geen beleid aanwezig betreffende informatiebeveiliging, alhoewel deze al wel in ontwikkeling is. Naast het hierboven genoemde beleid, waren geen andere relevante beleidsonderdelen aanwezig waar ik mee te maken had.

Het aantal gebruikers, met een computer in eigen beheer, dat gebruik maakt van het Haagse Hogeschool netwerk is de laatste jaren ook flink gestegen. Deze stijging is te danken aan de toename van laptops en de nieuwe studentenflat (Laakhaventoren). De gebruikers hebben een eigen computer in die ze zelf beheren. Deze computers worden dus niet door Dienst ICT beheerd.
De toename van het aantal gebruikers heeft tot gevolg dat er minder controle en zicht mogelijk is over de gebruikers van het netwerk.

Enkele tijd terug is de Haagse Hogeschool gefuseerd met de Technische Hogeschool Rijswijk. Er was op de THRijswijk een geheel zelfstandig ICT dienst, echter is deze voor een deel ook al samengevoegd met de Dienst ICT van de Haagse Hogeschool.

3 ◦ De opdracht

Na enige tijd in het bedrijfsleven gezocht te hebben naar een afstudeeropdracht, kwam ik uiteindelijk bij Dienst ICT terecht van de Haagse Hogeschool. Hier waren een aantal afgebakende projecten beschikbaar waar Dienst ICT zelf geen tijd voor had. Deze projecten hadden een lagere prioriteit dan het operationeel beheer en de migratie naar Windows XP. Ik kon uitkomst bieden door één van deze projecten te vormen tot een afstudeerproject. Het werd mij snel duidelijk dat het project betreffende netwerkbeveiliging dichtbij mijn persoonlijke interesses lag. De opdrachtgever was het mee eens dat het een leuk project zou worden.

3.1 ▫ Details opdracht

Definities
Omdat de gehele opdracht om authenticatie, autorisatie en identificatie draait, wordt eerst een definitie gegeven van deze begrippen in de context van de afstudeeropdracht:
Identificatie is het vaststellen met wie gecommuniceerd wordt.
Authenticatie is het zeker stellen dat degene waarmee gecommuniceerd wordt, ook werkelijk die persoon is die hij/zij beweert te zijn.
Autorisatie is het vaststellen van de rechten op een bepaald systeem van degene waarmee gecommuniceerd wordt.

Probleemstelling
Het doel van de afstudeeropdracht is onderzoek doen naar beveiligingsmaatregelen met als doel de beveiliging van het netwerk op de Haagse Hogeschool te brengen op het niveau van E2/F-C1 ITSEC-classificatie. Dit impliceert de authenticatie, autorisatie en logging van de authenticatie van de netwerkgebruikers. Aan de hand van de resultaten van het onderzoek en na overleg met de opdrachtgever zullen bepaalde maatregelen verder worden uitgewerkt in een adviesrapport. Op basis van het advies en na overleg met opdrachtgever worden enkele pilots uitgevoerd.

Doelstelling
Er zal een onderzoek worden gedaan naar de mogelijkheden om het netwerk op de Haagse Hogeschool beter te beveiligen tegen misbruik van het netwerk. Aan de hand van de resultaten van het onderzoek en in overleg met de opdrachtgever zullen bepaalde maatregelen verder worden uitgewerkt tot een adviesrapport en zal een pilot plaats vinden.

Oplevering producten
De volgende producten zullen voor de opdrachtgever worden opgeleverd:
- Onderzoeksrapport
- Ontwerp- en Adviesrapport
- Uitkomst van de pilot
- Informatievoorziening voor de gebruikers met de maatregelen.

Deze producten zullen uiterlijk 14 januari worden overhandigd aan de opdrachtgever.

3.2 ▫ Het project

Structuur
Ik had de verwachting bij aanvang van het afstudeerproject dat ik weinig conflicten zou hebben met andere parallel lopende projecten. Ook was bekend dat er geen legioen aan managers met mij bezig zouden houden. Dit omdat ze hier geen tijd voor konden vrijmaken. De verwachting was dan ook dat ik onafhankelijk aan het afstudeerproject kon gaan werken. Het onafhankelijk werken zou alleen niet ten koste mogen gaan van een tekort aan overleg. De opdrachtgever had aangegeven dat ik op elk moment langs kon komen voor overleg of adviezen. Ik ging er van uit dat ik regelmatig technisch opgelegde beperkingen (rechten op systemen, passwords, etc) met de opdrachtgever of andere verantwoordelijken moest gaan oplossen. Doordat de opdrachtgever had aangegeven spoedig klaar te zullen staan wanneer dit nodig zou moeten zijn, zou er een vrij 'platte' organisatie structuur ontstaan.

Risico's
Er is tijdens het afstuderen rekening gehouden met een aantal risico's.
Deze risico's zijn hieronder beschreven en de eventuele maatregelen die genomen kunnen worden om het risico te beperken of de schade te minimaliseren.

Ziekte opdrachtgever:
In geval van een zieke opdrachtgever was het belangrijk om een plaatsvervanger te hebben aangewezen en daarnaast goed plannen van activiteiten zodat de opdrachtgever niet a la minuut nodig was zodra een probleem optrad.
Ziekte afstudeerder:
Bij een lichte ziekte was het mogelijk om een deel van de activiteiten thuis uit te voeren. Voor een zware ziekte was geen echte oplossing, behalve het aanvragen van verlenging van de afstudeerperiode.
Hardware defecten:
Voor de hardware waren spare parts beschikbaar, de data werd regelmatig op een tweede computer/harde schrijf ge-backupped.
Dreiging project overbodig:
Flexibel inspringen op wijzigingen en aanpassen van de opdracht zover dit mogelijk zou moeten zijn.
Gebrek medewerking:
Minimaliseren van afhankelijkheden van andere personen.
Geen testapparatuur:
Realistische planning gemaakt voor het uitvoeren van de pilots en daarbij een correct pilot plan.

Methode en techniek
Er is voor het project de ontwikkelingsmethodiek ASI gekozen.
De ASI methode is gebaseerd op het *ASI rapport van het Nederlands Genootschap voor Informatica (NGI): Ontwerp en Ontwikkeling van systeem-/netwerkinfrastructuren.*
Deze methode is beschreven in de reader "ASI reader bij CS-05/ii-003".
Om een indruk te geven van de ASI methode, staat hieronder een quote met daarin de fases van deze methode:
"Een gefaseerde aanpak om een systeem-/netwerkinfrastructuur te ontwerpen en te ontwikkelen. De onderscheiden fasen zijn:

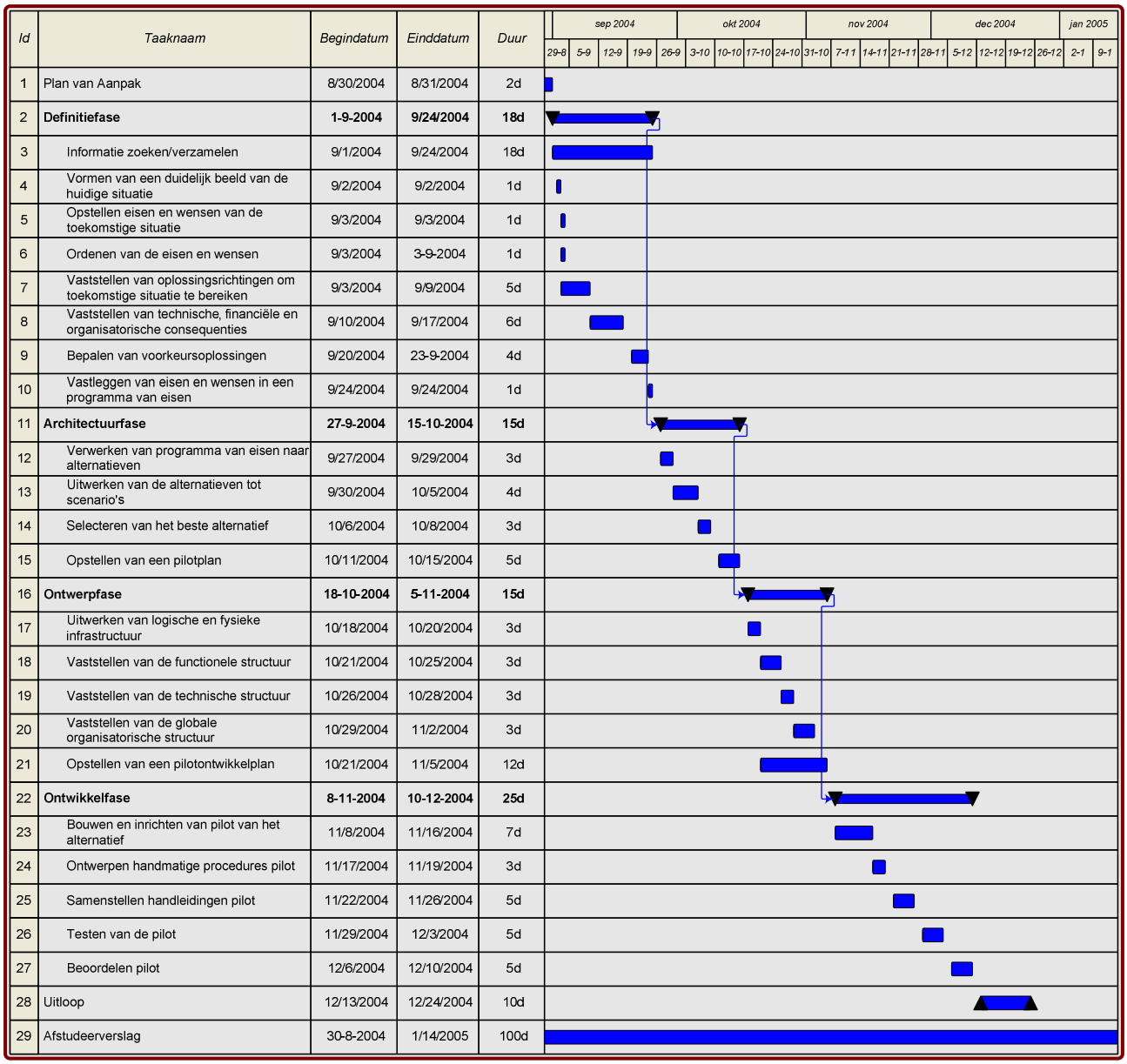
- Definitiefase: vastleggen wat het resultaat van het te doorlopen traject wordt, aan welke eisen het resultaat moet voldoen, en welke uitgangspunten er gehanteerd worden.
- Architectuurfase: opstellen van een blauwdruk van de te realiseren infrastructuur.
- Ontwerpfase: detail uitwerking van de architectuur naar de feitelijke geografische , technische en organisatorische context. Selectie van toe te passen producten en externe diensten
- Ontwikkelfase: toetsing van de goede werking en de schaalbaar¬heid van het ontwerp; realisatie van maatwerk aanpassingen en aanvullingen; opstellen van technische en procedurele richtlijnen." *(bron: ASI reader)*

Ook is gebruik gemaakt van de short/longlist techniek van bij het onderzoek, die ook beschreven staat in de ASI reader.

Planning

In de eerste dagen van het afstuderen heb ik een planning van de werkzaamheden in een Gantt Chart (figuur 3.1) gezet. Alle werkzaamheden zijn in fases onderbracht die bij de ASI-methode worden toegepast.

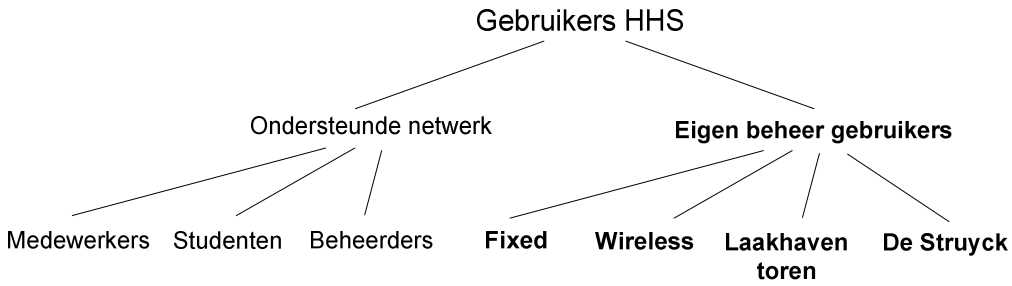
Id	Taaknaam	Begindatum	Einddatum	Duur
1	Plan van Aanpak	8/30/2004	8/31/2004	2d
2	**Definitiefase**	**1-9-2004**	**9/24/2004**	**18d**
3	Informatie zoeken/verzamelen	9/1/2004	9/24/2004	18d
4	Vormen van een duidelijk beeld van de huidige situatie	9/2/2004	9/2/2004	1d
5	Opstellen eisen en wensen van de toekomstige situatie	9/3/2004	9/3/2004	1d
6	Ordenen van de eisen en wensen	9/3/2004	3-9-2004	1d
7	Vaststellen van oplossingsrichtingen om toekomstige situatie te bereiken	9/3/2004	9/9/2004	5d
8	Vaststellen van technische, financiële en organisatorische consequenties	9/10/2004	9/17/2004	6d
9	Bepalen van voorkeursoplossingen	9/20/2004	23-9-2004	4d
10	Vastleggen van eisen en wensen in een programma van eisen	9/24/2004	9/24/2004	1d
11	**Architectuurfase**	**27-9-2004**	**15-10-2004**	**15d**
12	Verwerken van programma van eisen naar alternatieven	9/27/2004	9/29/2004	3d
13	Uitwerken van de alternatieven tot scenario's	9/30/2004	10/5/2004	4d
14	Selecteren van het beste alternatief	10/6/2004	10/8/2004	3d
15	Opstellen van een pilotplan	10/11/2004	10/15/2004	5d
16	**Ontwerpfase**	**18-10-2004**	**5-11-2004**	**15d**
17	Uitwerken van logische en fysieke infrastructuur	10/18/2004	10/20/2004	3d
18	Vaststellen van de functionele structuur	10/21/2004	10/25/2004	3d
19	Vaststellen van de technische structuur	10/26/2004	10/28/2004	3d
20	Vaststellen van de globale organisatorische structuur	10/29/2004	11/2/2004	3d
21	Opstellen van een pilotontwikkelplan	10/21/2004	11/5/2004	12d
22	**Ontwikkelfase**	**8-11-2004**	**10-12-2004**	**25d**
23	Bouwen en inrichten van pilot van het alternatief	11/8/2004	11/16/2004	7d
24	Ontwerpen handmatige procedures pilot	11/17/2004	11/19/2004	3d
25	Samenstellen handleidingen pilot	11/22/2004	11/26/2004	5d
26	Testen van de pilot	11/29/2004	12/3/2004	5d
27	Beoordelen pilot	12/6/2004	12/10/2004	5d
28	Uitloop	12/13/2004	12/24/2004	10d
29	Afstudeerverslag	30-8-2004	1/14/2005	100d



Figuur 3.1: Planning - Gantt Chart

4 ◦ Huidige Situatie

Om de huidige stand van zaken in kaart te brengen is de situatie geschetst zoals deze was toen de afstudeerder begon aan de afstudeeropdracht.
Door deze zaken in kaart te brengen komen onder andere de problemen en knelpunten naar voren die aanwezig waren. In dit hoofdstuk wordt de probleemstelling verder uitgewerkt tot specifieke problemen.
Globaal gezien zijn er twee verschillende typen gebruikersgroepen: gebruikers met een computer in eigen beheer en gebruikers die op het ondersteunde netwerk van de Haagse Hogeschool zijn aangesloten. Het verschil tussen deze twee groepen zit hem in het feit dat werkplekbeheer alleen support verleent aan de gebruikers van het ondersteunde netwerk. Bij de afstudeeropdracht zijn alleen de gebruikersgroepen van belang die onderdeel zijn van gebruikers met een computer in eigen beheer.
Deze laatst genoemde groep is weer onder te verdelen in vier verschillende gebruikersgroepen: fixed, wireless en studentenflats Laakhaventoren en De Struyck. De gebruikersgroepen van het ondersteunde netwerk zijn ook weer te onderverdelen in vele tientallen gebruikersgroepen. Deze zijn niet beschreven omdat ze buiten de scope van de afstudeeropdracht vallen.



Figuur 4.1: Overzicht gebruikersgroepen

Later in het hoofdstuk is een tekening te vinden van het netwerk van de Haagse Hogeschool en de studentenflats met een korte uitleg (figuur 4.3).
Dit is gedaan om de technische beperkingen in kaart te brengen en duidelijk te maken waar de verschillen zitten in apparatuur.
Aan het einde van het hoofdstuk zijn de gebruikte databases beschreven betreffende de authenticatie en autorisatie van de netwerkgebruikers. Deze databases zijn beschreven om een beeld te scheppen van de tekortkomingen van de huidige databases.

4.1 ▫ Gebruikersgroepen

Zoals in figuur 4.1 te zien is, zijn er vier groepen gebruikers die een computer in eigen beheer hebben. Bij aanvang van de afstudeeropdracht is er door de opdrachtgever besloten dat vooral een oplossing moet komen voor de wireless en fixed gebruikers. Er was bekend dat hier de zwaarst wegende problemen waren. Gebruikers bij deze twee groepen hoefden zich niet te authenticeren waardoor misbruik en problemen niet konden worden achterhaald. In een later stadium van het afstudeerproject is na overleg besloten om beide studentenflats ook in zijn geheel mee te nemen in de oplossingsmogelijkheden. Dit omdat de tijd dit toe liet en de mogelijkheden zich goed lieten uitbreiden.

Op de volgende pagina's zijn de problemen en knelpunten te lezen van de vier gebruikersgroepen. Deze zijn beschreven om tot oplossingsmogelijkheden te komen die zoveel mogelijk de knelpunten en problemen oplossen. Er is rekening mee gehouden dat het wellicht niet mogelijk is om deze allemaal op te lossen.
Aan de hand van meerdere interviews met de opdrachtgever en andere medewerkers van Dienst ICT zijn de problemen en knelpunten naar voren gekomen. De personen waren Jos Schutte, Ben Landmeter en Bert van Noort. Dit betroffen informele interviews waarbij de afstudeerder met pen en papier vragen los liet op de personen in kwestie. De nieuwe vragen die ontstonden tijdens het uitwerken van de interviews konden weer opnieuw gesteld worden.
Om een indruk te krijgen van de hoeveelheid gebruikers in de genoemde gebruikersgroepen, is in het onderstaande tabel het huidig aantal gebruikers weergegeven. Tot nu toe stijgt het aantal wireless gebruikers elk jaar. Dit komt vooral omdat steeds meer studenten een laptop met wireless netwerkmogelijkheden aanschaffen.
De huidige gebruikersaantallen:

Aantal	Gebruikersgroep
1376	Wireless gebruikers (Geregistreerde MAC-adressen)
300	Fixed netwerkaansluitingen
350	Laakhaventoren studentenflat
420	Studentenflat De Struyck
2446	Totaal aantal gebruikers

Tot slot is er ook nog de Technische Hogeschool Rijswijk. Hier is nog geen draadloos netwerk aanwezig, echter zijn al wel enkele access points aangeschaft om een wireless netwerk aan te leggen. Hierover is aan het eind van dit hoofdstuk iets meer te lezen.

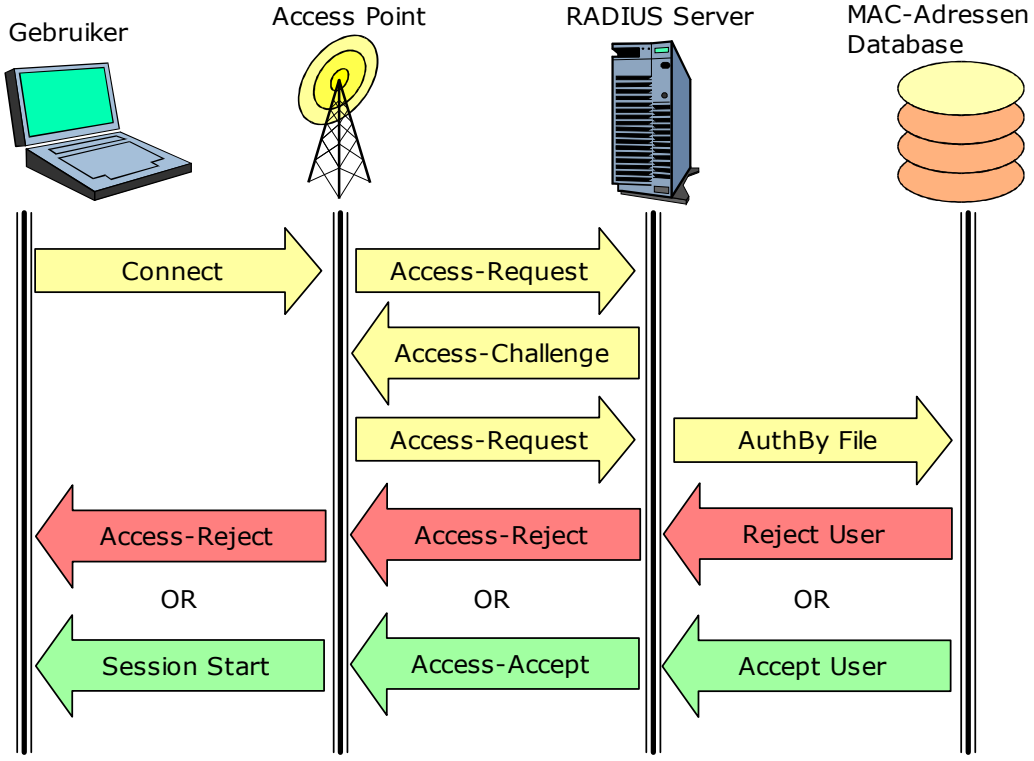
Gebruikersgroep: Wireless gebruikers
Er zijn hier meerdere knelpunten en problemen aanwezig:

- Authenticatie van gebruikers: door eenvoudig een MAC-adres te spoofen kan een gebruiker zich voordoen als een ander.
- Geen encryptie: Met een sniffer kan al het wireless data verkeer worden geanalyseerd. Zo zijn persoonlijke gegevens erg eenvoudig "uit de lucht" te halen, er hoeft alleen een sniffer gestart te worden om deze berichten te kunnen onderscheppen.
- Administratief: Om één gebruiker in de gebruikerslijst van MAC-adressen in te voeren zijn gemiddeld vijf minuten van ICT medewerkers nodig.
- Gebruikersgemak: Gebruiker moet wachten op de administratie van het MAC-adres om gebruik te kunnen maken van het wireless netwerk. Dit kan enkele dagen op zich laten wachten.

Hieronder zullen deze problemen verder worden uitgelegd.

Er zijn op een aantal locaties op de Haagse Hogeschool access points opgehangen (hotspots). De studenten en medewerkers kunnen op deze locaties gebruik maken van het wireless netwerk. Het wireless netwerk maakt gebruik van de IEEE 802.11b-standaard, waarmee maximale snelheden van 11Mbit gehaald kunnen worden.

Er wordt momenteel onderzocht door Dienst ICT of de IEEE 802.11g-standaard geïmplementeerd kan worden. Deze 802.11g-standaard is bijna vijf keer sneller (54Mbit) dan de tot nu toe gebruikte 802.11b-standaard, waarmee de 802.11g-standaard wel downwards compatible is.
Er zijn momenteel ongeveer 1376 geregistreerde MAC-adressen (Media Access Control hardwareadres) en elke week zijn tientallen nieuwe verzoeken om gebruik te kunnen maken van het wireless netwerk.
Voordat studenten/medewerkers gebruik kunnen maken van het wireless netwerk, moeten ze een verzoek indienen bij de ICT helpdesk. Bij dit verzoek moet de gebruiker het MAC-adres van de draadloze netwerkkaart aanleveren. De MAC-adressen die opgegeven worden door de gebruiker worden alleen gecontroleerd op juiste het formaat, niet of het daadwerkelijk het echte MAC-adres is van de netwerkkaart waarmee gewerkt zal worden. Het MAC-adres wordt vervolgens in een gebruikerslijst geplaatst. Er komt dus relatief veel administratief werk aan de pas voordat een gebruiker op het wireless netwerk kan.
In figuur 4.2 is de huidige situatie van het MAC authenticatie proces weergegeven. Zodra een gebruiker gebruik wil maken van het wireless netwerk *(Connect)*, zal het access point dat door de gebruiker wordt aangesproken de RADIUS (Remote Authentication Dial-In User Service) server raadplegen *(Access-request)*. De server wil vervolgens de echtheid van het access point op vragen *(Acces-Challenge).* Het access point verstuurt het gedeelde geheim van de RADIUS server mee met het MAC-adres, van de gebruiker die op het netwerk wil, naar de RADIUS server *(Access-Request)*. De RADIUS server zoekt dit MAC-adres op in de gebruikerslijst *(AutBy File)*. Indien dit MAC-adres in de lijst voorkomt zal de RADIUS server een bericht versturen naar het access point dat alles in orde is of niet *(Reject/Accept)*. Het access point zal vervolgens de sessie starten voor de gebruiker of deze de toegang weigeren *(Access-Reject/Session start)*.



Figuur 4.2: MAC-adres authenticatie

Authenticatie gebaseerd op het MAC-adres is niet geheel veilig, het is al enige tijd mogelijk om een MAC-adres te spoofen. Het is zelfs eenvoudig om het MAC-adres te spoofen; de tools die dit mogelijk maken zijn steeds makkelijker in gebruik en zijn vrij eenvoudig te bemachtigen.
Er wordt geen data encryptie zoals WEP (Wired Equivalent Privacy) of WPA (Wi-Fi Protected Access) gebruikt, dus het is ook goed mogelijk om het dataverkeer te analyseren met een sniffer.
Ook kost het veel administratief werk voordat een gebruiker zijn MAC-adres kan gebruiken.

Gebruikersgroep: Fixed aansluiting
De knelpunten/problemen zijn hier:

- Iedereen met een laptop zonder enige relatie met de Haagse Hogeschool kan gebruik maken van het netwerk.
- De gebruiker authenticeert zich niet voor internetgebruik waardoor het ook onmogelijk is een gebruiker te identificeren of te autoriseren. Indien de gebruiker zijn/haar home-directory wilt raadplegen, dient de gebruiker zich wel te authenticeren.

Op de afdeling Informatica zijn bepaalde locaties beschikbaar waar gebruikers gebruik kunnen maken van een fixed netwerkaansluiting.
Gebruikers sluiten hun netwerkkaart aan met behulp van een UTP (Unschielded Twisted Pair) kabel en kunnen vervolgens direct op het netwerk.
De laptop krijgt een IP adres van de DHCP (Dynamic Host Configuration Protocol) server zonder enige vorm van authenticatie en de gebruikers kunnen aan de slag.

Gebruikersgroep: Studentenflat de Struyck
De problemen en knelpunten bij de Struyck zijn:

- Er vindt geen authenticatie plaats waardoor ook niet studenten gebruik kunnen maken van de netwerkaansluiting.
- Er is een netwerk van (unmanageable) hub's waardoor het verkeer kan worden gesniffed.
- Een gebruiker die problemen veroorzaakt op het netwerk kan niet worden achterhaald. Er is dus geen relatie tussen een gebruiker en het gebruikte MAC-adres en/of IP adres.
- Administratief: Er zijn geen gegevens bekend over wie waar woont en welke netwerkaansluiting deze personen hebben.

De bewoners van de studentenflat de Struyck maken gebruik van de aanwezige UTP aansluiting die aanwezig is op hun kamer. De Struyck maakt gebruik van een netwerk van hub's en is met de Haagse Hogeschool verbonden door middel van een 100 Mbit draadloze verbinding.
De gebruikte hub's zijn in eigendom van de exploitant van de studentenflat en niet in het beheer van de Haagse Hogeschool. De hub's die gebruikt worden zijn niet te managen, waardoor niks vanaf een afstand kan worden aangestuurd. Een kenmerk van een netwerk van hub's is dat al het verkeer naar elke andere aansluiting wordt gestuurd zonder te bepalen voor wie dat netwerkverkeer bedoeld is.
De gebruikers in de studentenflat authenticeren zich niet. Er is een firewall aanwezig op de Struyck die ervoor zorgt dat de gebruikers niet geheel onbeschermd op het internet zitten. Daarnaast zijn geen gegevens beschikbaar over de aansluitingen en welke gebruiker daarbij hoort.

Gebruikersgroep: Studentenflat Laakhaventoren
Bij de Laakhaventoren zijn de knelpunten/problemen:

- Een gebruiker die problemen veroorzaakt op het netwerk kan niet worden achterhaald. Alleen een switchport in combinatie met kamernummer is bekend.
- Administratief: Er zijn geen gegevens bekend over wie waar woont en welk netwerkaansluiting deze personen hebben.

De Laakhaventoren maakt gebruik van een geheel geswitched netwerk en is via een glasvezelkabel verbonden met de Haagse Hogeschool. Bij elke kamer in de Laakhaventoren zit standaard ook een netwerkaansluiting.
In tegenstelling tot de Struyck wordt in de Laakhaventoren wel gebruik gemaakt van een volledig geswitched en manageable netwerk. Helaas zijn ook hier geen gegevens bekend over welke bewoner bij welke aansluiting hoort. Hierdoor is contact moeilijk te leggen tussen Dienst ICT en een gebruiker van een bepaalde poort. Wat wel bekend is, is welke kamer bij welke switchpoort hoort. Communicatie gebeurt nu door middel van anonieme brieven die bij de kamernummers afgeleverd worden.

Gebruikersgroep: Technische Hogeschool Rijswijk
Er is hier dus een globaal "probleem":

- Er moet een beveiligd wireless netwerk komen met authenticatie.

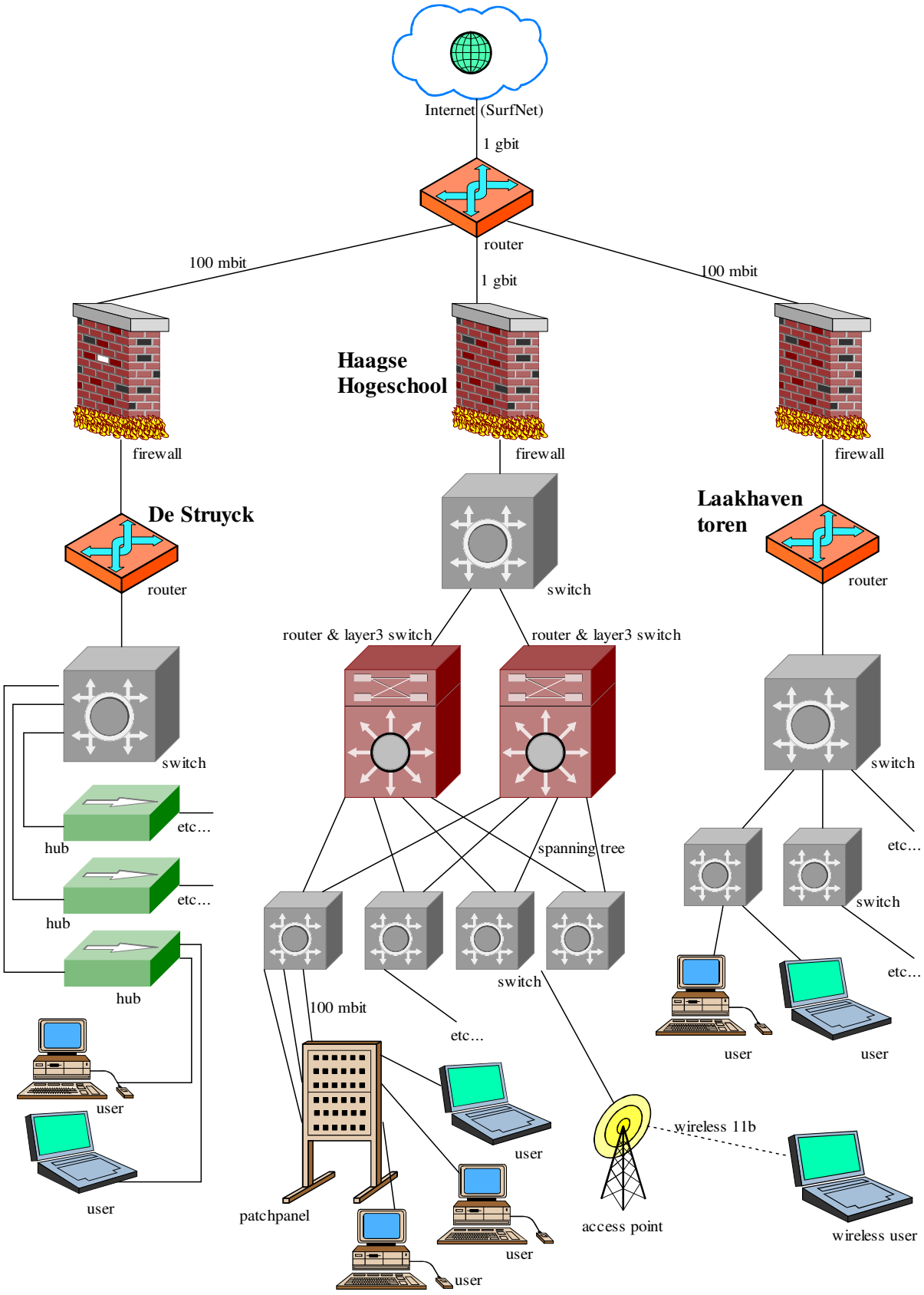
De Technische Hogeschool Rijswijk heeft nog geen netwerk voor gebruikers met een computer in eigen beheer. Er staat al enige tijd een wireless netwerk in de planning, echter is besloten om met de aanleg van deze te wachten op het resultaat van het onderzoek dat de afstudeerder uitvoert.
De afstudeeropdracht heeft dus ook betrekking tot de netwerkproblematiek in de THRijswijk. De afstudeerder is bij de Technische Hogeschool op bezoek geweest om daar informatie te vergaren betreffende het toekomstige wireless netwerk.

Problemen en knelpunten
De hierboven genoemde problemen en knelpunten zijn voortgekomen uit de interviews die zijn gehouden met de medewerkers van Dienst ICT, maar ook uit de conclusies die konden worden getrokken. Veel problemen konden ook worden afgeleid van andere problemen (oorzaak -> gevolg).

4.2 ▫ Overzicht netwerk

Op de volgende pagina (figuur 4.3) is een overzicht te zien van het Haagse Hogeschool netwerk. Het is geen detail tekening, wat inhoud dat niet elke switch/hub/gebruiker zichtbaar is.

Centraal in het netwerk van de Haagse Hogeschool staat een tweetal identieke "Layer 3" switches. Layer 3 switching is een uitdrukking voor een klasse van high-performance routers geoptimaliseerd voor het campus LAN of intranet. Eén van de switches is de backup van de andere, zodat in geval van storingen deze backup het werk kan overnemen.
De Layer3 switches zijn met de andere normale switches via glasvezel kabels (1 Gbit) verbonden. Deze switches bevinden zich in de zogenaamde "LAN-ruimtes" (verdeelruimte). Om alle computers op de HHS op het netwerk aan te sluiten zijn 17 LAN-ruimtes aanwezig. Deze ruimtes zijn door het hele gebouw verspreid omdat de maximale lengte van de gebruikte kabels (UTP) zo'n 100 meter is. Elk zo'n computer heeft een 100 Mbit netwerk aansluiting.
Om de beveiliging van de netwerken te verhogen is er een logische scheiding gemaakt tussen de vele netwerken van de studenten en medewerkers. Om dit te bereiken zijn er tientallen VLAN's aangemaakt. Deze VLAN (Virtual Local Area Network) bieden de mogelijk om netwerken van elkaar te scheiden zonder hier fysiek aparte netwerken voor aan te leggen.
SURFnet levert de Haagse Hogeschool een 1 Gbit internetverbinding. Momenteel maakt deze internetverbinding deel uit van het SURFnet5 netwerk. Dit netwerk verbindt allerlei hogescholen, universiteiten en onderzoekcentra met elkaar via glasvezelkabels. De internetverbinding naar de studentenflats zijn gelimiteerd tot elk 100 Mbit.

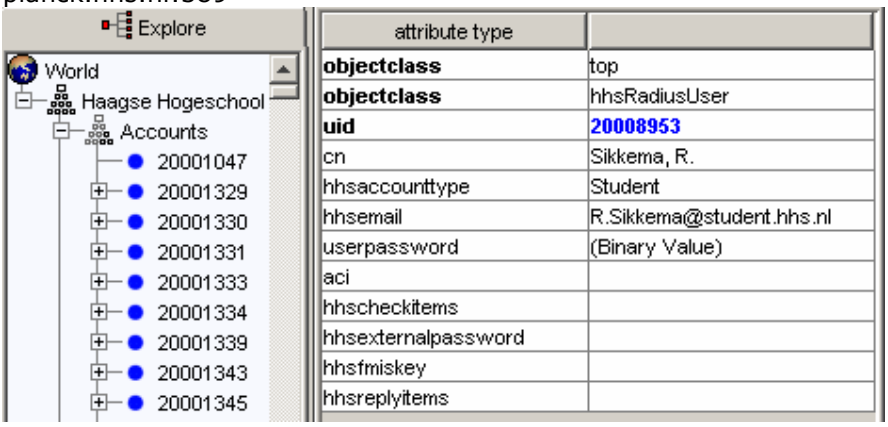


Figuur 4.3: Overzicht Netwerk Haagse Hogeschool en de twee studentenflats.

4.3 ▫ Databases

LDAP
De accountgegevens van de studenten en medewerkers van de Haagse Hogeschool zijn in één centrale database opgeslagen.
Deze database maakt gebruik van LDAP (Lightweight Directory Access Protocol). Dit is niet zozeer een echte database zoals bijvoorbeeld Oracle, maar een protocol om met directories te werken. LDAP is vooral bedoeld om snel en vaak gegevens op te vragen uit een grote hoeveel accounts.
Met behulp van een LDAP account met extra rechten heeft de afstudeerder informatie ingewonnen over de structuur van de LDAP server.
Voor elke gebruiker is een veld met de unieke identificatie, namelijk het veld "uid". Voor studenten bestaat dit veld uit acht cijfers, voor medewerkers uit onbepaald aantal letters.
Ook is voor elke gebruiker een encrypted password opgeslagen met behulp van het one-way hash mechanisme SHA (Secure Hash Algorithm Standard).
Daarnaast zijn er nog de verplichte velden "cn" (common name) met de achternaam en voorletter(s), email en accounttype (student of medewerker) altijd aanwezig.
Verder zijn er nog een aantal optionele velden die niet van belang zijn bij deze afstudeeropdracht.
In figuur 4.4 is de structuur van de LDAP server weergeven.

planck.hhs.nl:389



Figuur 4.4: LDAP structuur

MAC-adressen
De database die gebruikt wordt voor het wireless netwerk staat geheel los van de LDAP database.
Deze database is een plain text bestand dat telkens door een RADIUS server wordt geraadpleegd. Alle accounts van de wireless netwerk gebruikers staan dus in één lange lijst waar de precieze opmaak erg van belang is.
Een database die uit één lap tekst bestaat is erg gevoelig wat betreft foutieve invoer. Nieuwe accounts dienen dan ook zorgvuldig in de database geplaatst te worden.
De functionaliteit van deze database staat ook afgebeeld enkele pagina's terug in figuur 4.2.

5 ◦ Eisen en wensen

De problemen en knelpunten waren bekend, dus konden de eisen en wensen worden in kaart worden gebracht. De eisen en wensen zijn opgesteld in overleg met de opdrachtgever. De afstudeerder had een lijst bedacht met allerlei onderdelen waarop de opdrachtgever aangaf of dit een wens of eis was.
De eisen en wensen zijn in vier verschillende groepen verdeeld: technische, gebruikers platform, beveiliging en beheer.
Door de dunne scheiding tussen een eis en een wens, is per onderdeel aangegeven in welke mate dit naar een eis of wens neigt.

5.1 ▫ Technische eisen en wensen

De oplossingen zullen aan een aantal technische eisen en wensen moeten voldoen.

Database voor authenticatie
De afstudeeropdracht draait om authenticatie van gebruikers. Om gebruikers te authenticeren is een database nodig waar deze gebruikers in staan.
Er is hier onderzocht welke bestaande databases gebruikt kunnen worden en of eventueel nieuwe databases aangemaakt moeten worden.
De opdrachtgever had de eis dat de huidige standaard gebruikersaccount voor de authenticatie gebruikt zal worden. De gegevens van de standaard gebruikers account bevinden zich op de centrale LDAP database van de Haagse Hogeschool. De LDAP database maakt gebruik van een aantal attributen en velden (zie paragraaf 4.3). De structuur van de database mag op geen enkele wijze worden gewijzigd voor gebruik van deze afstudeeropdracht. De huidige LDAP database moet dus geheel ongewijzigd blijven en mogen geen accounts en/of attributen worden toegevoegd. Dit heeft te maken met de beveiliging en de bevoegdheden. Er mag eventueel een extra database gebruikt worden voor gebruikers met speciale rechten, maar de authenticatie dient normaal via LDAP te gaan. Er zijn ook een aantal gebruikers die niet van de Haagse Hogeschool zijn, maar toch gebruik moeten kunnen maken van het netwerk. Ook deze gebruikers kunnen in een aparte database komen te staan.

Authenticatie Server platform
Er moet worden bepaald op wat voor een operating system de serverapplicaties moeten kunnen draaien. De keuze van serverapplicatie word pas in hoofdstuk zes bepaald, maar het betreft hier in ieder geval applicaties voor de authenticatie en webservices. Hier wordt alleen vastgesteld op welk OS de applicaties kunnen draaien. Onderliggende kennis van de beheerders van Dienst ICT speelt hier een grote rol.

Solaris:
Momenteel worden vooral Solaris servers gebruikt binnen de Haagse Hogeschool. Een Solaris server is een optie, geen vereiste.
Linux:
Linux is ook een optie. Er is geen beleid wat betreft welke versie van Linux gebruikt moet worden.
Windows:
Het gebruik van een Windows server platform is geen optie.
MacOS:

Er mag geen MacOS gebruikt worden als operating system voor de server. Er is geen tot weinig kennis over dit besturingssysteem bij de medewerkers van Dienst ICT.
Aanschaf nieuwe serverapplicaties tegen betaling:
Nieuwe software pakketen kunnen alleen worden aangeschaft indien het niet anders kan.

Hardware
Welke hardware mag/moet worden gekocht en/of hergebruikt. Er is al een hoop netwerk apparatuur aanwezig op de Haagse Hogeschool. Bij nieuwe beveiligingstechnieken zal niet alle apparatuur altijd even goed werken.

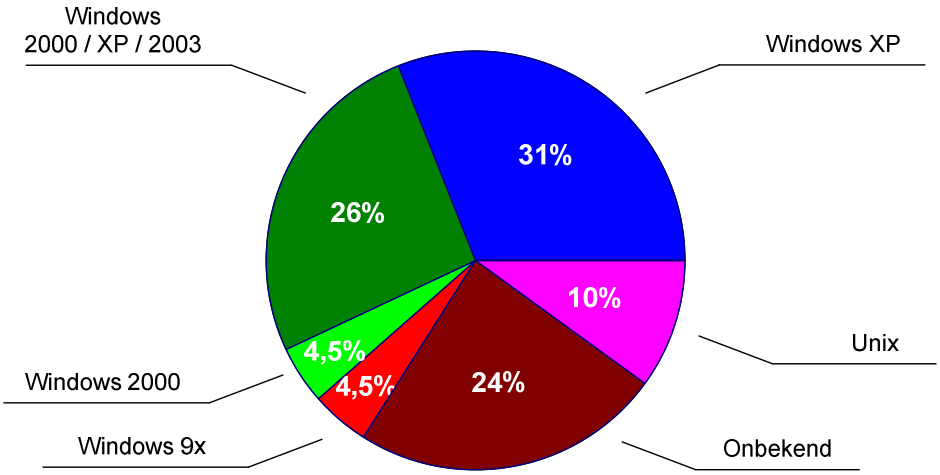
Access points:
De huidige access points moeten kunnen worden gebruikt en mogen niet worden vervangen door andere types. Nieuwe access points zullen alleen worden aangeschaft om het bereik van het wireless netwerk te vergroten.
Dit omdat de access points nieuw zijn en nog lang niet aan vervanging toe zijn.
Switches:
Er zijn in het Haagse Hogeschool netwerk veel verschillende types switches aanwezig. Alle moderne switches moeten kunnen worden hergebruikt. Er is ook een klein deel oude switches aanwezig, deze hoeven niet opnieuw gebruikt te kunnen worden en zullen eventueel vervangen kunnen worden.
Routers:
De huidige routers dienen te worden gebruikt en mogen dus niet worden vervangen. Ook kunnen geen nieuwe routers worden aangeschaft.
Authenticatie Server: Een nieuwe server aanschaffen is ongewenst, maar niet geheel onmogelijk. Er wordt een sterke voorkeur gegeven om gebruik te maken van een bestaande computer of server.

Website
De website moet de informatievoorziening voor de gebruikers met de maatregelen bevatten. Nadat duidelijk werd dat er een website moest worden gemaakt, zijn ook eisen en wensen geïnventariseerd betreffende de website.
De website moet in de style van de algemene website van de Haagse Hogeschool worden gemaakt. Dit betreft zowel lay-out, kleurgebruik en lettertype.
Het lettertype is “Verdana” (dit huidige lettertype) en de gebruikte kleuren zijn zwart, grijs, wit en blauw.
Door het gebruik van een eenduidige style zal het voor gebruikers duidelijk zijn dat het een website betreft van de Haagse Hogeschool.

5.2 ▫ Gebruikers platform eisen en wensen

Dit zijn de eisen en wensen voor de systemen van de gebruikers. Om een indruk te krijgen van het gebruik van operating systemen onder de gebruikers, heeft de afstudeerder, in samenwerking met de opdrachtgever, met het netwerkanalyse programma (GFI Languard) een inventarisatie gemaakt van de computers uit de twee studentenflats. Het resultaat van deze inventarisatie is in figuur 5.1 terug te lezen.
In de figuur is er een tweetal groepen die een toelichting nodig hebben: de computers met het resultaat “*onbekend*”, zijn computers die geen response gaven op de scans. Dit zijn bijvoorbeeld computers met een firewall die deze scans tegenhoudt.

De tweede opmerkelijke groep is de groep "*Windows 2000 / XP / 2003*". Het netwerkanalyse programma kon alleen vaststellen dat er een Windows versie gebruikt werd gebaseerd op de Windows NT engine.
Daarnaast is de huidige trend dat het gebruik van Windows XP toeneemt ten koste van de oudere Windows platformen. Deze trend is al enkele jaren bekend en zal tot de introductie van een nieuwe Windows platform ook waarschijnlijk niet veranderen.



Figuur 5.1: Operating System Platform Statistieken

Aan de hand van figuur 5.1 en in overleg met de opdrachtgever is besloten welke operating systemen ondersteunt moeten worden.

Ondersteuning gebruikers platform
Welk besturingssysteem moet worden ondersteund, onafhankelijk van eventuele extra software/hardware.

Windows 98:
Ondersteuning van Windows 98 is gewenst, maar niet noodzakelijk.
Windows 2000:
Ondersteuning van Windows 2000 is zeer gewenst, maar niet verplicht.
Windows XP:
Windows XP (Home/Pro) ondersteuning is een eis en hiervan kan niet van worden afgeweken. Dit omdat Windows XP verreweg het meest gebruikte OS is.
Windows CE:
Windows CE ondersteuning is gewenst maar niet noodzakelijk.
Linux:
Ondersteuning van Linux en varianten daarop zoals BSD is gewenst, maar niet noodzakelijk
MacOS:
Ondersteuning voor MacOS is optioneel, het is leuk als het ondersteunt wordt maar zeker geen noodzaak.

Gebruikers software
Mogelijkheid tot installatie/aanschaf van extra software voor gebruikers.

Geen extra software nodig voor Windows XP:
Deze keuze heeft de grootste voorkeur. Indien mogelijk dient een oplossing te worden gezocht waarbij geen extra software nodig is.
Gratis software voor Windows XP:
Als extra software nodig is, is het erg gewenst dat deze software gratis is.
Gratis voor elke client:
Als extra software nodig is, is het erg gewenst dat deze software gratis is. Naar mate de ondersteuning kleiner is voor de operating system, is het minder belangrijk dat hier gratis software voor beschikbaar is.
Commerciële software: Ongewenst. Dit is alleen een eventuele optie als een schoolbrede licentie kan worden gekocht en niet als hier een stukprijs aan verbonden is.

5.3 ▫ Eisen en wensen ten aanzien van beveiliging

Welke eisen en wensen zijn beschikbaar op het gebied van beveiliging. Deze maatregelen zijn erg uiteenlopend. Omdat het onmogelijk was om elke vorm van beveiliging te behandelen, zijn alleen de meest voorkomende maatregelingen behandeld.

Dataverkeer gecodeerd:
Enige mate van codering wel gewenst, echter hoeft niet al de data gecodeerd verstuurd te worden. Dit omdat niet uiterst gevoelig dataverkeer plaats vindt op de Haagse Hogeschool in tegen stelling tot bijvoorbeeld een bank.
Client Certificaat:
Client certificaten uitbrengen is zeer ongewenst en mag alleen gebruikt worden indien niets anders mogelijk is. Het werken met Client certificaten brengt veel administratie met zich mee. Ook moet dan een PKI (Public Key Infrastructure) worden opgezet.
Server Certificaat:
Het gebruik van server certificaten is optioneel. Een officieel VeriSign certificaat is op ten duur gewenst indien een server certificaat nodig blijkt te zijn. Een officieel certificaat heeft het voordeel standaard het root certificaat van Windows XP te ondersteunen.
Beveiliging tegen dictionary attacks:
Als het systeem tegen dictionary attacks is beveiligd, is dat wel zo prettig. De Haagse Hogeschool verplicht studenten en medewerkers ook om een password te gebruiken voor hun LDAP account dat bestand is tegen “dictionary attack”.
Beveiliging tegen Man-in-the-Middle (MitM) aanvallen: MitM aanvallen vormen niet een grote dreiging en het systeem hoeft hier niet tegen beschermd te zijn. Het kan geen kwaad als die dat wel is. Het is in het algemeen moeilijk om een heterogene omgeving te beschermen tegen MitM aanvallen. De Haagse Hogeschool is een heterogene omgeving door de diversiteit van systemen die aanwezig is.
Gebruik tijdelijke sessies:
Optionele maatregel. Het gebruik van een tijdelijke sessie brengt enkele voordelen met zich mee. Zo zal een “session hi-jack“ minder snel plaatsvinden.
Blacklist: Er moet een blacklist kunnen worden bijgehouden waar gebruikers, die zich niet houden aan de regels van het netwerkgebruik, op kunnen worden gezet.

Voorkeur op welke OSI laag te beveiligen:
Voorkeur gaat uit om op de linklaag (laag 2) te beveiligen.
Als op laag 2 beveiligd wordt, is normaal netwerkverkeer onmogelijk en kan de computer van de gebruiker alleen met de switchport / access point communiceren. Verkeer naar andere gebruikers toe is niet mogelijk.

5.4 ▫ Eisen en wensen ten aanzien van beheer

Welke eisen en wensen zijn verbonden aan het beheer van de beveiligingsmaatregelen.

Extra administratieve werkzaamheden:
Het is wenselijk dat een geheel geautomatiseerde oplossing mogelijk is.
Er zijn te weinig manuren aanwezig om veel handmatige procedures uit te voeren.
Logging: Het kunnen loggen is een harde eis. Er moet worden kunnen gelogged wanneer studenten inloggen met de daarbij behorende gegevens. Er dient minimaal een koppeling te zijn tussen de gebruiker en het netwerkgebruik met tijdstip van gebruik.
Opsporen gebruikers via log:
Gebruikers moeten kunnen worden achterhaald doormiddel van zoekopdrachten.
Accounting (registratie): Het gebruik van accounting is optioneel. Accounting is een uitbreiding op het normale loggen. Zo kan bij accounting informatie worden bijgehouden over duur van het netwerkgebruik en de hoeveelheid verzonden data.

6 ◦ Onderzoek oplossingsmogelijkheden

In dit hoofdstuk zal duidelijk worden gemaakt hoe te werk is gegaan bij het onderzoek naar de verschillende oplossingsmaatregelen.

6.1 ▫ Opzet onderzoek

Aan het begin van het onderzoek is alleen onderzocht wat voor mogelijkheden er zijn op het gebied van authenticatie en netwerkbeveiliging. In dit stadium van het onderzoek werd alleen globaal gekeken of deze technieken toepasbaar waren voor de Haagse Hogeschool.
Deze informatie is voornamelijk op het internet opgezocht. Interessante links en pagina's werden opgeslagen en/of uitgeprint. Helaas was het niet altijd even duidelijk of een bepaalde oplossing enigszins bruikbaar was. Dit omdat de afstudeerder veel onbekende termen of vage beschrijvingen tegen kwam. Het was ook moeilijk om te bepalen wanneer gestopt moest worden met het lezen over een bepaald onderwerp. Dit omdat sommige oplossingen erg uitgebreid zijn en ook veel documentatie bieden.
De uiteindelijk gekozen oplossingen zijn in een longlist gezet. De complete longlist inclusief informatie over de oplossing is in bijlage B te vinden.

Hier is een overzicht van de oplossingen uit de longlist:

- IPsec
- Mac adres authenticatie
- Firewall
- Authentication bridge
- VPN server
- 802.1x
- Kerberos
- A-select

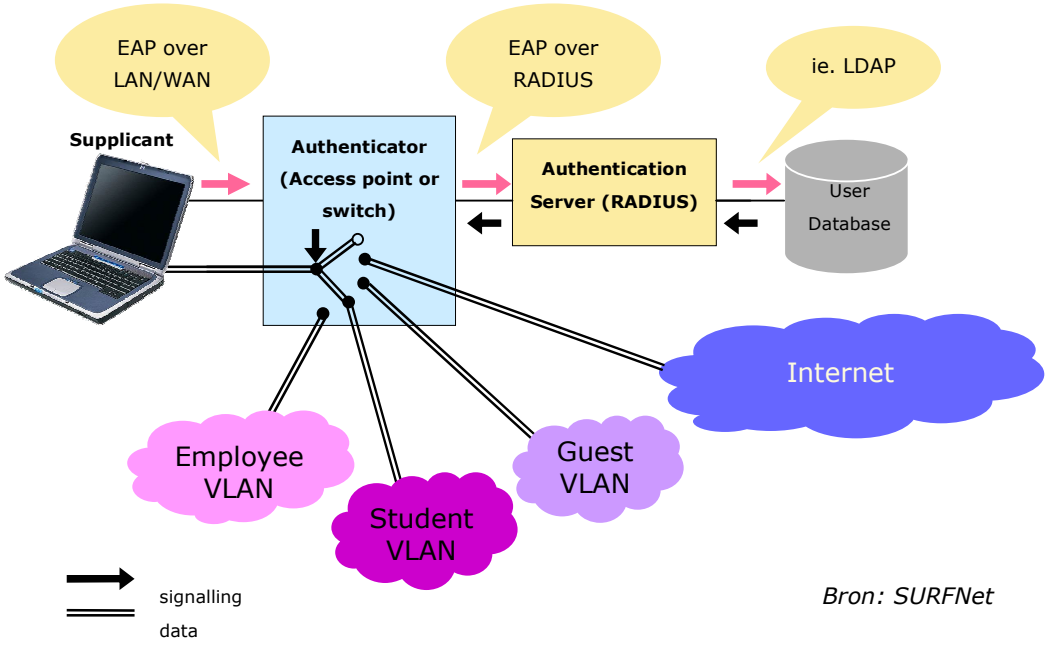
6.2 ▫ Resultaten onderzoek

Aan de hand van de eisen en wensen, problemen en knelpunten en doelstelling is een keuze gemaakt uit de longlist.
De oplossingen uit de shortlist bestaan ook weer uit deeloplossingen. Dit omdat de oplossingen meer een methode beschrijven die flexibel kunnen worden toegepast op verscheidene manieren.

De shortlist bestaat uit:

- 802.1x (EAP)
- firewall

In tegenstelling tot de gebruikelijke shortlist, bevat deze shortlist al de methodes die gebruikt zullen worden. In het verdere onderzoek is bepaald hoe deze methode op de Haagse Hogeschool het best kan worden toegepast.
Er is voor 802.1x gekozen als voornaamste oplossing. Deze oplossing kon echter niet worden toegepast op één doelgroep, studentenflat De Struyck. Voor deze doelgroep is gekozen voor een firewall oplossing.
In figuur 6.1 is beschreven hoe 802.1x in het algemeen werkt. De afstudeerder nam aan dat de werking van een firewall geen verdere uitleg nodig had.



Figuur 6.1: 802.1x in werking

In de IEEE 802.1x standaard staat beschreven hoe toegang tot een fixed of wireless netwerk geregeld kan worden met behulp van een flexibel authenticatie protocol, genaamd EAP (Extensible Authentication Protocol). In tegenstelling tot andere authenticatie oplossingen, kan 802.1x het netwerkverkeer op de linklaag (laag 2 OSI model) reguleren.
De gebruiker gebruikt 802.1x software (*suppicant)* op zijn of haar computer. Zodra de gebruiker connectie met het netwerk maakt, zal de supplicant met de switch of access point (*authenticator)* gaan communiceren via EAP. Deze authenticator verschaft de gebruiker toegang tot het netwerk, maar niet voordat de gebruiker zich kan authenticeren. De authenticatiegegevens worden bij de *Authentication Server* afgehandeld. Deze server verifieert de authenticatiegegevens met de gegevens uit de *User Database* (LDAP). De authentication server bepaald vervolgens in welk VLAN de gebruiker geplaatst moet worden.

Overzicht van EAP authenticatie mechanismen
Als men voor 802.1x authenticatie kiest, is het noodzakelijk om het juiste authenticatie mechanisme te kiezen. De juiste keuze van EAP authenticatie mechanisme is bepalend voor de rest van het netwerk; niet elke RADIUS/EAP server en netwerkapparatuur ondersteunt elke methode.
De voor en nadelen van verschillende EAP authenticatie mechanismen zijn in de onderstaande tabel gezet. Na de tabel volgt een uitleg van de gekozen EAP mechanisme en een verklaring waarom deze gekozen zijn.
Uit de voordelen en nadelen is een keuze gemaakt van bruikbare mechanismen. Er is voor PEAP en TTLS gekozen. Hieronder is een kleine uitleg te lezen van deze twee mechanismen met daaropvolgend een stuk waarom deze gekozen zijn. Het volledige rapport is in bijlage C te vinden.

EAP Mechanisme	LDAP support	Tunneled	Server Certificaat	Client Certificaat	Dynamische WEP key	Dynamische WEP key	Proprietary	Implementatie	Beveiliging
AKA	Nee	Nee	Nee	Nee	Ja	Ja	Nee	Moeilijk	Goed
FAST	Ja	Ja	Nee	Nee	Ja	Ja	Nee	Middelmatig	Goed
LEAP	Nee	Nee	Nee	Nee	Ja	Ja	Ja, Cisco	Makkelijk	Redelijk
MD5	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Makkelijk	Matig
PEAP	Ja	Ja	Ja	Nee	Ja	Ja	Nee	Makkelijk	Goed
SIM	Nee	Nee	Nee	Nee	Ja	Ja	Nee	Moeilijk	Redelijk
TLS	Ja	Ja	Ja	Ja	Ja	Ja	Nee	Moeilijk	Zeer Goed
TTLS	Ja	Ja	Ja	Nee	Ja	Ja	Nee	Middelmatig	Goed

Figuur 6.2: Overzicht van EAP authenticatie methodes

PEAP (Protected Extensible Authentication Protocol)
Het protocol bestaat uit twee fases; in de eerste fase wordt een sterk gecodeerde "outer" TLS (Transport Layer Security) tunnel opgezet. In de tweede fase van het proces worden authenticatie gegevens verstuurd via de "inner" methode. PEAP gebruikt de inner methode om vervolgens nog een tweede EAP uitwisseling mogelijk te maken. Deze is standaard EAP-MS-CHAPv2, maar PEAP ondersteunt ook EAP-TLS en EAP-GTC (Generic Token Card).

TTLS (Tunneled Transport Layer Security)
Net als PEAP bestaat het protocol bestaat uit twee fases; in de eerste fase wordt een sterk gecodeerde "outer" TLS tunnel opgezet. In de tweede fase van het proces worden authenticatie gegevens verstuurd via de "inner" methode.
In deze inner tweede fases kunnen verschillende mechanismen gebruikt worden zoals PAP, MS-CHAPv2 en MD5.

Keuze EAP
De Haagse Hogeschool maakt gebruik van een LDAP database voor het authenticeren van de gebruikers. Daarom is gekeken welke EAP mechanismen een LDAP database ondersteunen.

De volgende EAP mechanismen ondersteunen een LDAP database:
- EAP-FAST
- EAP-PEAP
- EAP-TLS
- EAP-TTLS

Elk van deze EAP methodes hebben bepaalde consequenties voor gebruikers en de Haagse Hogeschool. Deze consequenties worden per methode besproken. Algemene voor en nadelen zijn hieronder te lezen in de omschrijving van de methode (zoals bijvoorbeeld gevolgen van server certificaat).
Fast (Flexible Authentication via Secure Tunnelling)
FAST is momenteel nog alleen te gebruiken in combinatie met Cisco apparatuur, waardoor werkende netwerkkaarten van gebruikers vervangen moeten worden door Cisco netwerkkaarten. Ook moet een AAA server van Cisco worden aangeschaft. FAST is in zijn huidige vorm duur voor zowel de gebruikers als voor de Haagse Hogeschool.
PEAP (Protected Extensible Authentication Protocol)
PEAP in combinatie met MS-CHAPV2 is een makkelijke oplossing. Dit omdat Windows XP standaard van deze methode gebruik kan maken. Er zijn weinig instellingsmogelijkheden noodzakelijk in Windows XP voor PEAP, alles gaat automatisch. Dit is makkelijker voor gebruikers, echter biedt dit minder configuratiemogelijkheden. PEAP is zeker de moeite waard om verder te testen. Bij gebruik van PEAP in combinatie met GTC zullen de gebruikers extra apparatuur moeten aanschaffen (Tokencard) en software (Funk). Deze extra kosten die de gebruikers moeten maken zal niet in dank worden afgenomen, aangezien de gebruikers momenteel al een werkende netwerkverbinding hebben zonder extra kosten. Deze oplossing is om deze reden niet ideaal.
TLS (Transport Layer Security)
Om TLS te implementeren moet een PKI opgezet worden en daarnaast een Certificaten Manager worden aangesteld op de Haagse Hogeschool. Gebruikers moeten certificaten installeren en juiste server certificaat selecteren. Gezien de kosten en arbeid voor de Haagse Hogeschool die hiermee gemoeid zijn, wordt deze oplossing niet geprefereerd.
TTLS (Tunneled Transport Layer Security)
De consequenties bij invoeren van TTLS zijn vooral bij de gebruikers te vinden. Gebruikers moeten een 3rd party programma installeren om gebruik te kunnen maken van TTLS. Voor Windows XP/2000, Linux en Mac OS X 10.3 zijn gratis programma's te verkrijgen, voor overige besturingssystemen moeten gebruikers software kopen.

Helaas is geen enkele EAP methode perfect voor gebruik op de Haagse Hogeschool. Alle methodes hebben hun nadelen.
Van de vier verschillende methodes van hierboven komen PEAP en TTLS duidelijk als eerste keuzes naar voren. Om PEAP en TTLS in de praktijk te toetsen voor gebruik op de Haagse Hogeschool, zullen deze twee methoden in de pilots getest worden.

Keuze RADIUS Server
Er is een groot aanbod aan RADIUS server sofware. Een deel van dat aanbod is gratis te gebruiken omdat het bijvoorbeeld Open Source is. Het is cruciaal dat de gekozen EAP methode ondersteunt wordt door de RADIUS software. FreeRADIUS is verreweg de meest uitgebreide en stabiele RADIUS software die gratis te gebruiken is en ondersteunt dan ook de gekozen EAP methode. De Haagse Hogeschool heeft een onbeperkte licentie voor het gebruik van Radiator, een commercieel pakket.
Radiator biedt ook vrijwel alle functionaliteiten die FreeRADIUS heeft en biedt daarnaast nog vele configuratie en flexibiliteit opties. Er is al enige kennis van Radiator op de Haagse Hogeschool aanwezig en er zijn positieve ervaringen mee. Daarom is besloten de RADIUS server in te richten met Radiator in plaats van FreeRADIUS.

Server Certificaat
Voor enkele EAP methodes dient er een server certificaat geïnstalleerd te zijn op de RADIUS server. Voor elk van deze methodes wordt het server certificaat op dezelfde manier geïnstalleerd. Server certificaten kunnen gekocht of zelf gemaakt worden.
Een server certificaat kan worden aangeschaft bij een CA (Certificate Authority) zoals bijvoorbeeld VeriSign. Een voordeel om een certificaat van bijvoorbeeld VeriSign (of elk ander root certificaat) te gebruiken is dat Windows XP zulke standaard certificaten erkend en gebruikt.
Als alternatief kan er ook voor gekozen worden om zelf een CA te creëren. Deze CA kan worden gemaakt aan de hand van het Open Source programma OpenSSL. OpenSSL maakt CA certificaten aan en met behulp van deze CA certificaten kunnen er weer server certificaten worden gemaakt en ondertekend. Deze certificaten zullen echter niet worden erkend door enig instelling/programma. De certificaten zullen als “onbetrouwbaar” door het leven gaan omdat de zelf gemaakte CA niet een erkende root CA is. De gebruiker zal bij gebruik van deze onbetrouwbare certificaten zelf moeten aangeven of hij/zij het certificaat vertrouwen.
Een server certificaat van VeriSign is dus praktischer voor gebruikers, alleen is dit een commerciële oplossing in tegen stelling tot het gebruik van OpenSSL.
In een testsituatie is het gebruik van een OpenSSL certificaat wel aan te raden. Dit omdat een officieel uitgegeven certificaat eenmaal uitgegeven, niet meer gewijzigd kan worden. In een testsituatie zal het regelmatig voorkomen dat er wijzigingen doorgevoerd worden op de testsystemen.

7 ◦ De pilots

In dit hoofdstuk is de opzet van de verschillende pilots beschreven en de behaalde resultaten. De pilots zijn gebaseerd op de resultaten van het onderzoek, de eisen en wensen en de knelpunten van de huidige situatie.
Er is voor gekozen om eerst de meest eenvoudige vorm van 802.1x authenticatie uit te werken zonder hier extra functionaliteiten aan te verbinden. De verwachting was dat op die manier zo min mogelijk complicaties konden optreden en daarnaast was het een goede manier om bekend te raken met de materie. Vervolgens is door de afstudeerder aan de pilot gewerkt waarmee de authenticatie kan worden gelogd. De mogelijkheid om de authenticatie te loggen zou nuttig kunnen zijn voor de daaropvolgende pilots. De derde pilot was een losstaande pilot die niet veel tijd in beslag nam en eigenlijk tussendoor is gedaan. De vierde pilot is vervolgens een uitbreiding op de eerdere pilots. De vijfde pilot staat niet beschreven in de opdrachtomschrijving en had daarom een lagere prioriteit.

De volgende punten vormen de basis voor elke pilot en zullen in elke paragraaf worden beschouwd:

- Het doel van de pilot
- Hergebruik van vorige systemen en/of pilots
- De technische specificaties van de hard- en software
- De tijd en planning
- De gebruikte informatie bronnen
- Werkwijze
- De testresultaten en de problemen

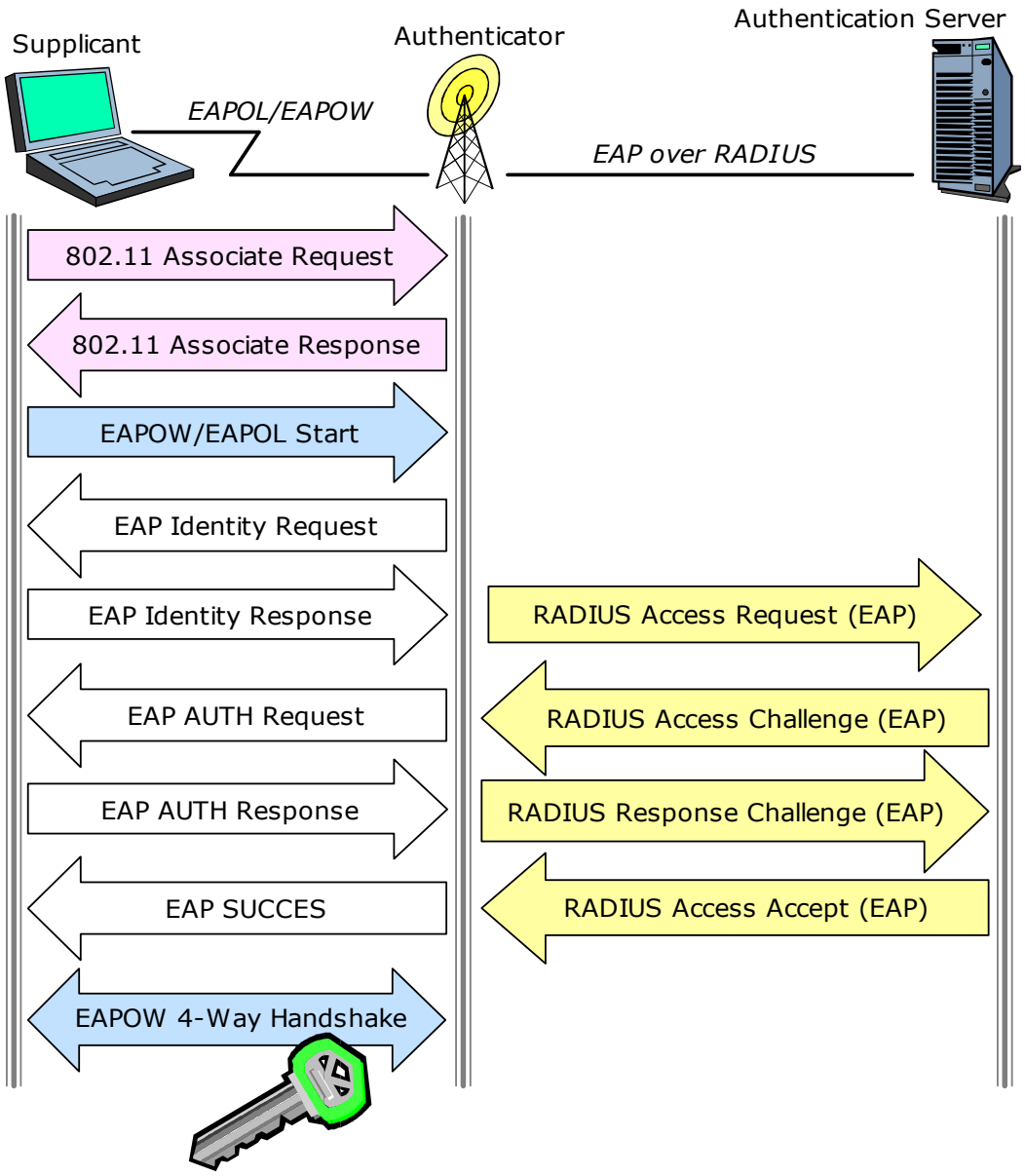
Daarnaast zijn alle verrichte handelingen gedocumenteerd door de afstudeerder. Door direct bij elke pilot correct te documenteren is voorkomen dat in een later stadium details over het hoofd gezien zijn. Deze documentatie is in bijlage D te vinden.

7.1 ▫ Pilot 1: 802.1x Authenticatie

Doel
Het doel van deze pilot was het tot stand brengen van authenticatie van een netwerkgebruiker via 802.1x. Deze authenticatie moest zowel via het wireless als fixed netwerk mogelijk zijn. Er is in het vorige hoofdstuk naar voren gekomen dat twee verschillende EAP protocollen onderzocht worden: TTLS (Tunneled Transport Layer Security) en PEAP (Protected Extensible Authentication Protocol). Er is onderzoek gedaan naar de voor- en nadelen van deze twee EAP vormen. Daarnaast is onderzocht welke “inner-tunnel” techniek gebruikt moest worden (PAP/MS-CHAPV2/etc.).
De volgende functionaliteiten zullen aanwezig zijn conform de eisen en wensen:

- Beperkte/geen netwerktoegang zonder authenticatie
- Authenticatie met behulp van de LDAP server
- Veilige overdracht van authenticatie gegevens
- Versleuteling van data over de ether (wireless)
- MAC-adres authenticatie naast 802.1x authenticatie laten werken ivm overgangsperiode

In figuur 7.1 is een tekening te vinden met het verloop van succesvolle authenticatie. Dit werkend krijgen is de primaire doelstelling van deze pilot.



Figuur 7.1: Succesvolle 802.1x authenticatie

Hergebruik
Een deel van de Radiator configuratie van de MAC-adres authenticatie uit de startsituatie is gebruikt om de nieuwe RADIUS server te configureren.
Omdat het de eerste pilot betrof kon voor de rest weinig worden hergebruikt.

Technische specificaties
De volgende hard- en software is gebruikt bij deze pilot:

- Authenticators: Als authenticators waren een switch met de mogelijkheid om 802.1x aan te zetten op porten en een access point met de mogelijk om een 802.1x SSID in te stellen nodig.
- Supplicant: Een computer met fixed en wireless netwerkmogelijkheden met administrator rechten. De laptop die de afstudeerder aan het begin van het project heeft gekregen is gebruikt.

- Authentication Server: Een RADIUS server. Er is een oude desktop PC beschikbaar gesteld om mee te testen. Op deze PC is Linux geïnstalleerd samen met Radiator, een RADIUS pakket.
- User Database: De LDAP server van de Haagse Hogeschool. Hier zullen de juiste credentials voor nodig zijn om connectie mee kunnen te maken met de RADIUS server.
- Een netwerkinfrastructuur tussen de hierboven genoemde hardware.

Tijd/Planning
Vanwege het feit dat allerlei onbekende apparatuur en software werd gebruikt, was onbekend hoeveel tijd nodig zou zijn voor de eerste pilot.
Een precieze schatting geven is hierdoor erg moeilijk, omdat onduidelijk is welke onderdelen veel problemen en tijd nodig hebben om te configureren.
De verwachting was dat het zo'n zeven werkdagen in beslag zou nemen om 802.1x authenticatie werkend te krijgen via het fixed en wireless netwerk. Daarna nog één dag om 802.1x naast het bestaande MAC-adres authenticatie systeem te laten draaien.
Deze verwachting klopte niet helemaal, in totaal heeft de eerste pilot 2 weken gekost. Er ging veel tijd verloren met het oplossen van problemen die van te voren niet waren ingeschat. Deze problemen worden verder toegelicht op de volgende pagina (resultaten).

Informatie bronnen
De informatie betreffende 802.1x authenticatie komt vooral van het Internet vandaan. Op de websites van de producenten van de apparatuur zijn de handleidingen van de desbetreffende producten gedownload. Er was bijvoorbeeld geen documentatie in papiervorm meegeleverd bij de Cisco apparatuur, alleen een verwijzing naar hun website. Op de mailarchieven van Radiator was een hoop informatie te vinden over problemen die optreden bij het configureren van de Radiator server.
De meest gebruikte en belangrijkste sites:

- www.cisco.com: Informatie over het configureren van de switch.
- www.open.com.au: De archieven en handleiding van Radiator.
- www.securew2.com: Alfa & Ariss SecureW2 EAP-TTLS client
- www.cpan.org: Perl modules voor Linux/Radiator
- www.utwente.nl: Op deze site is een document te vinden over een wireless 802.1x project

Werkwijze
In eerste instantie is de desktop PC met Linux (Red Hat 7.3) ingericht. Er waren geen eisen of wensen voor het gebruik van een bepaalde Linux versie, dus is er voor de meest praktische oplossing gekozen. Dit hield in dat de installatie CD's van Red Hat 7.3 aanwezig waren bij de opdrachtgever. Vervolgens is de nieuwste versie van Radiator (versie 3.9.2) gedownload en werd deze op de server geïnstalleerd. Voor Radiator is wel de nieuwste versie gebruikt, omdat hier regelmatig updates voor gepleegd zijn betreffende 802.1x authenticatie.
Vervolgens is de switch geconfigureerd via een terminal voor gebruik van 802.1x. Dit hield in dat op enkele poorten 802.1x ingesteld moesten worden en moest een authentication server worden gedefinieerd, de RADIUS server in dit geval.

Het access point is eerst via een fixed netwerkaansluiting geconfigureerd via de webinterface. De laptop zal de instellingen uitvoeren vanuit de standaard browser die al aanwezig is op het systeem.
Op de laptop werd de laatste versie van SecureW2 gedownload en geïnstalleerd. SecureW2 is een EAP-TTLS client van Alfa & Ariss.
Eerst werd de laptop ingesteld voor gebruik van EAP-PEAP om vervolgens de TTLS tegenhanger te testen. Radiator werd op de server geconfigureerd om alle mogelijke meldingen op het scherm weer te geven door middel van de variabele "trace 4". Dit hield in dat elke stap die Radiator onderneemt, wordt weergeven met debug, error, code, attributen, etc… informatie.
Na deze installaties en configuraties begon de afstudeerder met testen.
De documentatie die tijdens deze pilot is geschreven, is gebruikt voor een gebruikershandleiding betreffende de installatie van de EAP-TTLS client (SecureW2). Deze gebruikershandleiding is in de vorm van een eenvoudig HTML bestand gemaakt.

Resultaten
Tijdens het testen kwam al snel naar voren dat de installatie nog niet compleet was. Radiator gaf allerlei errors op het scherm weer zoals deze:

```
ERR: Could not load AuthBy module Radius::AuthLDAP2: Can't
locate Convert/ASN1.pm in @INC etc…
```

Na enig zoekwerk in de mail archieven van Radiator bleek het probleem te zitten in het feit dat allerlei verschillende Perl modules geïnstalleerd moeten worden op de server. Radiator biedt standaard veel mogelijkheden aan maar heeft wel de bijbehorende Perl modules nodig. Deze modules heeft de afstudeerder voornamelijk van de website van CPAN (Comprehensive Perl Archive Network) gehaald. Met behulp van de zoekopdrachten werd al snel duidelijk dat CPAN verreweg de grootste verzameling perl modules heeft. In eerste instantie werkte 802.1x authenticatie niet en was onduidelijk waar het probleem lag. Om het probleem te lokaliseren is het programma Ethereal gebruikt. Ethereal is een uitgebreid sniffer programma. Met behulp van een simpele hub kon al het netwerkverkeer met Ethereal gesniffed worden. Het probleem bleek een foutieve instelling op de switch te zijn die geen authenticatie gegevens door stuurde.
In eerste instantie werd met een lokaal bestand gewerkt (nog niet met LDAP) om EAP-PEAP authenticatie voor elkaar te krijgen. Dit ging goed totdat de LDAP server werd gebruikt ipv het lokale bestand. Na enig zoekwerk op de mailarchieven van Radiator bleek dat EAP-PEAP alleen LDAP ondersteunt indien deze server het gebruikers password in clear tekst opslaat. Dit komt omdat PEAP gebruik maakt van MS-CHAPV2 en zelf niet een clear password naar de RADIUS server stuurt. EAP-PEAP viel dus af als keuze voor 802.1x authenticatie.
De keuze van de inner-tunnel bij EAP-TTLS was om deze reden ook snel gemaakt; PAP (Password Authentication Protocol). PAP stuurt password in clear tekst formaat over een verbinding, dus dit leverde geen problemen op bij het authenticeren via de LDAP server.
Om MAC authenticatie naast 802.1x te laten draaien was het nodig meerdere SSID's in te stellen op de access point. Per SSID kan een authenticatie methode geselecteerd worden. Helaas kan een access point maar één SSID tegelijk broadcasten. Het was dus niet mogelijk om op de laptop een keuze te maken uit een lijst van beschikbare SSID's. Indien een SSID niet gebroadcast wordt, moet de precieze naam van de SSID bekend zijn. Om migratie problemen te voorkomen is het dus verstandig om voor het oude MAC authenticatie netwerk het huidige SSID te behouden, maar deze niet te broadcasten.

Tijdens het testen onderstonden ook problemen die niet direct met de inhoud van de pilot hadden te maken. Zo sneuvelden meerdere console monitors die op de switch/access point werden aangesloten. Deze consoles maakte het mogelijk directe toegang te bemachten tot de operating systems van de apparatuur. Na verschillende consoles (letterlijk) in rook te hebben zien op gaan hield uiteindelijk één het gedurende de rest van de pilots het vol.
Naast de problemen met de consoles begaf de harde schrijf van de Linux server het. De harde schrijf wou niet meer draaien en hierdoor was de schrijf onbruikbaar geworden, samen met de data die daar op stond.
Hierdoor moest Linux en Radiator volledig opnieuw worden geïnstalleerd. Om herhaling in de toekomst te verkomen, werd besloten om meerdere hard disks in het systeem te plaatsen. Nadat Linux en Radiator was geïnstalleerd en geconfigureerd, werd met Norton Ghost een exacte kopie gemaakt van de data en op de andere schrijf gezet (Ghost Image).

7.2 ▫ Pilot 2: Accounting/logging van gebruikers

Doel
Het doel van deze pilot is het "loggen" van het netwerkgebruik. Log bestanden worden bijgehouden om bij misbruik van het netwerk achteraf te kunnen zien wie hier verantwoordelijk voor was. Het netwerk wordt niet altijd bewust misbruikt, een computer kan ook besmet zijn een virus dat problemen veroorzaakt.
Er zijn een aantal attributen die vastgelegd moeten worden in een log bestand:

- Tijdstip begin van netwerkgebruik
- Gebruikersnaam
- IP-adres van de gebruiker
- MAC-adres van de gebruiker
- Naam en/of adres van de gebruikte switch/access port
- Tijdstip einde gebruik (of een teken van leven elke dertig minuten)

Deze attributen zijn overlegd met de opdrachtgever en gebaseerd op de bestaande log bestanden in gebruik bij de MAC-authenticatie.

Hergebruik
De configuraties van de hard- en software van de eerste pilot zijn hergebruikt. Vooral op het gebied van hardware waren niet veel wijzigingen nodig.

Technische specificaties
Naast de producten die gebruikt zijn in de eerste pilot is ook het volgende gebruikt:

- Database server: De logs zijn op een database opgeslagen. Op de RADIUS server is een database applicatie geïnstalleerd om dit mogelijk te maken. Er is een keuze gemaakt tussen een MySQL en PostgreSQL database. Allebei hebben ze veel overeenkomsten en zijn goed bruikbaar, echter is voor MySQL gekozen omdat deze simpeler in gebruik is en minder systeem resources nodig heeft. De database "radius" is aangemaakt en de tabel "accounting" is daarin opgenomen. In figuur 7.3 staat deze tabel beschreven.

Tijd/Planning
De verwachting was dat de pilot zo'n twee dagen in beslag zou nemen. Deze planning werd overschreven doordat problemen optraden die niet direct konden worden opgelost. In totaal zijn vier dagen aan deze pilot besteed.

Informatie bronnen
De afstudeerder was alleen bekend met Ingres als database dus was het nodig MySQL kennis op te doen. De primaire bron was de handleiding die op de website van MySQL te vinden is. Deze handleiding is erg uitgebreid en bevat veel gebruikerscommentaar zoals oplossingen voor de meest voorkomende problemen.

- http://dev.mysql.com/doc/mysql/en/index.html: MySQL Reference Manual, Zoekfunctie, met gebruikerscommentaar.

Werkwijze
Eerst is de server versie van MySQL geïnstalleerd op de server. Deze installatie verliep zonder problemen. Vervolgens was een koppeling nodig tussen Radiator en MySQL; de CPAN perl modules.
Al snel bleek dat Radiator ook de "Client programs" en "Dynamic client libraries" versie van MySQL nodig had om te kunnen werken.
Na de installatie kon een database worden aangemaakt en de Radiator configuratie worden aangepast.
In de handleiding van MySQL stond stap voor stap beschreven hoe een database kon worden aangemaakt en hoe deze ook kon worden beveiligd met gebruikersrechten. Met behulp van commando GRANT (=toekennen) zijn verschillende gebruikers aangemaakt en rechten bepaald. Radiator heeft alleen de SELECT,INSERT en UPDATE rechten nodig om de accounting gegevens te verwerken. Vervolgens is de Radiator configuratie aangepast om alle accounting verzoeken naar de database weg te schrijven. De access point en switch zijn hierna geconfigureerd om accounting verzoeken door te sturen naar de RADIUS server.

Resultaten
EAP-TTLS maakt gebruik van een "outer" en "inner" tunnel. De outer tunnel beschermt de inner tunnel van de buitenwereld. Om ervoor te zorgen dat kwaadwilligen niet kunnen traceren wie op een bepaald moment probeert te authenticeren, maakt de outer tunnel gebruik van een anonieme identiteit. Deze anonimiteit leverde problemen op bij het loggen van de inloggevens. Alle gebruikers werden in de database weggeschreven als "anonymous" waardoor de log onbruikbaar was.
Na enig zoekwerk op het mailarchief van Radiator bleek een perl hook (mini programma speciaal geschreven voor een applicatie) beschikbaar te zijn speciaal voor EAP-TTLS accounting. Na deze hook te hebben geconfigureerd met de database, werd met de juiste gebruikersnaam gelogd.
Helaas trad nog een probleem op: de IP-adressen van de gebruikers werden niet in de database gezet. Na verscheidene pogingen de configuratie te veranderen bleek dat hier het probleem niet lag. Aan de hand van het sniffer programma Ethereal werd al het netwerkverkeer naar de RADIUS server weer geanalyseerd. Het IP-adres van de gebruiker die zich authenticeerd had, werd in geen enkel pakketje gevonden. Na een korte literatuurstudie kwam ik tot de kern van het probleem; 802.1x werkt op de linklaag (laag 2) en op deze laag is alleen nog maar het MAC adres bekend. Op de access point is het IP adres wel bekend van de gebruiker, echter is momenteel geen mogelijkheid om deze mee te sturen met accounting. Via de opdrachtgever is dit nog nagevraagd bij Cisco of hier al oplossingen voor zijn die kunnen worden toegepast op de RADIUS server of access point. De enige oplossing die Cisco wist was het wegschrijven van de router ARP (Address Resolution Protocol) logs naar een aparte database.

Deze database kan dan weer gekoppeld worden met de accounting database op basis van het MAC-adres en tijdstip. Helaas was deze pilot dus niet geheel een succes en kon niet een geheel complete log in de database worden opgeslagen. Een voorbeeld van zo'n log:

```
mysql> SELECT USERNAME,TEXT_TIME_STAMP,ACCTSTATUSTYPE,ACCTSESSIONID,ACCTSESSIONTIME,
NASIDENTIFIER,CALLINGSTATIONID FROM ACCOUNTING;
+----------+---------------------+----------------+---------------+ ->
| USERNAME | TEXT_TIME_STAMP     | ACCTSTATUSTYPE | ACCTSESSIONID | ->
+----------+---------------------+----------------+---------------+ ->
| rsikkema | 2005-01-10 21:04:26 | Start          | 00001C27      | ->
| rsikkema | 2005-01-10 21:05:39 | Stop           | 00001C27      | ->
+----------+---------------------+----------------+---------------+ ->
+-----------------+---------------+------------------+
| ACCTSESSIONTIME | NASIDENTIFIER | CALLINGSTATIONID |
+-----------------+---------------+------------------+
|            NULL | 0011.5c2d.4af0 | 000d.54a1.8dc7   |
|              73 | 0011.5c2d.4af0 | 000d.54a1.8dc7   |
+-----------------+---------------+------------------+
2 rows in set (0.00 sec)
```

7.3 ▫ Pilot 3: Authenticatie via Firewall

Doel
De studentenflat De Struyck maakt gebruik van unmanageable hub's. Hierdoor is het niet mogelijk om gebruik te maken van de 802.1x technologie. Hiervoor is een alternatieve oplossing voor bedacht. Gebruikers in De Struyck zullen zich moeten authenticeren via een firewall. De firewall zal wel op dezelfde RADIUS server aangesloten worden die de gebruikergegevens uit de LDAP database haalt. De volgende functionaliteiten zullen aanwezig moeten zijn:

- De gebruiker authenticeert via de internet browser
- Gebruiker word naar website gestuurd bij mislukking authenticatie

Technische specificaties
Er was voor deze pilot de volgende hard- en software nodig:

- Firewall: Cisco PIX Firewall 515E
- RADIUS Server: Dezelfde RADIUS server als voorgaande pilots.
- Client: De eerder gebruikte laptop zal achter de firewall worden geplaatst.

Hergebruik
Voor deze pilot is de configuratie van een andere PIX firewall gebruikt. Een klein gedeelte van de Radiator configuratie kon ook worden hergebruikt betreffende de LDAP koppeling.

Tijd/Planning
Er werd verwacht dat niet al te veel tijd in zou zitten om deze pilot af te ronden aangezien er al een werkende PIX configuratie van een andere firewall beschikbaar was. De verwachte twee dagen voor dit onderdeel zijn dan ook een goede schatting geweest.

Informatie bronnen
Alle informatie over de PIX firewall was te vinden op de Cisco website (www.cisco.com).

Werkwijze
De PIX Firewall maakt gebruik van "feature proxy authenticatie". Standaard word al het netwerkverkeer geblokkeerd in de ACL (Access Control List).
In de ACL is een IP-adressen reeks ingevoerd. Alleen gebruikers met een IP-adres uit deze reeks kunnen door de firewall komen. Deze gebruikers moeten zich nog wel authenticeren ondanks het feit dat het IP-adres in de firewall staat.
Gebruikers kunnen zich via hun internet browser authenticeren. Zodra een ongeauthenticeerde gebruiker contact probeert te maken met een website (http verkeer), wordt de gebruiker door de firewall doorverwezen naar een inlogscherm (https). Nadat de gebruiker zich heeft geauthenticeerd, zal de firewall de verbinding open zetten. Afhankelijk van de instellingen van de firewall, dient er na 30 minuten inactief netwerkgebruik weer opnieuw geauthenticeerd te worden.
Met behulp van de ACL en adres translatie werd getracht gebruikers bij een mislukte authenticatie door te sturen naar een vast IP adres (URL redirect). Op dit adres zou dan een webserver kunnen worden gezet om zo gebruiker feedback te geven over de mislukken van authenticatie.

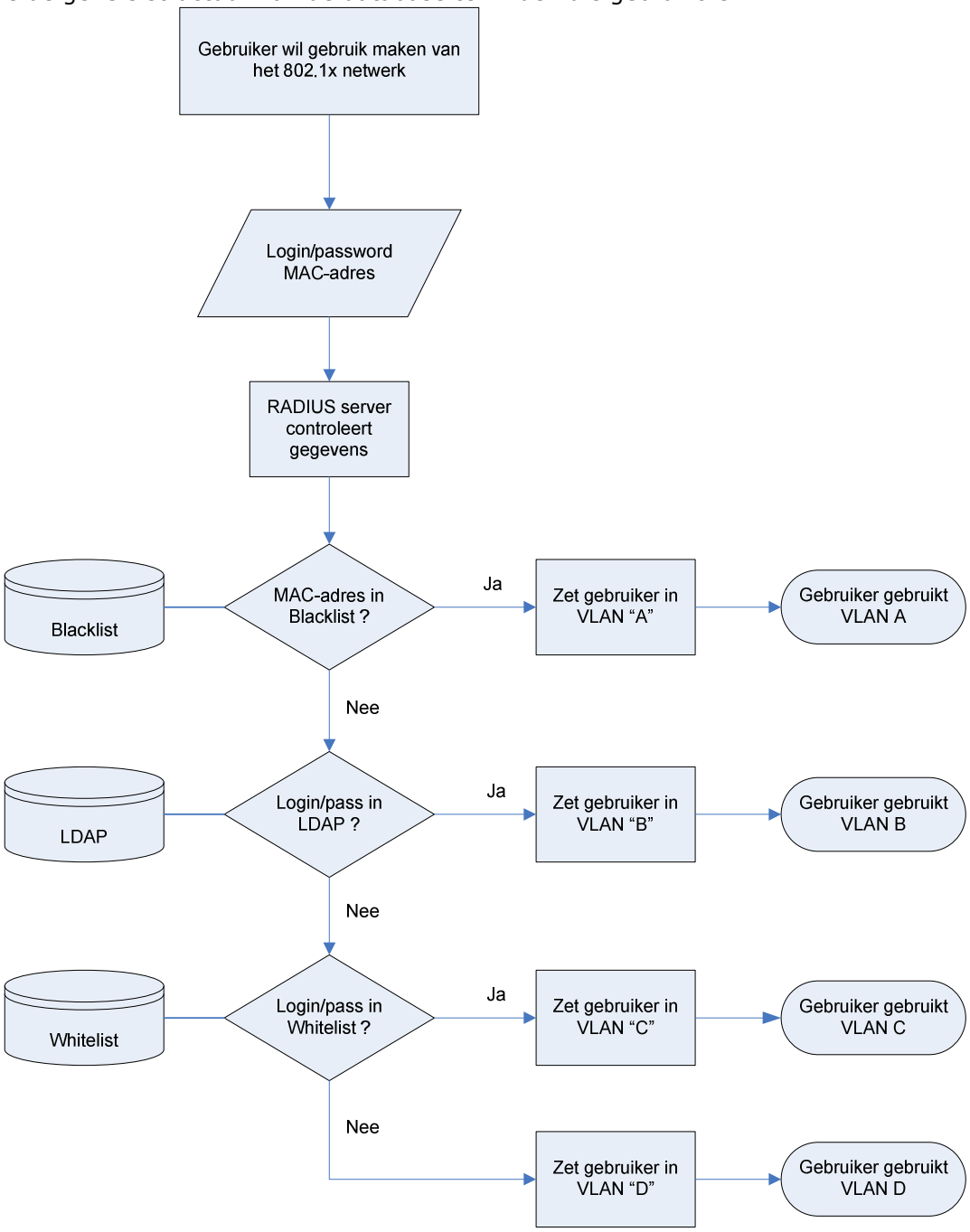
Resultaten
Standaard ondersteunt de PIX firewall geen URL redirect. Alleen de toplijn van Cisco ondersteunt dit momenteel. De afstudeerder had nog een idee om URL redirect via een omweg te realiseren, namelijk via adres translatie.
Het lukte niet met behulp van adres translatie en de ACL om bij een mislukte authenticatie een gebruiker automatisch door te sturen naar een website (=URL redirect). Dit omdat deze translaties alleen voor een los IP-adres werken en het invoeren van 2^{32} IP-adressen ook geen optie was.
Het was wel mogelijk om bij mislukking van authenticatie een bericht mee te sturen naar de gebruiker die in de internet browser wordt vertoont.
Dit bericht kan wel een verwijzing bevatten naar een ander IP-adres. Door dit IP-adres buiten de firewall te zetten kunnen gebruikers met authenticatie problemen toch naar dit IP-adres toe.

7.4 ▫ Pilot 4: Gebruik van VLAN's

Doel
Het doel van deze pilot is op basis van de authenticatie gegevens gebruikers in VLAN's te zetten. Door het gebruik van verschillende VLAN's kunnen bepaalde rechten en beperkingen aan gebruikers worden opgelegd. Het MAC-adres van een netwerkmisbruiker zal in een blacklist worden gezet. Zodra een gebruiker zich wil authenticeren, wordt de blacklist geraadpleegd op het MAC-adres waarmee de gebruiker connectie zoekt. Indien dit MAC-adres aanwezig is, zal de computer van de gebruiker in een VLAN worden gezet met weinig rechten en veel beperkingen. Dit om ervoor te zorgen dat de computer niet meer schade kan toebrengen aan het netwerk, zoals een met een virus besmette computer. Dit VLAN zal in een andere pilot worden ingericht als een compleet quarantainenetwerk.
Gebruikers die zich authenticeren aan de hand van LDAP zullen in een VLAN gezet worden met rechten en beperkingen vergelijkbaar met het huidige netwerk.
Niet iedere bewoner van de studentenflats heeft een LDAP account. Dit omdat ze bijvoorbeeld aankomend student zijn of student van een andere hogeschool. Deze uitzonderingen die toch gebruik mogen maken van het netwerk worden in een aparte database gezet, genaamd de whitelist.
Gebruikers die zich niet kunnen authenticeren met de 802.1x technologie zullen in een soort gast netwerk worden geplaatst.

In figuur 7.2 is een stroomdiagram getekend van het plaatsen in VLAN's op basis van de authenticatie gegevens. Elk VLAN (A,B,C,D) heeft zijn eigen rechten en beperkingen. Het VLAN waar blacklisted gebruikers in gezet worden, zal de gebruikers beperken tot een informatie website van de Haagse Hogeschool met links naar bijvoorbeeld antivirus applicaties.

Technische specificaties
Dezelfde RADIUS server, switch, access point, laptop en database server zijn voor deze pilot gebruikt als de vorige pilots.
In de database zijn twee tabellen aangemaakt: blacklist en whitelist. In figuur 7.3 is de gehele structuur van de database te vinden die gebruikt is.



Figuur 7.2: Stroomdiagram bij pilot 4

Hergebruik
Deze pilot zal de configuraties van pilot 1 en 2 hergebruiken en aanvullen. Dit geldt alle gebruikte apparatuur.

Tijd/Planning
De schatting was dat deze pilot een vier werkdagen in beslag zou nemen. Dit is uiteindelijk een werkweek geworden. Deze extra tijd zat hem vooral in het feit dat het configureren van Dynamische VLAN's op de switch sterk verschilde met de configuratie van de access point. Tot nu toe leken de configuraties van de twee authenticators op elkaar.

Informatie bronnen
De Cisco website en Radiator mailarchieven zijn opnieuw gebruikt voor deze pilot. Daarnaast is ook gebruik gemaakt van documentatie van surfnet:

- http://www.surfnet.nl/info/innovatie/wlan/802.1x.jsp: Authentication and Authorisation for (W)LAN using 802.1X

Werkwijze
Na het tekenen van de stroomdiagram was duidelijk hoe de Radiator configuratie moest worden opgebouwd. Met behulp van "`AuthByPolicy ContinueUntilAccept`" kon een lijst van "`AuthBy`" (Authenticatie door middel van SQL/LDAP/FILE) worden afgelopen totdat een "Accept" binnen komt. Als een gebruiker niet gevonden wordt in een AuthBy module, zal "reject" als response worden gegeven. Om een indruk te krijgen hoe zo'n Radiator configuratie er uit ziet is een klein deel hiervan weergegeven:

```
<AuthBy SQL>
        Identifier CheckWhitelistFixed
        …
        #Authenticeer gebruikers uit de whitelist. Password is SHA1 encrypted.
        AuthSelect select USERNAME from WHITELISTED where USERNAME='%n' and
                ENCRYPTEDPASSWORD=SHA1('%P')
        AuthColumnDef 0, User-Name, reply
        #Forceer whitelisted gebruikers in een VLAN (33)
        StripFromReply Tunnel-Type,Tunnel-Medium-Type,Tunnel-Private-Group-ID
        AddToReply Tunnel-Type=VLAN,Tunnel-Medium-Type=6,Tunnel-Private-Group-ID=33
        …
</AuthBy>
…
# Handler for Inner Authentication of EAP-TTLS tunnel
<Handler TunnelledByTTLS=1, Client-Identifier=/^CAT/ >
        …
        AuthByPolicy ContinueUntilAccept
        AuthBy CheckBlacklistFixed
        AuthBy InnerAuthFixed
        AuthBy CheckWhitelistFixed
        …
</Handler>
```

Nb. De complete configuratie kan gelezen worden in bijlage D.

Na Radiator te hebben geconfigureerd waren de authenticators aan de beurt om geconfigureerd te worden. In eerste instantie was het niet mogelijk om een dynamische VLAN in te stellen op de switch.

De operating systeem van de switch had een upgrade nodig om dynamische VLAN te ondersteunen. Op de access point werden meerdere SSID's en VLAN's ingesteld.

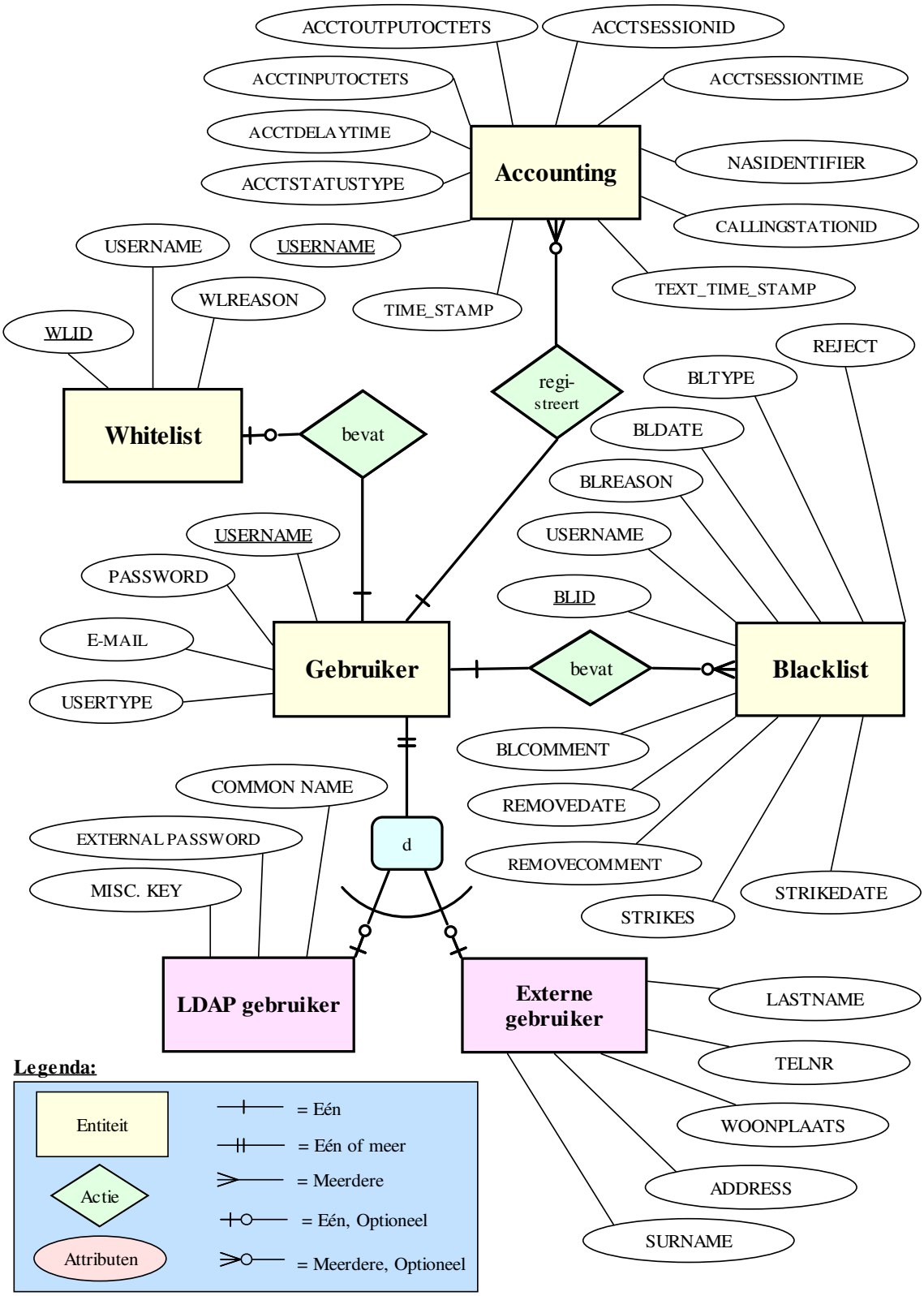
Resultaten

Na alles geconfigureerd te hebben werkte de dynamische VLAN's op zowel de switch als access point niet. Authenticatie verliep goed, alleen werd de laptop niet in een VLAN geforceerd. Er was voldoende informatie te vinden over dynamische VLAN's voor Cisco access points. Bij de access point was het probleem dat de VLAN's aan een SSID waren gekoppeld terwijl deze alleen los aangemaakt moeten worden. Na dit te hebben gecorrigeerd werkte dynamische VLAN via de access point goed.
Helaas werkte dezelfde Radiator configuratie niet in combinatie met de switch. Hier kon ik uit opmaken dat de supplicant en authenticating server goed werkte en dat het probleem bij de Authenticator (de switch) lag.
Er was weinig informatie te vinden over het gebruik van dynamische VLAN's bij switches. Wellicht omdat de switch dit pas sinds kort ondersteund. Tijdens het zoeken naar een oplossing kwam naar voren dat het probleem niet direct bij de switch lag, maar bij de variabelen die de RADIUS server naar de Authenticator verstuurd. Cisco heeft de onaangename eigenschap om niet geheel volgens dezelfde standaarden te werken. Dit komt mede doordat Cisco bedrijven opkoopt die goede producten maken en deze niet geheel zelf ontwikkelt.
De access point had "`AddToReply …,Tunnel-Private-Group-ID=1:33`" nodig als attribuut terwijl de switch de "`1:`" niet accepteerde. Een klein detail dat voor veel problemen zorgde.
Dit is opgelost door alle AuthBy modules en Handlers specifiek te schrijven voor gebruik van fixed of wireless gebruik. Nu was de vraag hoe Radiator verschil kon zien tussen een fixed of wireless "access-request".
Dit kon op drie verschillende manieren worden opgelost:

- Bij een "access-request" komen een aantal attributen binnen die de authenticator mee stuurt. Eén van die attributen is "NAS-Port-Type". In geval van de access point was dit "`NAS-Port-Type = Wireless-IEEE-802-11`" en bij de switch "`NAS-Port-Type = Ethernet`".
- In elke Radiator configuratie worden de client authenticators opgenomen die mogen communiceren met de server. Bij elk zo'n client hoort een gedeeld geheim en een IP-adres. Per client kan ook een identificatie naam worden opgegeven (optioneel). Door consequent gebruik van deze identificatie naam kan geselecteerd worden op een deel van de naam. Het voordeel hiervan is dat vele verschillende variaties mogelijk zijn. Een switch van merk A kan met "AA" beginnen, switch van merk B "BB", etc.
- Een perl hook die met tijdelijke variabelen werkt met behulp van bijvoorbeeld een MySQL database. (aanname dat dit mogelijk is)

Er is voor de tweede oplossing gekozen omdat in de toekomst wellicht andere merken en/of types worden aangeschaft en deze ook weer specifieke attributen nodig kunnen hebben. De eerste oplossing heeft te weinig uitbreidingsmogelijkheden en viel daarom af als oplossing. De derde oplossing zou veel tijd kosten om in elkaar te zetten aangezien de afstudeerder onbekend is met perl. Ook is het niet honderd procent zeker of het überhaupt mogelijk is met een perl hook en dat dit te weinig mogelijkheden zou bieden.

Het gebruikte Enhanced Entity Relationship Model van de database:



Figuur 7.3: Enhanced Entity Relationship Model

7.5 ▫ Pilot 5: Website voor quarantainenetwerk

Doel
Gebruikers met problemen met de authenticatie willen vaak graag weten waarom en hoe deze problemen op te lossen zijn.
Deze informatie zal op een website worden gezet. Deze website is weer gekoppeld aan de blacklist van de vorige pilot.
De website moet de volgende functionaliteiten bieden:

- Gebruikers informeren over wat het quarantaine netwerk inhoud
- Controle of computer in blacklist staat
- In sommige gevallen kan de gebruiker zich zelf uit blacklist halen (bijvoorbeeld bij virus)
- Informatie over oplossen en voorkomen van computerproblemen

Zoals in het vijfde hoofdstuk staat vermeld, is het noodzakelijk dat de website in de style van de Haagse Hogeschool portal wordt gemaakt.

Technische specificaties
Voor de website is een webserver nodig met software die het mogelijk maakt dynamische websites te generen:

- Web server: Er is voor de veel gebruikte combinatie van Linux, Apache, MySQL en PHP (LAMP) gekozen. Een geheel gratis oplossing, makkelijk voor beginners en erg uitgebreid. De keuzes van Linux en MySQL waren al in de vorige pilots vastgesteld, dus PHP en Apache waren een logische uitbreiding.
- Ontwikkelomgeving: Op de laptop van de afstudeerder is Dreamweaver MX geïnstalleerd om de pagina mee te ontwikkelen.
- Website: De website is in PHP, HTML en XHTML geschreven.

Hergebruik
Er kon voor deze pilot erg weinig worden hergebruikt.

Tijd/Planning
Deze pilot was een optionele pilot en was daarom niet echt ingepland. Er is aan deze pilot gewerkt nadat de andere pilots waren afgerond. De verslagen hadden voorrang en hierdoor is deze pilot nog niet geheel afgerond. De website is momenteel nog niet geheel compleet met inhoud. Er is nog zeer weinig aan de beveiliging van de website gedaan, dus deze kan nog niet echt ingezet worden voor gebruik.

Informatie bronnen
De ideeën van een quarantaine netwerk met website komen van de Technische Universiteit Twente. Daar hebben een aantal studenten het QNet (http://www.quarantainenet.nl/) ontwikkeld. Om hier een beter inzicht van te krijgen is een bezoek gepleegd in Twente. Daar heeft een interview plaats gevonden met de makers van QNet en is een demonstratie gegeven.
Voor de installatie van LAMP zijn verschillende bronnen van het internet gebruikt:

- http://www.lamphowto.com/lamp.htm: Building a LAMP Server
- http://www.php.net/docs.php: The PHP manual
- http://www.apache.org/: The Number One HTTP Server

Ook zijn uit de bibliotheek een aantal boeken geleend:

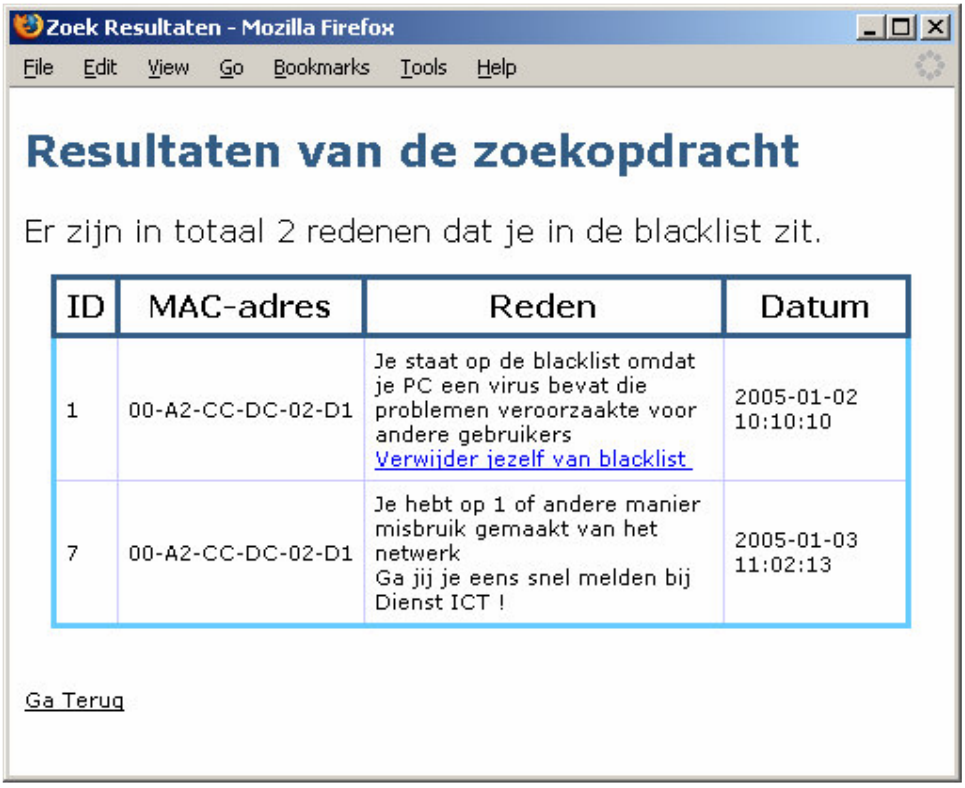
- Converse en Park: PHP 4 het complete handboek
  Franke, J: PHP 5 zonder stress

Werkwijze
De afstudeerder is begonnen met het schetsen van een stroomdiagram op papier met hoe de website voor de HHS in elkaar zou moeten steken. Nadat deze schetsen gemaakt waren, is er aan de schermenschetsen gewerkt.
Aan de hand van deze "papieren" website is er begonnen met het maken van de website. Eerst moest natuurlijk alle software geïnstalleerd en geconfigureerd worden. Door de duidelijke stap voor stap handleidingen ging tijdens het installeren niet veel mis.
Omdat de afstudeerder geen ervaring had met het bouwen van een PHP website, is eerst een voorbeeld website uit het boek gebouwd. Hierdoor is PHP/MySQL ervaring opgedaan om zo een "schone" website voor de HHS te kunnen maken. Hiermee wordt een website bedoeld zonder restanten en onduidelijke functies.

Resultaten
Bij het maken van de website kon regelmatig worden gecontroleerd of deze nog in orde is door gebruik te maken van de preview functie.
Er traden regelmatig fouten op: PHP errors, foute opmaak, dode links, etc. Deze fouten waren steeds eenvoudig te verhelpen door kleine aanpassingen in de broncode. Deze problemen traden op door bijvoorbeeld typefouten en incomplete/foute code.
Om een indruk te krijgen van de website zijn een aantal screenshots genomen. De rest van de website is in bijlage E te vinden. Omdat de website nog niet geheel af is tijdens het schrijven van het verslag kan het voorkomen dat er nog enkele bugs/taalfouten in zitten.
Op figuur 7.4 is te zien wat gebruikers krijgen als ze willen onderzoeken of ze op de blacklist staan. Een gebruiker voert een MAC-adres in en krijgt vervolgens een scherm te zien of dit MAC-adres voorkomt in de blacklist.
Omdat het hier om een MAC-adres betreft en niet om een username is geen password of iets dergelijks nodig.

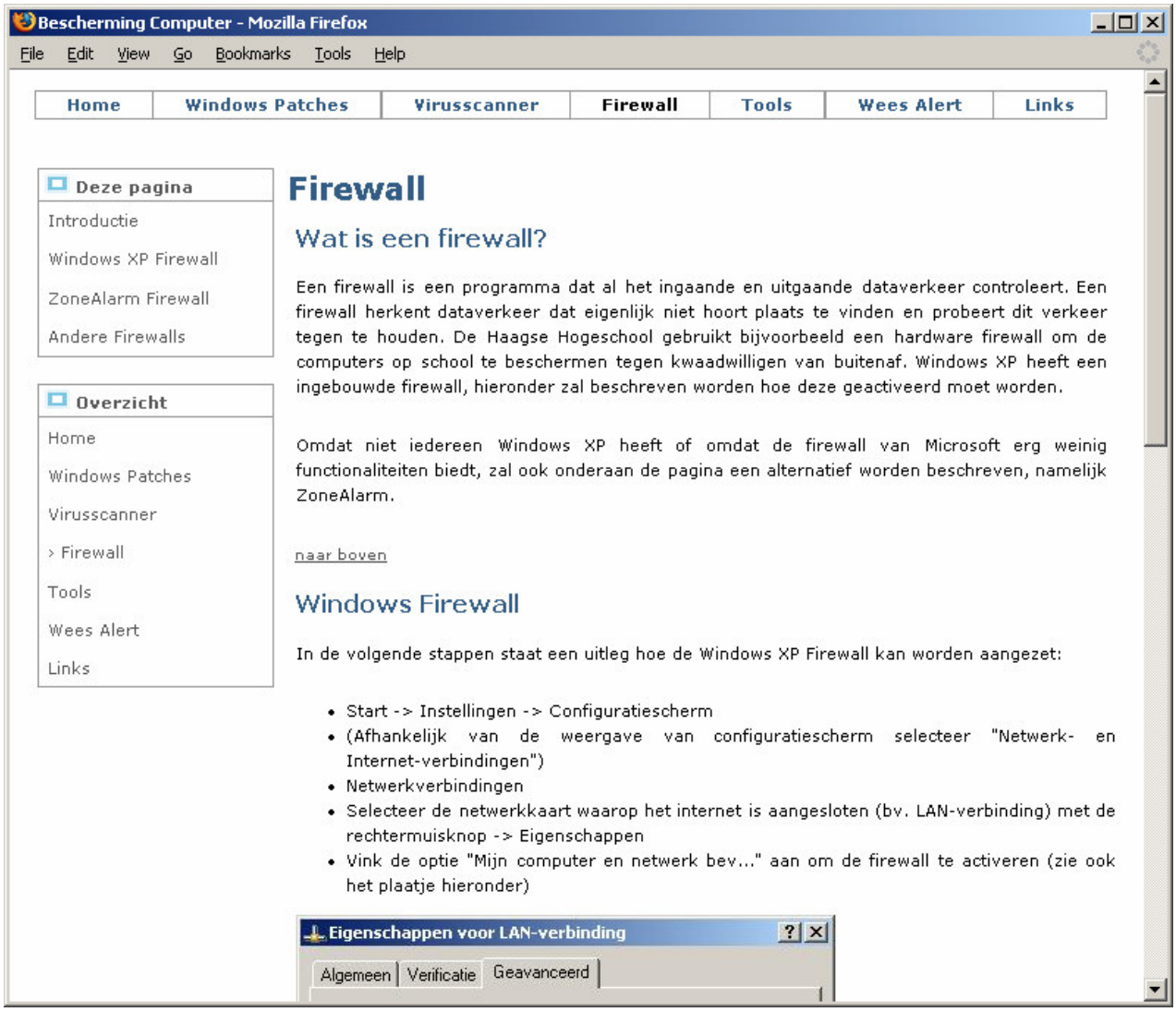
Figuur 7.4: Scherm - Opzoeken MAC-adres in blacklist

Op figuur 7.5 is het resultaat van de zoekopdracht te zien. Een MAC-adres kan om verschillende redenen meerdere keren in de database staan, al zal dit niet heel gebruikelijk zijn. Dit kan bijvoorbeeld komen als een computer eerst virussen aan het verspreiden is en later wordt ontdekt dat de computer ook verantwoordelijk was voor het platgooien van een website. Een gebruiker krijgt niet alle attributen te zien van de bewuste blacklist. Deze extra attributen zijn alleen zichtbaar voor de beheerders van de Dienst ICT.



Figuur 7.5: Scherm – Resultaten zoekopdracht

Om de gebruiker te informeren over de problemen die computers met zich mee kunnen brengen is er ook gedeelte over het oplossen van problemen en hoe deze in de toekomst kunnen worden voorkomen. Er wordt aan de hand van een voorbeeld beschreven hoe een met een virus besmette computer kan worden schoongemaakt. Nadeel van deze methode is dat het misschien een beetje persoonlijke site is geworden. Zie figuur 7.6 voor een indruk van deze informatievoorziening.



Figuur 7.6: Scherm – Informatie over voorkomen en oplossen van problemen

8 ◦ Evaluatie

In dit hoofdstuk is een persoonlijke evaluatie gegeven over het verloop van het afstudeertraject. Er zal zowel een beoordeling worden gegeven over het proces als de verschillende producten die zijn opgeleverd.

8.1 ▫ Proces evaluatie

Er is niet geheel volgens de ASI methode gewerkt. Het gebruik van een methode vind ik persoonlijk erg lastig als de opdracht een sterk onderzoekskarakter heeft. Het onderzoek betrof een onderwerp dat nog sterk in ontwikkeling is. Hierdoor is het in de beginfase van het afstudeerproject moeilijk vast te stellen wat voor een technische oplossingen gebruikt moeten worden.
Dit probleem deed zich vooral voor bij het opstellen van de eisen en wensen. De eisen en wensen hangen nauw samen met de technische middelen die mogelijk zijn. De eisen en wensen zullen realistisch moeten zijn, anders zal er geen oplossing bij gevonden kunnen worden. Ik zie het niet geheel kunnen volgen van de ASI methode niet als persoonlijke tekortkomingen, maar als een algemeen probleem bij gebruik van methodes bij opdrachten met een sterk technisch onderzoekskarakter.
De planning gaf mij houvast om de producten op tijd af te ronden, ondanks ik de planning niet geheel heb kunnen volgen. De definitiefase liep door het uitgebreide onderzoek uit, echter kon ik dat weer inhalen door de verkorte architectuur fase. Door deze verkorte architectuurfase was zelfs tijd ontstaan om een extra pilot uit te voeren. De planning was gemaakt voor een enkele grote pilot, echter heb ik vijf kleinere pilots gebruikt. Hierdoor wisselde het ontwerp en de ontwikkeling van pilots elkaar telkens af. Ik heb in de planning wel een goed moment gekozen om te beginnen met het ontwerpen en ontwikkelen van pilots. Hierdoor ontstond er goede balans tussen de hoeveelheid tijd die ik kwijt was aan het onderzoeken en de tijd dat ik praktisch bezig was met de oplossingen.
Het overleg tussen mijn en opdrachtgever is goed verlopen. Er kon dikwijls direct overleg gepleegd worden over de diverse aspecten die aan bod kwamen gedurende het verloop van het gehele project. Overleg vond of mondeling plaats of aan de hand van enkele documenten met aantekeningen of resultaten. Het regelmatige overleg tussen mij en de opdrachtgever heeft de kwaliteit van het afstuderen gewaarborgd.
Momenteel wordt er door Dienst ICT in beraad genomen om mij de komende maanden in dienst te nemen om te helpen het afstudeerproject te implementeren op de Technische Hogeschool Rijswijk en Haagse Hogeschool. Ik zal in ieder geval de komende weken de documentatie bij de pilots verder uitwerken en de website afronden.

8.2 ▫ Product evaluatie

Onderzoeksrapport
Bij het onderzoeken van beveiligingsmaatregelen was het lastig om correcte informatie te bemachtigen. Veel bedrijven willen op dit gebied geld verdienen. Daarom is niet alle informatie even volledig. Een bedrijf zal niet met de beperkingen van hun product reclame maken. Het was dus belangrijk dat de informatie kon worden geverifieerd bij een onafhankelijke bronnen.
Er was veel informatie te analyseren en dit worp ook zijn vruchten af. Er was een uitgebreide shortlist ontstaan met daarin de mogelijke oplossingen.
Per oplossing is een samenvatting gemaakt met de belangrijkste kenmerken.

Ontwerp- en adviesrapport
Er was snel besloten welke maatregel de voorkeur had. Aanvankelijk was de verwachting dat dit een moeilijkere beslissing zou zijn. Eén oplossing viel op door de goede toepasbaarheid op de Haagse Hogeschool, 802.1x.
Achteraf kwam ik tot dezelfde conclusie als vele andere hogescholen en niet voor niks. 802.1x is erg flexibel en daarom goed te gebruiken op een instelling waar de gebruikersgroepen erg divers zijn, zoals de Haagse Hogeschool.
Het enige minpunt aan deze oplossing was dat de studentenflat De Struyck niet kan worden ingericht met 802.1x. Hier moest voor een alternatief worden gekozen die minder beveiliging biedt, maar wel goed schaalbare oplossing is.

Uitkomst van de pilot
In het algemeen was ik tevreden met de resultaten van de pilots. De belangrijkste doelstellingen heb ik weten te halen. Gebruikers kunnen veiliger gebruik maken van het netwerk en beheerders kunnen eenvoudig problemen achterhalen.
Omdat er een geheel geautomatiseerde oplossing gekozen is (gebruikers kunnen hun bestaande login/pass gebruiken), zal tijd bespaard worden bij Dienst ICT.
Tot mijn spijt konden sommige functionaliteiten niet gerealiseerd worden door technische beperkingen. De meeste problemen die op traden tijdens het testen heb ik daarentegen wel weten op te lossen.
De pilots zijn enigszins beknopt beschreven in de documentatie. Dit komt vooral omdat ik zelf de informatie van andere bronnen heb gebruikt, zoals de handleidingen die bij het product kwamen. Deze handleidingen waren erg uitgebreid en duidelijk. Daarom is er in de documentatie regelmatig verwezen naar deze handleidingen.
Om reproduceerbaarheid te kunnen toetsen heb ik ook een testopstelling in Rijswijk gebouwd. In Rijswijk is het ook gelukt om 802.1x authenticatie toe te passen door middel van een koppeling met de LDAP server in Den Haag.

Informatievoorziening voor de gebruikers met de maatregelen
Bij aanvang van de opdracht was nog geen sprake van het maken van een website. Gaande weg is besloten deze toe te voegen tot aan project.
De website voor de gebruikers is niet geheel compleet. Ik denk dat ik toch een aardig eind ben gekomen met de website en ik zal deze website na 14 januari nog complementeren. Momenteel bevat de website wel de elementaire informatie die nodig is voor 802.1x gebruik.

9 ◦ Conclusie

De noodzaak van netwerkbeveiliging is de laatste jaren sterk toegenomen. Dagelijks zijn gebruikers problemen aan het veroorzaken op het Haagse Hogeschool netwerk. Dit levert zowel problemen op bij de gebruikers als bij beheerders. Door het authenticeren van gebruikers en hun netwerkgebruik te loggen, kunnen er verdere stappen worden genomen op het gebied van beveiliging. Misbruikers kunnen worden geïdentificeerd waardoor verdere maatregelen kunnen worden getroffen om het misbruik van de gebruiker te stoppen.

De techniek 802.1x biedt veel mogelijkheden op het gebied van authenticatie. Deze mogelijkheden zullen in de toekomst alleen nog maar verder toenemen. 802.1x wordt momenteel vooral op hogescholen en universiteiten gebruikt. De laatste tijd zijn bedrijven ook geïnteresseerd in deze techniek. Zo heeft T-Mobile USA (mobiele telefoon/internet provider) bekend gemaakt de 802.1x techniek te gaan gebruiken voor haar WiFi hotspots.
Mijn verwachting is dat er vooral op wireless gebied veel gebruik gemaakt zal worden van 802.1x.

SURFnet (internet provider HHS) biedt ook allerlei 802.1x diensten aan. Zo kan de RADIUS server op de Haagse Hogeschool worden aangesloten op de RADIUS Proxy servers van SURFnet. Doordat andere hogescholen en universiteiten hetzelfde kunnen doen met hun RADIUS server, ontstaat er een groot 802.1x netwerk. Er kan dan met de login/password gegevens, van een Haagse Hogeschool student of medewerker, gebruik worden gemaakt van de 801.x netwerkdiensten in bijvoorbeeld Twente. En vice versa kan een medewerker uit Twente ook gebruik maken van het netwerk van de Haagse Hogeschool.
Dit is slecht één van de mogelijkheden die met 802.1x mogelijk zal zijn. Het gebruik van 802.1x zal de netwerkbeveiliging opschroeven en daarnaast veel uitbreidingsopties bieden.

Literatuurlijst

Boeken

- Converse en Park: PHP 4 het complete handboek (3e oplage), november 2001, Academic Service
  ISBN 90 395 1610 3

- Franke, J: PHP 5 zonder stress, 1ste druk, 2004, Easy Computing
  ISBN 90 456 3423 6

- Tolido, R.J.H: IAD Het evolutionair ontwikkelen van informatiesystemen, 6e oplage, oktober 2003, Academic Service
  ISBN 90 395 0401 6

Reader

- Nederlands Genootschap voor Informatica: ASI reader (Ontwerp en ontwikkeling van systeem /netwerkinfrastructuren), 2003, gebruikt bij modules CS-05/ii-003

Online literatuur

- Cisco
  http://www.cisco.com

- CPAN
  http://www.cpan.org

- The Internet Engineering Task Force (RFC's)
  http://www.ietf.org

- MySql
  http://www.mysql.com

- PHP: Hypertext Preprocessor
  http://www.php.net

- Pilot 802.1x Technische Universiteit
  http://www.utwente.nl/itbe/ictinfra/netwerk/WLAN/pilot8021x.doc/

- Radiator
  http://www.open.com.au

- SurfNet
  http://www.surfnet.nl

Interne Bijlagen

Bijlage I: Glossarium

In deze bijlage zijn de gebruikte afkortingen en begrippen te vinden met hun betekenis.

802.1x
802.1x is een techniek om op linklaag (laag 2) de mogelijkheid te bieden aan andere protocollen om gebruikers te authenticeren.

AAA *(Authentication, Authorization, Accounting)*
Een raamwerk voor het intelligent beheren van toegang tot computer apparatuur, handhaven van beleid, gebruik controleren en registreren.

AP *(Access Point)*
Een switch voor draadloze netwerken; netwerkkruispunt. Zoals een vaste computer via een netwerkkabel op een switch/hub dient worden aangesloten, zal een draadloze computer een connectie moeten maken met een Access Point.

CA *(Certificate Authority)*
Instelling die certificaten uitdeelt en ondertekent.

CPAN *(Comprehensive Perl Archive Network)*
Een verzameling van Perl modules, scripts, documentatie en source code. Al deze informatie is zonder kosten te downloaden van de CPAN website (www.cpan.org).

DHCP *(Dynamic Host Configuration Protocol)*
Een protocol dat ervoor zorgt dat computers in een netwerk automatisch goede TCP/IP instellingen krijgen.

EAP *(Extensible Authentication Protocol)*
Een raamwerk dat de mogelijkheid biedt voor een authenticatie protocol om vele verschillende authenticatie methoden en technieken te transporteren.

IEEE *(Institute of Electrical and Electronics Engineers)*
Een technisch genootschap van professionals uit het bedrijfsleven die een gemeenschappelijk doel hebben in de vooruitgang van alle communicatie technologieën.

ITIL *(Information Technology Infrastructure Library)*
ITIL biedt richtlijnen aan betreft het inrichten van een ICT beheer organisatie.

LAN *(Local Area Network)*
Een communicatie systeem waarin meerdere computers en andere netwerkapparaten aan gekoppeld zijn en informatie met elkaar kunnen delen. Zoals de naam al impliceert, een LAN is beperkt tot een lokaal netwerk.

LDAP *(Lightweight Directory Access Protocol)*
Een client-server protocol om directory informatie binnen te halen en te beheren. Het wordt vooral gebruikt als een database waar vooral van gelezen moet worden en niet zo zeer veel schrijf operaties nodig zijn.

MAC *(Media Access Control)*
De datalink laag is verdeeld in twee sublagen waarvan één de MAC laag is. De MAC laag zorgt voor de koppeling tussen het netwerkmedium en de andere datalink laag. Om deze MAC laag aan te spreken heeft deze een uniek hardwarematig adres.

MD5 *(Message Digest Algorithm #5)*
Een algoritme om berichten te versleutelen. Origineel bedoeld voor digitale handtekeningen.

PAP *(Password Authentication Protocol)*
PAP is een authenticatie protocol dat gebruiker informatie als gebruikersnaam en wachtwoord uitwisselt tussen de gebruiker en het beveiligde systeem. PAP verstuurt de informatie in platte tekst waardoor PAP op zich zelf een erg zwakke authenticatie methode is.

PEAP *(Protected Extensible Authentication Protocol)*
Een methode om authenticatie uit te wisselen. (zie paragraaf 6.2)

PKI *(Public Key Infrastructure)*
Een cryptografie techniek die gebruik maakt van een public en private sleutel (key).

RADIUS (Remote Authentication Dial-In User Service)
Radius is een server om gebruikers van een andere locatie te authenticeren en registreren. Een Radius server wordt door een ander netwerkapparaat benaderd (niet door gebruiker zelf) en de Radius server benaderd vervolgens een gebruikersdatabase om zo bepaalde rechten aan een gebruiker toe te kennen.

SHA *(Secure Hash Algorithm Standard)*
Een hashing algoritme voor het versleutelen van een password, email en documenten.

SLA *(Service Level Agreements)*
Een afspraak tussen een klant en leverancier om een bepaalde services aan minimale kwaliteitseisen te laten voldoen.

SSID *(service set identifier)*
Een opeenvolging van karakters dat op een unieke wijze een naam geeft aan een wireless local area network.

TLS *(Transport Layer Security)*
Aan de hand van certificaten wordt een veilige verbinding tussen twee partijen opgebouwd.

TTLS *(Tunneled Transport Layer Security)*
Een methode om authenticatie uit te wisselen. (zie paragraaf 6.2)

UTP *(Unschielded Twisted Paor)*
Netwerkkabel dat uit vier gedraaide aderparen bestaat.

VLAN *(Virtual Local Area Network)*
Een VLAN netwerk kan zich voordoen als een netwerk van computers dat aaneengesloten is aan dezelfde kabels, terwijl ze fysiek gezien op een totaal andere locatie van het LAN kunnen bevinden. VLAN is softwarematig geconfigureerd in tegen stelling tot hardwarematig waardoor een VLAN erg flexibel is.

WAP *(Wireless Access point)*
Andere benaming voor AP (zie AP).

WEP *(Wired Equivalent Privacy)*
Het WEP algoritme word gebruikt ter beveiliging van draadloze netwerkcommunicatie.

Bijlage II: Lijst van figuren

Hieronder staat een lijst van figuren met een korte uitleg en op welke pagina het desbetreffende figuur te vinden is.

Figuur #	Beschrijving	Bladzijde
2.1	Organogram Dienst ICT	3
3.1	Planning - Gantt Chart	8
4.1	Overzicht gebruikersgroepen	9
4.2	MAC-adres authenticatie	11
4.3	Overzicht Netwerk Haagse Hogeschool en de twee studentenflats.	15
4.4	LDAP structuur	16
5.1	Operating System Platform Statistieken	19
6.1	802.1x in werking	23
6.2	Overzicht van EAP authenticatie methodes	24
7.1	Succesvolle 802.1x authenticatie	28
7.2	Stroomdiagram bij pilot 4	35
7.3	Enhanced Entity Relationship Model	38
7.4	Scherm - Opzoeken MAC-adres in blacklist	40
7.5	Scherm – Resultaten zoekopdracht	41
7.6	Scherm – Informatie over voorkomen en oplossen van problemen	42