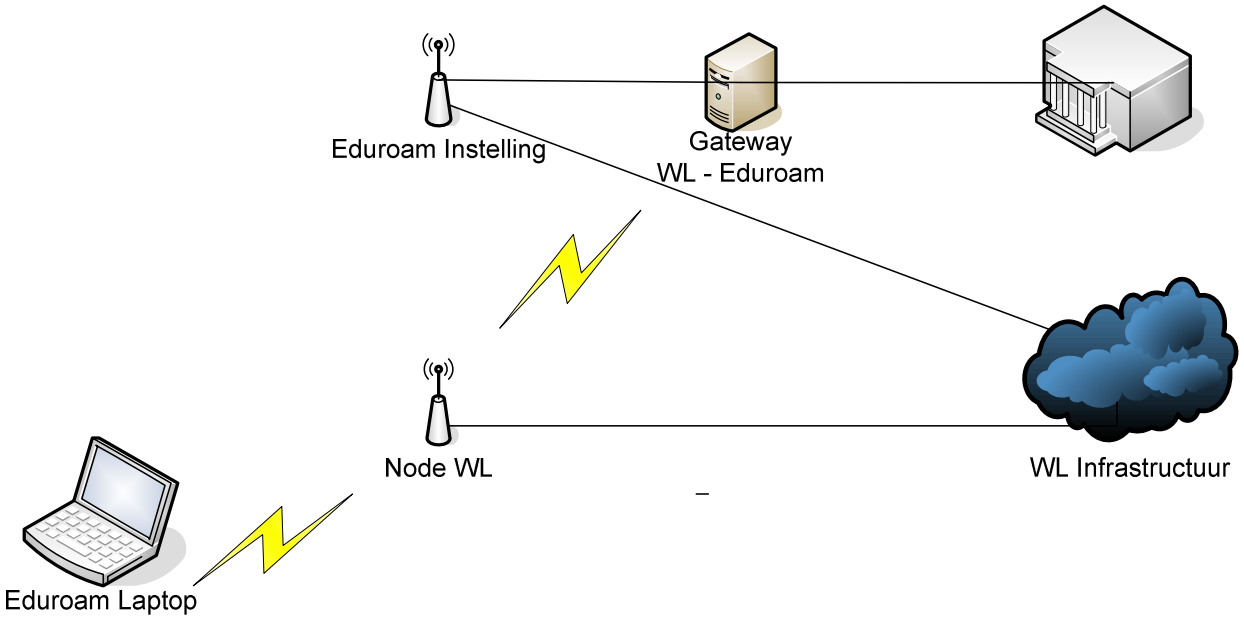
Wireless Leiden

Eduroam bij Wireless Leiden
802.1x



Afstudeerverslag

Naam	:	Richard van Mansom
Organisatie	:	Wireless Leiden
Datum	:	9 Juni 2008
Opleiding	:	Hogeschool Leiden Informatica
Document	:	Afstudeerverslag
Versie	:	1.0

Inhoudsopgave

Gegevens

Gegevens student

Naam:	:	Richard van Mansom
Adres:	:	Terschelling 244
Postcode:	:	3524az
Plaats:	:	Utrecht
Telefoon:	:	(06) 1248 1824
E-Mail	:	richard@vanmansom.net
School E-Mail:	:	s1001962@student.hsleiden.nl
StudentNR:	:	1001962
Mentor:	:	Eric van Wessel

Gegevens stageorganisatie

Naam	:	Wireless Leiden
Contact	:	Gebruik relevante mailinglist (http://lijst.wirelessleiden.nl)
Internet	:	http://www.wirelessleiden.nl

Bezoekadres

Adres	:	Langebrug 56a
Postcode	:	2311 TM
Plaats	:	Leiden

Postadres

Adres	:	Langebrug 56a
Postcode	:	2311 TM
Plaats	:	Leiden

Gegevens stagebegeleider

Naam	:	Huub Schuurmans
Email	:	huub@wirelessleiden.nl
Telefoon	:	Ga naar de website en klik contact. Zie paragraaf pers.
Functie	:	Bestuursraadlid / Penning meester / Persvoorlichter

Gegevens stagedocent

Naam	:	Peter van der Wijden
Email	:	wijden.vd.p@hsleiden.nl
Telefoon	:	(071) 518 85 97

Terminologie

Term	Uitleg
Eduroam	Een initiatief van Surfnet om studenten/docenten van opleidinginstantie 1 gebruik te laten maken van het netwerk van opleidinginstantie 2 (en andersom). Dit is een netwerk van uitwisselingen.
Eduroam instelling	De instelling die de fysieke netwerk connectie biedt tussen Wireless Leiden en Surfnet.
Student	Richard van Mansom afstudeerder bij Hogeschool Leiden StudentNR: s1001962, auteur van dit verslag.
Surfnet	Internet Service Provider van Hogescholen / Universiteiten in Nederland
Vrijwilliger	Wireless Leiden vrijwilliger
Wireless Leiden Vrijwilliger	Het vrijwillig personeel van Wireless Leiden
WL	Wireless Leiden

1. Opdracht

Een prototype node opzetten (en achterliggende infrastructuur) voor Wireless Leiden die 802.1x authenticatie gebruikt om studenten/docenten die gebruik maken van het Wireless Leiden netwerk toegang te verschaffen tot een Eduroam netwerk en het verbonden internet.

1.1 Deelvragen

1. Kan de 802.1x authenticatie gebruikt worden met behoud van het huidige volledig vrij toegankelijke netwerk.
2. Hoe wordt de toegang beveiligd tot het Eduroam netwerk tegen niet geauthenticeerde gebruikers.

1.2 De doelstelling

Het verschaven van beveiligde toegang tot Eduroam en daarbij ook internet met behulp van het Wireless Leiden netwerk voor Eduroam studenten/docenten.

1.3 Eisen

Het eindproduct dient aan de volgende eisen te voldoen

- De software moet toepasbaar zijn op de huidige nodes.
- Alle software dient ‘open source’ te zijn.
- Er staat geen vertrouwelijke informatie op de node of deze moet ontoegankelijk zijn gemaakt voor gebruikers die (remote) op de node zijn ingelogd (bijvoorbeeld: Terminal Sessie).
- Aanvullende eisen van Surfnet.

1.4 Online Documentatie

Ondersteunende documenten zoals onder andere vervolgopdrachten, notulen en de topologie zijn te vinden op http://svn.wirelessleiden.nl/svn/projects/802.1x/

2. Proces

Een 802.1x omgeving bestaat uit verschillende samenwerkende systemen. Het is niet realistisch om in 1 keer alle systemen te installeren en vervolgens er vanuit te gaan dat alles werkt. Er is voor gekozen om te beginnen met een zo basis mogelijke opstelling en deze dan telkens (indien mogelijk) met 1 systeem uit te breiden.

De volgende stappen geven het proces weer waarmee de omgeving tot stand is gekomen.

2.1 Hardware + Besturinggsysteem

De beschikbare hardware is een Soekris. Deze moet als node functioneren in het proof of concept. Een Soekris is een Embedded Computer, omdat het niet beschikt over een videokaart maar over een RS-232 seriële aansluiting, is een standaard installatie niet mogelijk. Er is onderzoek gedaan naar verschillende ready to run distributies van FreeBSD. Het doel van deze distributies is een gestandaardiseerde kant en klare oplossing. Echter is dit voordeel meteen het nadeel. Doordat deze distributies zijn ontworpen voor een qua hardware gelimiteerde omgeving is het geïnstalleerde softwarepakket erg uitgekleed. Essentiële (anders standaard aanwezige) software is uit de omgeving gehaald. Dit maakt deze omgevingen onbruikbaar.

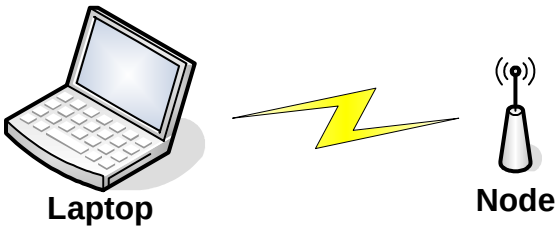
Er is gekozen om een 512MB FlashCard te gebruiken en hier een minimale installatie op te plaatsen (deze is ongeveer 275MB groot). Deze installatie is achteraf nog volledig aan te passen. Deze installatie wordt via een FlashCard lezer in een VMWare machine (een programma dat virtuele computers creëert) direct op de FlashCard geplaatst. Echter dienen er aanpassing doorgevoerd te worden op de installatie. Dit omdat deze installatie er vanuit gaat dat de installatie achteraf (ook) een Video console tot zijn beschikking heeft. Door deze aanpassingen is het mogelijk om deze standaard installatie met de Soekris compatible te maken.

2.2 Onbeveiligde verbinding

Voor er een beveiligde verbinding opgezet kan worden wordt er eerst een onbeveiligd Access Point gecreëerd. Voor een beveiligde verbinding worden er meer onderdelen van het systeem gebruikt. Alle onderdelen die nodig zijn voor een onbeveiligde verbinding, zijn ook nodig voor een beveiligde verbinding. Mocht er iets mis gaan dan is de oorzaak sneller gevonden.

Alle onderdelen die nodig zijn voor een onbeveiligd Access Point zijn al standaard aanwezig in een minimale installatie van FreeBSD. De beschikbaar gestelde Soekris bevatte al een werkende Access Point. De configuratie van deze node is als voorbeeld gebruikt om de node in werking te stellen als een onbeveiligd Access Point. Deze configuratie kan overgenomen worden omdat alle operationele Access Point (of bij Wireless Leiden OMNI's genoemd), gebruik maken van diezelfde onbeveiligde verbinding.

2.3 WPA node



De uiteindelijke node moet een WPA signaal kunnen uitzenden. Het programma wat gekozen is om 802.1x te ondersteunen heeft ook de mogelijkheid om WPA te ondersteunen. Er is een groot deel van het project uitgetrokken om WPA te implementeren. Dit omdat bij de voorgaande poging (tijdens mijn IMSM-Minor), dit een bottleneck was waar we niet overeen gekomen zijn. Voor WPA is alleen 1 node en een Laptop nodig. De testomgeving bevat nog geen onderdelen die later nodig zijn voor de 802.1x omgeving.

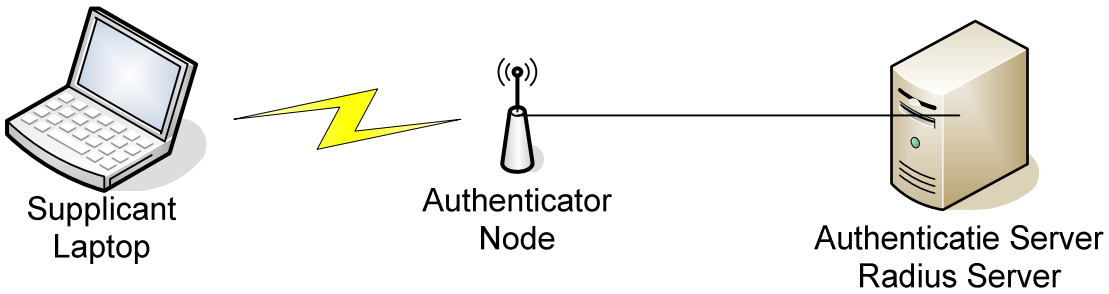
Tijdens de minor is gebleken dat de Senao kaarten (NIC's) geen WPA ondersteunen. Dit kwamen wij op een aantal internet pagina's tegen. Echter was onze kennis van FreeBSD en zijn software gelimiteerd en gingen wij er van uit dat de contactpersoon van Wireless Leiden destijds de waarheid sprak toen hij vertelde dat dit zeker wel mogelijk was. Wij hebben toen al onze tijd besteed om dit op te lossen maar uiteraard niet gelukt omdat de Senao kaart geen WPA ondersteund.

In de beschikbare gestelde Soekris bevinden zich twee Senao kaarten en 1 Atheros kaart. Door toeval is er gekozen om een aantal WPA tests te draaien via de Atheroskaart. Zonder al te veel moeite (lees 1.5 Dag internet zoekwerk) ondersteunde de Soekris WPA, kon er verbonden worden en een IP adres uitgedeeld werden. Dit was een aangename maar onverwachte verassing. Na dezelfde test gedraaid te hebben op de Senao kaart bleek dat deze met dezelfde configuratie niet werkte. Het feit dat de Senaokaarten geen WPA ondersteunen bleek wel te kloppen. Dit is later bevestigd door twee andere vrijwilligers.

2.4 Basis 802.1x node

Voor het toepassen van een basis 802.1x installatie zijn naast de node nog twee extra apparaten nodig, namelijk een laptop die 802.1x ondersteunt (een supplicant genoemd) en een RadiusServer (een authenticatieserver genoemd). Tijdens de voorgaande minor is een werkende RadiusServer geproduceerd, echter niet in combinatie met 802.1x. Zie voor problemen het hoofdstuk "Uitdagingen bij basis 802.1x".

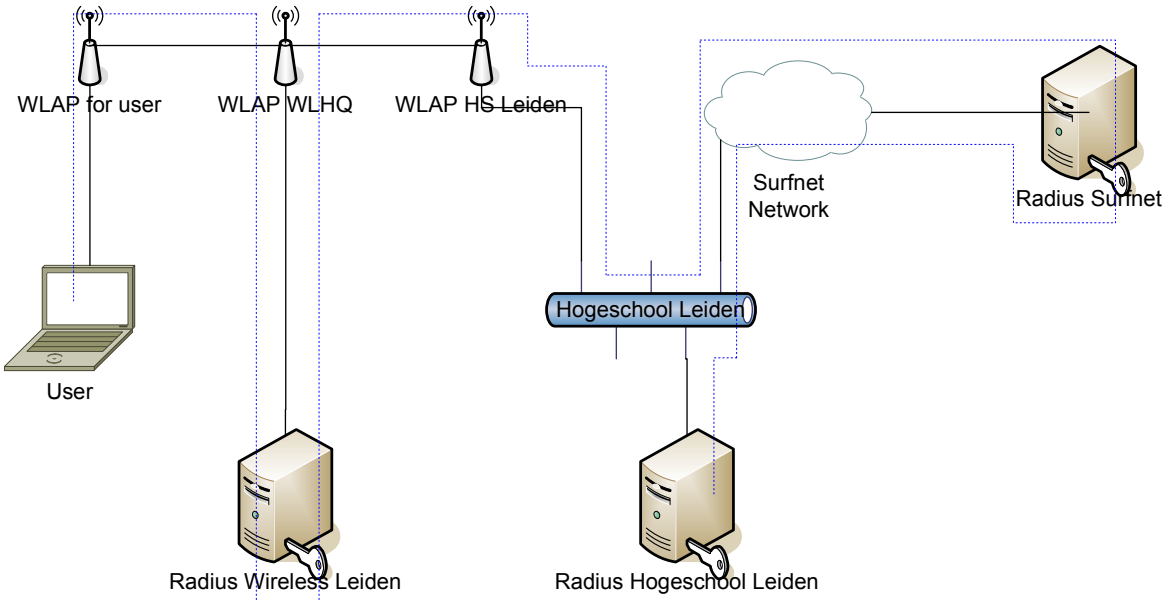
De testomgeving ziet op er dit moment als volgt uit:



2.5 Extra RadiusServer

Eduroam gaat verder dan 1 RadiusServer in combinatie met een node. Achter de node liggen verscheidene RadiusServers, zoals op dit plaatje te zien is. In dit voorbeeld zijn het er drie, echter is er in het 'echte' Eduroam netwerk sprake van verschillende instellingen en bestaat de Radius infrastructuur uit een boom van RadiusServer.

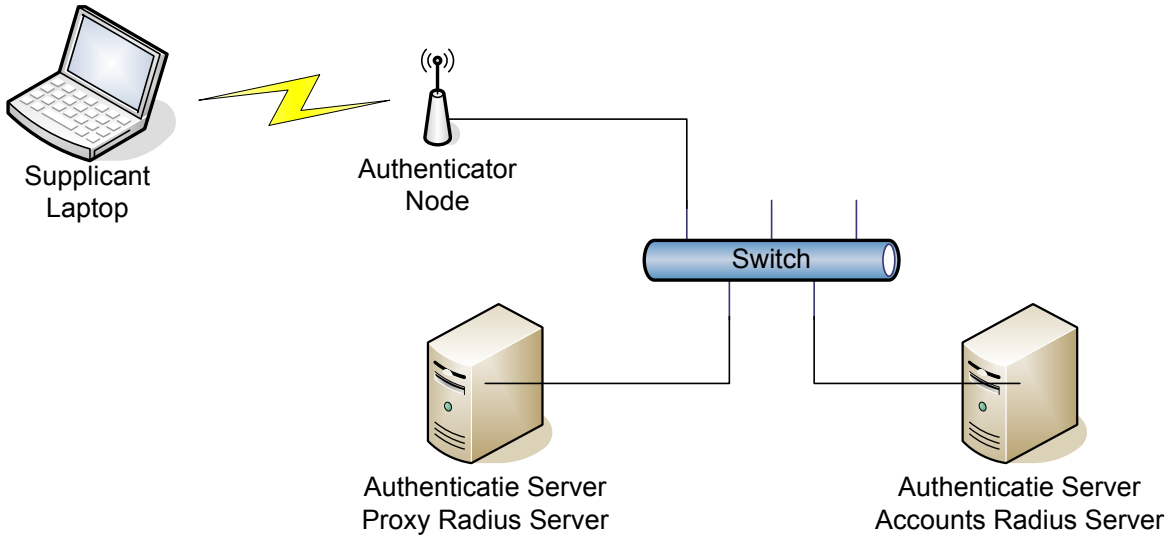
Een plaatje dat gemaakt is tijdens de IMSM Minor



In dit plaatje is er van uit gegaan dat de Eduroam connectie via de hogeschool gaat. De laptop maakt een verbinding met een node. De node (In het plaatje "WLAP for User" genoemd) maakt een verbinding met de RadiusServer van Wireless Leiden. De RadiusServer kent de authenticatie gegevens niet en zet het verzoek door naar de RadiusServer van Surfnet. Deze server kent de gegevens ook niet omdat deze geen gebruikersgegeven bevat. Deze server zet op basis van de gebruikersnaam (en zijn realm) het verzoek door naar de desbetreffende RadiusServer tot welke de gebruiker van de laptop behoord, dit zijn in de praktijk de Hogescholen en Universiteiten die zijn aangesloten bij het Eduroam project.

Het is zaak om de RadiusServer van Wireless Leiden in te stellen en te zorgen dat deze het verzoek doorzet naar de RadiusServer van Surfnet. Om dit proces te testen moeten er twee RadiusServer aanwezig zijn. 1 Server die het verzoek doorzet, een tweede die de accounts bevat. De server die de accounts bevat staat normaliter bij de Onderwijsinstelling zelf, echter ziet of weet de RadiusServer van Wireless Leiden dat niet. Het is dus niet relevant om een derde server te plaatsen die de rol van de RadiusServer van Surfnet simuleert.

De testomgeving ziet er op dit punt als volgt uit:



Communicatie stappen op het netwerk

1. De laptop zoekt verbinding net de node
2. De node maakt verbinding met de Proxy RadiusServer
3. De Proxy RadiusServer zet het verzoek door naar de Accounts RadiusServer

Het antwoord van de Accounts RadiusServer (Reject of Accept) wordt terug verzonden via hetzelfde pad.

2.6 Tunnel

Het Wireless Leiden netwerk bestaat uit verscheidene onbeveiligde nodes. Al het verkeer dat over deze nodes verzonden wordt, is onbeveiligd. Er moet een oplossing komen waarmee het verkeer over de nodes beveiligd verzonden wordt naar een ander punt op het netwerk.

Voor dit doeleinde zijn tunnel uiterst geschikt. Een tunnel echter is in zijn basis alleen een middel om verkeer van punt 1 naar punt 2 over het netwerk te verzenden (routeren). Om in een klap het beveiligingsprobleem op te lossen zou een oplossing gekozen moeten worden die het verkeer versleuteld over de tunnel stuurt.

Er zijn verschillende oplossingen voor dit probleem. Eigen onderzoek en later advies van Surfnet zetten OpenVPN boven aan het lijstje. Echter is er door een vrijwilliger eerder onderzoek gedaan naar dit deelprobleem (tunnels over Wireless Leiden). Bij dit onderzoek is IPsec gekozen als ideale oplossing. Zie voor dit proces hoofdstuk “Uitdagingen bij de koppeling van de node met Eduroam.”

Met Surfnet is gesproken om de motivatie achter de voorkeur voor OpenVPN te achterhalen, in dit gesprek kwam naar voren dat OpenVPN aan de beveiligingseisen voldoet die vereist zijn voor de implementatie (ook een belangrijk punt in het eigen onderzoek). Zij schreven IPsec echter niet af als optie. Echter de uitspraak dat OpenVPN aan Surfnet zijn beveiligingseisen voldeed, is een sterk argument om OpenVPN te gebruiken. De beveiliging op het netwerk is een relatief groot probleem. Ook vertelde zij dat OpenVPN hoog waarschijnlijk zwaarder was dan IPsec. Dit verhaal werd tegen gesproken door de Wireless Leiden vrijwilligers.

Omdat deze twee partijen elkaar tegenspraken (en mijn eigen onderzoek te valideren) is er een snelheid test gedaan met zowel IPsec als OpenVPN op dezelfde hardware met dezelfde omstandigheden. In dit vergelijkingsonderzoek kwam naar voren dat IPsec bijna twee keer zo snel is dan OpenVPN. Dit is een grote pre om IPsec te gebruiken

2.7 Multiple SSID

Eduroam vereist een eigen BSS. Deze BSS heeft zowel een andere beveiligingeis (WPA tegen onbeveiligd), als een andere SSID naamstandaard dan de huidige OMNI's. De techniek bestaat om op 1 Wireless Nic twee BSS'en uit te zenden. Echter is niet duidelijk hoe. Het programma dat de authenticator levert heeft deze optie volgens de handleiding. Echter bleek na verder onderzoek dat deze optie niet goed is geïmplementeerd. Ook zijn er verschillende handleidingen die melden dat het mogelijk was om VAP's (Virtuele Access Points) op te zetten en op deze manier een extra BSS uit te zenden.

Na elke week tijd apart gezet te hebben om een oplossing te zoeken voor dit probleem bleek 1 post alle onduidelijkheid op te lossen. De oplossing bestaat nog niet in de huidige versie van FreeBSD. Deze optie komt beschikbaar in de volgende versie van FreeBSD (FreeBSD 8.0). De code voor dit besturingsysteem is publiekelijk beschikbaar. Na een aantal testen gedraaid te hebben, is deze feature werkend gekregen in een FreeBSD 8.0-Current omgeving (met dezelfde Soekris waar de overige test opgedraaid werden). Echter door problemen met de Current versie (Deze bevindt zich in de Beta fase) zijn snelheid metingen niet mogelijk. De Multiple SSID optie zou ideaal zijn om Eduroam aan te bieden. Dit omdat er in deze omgeving geen extra Wireless Nic's in de verschillende nodes nodig zijn (wat in veel gevallen zelfs niet mogelijk is). Ook de kosten en implementatie van een extra antenne zijn niet nodig. De release versie van FreeBSD 8.0 is gepland voor 2009, tot die tijd is een FreeBSD 8.0 node niet realistisch, wat de Multiple SSID optie tot die tijd niet mogelijk maakt.

3. Keuzes

3.1 RadiusServer binnen Wireless Leiden

Technisch gezien is het niet nodig om een RadiusServer binnen Wireless Leiden te hosten. Er zijn echter wel voordelen aan.

De keuze wordt gemaakt volgens het score model

Afwegingen worden gemaakt op de volgende punten

- Extra te beheren service
  De RadiusServer is een extra server die beheert dient te worden door de Wireless Leiden vrijwilligers. Dit is extra werk en kan als nadeel gezien worden.
- Minder afhankelijk van de Eduroam deelnemer
  Als de Eduroam instelling een verandering doorvoert in de Radius infrastructuur dan bestaat de kans (bijvoorbeeld bij IP veranderingen) dat Wireless Leiden zijn instellingen moet veranderen. Als er een RadiusServer is, dient deze instelling op 1 punt veranderd te worden. Indien er geen RadiusServer aanwezig is dan worden alle individuele nodes verbonden met de RadiusServer van de Eduroam instelling. Dus dient de instelling op alle individuele nodes veranderd te worden. Ook andersom werkt dit. Als een node wordt toegevoegd aan het Wireless Leiden Eduroam netwerk dan is dit een extra client voor de RadiusServer. Deze wordt in het geval van een extra RadiusServer toegevoegd op de Wireless Leiden RadiusServer. In het geval dat de RadiusServer niet wordt opgezet dient bij elke toevoeging van een node deze doorgevoerd te worden op de RadiusServer van de Eduroam instelling.
- Kan gebruikt worden bij toekomstige projecten
  Radius is een relatief oud maar ook veel gebruikt protocol bij authenticatie. Doordat het breed gebruikt wordt kan het ook bij toekomstige projecten gebruikt worden waarbij authenticatie vereist is.
- Maakt de 802.1x infrastructuur complexer
  Een enkele tunnel van de node naar de Eduroam instelling is niet langer genoeg. Er moet een uitbreiding worden doorgevoerd zodat ook de nodes gebruik kunnen maken van de RadiusServer.

Afweging	Ja een Radius	Nee geen Radius
Extra te beheren service (0.20)	1 -> 0.20	2 -> 0.40
Minder afhankelijk van de Eduroam deelnemer (0.30)	2 -> 0.60	1 -> 0.30
Kan gebruikt worden bij toekomstige projecten (0.35)	2 -> 0.70	1 -> 0.35
Maakt de 802.1x infrastructuur complexer (0.15)	1 -> 0.15	2 -> 0.30
Totaal	1.65	1.35

De keuze wordt gemaakt om wel een RadiusServer te gebruiken binnen Wireless Leiden.

3.2 Gekozen Software

802.1x bestaat uit verschillende systemen en software. Bovenop deze software die voor 802.1x nodig is zijn er additionele software pakketten nodig om aan andere eisen te voldoen (met name beveiliging). In de volgende paragrafen wordt de gekozen software toegelicht.

3.2.1 Supplicant

De Supplicant is de client in de 802.1x omgeving. Dit zijn de laptops (en de software daar op) die verbinding zoeken met het netwerk. Een eis van Surfnet is dat de gebruiker van het netwerk geen verschil mag zien in het gebruik van Eduroam bij Wireless Leiden of op de school zelf.

Het is het doel om de Eduroam omgeving te laten werken op meerdere besturingsysteem (tests worden gedraaid op Windows, Mac en Linux). Echter is 802.1x een protocol dat vrij te gebruiken is en dus niet gekoppeld is aan een besturingsysteem (technisch of qua licentie).

Surfnet raadt een aantal software pakketten aan. Omdat Surfnet uiteindelijk een definitieve GO moet geven, moeten deze pakketten zeker werken. Daarom wordt er vanuit gegaan dat deze pakketten als Supplicant gebruikt worden

Windows : SecureW2
Mac : Wordt standaard ondersteund
Linux : Xsupplicant

3.2.2 HostAPD

In een eerder project is de keuze gevallen op HostAPD als authenticator. Reden die toen gegeven werden waren:

- Actieve community
- Goede documentatie
- Open Source
- Wordt doorontwikkeld

Tijdens dit voorgaande project was FreeBSD 6.3 de laatste stable release van FreeBSD. In tegenstelling tot de huidige release versie (FreeBSD 7.0) werd in FreeBSD 6.3 HostAPD niet meegeleverd bij de installatie. In FreeBSD 7.0 wordt HostAPD wel meegeleverd (ook bij de minimale installatie).

Doordat er eerder werk verricht is met HostAPD (en er geen nadelen gevonden waren), het voldoet aan de eisen en het in de huidige versie standaard meegeleverd wordt is er geen onderzoek gedaan naar andere software pakketten.

3.2.3 FreeBSD

De huidige nodes zijn ontwikkeld op een FreeBSD besturingsysteem. Het is mogelijk om de software op ieder ander platform te ontwikkelen echter is er gekozen voor FreeBSD omdat de nodes hier tijdens de opdracht op werken.

3.2.4 FreeRADIUS

Voor het testen van 802.1x zijn een aantal RadiusServer uitgeprobeerd. Het is gebleken dat alle geteste open source RadiusServers op FreeRADIUS na geen ondersteuning hebben voor de Outer Identity (een deel van 802.1x). Na het operationeel krijgen van de Radius Infrastructuur is niet verder gekeken naar andere RadiusServers om te controleren of deze ook werken. Het is gebleken dat FreeRADIUS qua opties ook de meest uitgebreide RadiusServer is. Dit maakt het interessant voor eventuele toekomstige projecten.

3.2.5 Tunnel software

OpenVPN

In de eerste instantie is uit eigen onderzoek en later door Surfnet geopperd dat OpenVPN een goede optie zou zijn voor de scheiding van het netwerk en de beveiliging van het verkeer. Deze optie bleek uit testen (en eerder door vrijwilligers geopperd) te zwaar te zijn.

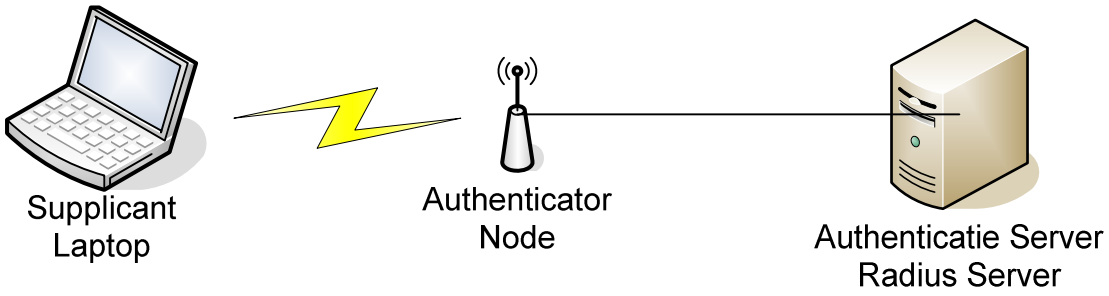
IPsec

Er is eerder onderzoek gedaan door vrijwilligers naar het gebruik van IPsec. Er is van dit onderzoek gebruik gemaakt en daardoor is IPsec als optie gaan gelden. IPsec is niet door Surfnet weggestreept als optie (al werd er verteld “OpenVPN voldoet aan onze eisen”). IPsec bleek van de gekozen opties qua veiligheid aan de eisen te voldoen en de hoogste snelheid te halen (of met dezelfde bandbreedte lagere load voor de nodes te bezorgen).

3.3 802.1x Alternatieven

Er is geen alternatief voor de gebruikte techniek. De reden volgt

Een plaatje van een basis 802.1x omgeving



3.3.1 Authenticatieserver

De authenticatieserver dient het Radius protocol te ondersteunen om te kunnen communiceren met de RadiusServer van Surfnet. Dit maakt een alternatief niet mogelijk.

3.3.2 Authenticator

Het is mogelijk om op dit punt in de keten een alternatief te kiezen. Echter alleen als deze compatible is met het 802.1x protocol vanuit de laptops/clients. Een alternatief zou het authenticatieverzoek moeten doorzetten naar een RadiusServer. Als een alternatief deze technieken ondersteund is er in dit gedeelte van de infrastructuur geen bezwaar tegen een alternatief.

Volledige compatibiliteit met de clients en authenticatieserver is een eis voor de authenticator. Het 802.1x protocol is 1 standaard. Als er gebruik gemaakt wordt van dit protocol dan is het zeker dat de communicatie zonder problemen verloopt. Echter een alternatief hoeft zich niet te houden aan alle (communicatie) regels die binnen het protocol gesteld zijn. Dit betekent dus dat er geen garantie bestaat dat de communicatie probleemloos verloopt. Als aan alle communicatieregels voldaan wordt dan is het in principe een 802.1x authenticator. Waardoor een alternatief of zich niet aan de communicatieregels houd, of het is een 802.1x authenticator.

3.3.3 Supplicant

De laptops zijn in eigen beheer van de individuele gebruiker van het Eduroam netwerk. Het is als eis gesteld dat deze zonder herconfiguratie gebruik kan maken van het Eduroam netwerk. Dit zou betekenen dat het alternatief hier op kan inspelen. Echter hoeven deze laptops alleen 802.1x te ondersteunen en maakt dit een alternatief onmogelijk.

3.3.4 Mogelijk verandering

De enige communicatie waar Wireless Leiden controle over heeft is de communicatie tussen de authenticator en de RadiusServer van Wireless Leiden. Al is het in theorie mogelijk om op dit punt een alternatief te plaatsen, is de communicatie achter de RadiusServer van Wireless Leiden ook Radius. Om een zo transparant mogelijke infrastructuur te creëren is er voor kozen om de standaard infrastructuur van 802.1x te handhaven (ook mede omdat er geen reden is om een alternatief te kiezen).

3.4 Instellingen van een programma.

Er is niet eerder gewerkt met het gros van de als optie geldende applicaties. Als gevolg hiervan zijn de instellingen die het programma moeten laten werken ook onbekend. Er zijn vaste fases doorlopen bij elke applicatie met instellingen.

Aanname

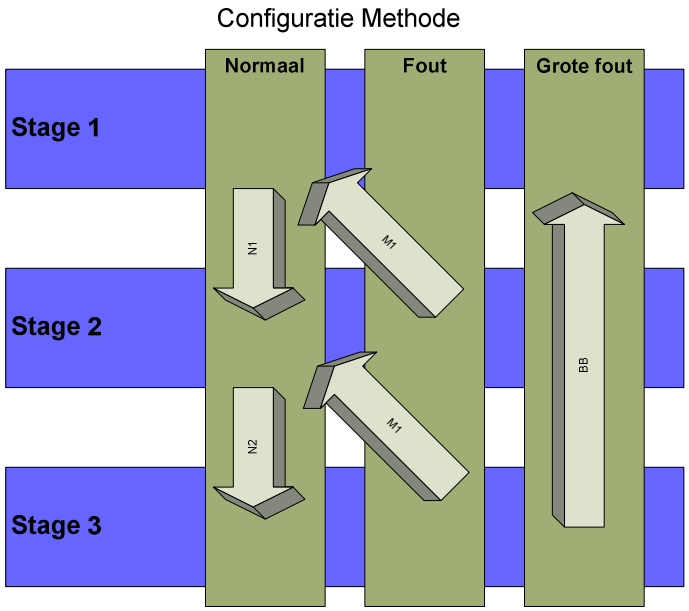
- Er is geen ervaring met het gebruikte programma.
- Het is bekend dat het gebruikte programma toepasbaar is op het doel.

3.4.1 Minimaliseer het aantal applicaties

Er wordt zoveel mogelijk aan 1 applicatie tegelijkertijd gewerkt. Als er een configuratie veranderd moet worden en er gaat iets mis, dan is het meteen duidelijk welke applicatie verantwoordelijk is voor het falen. Een keten zoals die in 802.1x dient eerst met een basis te beginnen die zich dan evolueert naar een volledig werkende omgeving. Dit maakt het mogelijk dat een programma tijdelijk configuratieregels heeft die uiteindelijk niet worden gebruikt in de final opzet. Een voorbeeld zoals dat is voorgekomen (van basis installatie node tot aan 802.1x node)

1. Begin met een onbeveiligde node.
2. Zet een WPA Access Point op
3. Voeg 1 RadiusServer en Supplicant toe
   Helaas is er geen tussenstap mogelijk waardoor de RadiusServer (authenticator) en de Supplicant apart opgezet kunnen worden.
4. Voeg een additionele RadiusServer toe

3.4.2 Schematische weergave



3.4.3 Stages

De volgende fases zijn doorlopen bij elk programma dat instellingen heeft en geconfigureerd dient te worden.

Stage #1: Voorbeeld

Omdat er nog geen ervaring is met de meeste van de gebruikte producten is het eerste doel een voorbeeld opzet te creëren. Deze voorbeelden worden van internet afgehaald. Deze voorbeelden hoeven niet per definitie te voldoen aan alle eisen waar het programma uiteindelijk aan moet doen. Het belangrijkste is het bewijzen dat het programma in grote lijnen kan doen wat het zegt dat het kan doen. Voorbeeld: Verkeer beveiligen bij de authenticator, of gebruikersaccounts authenticeren bij een RadiusServer.

Stage #2: Strippen

De volgende stap is het strippen van zoveel mogelijk configuratieregels die niet belangrijk zijn voor het doel van het programma. Op dit punt moet duidelijk zijn wat elke configuratieregel in de configuratiebestanden als doel heeft. Vaak zijn er bij de gekozen voorbeelden overbodige configuratieregels opgenomen (of per definitie omdat ze default zijn, of omdat het doel van de configuratieregel niet belangrijk is voor het doel van het programma waar het in de opzet voor gebruikt wordt). Het is belangrijk om op dit punt een kopie te hebben van het eindproduct van de eerste stage, ook een versiebeheer voor de verschillende gestripte versies zijn nuttig. Vaak wordt het strippen in fases gedaan, dit zodat bij een foute strip meteen duidelijk is welke regel wel nuttig is en toch gestript is. Het versiebeheer is nuttig omdat een hoge waarschijnlijkheid heeft dat er 1 of meerdere fases terug gegaan moet worden. Het is wel mogelijk om kennis opgedaan in het strippen opnieuw toe te passen.

Stage #3: Toevoegen

Op dit moment is er een programma dat in grote lijnen doet wat het zou moeten doen maar nog niet aan alle eisen voldoet. Door configuratieregels te wijzigen en (vooral) toe te voegen kan de functionaliteit aangepast worden aan de eisen van het programma. Op dit moment is het niet verstandig om grote veranderingen door te voeren in het programma, vele kleine stappen zijn vaak efficiënter dan 1 grote stap, mocht er iets mis gaan dan is het op dat moment meteen duidelijk welke configuratieregel(s) het probleem veroorzaken.

Note

Het kan nuttig zijn na Stage 3 terug te keren naar Stage 2. Het is echter niet verstandig om een nieuw voorbeeld op te zoeken en deze te verwerken in de setup. In veel gevallen is het meer werk om een enkel probleem op te lossen dan een nieuw bestand te gebruiken. Bij grote incompatibiliteit is het wel mogelijk om het gebruikte configuratiebestand af te wijzen en het volledige proces opnieuw te beginnen. Er is in dit geval vaak een fout gemaakt in Stage 1. Niet elke configuratiebestand is geschikt voor deze methode, er dient dus ook bij stage 1 nagedacht te worden over de overige stages.

Efficiënt

Al is het mogelijk om een stap terug te doen is het belangrijk om pas van stage te wisselen als de huidige stage afgesloten is. Dit zorgt er dat het eindresultaat het meest efficiënt (behaald) is.

3.4.4 Actie

Pijl N1

Op het moment dat er een configuratievoorbeeld is gevonden dat aan de eisen voldoet wordt er over gegaan naar Stage 2.

Pijl N2

Op het moment dat het configuratiebestand zodanig is gereduceerd (echter nog wel werkzaam is) dat het onwaarschijnlijk is dat er nog overbodige configuratieregels in aanwezig zijn kan er overgestapt worden naar Stage 3.

Pijl M1

Als in Stage 2 blijkt dat het gekozen voorbeeld niet overeenkomt met het doel van het eindproduct kan er terug gestapt worden naar Stage 1. Dit is mogelijk omdat er in deze fase onderzoek gedaan wordt naar de betekenis van de verschillende configuratieregels. Dit onderzoek (indien grondig uitgevoerd) geeft ook veel andere functionaliteiten van het programma weer. Een ander begin punt is in een aantal gevallen nuttiger. Bijvoorbeeld als in stage 2 het configuratiebestand zodanig gereduceerd moet worden dat de gewenste functionaliteit (welke is stage 1 aanwezig was) verdwijnt door het wijzigen van het configuratiebestand. De keuze kan gemaakt worden om de opgedane kennis te gebruiken om een nieuw configuratiebestand in te stellen. Echter is er op dit moment dan zodanig veel kennis opgedaan dat deze methode minder effectief is.

Pijl M2

Na het toevoegen van configuratieregels kan het duidelijk worden dat een andere configuratieregel overbodig wordt (of door testen of door andere vormen van onderzoek). Het is dan nodig om 1 stap terug te zetten omdat het verwijderen van configuratieregels in Stage 2 gebeurt. Onmiddellijk daarna kan het normale proces voortgezet worden.

Pijl BB

Mocht er ergens in het proces blijken dat de ingeslagen hoek niet effectief is dan kan de keuze gemaakt worden om terug te gaan naar een basis configuratie (of het bestand uit Stage 1 of om Stage 1 opnieuw uit te voeren). Dit is een stap die niet licht genomen moet worden, vaak is het werk wat eerder gedaan is niet herbruikbaar, dit geldt wel voor de kennis die is opgedaan.

Versie beheer

Versie beheer is erg belangrijk. Veel handleidingen, mailinglist en forums die beschikbaar zijn op internet, zijn alleen van toepassing op specifieke situaties (in mindere mate voor officiële handleidingen). In de praktijk blijkt het scenario in een uitleg op een forum of mailinglist niet altijd overeen te komen met de eigen situatie. Echter kunnen dit soort posts nuttige informatie op leveren. Echter door niet overeenkomende scenario’s kan het voorbeeld niet altijd relevant zijn. Door oude versies bij te houden kan er eenvoudig een kleine stap terug gezet worden.

4. Uitdagingen

In de loop van de opdracht zijn er verschillende uitdagingen geweest. Deze zijn veelal in groepen verwerkt. Dit omdat een bepaalde functionaliteiten aan elkaar gekoppeld zijn (of juist niet).Als de verschillende uitdagingen los van elkaar worden aangepakt is dit niet erg efficiënt. Dit omdat informatie verkregen uit een de ene uitdaging vaak input geeft voor een volgende uitdagingen.

Deze uitdagingen zijn dan ook gekoppeld opgenomen in de volgende hoofdstukken.

4.1 Uitdagingen bij basis 802.1x

4.1.1 Probleemstelling

Er moeten drie systemen geïnstalleerd worden die afhankelijk zijn van elkaar. Alle drie moeten zonder problemen werken om de keten te laten slagen.

Drie objecten

- Supplicant
- Authenticator
- Authenticatieserver

Na een standaard installatie plus een basis configuratie voor 802.1x werkt de 802.1x keten niet.

4.1.2 Symptomen

Supplicant (SecureW2)

- Geeft veel foutmeldingen in logboek, door fout van Windows zijn deze niet te lezen.
- Windows blijft een aantal seconden op “validating” staan waarna er opnieuw om een wachtwoord gevraagd wordt.

Authenticator (HostAPD)

- Verbreekt de verbinding zodra er geauthenticeerd is.
- Broadcast een WEP signaal

Authenticator Server (FreeRADIUS)

- Geeft twee Authenticatieverzoeken, een van de gebruiker de andere van “anonymous”

4.1.3 Uitsluiting

Mijn broertje volgt een opleiding bij een Universiteit die deelneemt aan het Eduroam project. De laptop van mijn ouders heeft een werkende SecureW2 client (werkend op Technische Universiteit Eindhoven). Omdat deze laptop volgens de Eduroam richtlijnen is geïnstalleerd is er een test uitgevoerd op de werking van deze laptop op het 802.1x testnetwerk. De drie objecten reageren op dezelfde manier als de originele testlaptop.

4.1.4 Tweede check.

De systeembeheer afdeling van de Hogeschool Leiden melde ongeveer een jaar geleden dat het Eduroam netwerk op school wel werkt. Op het moment van schrijven vertelde de IT dienst van de Hogeschool Leiden dat dit Eduroam netwerk niet werkt. Een test met de SecureW2 client van de testlaptop maakte een succesvolle verbinding op het Eduroam netwerk van de hogeschool.

4.1.5 Supplicant werkt

Zowel de test met een werkende supplicant als de test op een werkend 802.1x netwerk tonen aan dat de Supplicant goed werk. De Supplicant kan worden uitgesloten als oorzaak van het probleem.

4.1.6 Logs

Nu er een factor is uitgesloten blijven er twee objecten over. Zowel de Authenticator als de Authenticatieserver hebben een uitgebreide log functie. Na het lezen van deze log regels (en uitzoeken wat deze regels betekenen) komt naar voren dat er een gebruikers “anonymous” probeert te authenticeren. Deze gebruiker wordt de toegang ontzegt, er wordt een reject reactie gestuurd naar de node voor het MAC adres van de test laptop. Hierna wordt de verbinding verbroken.

4.1.7 Outer Identity

Wat is de Outer Identity

De outer Identity ook wel de eerste fase genoemd (Phase 1) is een identiteit van de supplicant zoals deze zichtbaar is buiten de 802.1x tunnel. De Outer Identity is onbeveiligd en is daardoor niet geschikt (of bedoeld) voor authenticatie. De gebruikersnaam en wachtwoord wordt ook wel de “inner identity” genoemd, deze wordt versleuteld is in de tunnel. De Outer Identity is publiek de Inner Identity niet.

Als het authenticatieverzoek inclusief outer identity aankomt bij de RadiusServer. Dan ziet FreeRADIUS de outer identity als een gebruikersnaam. Omdat de Outer Identity geen gebruikersnaam is (het bevat ook geen wachtwoord) zal FreeRADIUS reageren met een Reject. Dit heeft als gevolg dat de connectie met de supplicant (client) verbroken wordt.

De kans bestaat dat er (Eduroam) netwerken zijn die de Outer Identity gebruiken, dit betekend dat het netwerk compatible moet zijn met de Outer Identity. Het negeren van de Outer Identity dient dus te gebeuren op de RadiusServer die de gebruikersaccounts bevat. Deze wordt niet gebruikt bij een live omgeving. Deze staat bij de onderwijsinstellingen zelf en is opgezet omdat de werking van de andere systemen getest moet worden.

Na het gebruik van internet blijkt dat FreeRADIUS de outer identity kan negeren. Na het invoeren van deze configuratieregel veranderd het gedrag van de laptop bij de authenticatie.

4.1.8 Acquiring network address

Na het opzetten van een verbinding veranderd de tekst in de Windows Draadloze client van “validating” in “acquiring network address”, waarna er opnieuw om een gebruikersnaam en wachtwoord gevraagd wordt. FreeRADIUS geeft op dit moment alleen een Accept voor de gebruikersnaam en er komt geen anonymous voor in de logs van FreeRADIUS. HostAPD geeft aan dat er een connectie gemaakt is waarna er een nieuwe authenticatieverzoek opgezet wordt.

4.1.9 Authenticator (node)

Op dit moment is node de oorzaak van het niet werken. Eerder was de Supplicant uitgesloten als oorzaak van het probleem. Op het moment dat de Supplicant de tekst geeft ‘acquiring network address” betekend dat dat de node verkeer doorlaat niet zijnde 802.1x verkeer. Dit betekend dat de RadiusServer een succesvolle accept heeft gegeven. Dit blijkt ook uit de logs van zowel HostAPD als FreeRADIUS.

4.1.10 Macintosh

Na een test vanaf een Macintosh blijkt dat de Macintosh een WEP (encryptie) signaal denkt te ontvangen, Windows XP ziet een WPA signaal. Na in HostAPD expliciet op te geven dat deze een WPA signaal moet broadcasten blijkt dat er ook daadwerkelijk een netwerk adres wordt toegekend aan de supplicant. De student was onterecht onder de indruk dat bij het gebruik van 802.1x WPA standaard is.

4.2 Uitdagingen bij een extra RadiusServer

4.2.1 Toelichting

De basis 802.1x omgeving is opgesteld (supplicant, authenticator, authenticatieserver). Op de authenticator server staan gebruikersaccounts. Echter staan in een Eduroam omgeving de gebruikersaccounts niet op de RadiusServer van Wireless Leiden. Dit betekend dat er een additionele RadiusServer opgezet moet worden om als Proxy te functioneren tussen de Authenticator en de RadiusServer die de gebruikersaccounts bevat.

Benamingen

De RadiusServer die de gebruikersaccounts bevat, welke de servers buiten het Wireless Leiden netwerk representeren wordt de Accounts RadiusServer genoemd. De RadiusServer die de RadiusServer van Wireless Leiden simuleert wordt de Proxy RadiusServer genoemd. Wat Proxy betekend wordt in de paragraaf Theorie van dit hoofdstuk besproken.

4.2.2 Problemen

- Authenticatie mislukt met valide inloggegevens.
- De realm naam dient in de gebruikersnaam behouden te worden (standaard wordt deze verwijderd bij een proxy naar een andere RadiusServer).

4.2.3 Uitsluiting

Dit scenario bestaat uit 4 objecten (supplicant, authenticator en 2 RadiusServers / authenticatieservers). De werking van de supplicant en de authenticator staat vast. De gegevens die op deze objecten worden verwerk komen overeen met het eerder werkende scenario. Echter door het toevoegen van een extra RadiusServer worden de gegevens gemanipuleerd in de Radius infrastructuur.

4.2.4 Theorie

Proxy

De Authenticatieserver is een RadiusServer. Deze server bevat volgens het 802.1x protocol de gebruikersaccounts. De gebruikersaccounts van Eduroam instellingen zijn niet beschikbaar bij andere instelling (dus ook niet bij Wireless Leiden). Om 802.1x/Eduroam op het Wireless Leiden netwerk te laten werken zijn er geen gebruikersaccounts nodig, de authenticatieverzoeken moeten doorgezet worden naar de Surfnet RadiusServer, dit doorzetten wordt proxy genoemd. De Surfnet RadiusServer stuurt het verzoek op zijn beurt door naar de RadiusServer van de deelnemende instelling tot welke de gebruiker van de supplicant behoort. De RadiusServer van deze deelnemende instelling bevat de gebruikersaccounts. De Accept of de Reject op het authenticatieverzoek wordt via het zelfde pad terug gestuurd, waarna de node toegang verschaft (of niet).

Realms

Een RadiusServer kan authenticatieverzoeken doorsturen naar verschillende (andere) RadiusServers. Als er meerdere RadiusServer zijn dan wordt er gebruik gemaakt van Realms. Op basis van een Realm wordt het authenticatieverzoek doorgestuurd naar een andere RadiusServer.
Een Realms is een deel van de gebruikersnaam.

Er zijn standaard verschillende syntaxen in FreeRADIUS, een aantal voorbeelden

De emailadres syntax
s1234567@student.hsleiden.net

De NT Domein syntax
student.hsleiden.nl\s1234567

In beide syntaxen is “s1234567” de gebruikersnaam en “student.hsleiden.nl” het Realm.

4.2.5 Logs

Omdat er nog geen aangrijpingspunten zijn om een onderzoek te starten naar de oorzaak van het probleem is de eerste stap het doorzoeken van de logs van de twee RadiusServers. De Proxy RadiusServer ontvangt een Reject en stuurt deze door naar de Authenticator. De Accounts RadiusServer geeft een foutmelding met betrekking tot EAP.

4.2.6 Zoekmachine

De foutmelding die de Accounts RadiusServer geeft wordt ingevoerd in een zoekmachine op internet. Na een aantal pagina’s word er een pagina gevonden die de foutmelding koppelt aan een Proxy RadiusServer. Het scenario op deze webpagina is vergelijkbaar met het testscenario. Het probleem is dat EAP het wijzigen van een gebruikersnaam niet toestaat. In dit voorbeeld: het verwijderen van het Realm uit de gebruikernaam is niet toegestaan. Door de instructie te volgen van de webpagina voor het behouden van de realmnaam in de gebruikersnaam blijft de gebruikersnaam intact en volgt een succesvolle authenticatie. Bij het doorsturen van het authenticatieverzoek moet de realmnaam in de gebruikersnaam behouden blijven. Mocht de authenticatieserver (RadiusServer) de realmnaam verwijderen dan is deze informatie niet langer beschikbaar voor Surfnet. Zonder deze informatie kan de authenticatieserver van Surfnet het verzoek niet doorsturen naar de betreffende authenticatieserver van de onderwijsinstelling dit omdat de Realm naam de instelling representeert.

4.3 Uitdagingen bij de koppeling van de node met Eduroam

4.3.1 Probleem

Het verkeer afkomstige van een Eduroam SSID moet van de node naar een ander netwerk gerouteerd worden. Verkeer niet afkomstig van de Eduroam SSID mag geen toegang hebben tot dit verkeer of netwerk.

4.3.2 Oplossingen

- Routing Protocol
- Client-server VPN
- Netwerk Layer ACL's
- Tunnels

4.3.3 Criteria

Beveiliging

Een eis van Surfnet is dat het signaal verzonden over het netwerk beveiligd is tegen het lezen door derde. Deze eis wordt meegenomen in de evaluatie.

WPA

De mogelijkheid bestaat om de interlinks met WPA te beveiligen. Door ze hier mee te beveiligen wordt de data versleuteld verzonden over de backbone. Deze versleuteling moet (als eis van Surfnet) ook worden toegepast op de Eduroam SSID's. Een groot deel van de interlinks maakt op het moment gebruik van de Senao draadloze NIC's. Deze bieden geen WPA mogelijkheid. In de toekomst worden alle interlinks vervangen door Atheros kaarten zodat deze gebruik kunnen maken van 802.11a. Deze Atheros kaarten kunnen ook gebruik maken van WPA. In de toekomst is het mogelijk om de beveiliging te verhogen. Echter is dit op het moment nog niet mogelijk.

Ivm met de relatief slechte beveiliging is het advies: implementeer WPA boven op een ander vorm van beveiliging op het moment dat dit mogelijk wordt. Tot die tijd dient een andere vorm van beveiliging voldoende te zijn, ook deze beveiliging dient voldoende te zijn volgens de eisen van Surfnet.

Impact

Een zelf opgestelde eis is dat de keuze zo min mogelijk veranderingen tot gevolg mag hebben in het Wireless Leiden netwerk. Het netwerk werkt nu en er is werk ingestoken door vrijwilligers. Als er geen duidelijke reden is om een systeem om te bouwen (lees: er is geen beter alternatief) dan dient het systeem intact gelaten te worden.

Vrijwilligers

Wireless Leiden is afhankelijk van vrijwilligers. Het is mijn mening dat de keuzes minimaal werk op moeten leveren voor de vrijwilligers. Dit werd bevestigd toen de volgende tekst gestuurd werd door een vrijwilliger via in een chatsessie “Zeker hoe minder de client / vrijwilliger moet instellen hoe beter lijkt me zo.”

4.3.4 Oplossingen: De afweging

Routing Protocol

Het routing protocol dat gebruikt wordt binnen Wireless Leiden (LT Routed) is gemaakt door een vrijwilliger. Standaard biedt dit protocol geen ondersteuning voor gedistribueerde default routes. Er zijn routing protocollen die deze functie wel bieden. Echter is het Wireless Leiden netwerk in opzet uniek en is er door eerder onderzoek gebleken dat standaard routing protocollen moeilijkheden ondervinden in het netwerk. Als optie blijft over, het aanpassen van het huidige protocol.

Afwegingen

- Beveiliging
  Een gedistribueerde default routes heeft standaard geen beveiliging geïmplementeerd, beveiliging is een aparte techniek. Het is wel mogelijk om dit bij ontwikkeling mee te nemen.
- Impact
  Bij de implementatie dient het volledige netwerk aangepast te worden. Elke node heeft een router functie en dient hierdoor aangepast te worden. Ook dienen alle nodes tegelijkertijd bijgewerkte te worden voor optimale communicatie.
- Vrijwilligers
  Deze optie vraagt veel input en medewerking van de vrijwilligers. Het routing programma moet herschreven worden en alle nodes dienen (handmatig) geüpgrade te worden.

Client – Server VPN

VPN staat voor Virtueel Private Network en is een tunnel protocol tussen twee punten. Er zijn verschillende applicaties die deze optie mogelijk maken, elke met eigen voor en nadelen.

Afwegingen

- Beveiliging
  De mogelijkheden hangen af van de gekozen applicatie. Echter is het vrij standaard dat een tunnel beveiligd kan worden. Op basis van de wensen dient een applicatie gekozen te worden
- Impact
  Elke node die Eduroam mogelijkheden biedt dient aangepast te worden. Echter hebben al deze nodes al aanpassing nodig ivm het Eduroam SSID. Nodes die geen Eduroam gaan uitzenden hoeven niet aangepast te worden. Ook niet wanneer er Eduroam verkeer over de interlinks gaat.

Netwerk Layer ACL

Het scheiden van verkeer op laag 3 (network layer) met Access Control Lists (ACL’s). Op deze manier wordt het verkeer gescheiden en is op de rand van het netwerk onderscheid te maken welk verkeer er van de Eduroam SSID afkomstig is en het verkeer dat afkomstig is van de wLeiden.net SSID’s. Er zijn

ACL's nodig omdat het verkeer van wLeiden.net niet gecontroleerd wordt en dus gescheiden moet worden van het verkeer afkomstig van een Eduroam SSID.

Afwegingen

- Beveiliging
  Het verkeer wordt gescheiden met ACL's dit biedt beveiliging tegen het verzenden van verkeer via een onbeveiligde verbinding (wLeiden.net SSID's) echter wordt het verkeer niet versleuteld en er is dus onderscheppinggevaar. Het verkeer verzonden over de Interlinks kan opgevangen en gelezen worden.
- Impact
  Al de nodes dienen aangepast te worden. Als niet alle nodes worden aangepast ontstaat een beveiligingslek. Via een node zonder ACL kan verkeer van het ene netwerk naar het andere netwerk gerouteerd worden.

Tunnels

Een tunnel is een connectie tussen twee computers (of in het geval van Wireless Leiden twee nodes). Er zijn verschillende implementaties voor beschikbaar (protocollen). Als data op het Eduroam SSID binnen komt moet deze doorgestuurd worden over de tunnel naar het andere (eind) punt op het netwerk. De data wordt over het netwerk verzonden, echter lijkt dit voor het pakket 1 hop. Als bijvoorbeeld een traceroute commando wordt gegeven dan zijn de tussenstappen (de tussenliggende nodes) niet zichtbaar.

Afwegingen

- Beveiliging
  De beveiliging hangt af van de gekozen implementatie. Er zijn verschillende vormen van beveiliging. Indien nodig kan een erg scherpe of juist minder scherpe beveiliging gekozen worden.
- Impact
  Elke nodes moet apart worden aangepast indien deze gebruik maakt van de Eduroam SSID. Dit is echter al nodig omdat de node nog geen Eduroam SSID uitzendt. Dit werk kan in dezelfde batch meegenomen worden.
  Elke node heeft een tunnel naar een centraal punt. Op dit centrale punt moet afzonderlijk een tunnel worden definieert voor alle nodes die een tunnel hebben. Bij het toevoegen van een nieuwe tunnel moet het centrale punt worden aangepast.

Verschil Tunnel en Client Server VPN

Een Client Server VPN maakt gebruik van een tunnel maar biedt de server-client mogelijkheid (zoals de naam al indiceert). Het is niet nodig om voor elke tunnel een tunnelinterface te definiëren op de server. Bij (bijvoorbeeld) 60 nodes dienen bij een tunnel 60 tunnelinterfaces gedefinieerd te worden. Dit is meer werk en vraagt meer van de hardware van de gateway dan een enkele regel in de VPN server.

4.3.5 Samengevat

	Beveiliging	Impact	Vrijwilligers
Routing Protocol	+/-	-	-
Client Server VPN	+	+	+
Netwerk Layer ACL	-	-	-
Tunnel	+	+/-	+/-

\+ = Voordeel
+/- = Neutraal
\- = Nadeel

De keuze
Er wordt gekozen voor Client – Server VPN door zijn score in de drie categorieën waar op beoordeeld is.

3.3.6 Tunnel of Tap voor de VPN implementatie

Een vergelijkbare opties met een Tunnel is een Tap. Beide encapsuleren het pakket in een ander pakket echter is de implementatie anders. Door het verschil in implementatie zijn er een aantal verschillende voor en nadelen in de beide opties.

Broadcast

Een IP tunnel laat geen (IP) broadcasts door. Dit is geen nadeel omdat er van uit gegaan kan worden dat er ergens in het path in het netwerk van de Eduroam instelling een router aanwezig is. Een router laat geen broadcast pakketten door. Deze eigenschap van een tunnel kan ook als voordeel gezien worden omdat broadcasten op een eerder punt in het pad worden afgevangen en er geen netwerkverkeer over de lijn gaat.

Layer 3

Een tunnel laat alleen IP toe op de netwerk layer, een Tap laat alle netwerk layer protocollen toe. Zowel Wireless Leiden, Surfnet, de Hogeschool Leiden als Universiteit Leiden maken gebruik van IP netwerken. Dit maakt deze beperking geen probleem.

Resources

Een tunnel gebruikt minder resources (geheugen en CPU Time) dan een Tap. De nodes zijn geen krachtige computers. Een voordeel voor de tunnel.

4.3.7 Gekozen programma

Eisen aan het VPN programma

- Ondersteund Tunnels
- Goed gedocumenteerd
- Actieve communicatie
- Succes verhalen beschikbaar
- Client – Server ondersteuning (node = client)
- Ondersteund PKI/certificaten
- Ondersteund verschillende versleutelmethode (hoog en gemiddelde sterkte)

In een Google zoekopdracht komt OpenVPN naar voren als de optie die het beste voldoet aan de bovenstaande eisen. Er is eerst een longlist gemaakt met alle gevonden oplossingen, hier staan de oplossingen op welke initieel aan de eisen lijken te voldoen. Op de individuele oplossingen is verder onderzoek gedaan en daar is een shortlist uit gekomen om zeker te stellen of alle eisen daadwerkelijk aan de eisen voldoen. Hier is OpenVPN uitgekomen als voorkeur.

4.3.8 Een week later

Na ongeveer een week bezig te zijn geweest om een Open VPN testopstelling te maken, is er over dit onderwerk communicatie geweest met de vrijwilligers van Wireless Leiden. Zij gaven mij het advies om tunnels te kiezen (boven Client-Server VPN) om de volgende redenen.

- Een client-server vpn is in vergelijking met een tunnelprotocol erg zwaar voor de individuele nodes.

  Mijn analyse:
  In de basis is een client-server vpn niets anders dan een tunnel (voor de client). Als de oplossing te zwaar is zou dit betekenen dat de oplossing te veel opties heeft (wat extra verkeer of extra CPU time met zich mee zou brengen). Indien een product te zwaar is zou deze oplossing mogelijk zijn, echter is het verkeerde product gekozen.
- Er is extra verkeer nodig op het netwerk om de connectie in stand te houden (keep alive singals).

  Mijn analyse:
  Als het enige doel is om de lijn in stand te houden en geen time-outs te veroorzaken dan is een klein pakketje genoeg, de grote van een pakket is niet belangrijk alleen dat er een pakket over de lijn gaat.
  Als het doel is om de beveiliging in stand te houden, dus een nieuwe sleutel te onderhandelen, dan zou er inderdaad meer informatie over de lijn heen gaan, echter draagt dit dan wel bij aan de veiligheid.
- Er werd aangegeven dat een client server vpn een oplossing is voor “road warriors.”

  Mijn analyse:
  Al is dit ook een implementatie, is dit technisch geen reden om deze optie niet te gebruiken.
- Als de tunnel eenmaal ingesteld is, dan is er geen werk van de vrijwilliger nodig. Dit werk is geen probleem.

4.3.9 Nieuwe afwegingen

Aangezien nodes minder sterke machines zijn en de bandbreedte (relatief) beperkt is op het netwerk is de gekozen optie (OpenVPN) achteraf minder geschikt. Ook een belangrijk voordeel, minder werk voor de vrijwilligers, blijkt minder belangrijk als initieel werd aangenomen.

Een voordeel van de gekozen optie Open VPN is dat het verschillende opties en sterktes heeft met betrekking beveiliging. Als er een werkende opzet is kan eenvoudig het niveau van de beveiliging aangepast worden. Omdat de meeste tunnel opties minder flexibel zijn moet hier in een eerder stadium over na gedacht worden. Er is contact opgenomen met Surfnet om hun eisen qua beveiliging mee te laten nemen in de overweging.

4.3 10 Surfnet

In een gesprek met Surfnet is de keuze tussen tunnels (met name IPsec tunnels) en OpenVPN besproken. Surfnet vond het onwaarschijnlijk dat OpenVPN niet op de hardware van Wireless Leiden kon draaien. Zij vergeleken de hardware met een Linksys Router. Op deze routers is het mogelijk om OpenWRT te draaien. Dit is een open source software systeem dat ter vervanging geldt voor de originele Linksys software. Op dit OpenWRT systeem draait ook OpenVPN en de hardware is vergelijkbaar met de hardware die Wireless Leiden gebruikt. Ook werd geopperd dat OpenVPN waarschijnlijk lichter is dan het alternatief IPsec.

Surfnet heeft geen voorkeur, echter hebben zij wel geopperd dat OpenVPN aan hun eisen voldoet, zij hebben ook andere implementaties van OpenVPN. De mening van Surfnet in dit verhaal is erg belangrijk. Dit omdat zonder hun consensus een implementatie niet mogelijk is. Wel wijzen zij alternatieven niet af.

4.3.11 Testen

Wireless Leiden vrijwilligers en Surfnet medewerkers zijn het niet met elkaar eens. Een test zal moeten uitwijzen welke van de twee gelijk heeft. Omdat OpenVPN en IPsec (die door een aantal vrijwilligers en Surfnet werd aangeraden) verschillende versleutel methode ondersteunen is het vergelijken er van op basis van de huidige testomgeving niet goed mogelijk. Dit doordat verschillende versleutel methode voor verschillende resultaten zorgen. Een vrijwilliger heeft aangeboden om ‘Crypto kaarten’ ter beschikking te stellen. Dit zijn kaarten die de versleutel berekeningen van de processor over neemt. Dit zorgt er voor dat de versleutel methode geen invloed heeft op de performance (CPU load en bandbreedte).

4.3.12 Ondersteuning van FreeBSD

De ondersteuning van deze Crypto kaarten door FreeBSD zou mogelijk moeten zijn met het doorvoeren van een drietal wijzigingen in het kernel configuratiebestand (en deze te hercompileren). Dit is echter niet het geval. Na contact opgenomen te hebben met de vrijwilliger die deze kaarten geleverd heeft blijkt er iets niet goed te zijn in FreeBSD. Zowel de deze vrijwilliger als internet handleidingen bevestigen dat de doorgevoerde wijzigingen voldoende zouden moeten zijn. Op advies van de vrijwilliger is dit probleem voorgelegd aan de ‘FreeBSD hackers mailinglist’.

Resultaten van de mailinglist

- Crypto kaarten hebben geen nut met een enkele tunnel. Deze worden pas nuttig wanneer er meerdere connecties worden gelegd die samenkomen op het systeem dat over de cryptokaart beschikt.

  Mijn analyse:
  Al is het mogelijk om meerdere instanties van de tunnel software te gebruiken en op deze wijze meerdere connecties te simuleren zou dit de test resultaten beïnvloeden. Bij deze opzet zijn er delen van de software die gedeeld worden door alle instanties, en delen die door elke instantie apart worden uitgevoerd. Dit maakt een vergelijkingstest niet representatief.
- Versleuteling wordt niet automatisch door de cryptokaart overgenomen (in tegenstelling tot wat de vrijwilliger vertelde en een aantal handleidingen op internet melden). Dit is een reactie die ik ook verwacht zou hebben door eigen onderzoek. Bij het testen van de cryptokaart door het versleutelen van random gegenereerde data, bleek dat er een groot verschil zat tussen de test waarin de encryptie engine (de cryptokaart) werd opgegeven en de test waarin deze niet expliciet werd opgegeven.

De zelf uitgevoerde test.
Versleutel 10 MB aan random gegenereerde data en versleutel deze met en zonder expliciet op te geven dat de cryptokaart gebruikt moet worden. Voer deze test 3 maal uit en neem hier de gemiddelde van.

Met specificatie	**22 seconde**
Zonder specificatie	**48 seconde**

Deze testen werden bevestigd door de meldingen van de FreeBSD mailinglist.

4.3.13 Vergelijkbare versleuteling

Omdat er een test uitgevoerd moest worden op de optie die de beste keuze is, is er verder onderzoek gedaan naar de verschillende versleutelmethode.

Al is er een verschil in de implementatie van de verschillende versleutelmethode blijkt dat er een drietal versleutelmethode in beide programma's toegepast zijn. Een van deze versleutelmethode wordt gebruikt en er wordt een snelheidstest uitgevoerd met deze methode. Al is deze test van mindere kwaliteit dan de eerder genoemde cryptokaart (die niet bleek te werken) is er geen andere methode om de twee producten met elkaar te vergelijken.

De keuze is gevallen op de versleutelmethode DES. De reden hiervoor is dat deze van de drie opties de lichtste encryptie sleutel heeft. Dit resulteert in minder gebruikte kracht voor de versleuteling wat een betere vergelijking geeft. De opties zijn

Naam	Sleutel (bit)
DES	64
Blowfish (BF)	128
AES	192

Alle testen zijn 3 keer uitgevoerd onder identieke omstandigheden, resultaten zijn gemiddelde.

Duur Applicatie	OpenVPN	IPsec
30 Seconden	0.815 Mb/s	1.51 Mb/s
30 Minuten	0.838 Mb/s	1.52 Mb/s

Het testprogramma vroeg bij alle testen gemiddelde (ongeveer) 50% van de processor kracht. De resultaten zijn daardoor niet vergelijkbaar met resultaten in een echte omgeving. Echter was de gebruikte processor kracht in alle gevallen vergelijkbaar waardoor de test wel representatief is.

IPsec is de beste keuze.

4.3.14 Keuze voor demo

Al is IPsec de beste keuze zal er in de presentatieomgeving gebruik gemaakt worden van OpenVPN. De reden hiervoor is dat een implementatie binnen Wireless Leiden onder de huidige omstandigheden niet mogelijk is. Al is er geen reden om aan te nemen dat IPsec niet geïmplementeerd kan worden, zijn er bij de testopstelling een aantal problemen geconstateerd waardoor een demo niet mogelijk is. Een demo met OpenVPN is wel mogelijk.

4.4 Uitdagingen met meerdere BSS'en

4.4.1 Probleem

Een eis vanuit Surfnet is dat clients met hun laptops kunnen inloggen op het Eduroam netwerk zonder hun laptop te her configureren. Een deel hiervan is dat de SSID "Eduroam" moet zijn in combinatie met WPA. Dit zijn twee punten waar de huidige OMNI's (de accesspoints antennes van de node) niet aan voldoen. Zij hebben een onbeveiligde verbinding in combinatie met een (op elke locatie) andere SSID.

4.4.2 Oplossingen

- Extra NIC's inclusief antenne op de node plaatsen.
- 1 NIC twee SSID's laten broadcasten.

4.4.3 Extra Nic

Dit zou betekenen dat elke node (die Eduroam gaat gebruiken) omgebouwd moet worden.

Er zijn een aantal problemen

- Kosten
  Een NIC en antenne kosten geld. Geld dat ook anders besteed kan worden.
- Activiteiten
  Het ombouwen van de node inclusief software en antenne is erg arbeid intensief.
- Soekris
  Een aantal nodes binnen Wireless Leiden zijn opgebouwd uit Soekrissen. Dit zijn embedded systems. Niet alle Soekrissen hebben ruimte voor een extra Wireless NIC.

4.4.4 Extra SSID

Een extra SSID laten broadcasten is in theorie de beste optie, vooral omdat er geen extra hardware nodig is en alle veranderingen softwarematig zijn, wat de genoemde punten voor een extra NIC te niet doen.

HostAPD

HostAPD heeft volgens zijn handleiding de mogelijkheid om een meerdere SSID's te broadcasten. Dit deel van zijn handleiding blijkt niet te kloppen. De reden hiervoor is dat HostAPD zijn oorsprong heeft in Linuxland en het programma geport is naar FreeBSD. Dit betekend dat de source code zo is aangepast dat deze ook op FreeBSD werkt. Echter is in deze transactie de extra SSID optie niet meegenomen. De handleiding is 1 op 1 overgezet waardoor het pas na Internet zoekwerk blijkt dat dit niet mogelijk is. Op internet staan verschillende handleiding over hoe HostAPD een extra SSID kan hosten. Echter wordt in vrijwel alle gevallen verzwegen dat dit om een Linux installatie gaat.

VAP

VAP staat voor Virtual Access Point. Dit is een techniek om 1 Fysieke Wireless NIC om te bouwen tot 2 (of meer) virtuele Wireless NIC's. Aan 1 VAP wordt de bestaande OMNI gekoppeld, aan de andere VAP het Eduroam netwerk. Dit is een techniek die in Linuxland al enige tijd bestaat. Ook zijn er een aantal internetpagina's die beschrijven dat dit ook met FreeBSD mogelijk is. Echter is dit niet het geval. FreeBSD heeft deze optie (nog) niet. De reden waarom dit nog niet zou werken is dat het een kleine doelgroep is die deze techniek gaat gebruiken. Het heeft daarom geen prioriteit om deze optie te realiseren.

4.4.5 Linux

De HostAPD versie van Linux zou de gewenste optie hebben. Daarom is een Linux testomgeving opgezet. Linux op de Soekris installeren bleek een probleem. De methode die gebruikt wordt om een besturingsysteem op de Soekris te plaatsen is de FlashCard aan een PC te hangen en hier een installatie op te plaatsen. Vervolgens worden er verschillende parameters veranderd zodat de installatie ook werkt op een computer zonder videokaart maar met een Serial (RS-232) aansluiting. Er zijn 6 verschillende distributies geprobeerd en elk vertoont 1 van twee problemen.

Namelijk

- De minimale installatie is te groot voor de 512MB Compact FlashCard.
- Nadat alle instellingen zijn ingesteld en de installatie begint, bevriest de installatie.

Omdat er iets mis gaat met een installatie direct op de FlashCard en het doel is om een Linux installatie op de FlashCard te plaatsen wordt er een andere aanpak gekozen. Namelijk een kant en klare installaties voor Embedded Systemen. Deze zijn qua standaard geïnstalleerde software minder vrij op keuze maar dit is achteraf installeerbaar. De eerst werkende versie is "Voyage Linux" deze moest vanaf een Linux systeem geïnstalleerd worden. Een probleem omdat er geen ongebruikt systeem beschikbaar is waarop Linux geïnstalleerd kan worden. Er wordt gekozen om een Linux LiveCD te gebruiken. Deze heeft als voordeel dat het op een systeem gebruikt kan worden dat volledig is geïnstalleerd met een ander besturingsysteem. Nadeel is wel dat na een (systeem) herstart, alle informatie die niet op de FlashCard geschreven is, verloren gaat. Dit heeft er voor gezorgd dat er na een aantal testen ook een aantal keer alle software gedownload moest worden. Het is ook mogelijk om de software naar de harde schijf te downloaden, echter is er bij een eerder project op deze manier de inhoud van een harde schijf verloren, wat het geen ideale optie maakt.

Headers

Linux bevindt zich nu op de Soekris. HostAPD is niet standaard aanwezig. De installatie wordt uitgevoerd volgens de handleiding. De volgende stap is om HostAPD te laten werken met 1 SSID (als test). Dit blijkt niet te werken. HostAPD ondersteund verschillende drivers. Echter is geen van deze drivers standaard aanwezig in de gekozen distributie. Een installatie (is na verschillende pogingen) niet mogelijk gebleken. Dit omdat voor de installatie de Linux kernel headers nodig zijn. Deze kunnen geïnstalleerd worden. Echter is er dan geen ruimte meer over voor de (tijdelijke bestanden) van de driver installatie.

4.4.6 Externe hulp

Terwijl er een poging gedaan werd om de Linux installatie werkend te krijgen is er contact opgenomen met een docent van de Hogeschool (Peter van Vliet). Deze heeft kennis van de programmeertaal C (de taal waarin HostAPD geschreven is). Deze vertelde dat het omzetten (porten) van het programma niet zo gemakkelijk was als het verzoek in de mail deed overkomen. Er zijn grote verschillende in de manier waarop een programma onder Linux geprogrammeerd moet worden en op FreeBSD (verschillen in API's). Omdat er een alternatieve manier is gevonden om Multi SSID op FreeBSD werkend te krijgen is de hulp van deze docent afgezegd.

4.4.7 VAP's onder FreeBSD

Er werd elke week tijd besteed om nieuwe manieren te vinden waardoor de extra SSID mogelijk wordt op FreeBSD. Op 16 april 2008 werd een post gevonden (van 13 april 2008) waarin werd verteld dat de VAP optie is toegevoegd aan FreeBSD, het gaat hier om een FreeBSD 8.0-Current. Dit is een versie van FreeBSD die zich nog in de Beta fase bevindt. Echter is deze versie te downloaden voor testen. Na een aantal vragen gesteld te hebben over de installatie via een Wireless Leiden mailinglist, bood een vrijwilliger zich aan om dit proces uit te leggen in een weekend. Deze vrijwilliger heeft het proces persoonlijk uitgelegd in het volgende weekend. Na een drietal dagen is het gelukt om op FreeBSD 8.0-Current een VAP te hosten.

4.4.8 Snelheid

Volgens de theorie van Multiple SSID is het goed mogelijk dat de snelheid van Multiple SSID achteruit gaat. Om een vergelijking te maken moet er een baseline gesteld worden. Deze baseline zou de maximale snelheid zijn van een enkele SSID (direct op de fysieke NIC). Echter blijkt dat in de versie waarin VAP mogelijk werd de directe toekenning een probleem op te leveren. Bij het toekennen van de instellingen veranderen foutmeldingen van dag tot dag. Dit geeft aan dat er aan gewerkt wordt. Het is nu gebleken dat de FreeBSD community een Multiple SSID mogelijk wenst. Er dienen verdere testen uitgevoerd te worden op het moment dat de Current versie van FreeBSD 8.0 en met name de VAP's in een verdere staat van ontwikkeling is.

4.5 Uitdagingen bij het testen van Tunnels

4.5.1 Probleem

Het is nu zeker dat er tunnels gebruikt gaan worden om het verkeer te beveiligen en onderscheid te gaan maken tussen de verschillende netwerken (Eduroam / Wireless Leiden verkeer). Het is nog niet duidelijk wat de eisen zijn van Surfnet aan de beveiliging van het verkeer. Er zijn al een aantal eisen aan de tunnels gesteld bij voorgaande uitdagingen.

4.5.2 Onbeveiligde tunnel

Omdat een groot deel van de te volgen stappen er van uit gaan dat er een tunnel ligt is er voor gekozen om een onbeveiligde tunnel te gaan gebruiken om testen te draaien. Er is gekozen voor een GIF tunnel. Dit is een tunnel die standaard aanwezig is in FreeBSD en is een “No Nonsance” oplossing, het is een tunnel en niets meer. Dit is dan ook de reden waarom er voor een GIF tunnel gekozen is. Als er een oplossing gekozen wordt die een extra functie/techniek heeft ingebouwd, bestaat de kans dat de tunnel werkt door deze extra mogelijkheden. Als er in dat scenario een andere oplossing gekozen wordt die deze functionaliteit niet heeft dan werkt de rest van de opstelling niet. Als er meer eisen bekend zijn, kan de GIF tunnel worden vervangen door een betere optie.

Omdat de GIF tunnel standaard in FreeBSD aanwezig is was het relatief eenvoudig om de GIF tunnel in werking te stellen.

4.5.3 Bridge

In de aanloop naar de huidige opzet is de term bridge regelmatig tegen gekomen in combinatie van een Access Point en FreeBSD. Dit was tot op dit punt niet relevant en de implementatie van de Bridge in FreeBSD was nog redelijk vaag. Echter wat een bridge is in netwerk termen (een Layer 2 repeater) was wel duidelijk. De beredenering was dat als zo’n bridge als repeater op kan treden tussen een Wireless Interface en een GIF dan zou al het verkeer dat via de Eduroam SSID verstuurd wordt, over de tunnel door gezonden kunnen worden naar de centrale gateway. Dit zou perfect zijn omdat dan al het verkeer van de Eduroam SSID naar 1 punt op het netwerk gestuurd kan worden, waar het dan gerouteerd kan worden naar het netwerk van de Eduroam instelling.

4.5.4 Broadcasts

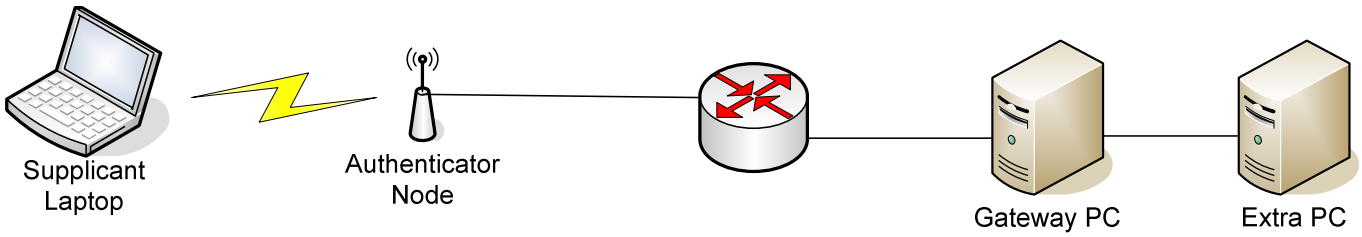
Na het opzetten van de tunnel en de bridge reageert de interface op de andere kant van de tunnel niet. Om het probleem te analyseren worden er TCP dumps gemaakt van de draadloze netwerkkaart en de beide uiteinden van de tunnel.

De draadloze netwerk kaart geeft weer dat er een ARP request worden verstuurd. De bridge geeft onleesbaar verkeer weer. Een ARP request is een broadcast. Zoals eerder besproken, was een van de voordelen van een tunnel dat het geen Broadcasts doorlaat. Echter omdat al het verkeer van de draadloze netwerkkaart doorgezet wordt, vallen hier ook de ARP requests onder. Een TCP/IP verbinding werkt niet zonder het ARP protocol (een ARP request staat voor Address Resolution Protocol en zet een IP adres om in een MAC adres). Er werd vanuit gegaan dat het probleem hier lag.

4.5.5 Ether IP

Na onderzoek gedaan te hebben naar de combinatie van een GIF en een Bridge blijkt dat FreeBSD deze opzet detecteert en het verkeer dat van een bridge een GIF opgestuurd wordt omgezet wordt in EtherIP verkeer. Dit Ether ip is een extensie van een tunnel. Het encapsuleert al het verkeer (dus ook broadcasts) in een EtherIP pakket en verstuurd dit over de tunnel. Dit werd bevestigd door het feit dat een TCPdump aan de andere kant van de tunnel ook onleesbaar verkeer weer gaf zodra er verkeer over de draadloze netwerk kaart gestuurd werd, het voor TCP dump onleesbare verkeer is EtherIP verkeer. De oplossing is (als test) het verkeer van de tunnel over een bridge te sturen naar een tweede netwerk kaart, het verkeer zou dan van EtherIP verkeer terug gezet moeten worden naar regulier verkeer. Deze netwerkkaart werd aangesloten op een extra computer, deze computer zit in hetzelfde IP netwerk als de laptop.

De opstelling is als volgt:



Er is op dit moment een directe verbinding tussen de laptop en de extra geplaatste computer (“Extra PC” in het plaatje). Met een TraceRoute (of Tracert) commando is er sprake van 1 hop tussen de laptop en de extra pc. De tussen liggende systemen zijn op IP niveau niet zichtbaar.

4.5.6 Tunnel uiteinde

Een aanvullend probleem is dat de uiteinden van de tunnel ook bereikbaar moet zijn buiten (en via) de tunnel. Op de authenticator draait een programma dat door de tunnel een Radius verzoek moet sturen. Standaard is dit niet mogelijk omdat een bridge het verkeer volledig afsluit voor ander verkeer.

Na op internet gezocht te hebben werd er een patch gevonden die dit mogelijk moet maken. Dit bleek pas te werken na het programma afgeschreven te hebben als werkzaam. Er bestaan verschillende handleidingen op internet over de werking er van. Echter is de officiële documentatie alleen beschikbaar in de Russische taal. Na niet opgeven en bij toeval een (andere) handleiding gevonden te hebben over deze patch (Engels) bleek deze optie wel te werken. In de test opzet, kan de Laptop verbinding maken met de Node en de Gateway PC (de twee uiteinden van de tunnel die gebridged zijn). Ook kan vanaf de Node de Gateway gepingt worden via de tunnel.

Omdat het nu mogelijk is om van zowel de Laptop als de Node de Gateway PC te pingen via de tunnel vond een beredenering plaats. In het testen met de patch wordt de extra pc niet gebruikt maar toch is deze Gateway bereikbaar via de tunnel. Wat zou er gebeuren als op de Gateway een bridge wordt geïmplementeerd met een enkele aansluiting (zijnde de Tunnel dus zonder de NIC welke gekoppeld is aan de extra pc). Dit bleek een valide beredenering, ook nu is de Gateway bereikbaar via de tunnel.

Vervolgens komt de vuurproef. Plaats op de Gateway PC een RadiusServer, op de node een authenticator (een 802.1x omgeving). Kan de laptop dan geauthenticeerd worden via de tunnel en vervolgens in 1 hop bereikbaar te zijn tot de Gateway PC. Dit blijkt mogelijk te zijn.

4.6 Uitdagingen bij Usertracking

4.6.1 Probleem

Een reden waarom Eduroam instellingen terughoudend zijn met het geven van medewerking en het beschikbaar stellen van hun internet verbinding, is de opinie dat Surfnet hun internet verbinding zou blokkeren bij misbruik. Surfnet noemde als oplossing het gebruik van een aparte IP range voor Wireless Leiden. Deze IP range kan door de Eduroam instelling aangevraagd worden zonder kosten. Mocht er misbruik plaatsvinden via het Wireless Leiden netwerk dan is dit direct te traceren op basis van het gebruikte IP adres. Echter zou dit als gevolg hebben dat Wireless Leiden afgesloten wordt van Surfnet internet (in plaats van de Eduroam instelling). Wireless Leiden zou in DHCP en Radius logs kunnen kijken om te controleren welke gebruiker verantwoordelijk is voor de overtreding. Dit is echter veel werk en een eenvoudigere oplossing zou wenselijk zijn.

4.6.2 Surfnet

In een gesprek met Surfnet is dit scenario besproken. Surfnet heeft een programma genaamd “Usertracking” ontwikkeld. Dit programma is in staat IP adressen, MAC adressen en gebruikersnamen (van Eduroam gebruikers) te koppelen en deze in een database op te slaan. Dit maakt het koppelen van een IP adres bij misbruik met zijn gebruikersnaam een stuk eenvoudiger. Voor zover bekend zijn er geen andere programma’s die over dezelfde functionaliteit beschikken.

4.6.3 Werking

Usertracking houd zijn gegevens bij door verschillende log file te controleren en deze gegevens in een (MySQL) database te plaatsen. Onder andere worden de ARP logs, de DHCP logs en de Radius logs gecontroleerd.

4.6.4 Linux

Usertracking is ontworpen voor Linux (documentatie noemt Debian). De gateway pc maakt gebruik van FreeBSD. Dit omdat alle server en nodes binnen Wireless Leiden gebruik maken van FreeBSD. FreeBSD heeft de mogelijkheid om Linux applicaties te draaien. Echter maakt Usertracking gebruik van een aantal Linux specifieke directory paden. Deze bestaan niet in FreeBSD.

4.6.5 Perl

Alle scripts (niet zijnde voor de website) zijn Perl scripts. Al heeft de student geen voorgaande ervaring met deze taal, is het installatie script ingezien. In dit script zijn de kopieer opdrachten naar Linux padden geïsoleerd. Deze padden zijn aangemaakt op het bestandssysteem. Doordat deze padden op dit moment bestaan worden de bestanden zonder problemen gekopieerd. Echter zijn deze bestanden naar directories gekopieerd die als doel hebben om bij het opstarten van het systeem, opgestart te worden. Vandaar dat deze bestanden na installatie verplaatst worden naar de directories die door FreeBSD gebruikt worden om (automatisch) op te starten.

4.6.6 Radiator

De website die als interface functioneert werkt echter geeft deze op de plaats waar de tekst “RadiusServer” verwacht zou worden de tekst “Radiator.” Radiator is een RadiusServer, die tijdens de IMSM minor werd aangeraden door de IT dienst van de Hogeschool Leiden. Dit was en is geen opties omdat er geen gratis of Open Source licentie voor verkrijgbaar is (op een 30 dagen probeerversie na).

Na de installatie van Usertracking geeft het opstarten van de verschillende onderdelen een aantal foutmeldingen.

4.6.7 Incompatible

Omdat de webinterface de tekst radiator weergeeft en bij het opstarten verschillende foutmeldingen gegeven worden, wordt eerst onderzocht of Usertracking wel compatible is met FreeRADIUS.

Dit blijkt niet het geval te zijn.

4.6.8 Waarom

Na het doorzoeken van verschillende bestanden (vooral perl en cshell scripts) blijkt een aantal keer het path “/etc/radiator” gebruikt te worden. Usertracking heeft als eis dat zijn dependencies op standaard locaties geïnstalleerd staan, het heeft geen configuratiebestand dat het path specificeert. Dit maakte het traceren van de paden een uitdaging. “/etc/radiator” is de standaard installatie directory van Radiator. Dit zou betekenen dat Usertracking afhankelijk is van Radiator. Dit wordt mede bevestigd door de methode waarop Usertracking zijn gegevens ophaalt. Het doorzoeken van log bestanden. Elke programma gebruikt zijn eigen syntax. Waardoor Usertracking alleen samen kan werken met de programma’s waar het specifiek voor geschreven is.

Om dit te controleren wordt op internet opgezocht of de beredenering klopt over de incompatibiliteit met andere RadiusServer dan Radiator met Usertracking. Er zijn geen website gevonden die hard vasttellen dat het niet mogelijk is om Usertracking met FreeRADIUS samen te laten werken (of andere RadiusServers). Echter wordt wel een link gelegd tussen Radiator en Usertracking. Teksten als “Usertracking works closely together with radiator” geven wel weer dat Usertracking ontworpen is om te functioneren met Radiator.

5. Eduroam kan (niet)

5.1 Techniek / beheer

5.1.1 Software

Er is (open source) software in overvloed om aan alle technische eisen te voldoen. De software is geen probleem. Dit is te zien in het kopje software. Elk onderdeel kan volledig worden beveiligd tegen kwaadwillende gebruikers van het netwerk.

5.1.2 Belangen

Het probleem bevindt zich in de verschillende partijen en hun belangen / eisen.
Namelijk

- Gebruiker
  Dit is de student of medewerker die is aangesloten bij een opleiding instantie welke is aangesloten bij het Eduroam. Het is geen probleem om kwaadwillende in deze groep het moeilijk te maken en later te identificeren.
- Eduroam instelling
  Deze hebben de vrees dat hun internet verbinding misbruikt wordt via het Wireless Leiden netwerk. Mocht dit het geval zijn dan zijn er technieken mogelijk om te identificeren dat het Wireless Leiden netwerk hiervoor verantwoordelijk is. Deze partij loopt in principe geen risico.

- Surfnet
  Surfnet heeft als eis gesteld dat het onder geen geding mogelijk mag zijn om als niet geauthenticeerde gebruiker gebruik te maken van Surfnet internet. Ook hebben zij als eis gesteld dat een gebruiker geen verschil mag merken of hij zich op zijn onderwijsinstelling bevind of dat hij gebruik maakt van Eduroam via Wireless Leiden.
- Wireless Leiden vrijwilligers
  De nodes van Wireless Leiden zijn in het beheer van de vrijwilligers, deze zijn aangesloten bij de stichting. Al is het niet het geval is het theoretisch mogelijk dat alle vrijwilligers aan de root wachtwoorden kunnen komen.

5.1.3 Conflicterende belangen

Surfnet heeft aangegeven dat een gebruiker geen verschil mag merken bij het gebruik van Eduroam via Wireless Leiden en met zijn internet verbinding op school. Dit betekend dat er op de client geen extra software geïnstalleerd mag worden. Het enige wat deze nodig heeft is een 802.1x client in combinatie met een WPA kaart (voor de WPA encryptie die gebruikt wordt bij Eduroam netwerken).

802.1x heeft als doel om op basis van authenticatie gegevens een computer toegang te verschaven tot het netwerk of juist niet. Dit gebeurd op de node. Het verkeer is beveiligd tussen de laptop en de node, echter als het verkeer op de node aankomt zijn er andere technieken nodig om het verkeer naar de Eduroam instelling te sturen en dit te versleutelen (tegen het plaatsten van een listener). Het enige punt

op het netwerk waar dit mogelijk is, is de node. Deze node kan technisch gezien aan alle eisen voldoen echter blijft de factor vrijwilliger over.
Iedereen kan lid worden van Wireless Leiden als vrijwilliger. Elke vrijwilliger heeft in theorie toegang tot het root wachtwoord. Niet elke vrijwilliger heeft dit wachtwoord echter blijkt het in de praktijk geen probleem te zijn om dit via een andere vrijwilliger te achterhalen.

5.1.4 Wachtwoorden achterhalen

De student is achter het wachtwoord gekomen door een scenario te noemen waarin dit handig is om te weten. De student moest vanaf buiten Wireless Leiden toegang hebben tot het Wireless Leiden netwerk en een vrijwilliger noemde de mogelijkheid om via de Proxy servers in te loggen op het netwerk. Zonder verder doorvragen werd het root wachtwoord gegeven.

Een andere vrijwilliger noemde het scenario waarin een node defect is. Als een vrijwilliger bereid is hier tijd in te steken dan is het voor hem nodig om root toegang te hebben (en zo niet is het in ieder geval ‘handig’). Deze vrijwilliger vertelde “Het is belangrijker dat de node terug in de lucht is, dan de veiligheid van het root wachtwoord”.

Met root toegang tot de verschillende nodes is het mogelijk om op afstand (via SSH) toegang te krijgen en deze node zo te modificeren dat de kwaadwillende en/of ieder ander via deze node toegang heeft tot het Eduroam netwerk.

5.1.5 Fysiek

Naast de bescherming tegen vrijwilligers is er de factor fysieke benadering. De nodes staan verspreid door de stad. Zij staan op plekken waar de pandbeheerder heeft aangegeven mee te willen werken aan Wireless Leiden. Wireless Leiden zet (na een proces) hier een node neer. Deze node kan fysiek aangevallen worden. Als een persoon fysieke toegang heeft tot het systeem is geen beveiligingsmaatregel veilig genoeg. Elke besturingssysteem heeft zwakheden op het gebied van fysieke toegang. In FreeBSD, het gebruikte besturingssysteem kan de node herstart worden (zonder wachtwoorden kan er een koude herstart uitgevoerd worden). Op dit moment kan er gewisseld worden naar ‘single user mode’ Dit is een onderdeel van het systeem waar geen wachtwoord nodig is maar wel wachtwoord gegevens gewijzigd kan worden. Het root wachtwoord kan dan naar eigen keuze ingesteld worden waarna het systeem volledig toegankelijk is na een herstart. Ook is het mogelijk om een FlashCard te verwijderen, deze te kopiëren, terug te plaatsen, de kopie te wijzigen, de FlashCard uit de machine halen de image op de FlashCard te plaatsen en zo een gewijzigde versie te installeren.

Een Eduroam verbinding zou een drieluik overeenkomst zijn tussen Surfnet, Wireless Leiden en de Eduroam instelling. De gebruikers van de fysiek locatie hebben geen verplichtingen om de belangen van deze drie partijen te behartigen. Er is contractueel niks vastgelegd om dit te voorkomen. Het contract tussen Wireless Leiden en de locatie is van toepassing tussen het de beheerder en niet per definitie met alle gebruikers van het pand.

Er is een vervolgopdracht gespecificeerd welke het gevaar van de fysieke toegang tot de node verkleind. Zie paragraag vervolgopdrachten.

5.2. Oplossingen

Er zijn een aantal oplossingen mogelijk om dit probleem ten delen op te lossen. Echter is het niet mogelijk om het probleem volledig op te lossen.

5.2.1 Extra node

In de huidige infrastructuur is het niet mogelijk om de node te beveiligen. Echter met een extra node op locatie is het mogelijk om alleen een beperkte (vertrouwd) groepje toegang te verschaffen tot deze node. In dit scenario is de veiligheidsfactor vrijwilliger geen probleem. Niet elke vrijwilliger heeft toegang nodig tot deze extra node. Deze zou dan als client op de bestaande node ingelogd zijn. Dit betekend dat er geen extra interlinks nodig zijn. Alleen kabel naar de bestaande node + een antenne (OMNI) is effectief.

5.2.2 Beleid

Een verandering in de mentaliteit van de vrijwilligers zou nieuwe mogelijkheden openen. Als de toegangsgegevens worden veranderd, niet elke vrijwilliger toegang heeft tot deze gegevens en dat dit beleid ook naar buiten toe bewezen kan worden dan zou de veiligheidsfactor vrijwilliger geminimaliseerd worden. Het bewijs naar buiten zou erg belangrijk zijn omdat deze verandering een groot cultuur verschil te wegen zal brengen. De open cultuur is zo ingebakken in Wireless Leiden dat het erg moeilijk zal zijn dit door te voeren, bewijskracht is dus nodig. Mensen zijn gewoonte dieren en zonder harde autoriteit (deze is er niet in Wireless Leiden) zal niet iedereen zich gedwongen voelen het nieuwe beleid te honoreren. Geheim houding zal ten slotte in gaan tegen het open karakter van Wireless Leiden. De controle op dit beleid zou dicht bij onmogelijk zijn. Vrijwilligers spreken elkaar ook buiten officiële kanalen (Skype / Mailinglijsten) om.

Wat moet er veranderen

- Eduroam nodes krijgen nieuwe wachtwoorden
- Beperken van het aantal mensen dat over dit wachtwoord beschikt
- Vrijwilligers die over het wachtwoord beschikken hebben een geheimhouding plicht.
- Dit beleid moet naar buiten bewezen worden (Surfnet / Eduroam instelling)

5.2.3 Client software

Om alle genoemde veiligheidsrisico's van Wireless Leiden op te lossen is er een authenticatie methode nodig waarin Wireless Leiden als netwerk wordt gebruikt maar er op de infrastructuur (die in het beheer is van Wireless Leiden) geen authenticatiepunten aanwezig zijn. Iedereen kan gebruik maken van het netwerk. Er moet een punt zijn voor de koppeling met Eduroam. Dit kan totaal buiten het beheer van Wireless Leiden om. Iedereen kan een koppeling opzetten op het netwerk (al dan wel draadloos). Ook kunnen clients zonder verdere problemen connectie zoeken naar het netwerk. Op dit moment is er geen veiligheid of connectie van de client naar Eduroam. Dit kan oplost worden door een VPN oplossing. Wireless Leiden stelt zijn netwerk aan een ieder beschikbaar en is in dit verhaal (qua eisen) dan ook geen factor. Echter heeft Surfnet als eis gesteld dat er niets extra's op clients geïnstalleerd mag worden. Dit is bij een VPN oplossing in dit ontwerp wel nodig. Dit maakt deze optie binnen de huidige eisen onmogelijk. Een apart initiatief van de Hogeschool (deze gebruikt VPN) zou wel een optie zijn. Het zou zelfs mogelijk zijn om een VPN aan Eduroam te koppelen,als de eisen dit toe zouden laten.

5.3 Of toch wel

In de gesprekken met Surfnet heeft Surfnet aangegeven open te staan over de mogelijkheid om Wireless Leiden tot Eduroam toe te laten. In deze communicatie met Surfnet zijn een aantal eisen gesteld. In de eindpresentatie bij Wireless Leiden kwam naar voren dat de theoretische eisen van Surfnet in de praktijk waarschijnlijk minder streng zijn. De toon van de eindpresentatie was: 802.1x bij Wireless Leiden kan, Eduroam bij Wireless Leiden kan niet.

Met de toon van de presentatie waren de vrijwilligers het niet eens. Met name Rudi van Drunen en Huub Schuurmans hadden een aantal tegen argumenten.

5.3.1 Ex-student

Het voorbeeld werd genoemd dat studenten na het afsluiten van de opleiding vaak een half jaar lang nog toegang tot het schoolnetwerk hebben. Dit zou volgens de gestelde eisen niet mogelijk moeten zijn. In de praktijk gebeurt dit wel, zonder verdere consequenties. Op het moment dat er toegang is tot het netwerk, is er toegang tot internet voor de student, wat tegen de eisen van Surfnet is.

5.3.2 Service accounts

De identificatie van de gebruiker is op dit moment nog mogelijk. De school heeft personalia van de student, dus bij misbruik van het Surfnet internet is het nog mogelijk om dit te traceren naar een student om verdere stappen te nemen. Echter is een vrijwilliger van Wireless Leiden eerder onder contract geweest van Surfnet. Deze vrijwilliger vertelde dat zijn account op een universiteit, deze was nodig voor de opdracht, nog steeds geldig is, terwijl de opdracht drie jaar geleden plaats vond. Ook heeft de vrijwilliger toegang tot twee service account die gekoppeld zijn aan een groep en dus niet terug te traceren zijn naar een enkele gebruiker. Dit beleid gaat in tegen de eisen die Surfnet gesteld heeft aan Wireless Leiden.

5.3.3 Vervolgopdrachten

Er zijn een aantal vervolg opdrachten gespecificeerd. Als deze opgevolgd worden staat Wireless Leiden een stuk steviger in de schoenen. Er blijven een aantal beveiligingsproblemen, echter bestaan deze in de praktijk ook in het Surfnet netwerk. De vraag is dan ook: hoe erg vindt Surfnet het. Er moet tenslotte moeite gedaan worden om toegang te krijgen tot het Surfnet netwerk (vooral voor een niet vrijwilliger). Geen systeem is waterdicht en de genoemde techniek: social engineering, is op alle punten van het Surfnet netwerk een zwak punt, want het wordt tenslotte beheerd door mensen.

De vervolg opdrachten staan op Wireless Leiden SVN (link: zie paragraaf “online documentatie”).

5.3.4 Status

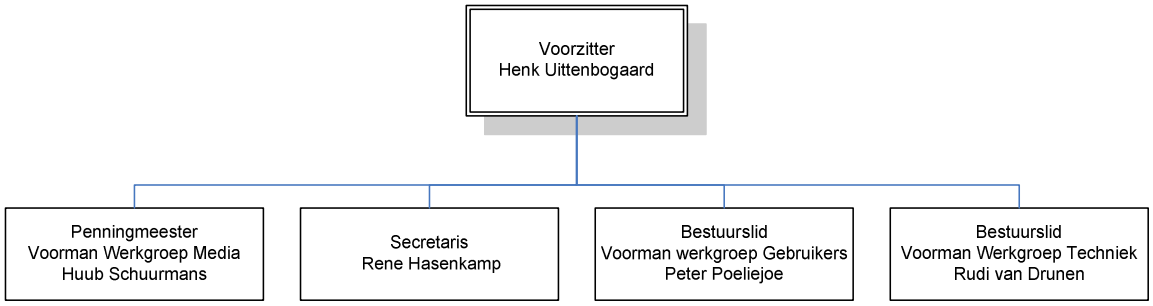
Om duidelijkheid te verschaffen in het verschil in eisen (praktijk en gesteld) is er contact opgenomen met Surfnet. Op het moment van inleveren van dit verslag is de enige reactie vanuit Surfnet geweest, de mail die melde dat zij een antwoord aan het formuleren zijn. Het verzoek voor verduidelijking is twee weken voor einddatum van dit verslag verstuurd.

6. Organisatie

6.1 De stichting

Wireless Leiden is een stichting die officieel bestuurd wordt door een raad, deze raad bestaat uit minimaal drie en maximaal zeven leden, op het moment bestaat de raad uit vijf leden. Ook als de raad uit minder leden bestaat zal deze blijven functioneren als bestuursorgaan van Wireless Leiden. Een bestuursraad wordt benoemd voor een maximale periode van drie jaar.

De huidige structuur:



Er is gekozen voor een stichting door de mogelijkheid van het nemen van snelle beslissingen. Een genoemd alternatief is een samenwerking met de leden. Dit brengt bij het nemen van beslissing in de praktijk problemen met zich mee.

6.1.1 Oprichting

Wireless Leiden is opgestart in 2002. In 2002 stond draadloze technologie nog relatief in de kinderschoenen. Voor het initiatief waren veel vrijwilligers te vinden en media aandacht was geen probleem. Door de medewerking van de vele vrijwilligers op verschillende vakgebieden heeft Wireless Leiden zich kunnen ontwikkelen tot de volwassenheid waar het nu is. In tegenstelling tot vergelijkbare initiatieven in andere steden die in veel gevallen snel weer verdwenen. Dit is vooral te wijten aan het puur richten op het bouwen van een draadloos netwerk (in tegenstelling tot het ook richten op andere functies). Wireless Leiden heeft vrijwilligers op allerlei gebieden. Op de website van Wireless Leiden staat ook de volgende tekst:

“Ook wie mee zou willen helpen als vrijwilliger (*technisch of niet-technisch*) is van harte welkom!”

6.1.2 Besluitvorming

De bestuursraad maakt besluiten met het houden van stemmingen. Elk persoon in dit orgaan heeft 1 stem. De keuzes worden gemaakt door de meerderheid. In het geval van stemming over zaken en de stemming heeft geen meerderheid in stemmen opgeleverd dan wordt het voorstel als verworpen beschouwd. In het geval van een stemming gaande over personen dan wordt er bij een gelijke meerderheid in stemmen een herstemming gehouden met de personen die de hoogste en een na hoogste keuze hebben gemaakt.

6.1.3 Adviesraad

Wireless Leiden werkt met een adviesraad. Leden van deze raad dienen natuurlijke personen te zijn (dus geen rechtspersonen). Leden van deze adviesraad dienen actieve vrijwilligers te zijn van Wireless Leiden. De bestuursraad beslist welke vrijwilligers er toegelaten worden tot de adviesraad.

6.1.4 Power to the people

Omdat Wireless Leiden een stichting is, is het gebonden aan bepaalde reglementen. Zo is officieel het bestuur de besluitnemer. Echter licht onofficieel de besluitvorming bij de actieve vrijwilligers. Als een actieve vrijwilliger initiatief neemt en hij of zij heeft hier draadvlak voor onder de andere vrijwilligers dan zal in de praktijk het bestuursorgaan hier niet op tegen zijn.

6.1.5 (niet) actieve vrijwilligers

Op de website van Wireless Leiden is een overzicht van de vrijwilligers die zijn verbonden aan de stichting. Dit zijn er op het moment tachtig (80). Onder deze vrijwilligers is er een verschil in actieve en minder actie deelnemers. In principe kan iedereen lid worden als vrijwilliger, er zijn geen eisen over het niveau van participatie.

6.1.6 Kosten

Een grote kostenpost voor veel organisaties zijn de werknemers. De vrijwilligers zijn zoals de naam aangeeft vrijwillig gekoppeld aan Wireless Leiden, dit houdt dus in dat deze kostenpost niet bestaat. De hardware die nodig is om het netwerk uit te breiden wordt gesponsord. Als een bedrijf bereid is om een node te financieren dan wordt deze node naar dit bedrijf vernoemd. Op deze manier wordt er reclame gemaakt terwijl Wireless Leiden een extra toegangspunt heeft (node). Een win-win situatie voor beide partijen.

Op dit moment is Wireless Leiden in het bezit van een extra node. Veel bedrijven maken de keuze om apparatuur in termijnen af te schrijven. Wireless Leiden probeert het kapitaal zo laag mogelijk te houden en schrijft de node (en de kosten er van) direct af.

Wireless Leiden heeft geen maandelijkse kosten, zo wordt het internet gesponsord door een internet provider en stelt de gemeente een pand kostloos ter beschikking. Dit heeft als gevolg dat er geen maandelijkse inkomsten nodig zijn. Indien er geen inkomsten zijn betekend dit geen groei, dit brengt geen gevaar voor de continuïteit van Wireless Leiden.

6.1.7 Open

Wireless Leiden stelt al zijn bevindingen en software (altijd open source) te allen tijde kosteloos ter beschikking tot andere initiatieven. Mochten er andere steden zijn die een vergelijkbaar initiatief nemen dan is het mogelijk om dit 1 op 1 te kopiëren. In de gevallen waar dit gebeurd is de organisatie vaak de grootste uitdaging. Op dit punt lopen de meeste organisaties stuk, Wireless Leiden is op dit punt juist erg succesvol geweest.

6.2 Personen

De volgende vrijwilligers zijn betrokken geweest bij de opdracht, of hebben informatie geleverd die nodig was om de opdracht op dit punt te brengen.

6.2.1 Huur Schuurmans

Functie : Oprichter / Penningmeester
Relevantie : Begeleider

Huub Schuurmans is de persoon die weet welke persoon binnen Wireless Leiden welke kennis bezit, ook heeft hij de contacten buiten Wireless Leiden beschikbaar gesteld voor informatie. Op advies van Huub Schuurmans (maar na actie van Student) zijn er gesprekken geweest met de Universiteit Leiden, Gandallf en twee vertegenwoordigers van Surfnet (plus een herhaalgesprek met 1 van hen).

Verantwoording

In de eerste instantie werd de voortgang ook aan Huub Schuurmans verantwoord. Echter is dit in de loop van de stage verschoven naar de Techniek mailinglijst (waar Huub Schuurmans ook lid van is). Dit is een mailinglijst die gebruik wordt binnen Wireless Leiden om aan de techniek gerelateerde onderwerpen te bespreken. Dit is nuttig gebleken nadat er keuzes gemaakt waren die achteraf bijgesteld werden op advies van leden van de Techniek mailinglijst.

6.2.2 Rick van der Zwet

Functie : Vrijwilliger
Relevantie : Technische kennis

Tijdens een avond is de student uitgenodigd bij Huub Schuurman op een Hack avond. Dit is een ‘evenement’ waarin een aantal vrijwilligers samenkomen om (vooral) technische problemen op te lossen. Rick van der Zwet heeft mij op deze avond geassisteerd bij het opzetten van de 802.1x basis node. Op dit moment werkte reeds de RadiusServer en de Supplicant echter gaf de Authenticator (node) nog een aantal problemen. Mede dankzij het in bezit hebben van een alternatieve supplicant (de standaard MAC OS X supplicant) is deze opzet gerealiseerd. Rick van de Zwet heeft extra kennis verschaft en overgebracht over het gebruik van FreeBSD.

6.2.3 Roland van der Laar

Functie : Vrijwilliger
Relevantie : Technische kennis / Woont in Utrecht

Nadat het bekend was gemaakt vanuit het FreeBSD platform dat de nieuwste versie van FreeBSD (8.0-Current) een VAP optie heeft, zijn er vanuit de student uit een aantal vragen gesteld op de Techniek mailinglijst over de toepassing er van. Ook Roland van der Laar is hier lid van en stelde voor de initiële set-up vereist voor de VAP toe te lichten. Na uitgelegd te hebben hoe deze set-up werkte, werkte de node initieel nog niet. Er was een fout gemaakt door de student waardoor het proces verkeerd verliep. Na

dit onderzocht te hebben was de kennis uitgelegd door Roland van der Laar van essentieel belang om de verder uitwerking van Multiple SSID's in een FreeBSD te realiseren

6.2.4. Ed Kikkert

Functie : Vrijwilliger / Collega werk
Relevantie : GRE tunnels / Extra Soekris

GRE Tunnels

Door Huub Schuurmans is verteld dat er eerder met tunnels is gewerkt binnen Wireless Leiden. Dit was nodig voor een eerder project (HCC-NET). Voor deze tunnel zijn GRE tunnels als optie gesteld. Om niet nogmaals hetzelfde werk te doen is geadviseerd om informatie hier over aan Ed Kikkert te vragen. Deze heeft dit verschaft en daardoor (waarschijnlijk) aanzienlijk werk bespaart.

Extra Soekris

Ed Kikkert is vrijwillig bij Wireless Leiden en ook collega op mijn bijbaan. Deze combinatie is gebruikt om hardware te lenen van men werkgever. Er was een extra FreeBSD machine nodig en bij voorkeur portable. Er was een Soekris over bij mijn werkgever (bijbaan) en deze is gebruikt om de FreeBSD machine op te vullen.

6.2.5 Dirk Willem van Gulik

Functie : Vrijwilliger
Relevantie : Algemene vraagbaak

De twee meest gebuikte informatie bron van Wireless Leiden vrijwilligers zijn de mailinglijsten en Skype. Dirk Willem heeft via deze wegen een aantal technische vragen beantwoord over het overkomen van beveiliging en de communicatie tussen twee punten zonder kennis van het tussenliggende netwerk.

Dirk Willem heeft een tweetal Soekrissen geleverd inclusief Crypto kaarten plus informatie over deze apparaten.

5.3.6 Rudi van Drunen

Functie : Vrijwilliger
Relevantie : Commentaar op eindpresentatie

Rudi van Drunen heeft eerder met Surfnet gewerkt. Hij heeft deze kennis gebruikt in de eindpresentatie om commentaar te leveren op de eindpresentatie. Er is voor deze presentatie niet eerder contact geweest met Rudi van Drunen.