NTNU
Det skapende universitet

Sikret aksess under nød og beredskaps -prioritering

Chien-Lung Yee

Master i kommunikasjonsteknologi
Oppgaven levert: Juli 2006
Hovedveileder: Steinar Andresen, ITEM

Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Oppgavetekst

Under unormale situasjoner kan det være nødvendig å sikre et utvalg autoriserte personer tilgang til teleressurser. Dette kan f.eks. ordnes ved at disse har terminaler med spesielle id-er som gir prioritert tilgang i visse tilfelle.

I oppgavene skal man diskutere og studere forskjellige løsninger for slike problemer i en WLAN sammenheng. Man kan ta utgangspunkt i et nett likt det som skisseres for Trådløse Trondheim (basert på IEEE 802.11 standarden) og vurdere hvordan viktige personer/terminaler kan gis sikret aksess under f.eks. alminnelige nødsituasjoner og erklærte beredskapssituasjoner* - I samarbeid med faglærer kan oppgaven eventuelt utvides til også å dekke WiMAX og/eller UMTS (inkl.GSM).

Oppgaven vil bli utført i samarbeid med Post og teletilsynet.

*Med en erklært beredskapssituasjon menes en situasjon som er definert av en myndighet, f.eks. politimesteren i en by (studenten behøver ikke detaljere hvem som skal definere denne situasjonen). I dette tilfelle kan det gå en melding til nettverksoperatøren som kan iverksette (via” Network Management” funksjoner en omlegging av nettets funksjoner).

Oppgaven gitt: 03. februar 2006
Hovedveileder: Steinar Andresen, ITEM

Forord

Denne rapporten er et resultat av en masteroppgave avholdt ved Norges Teknisk og Naturvitenskaplige Universitet, i Trondheim våren 2006.

Målet med prosjektet er å se på mulige løsninger som kan sikre teleressurser for et utvalg autoriserte mennesker, basert på IEEE 802.11, og konseptuelt se på løsningene i kontekst med Trådløse Trondheim. En del av oppgaven har vært å karakterisere behovet som ligger til grunn og hvilket sikkerhetsspørsmål som binder seg til problemstillingen.

Nød og beredskap i kommunikasjonsnett er et spennende felt, spesielt i sammenheng med prioritering. Gjennom perioden har jeg fått god innblikk i IEEE 802.11 familien, dets funksjoner og tilhørende sikkerhetsprotokoller. Prosessen frem mot mulige metoder for sikret aksess i WLAN vært dog vært utfordrende, ikke minst på grunn av omfanget et slikt felt dekker. Emner kunne vært lagt til og emner kunne vært trukket fra, men alt i alt er jeg tålelig fornøyd med resultatet.

Prosjektet ble foreslått av professor Steinar Hjelde Andresen ved NTNU, som også fungerte som min veileder. En stor takk rettes til ham for tips og støtte underveis.

Trondheim, 7. Juli 2006

Chien Lung Yee

Innholdsfortegnelse

1.0 – Innledning

Kommunikasjon har igjennom alle tider hatt stor betydning for mennesket. Telekommunikasjon har da også siden Alexander Graham Bell gjennomførte sin første telefonsamtale, i 1876, hatt en rivende utvikling [Telemuseum]. Hvilke sosiale betydninger telefonen medførte er ikke en del av denne rapporten, men det er hevet over en hver tvil at teleteknologien har hatt innvirkning på hvordan samfunnet har utviklet seg. Således har teleressursene etter hvert blitt så sentral at et velfungerende samfunn er avhengig av tilgjengeligheten av disse. Dermed gjenspeiler viktigheten av disse ressursene også hvor kritisk det er å ha løsninger som klarer å behandle de ulike belastningene i forskjellige situasjoner.

1.1 - Bakgrunn

"Under unormale situasjoner kan det være nødvendig å sikre et utvalg autoriserte personer tilgang til teleressurser. Dette kan f.eks. ordnes ved at disse har terminaler med spesielle id-er som gir prioritert tilgang i visse tilfelle.

I oppgavene skal man diskutere og studere forskjellige løsninger for slike problemer i en WLAN sammenheng. Man kan ta utgangspunkt i et nett likt det som skisseres for Trådløse Trondheim (basert på IEEE 802.11 standarden) og vurdere hvordan viktige personer/terminaler kan gis sikret aksess under f.eks. alminnelige nødssituasjoner og erklærte beredskapssituasjoner[1] - I samarbeid med faglærer kan oppgaven eventuelt utvides til også å dekke WiMAX og/eller UMTS(inkl. GSM)."

Overnevnte problemstilling henger sammen med ønsket om å sikre telenettet og -tjenester under ulykker, natur katastrofer, krig, terror og lignende. Slike tilfeller fører ofte til en overbelastning på teleressursene og det blir dermed viktig å prioritere ressursene til det beste for samfunnet. 11. september katastrofen i New York, er et eksempel på hvor store deler av

[1] Med en erklært beredskapssituasjon menes en situasjon som er definert av en myndighet, f.eks. politimesteren i en by (studenten behøver ikke detaljere hvem som skal definere denne situasjonen). I dette tilfelle kan det gå en melding til nettverksoperatøren som kan iverksette (via " Network Management" funksjoner en omlegging av nettets funksjoner)

eksiterende teleinfrastruktur kan være satt ut av funksjon eller være tungt belastet [Flickenger June 2002].

Uvilkårlig vil mennesker som betjener viktige posisjoner for samfunnet ha behov for å ha kommunisere med hverandre for å kunne løse problemene i slike situasjoner. Resultatet kan være katastrofale om tilgjengligheten av disse ressursene ikke er tilstede. Således er det kritisk at disse brukerne får prioritert tilgang på teleressurser i forhold til allmennheten [TIFKOM 20 mars 2000]. Dette er også bakgrunnen for problemstillingen og kan sees i sammenheng med totalforsvaret nevnt i TIFKOM rapporten.

1.1.1 - Historisk

Både før og rett etter avmonopoliseringen av telemarkedet var det Televerket som ivaretok telesikkerheten og beredskap som beskrevet i avsnitt 1.2. Det eksisterte en løsning hvor et utvalg av autoriserte mennesker som ble ansett som viktige for samfunnet, fikk prioritet eller sikret tilgang på teleressurser under nød og beredskap. Den gang var dette langt enklere da Televerket var ene leverandør i telemarkedet og de reelle teknologivalgene færre.

Siden den gang har teknologien fortsatt sin utvikling og markedet blitt mer komplekst. I disse konvergenstider eksisterer det et uttall operatører innenfor kommunikasjonssektoren og teknologisk eksisterer det flere kommunikasjonstyper enn tidligere [PT 9.mai 2005]. ”Ettersom andre operatører også vinner frem i markedet og tar markedsandeler, kan det heller ikke forventes at Telenors telenett og tjenester alene ivaretar telesikkerhet og beredskap på nasjonens vegne i de allmenne nett” [TIFKOM 20 mars 2000].

1.1.2 – Hvorfor vurdere WLAN

Teleressurser i tradisjonell forstand, har ikke samme betydning som tidligere. En stadig større konvergens mellom tele og datatjenester, og ikke minst på grunn av en større integrasjon mellom tradisjonell tele og datanettverk, gjør uttrykkene mellom de to verdene mer glidende og omfattende. IP telefoni er et eksempel på at ny teknologi som opererer på andre nettverk enn tradisjonell telefoni. Det er også viktig å understreke at moderne kommunikasjon ikke kun dreier seg om tale lenger, men også data og video.

Såkalte ”Community Networks” eller fellesskapsnettverk prosjekter har blitt stadig flere og aktualitetsgraden stadig høyere. Dette er fellesskapsnettverk bygd opp rundt WLAN

teknologien for å tilby trådløs Internett aksess. Eksempler på dette er prosjekter som NYCWireless og Seattle Wireless. Trådløse Trondheim er et lignende prosjekt, men har noen andre mål enn de to nevnte. Felles er at en del av Trådløse Trondheim realiseres med WLAN som et ledd å dekke hele Trondheim med trådløs Internett aksess. Disse nettene vil være offentlig tilgjengelige og med den stadig større konvergensen, vil de gå under betegnelsen det ”allmenne nett.” Således er det hensiktsmessig å vurdere WLAN opp nød og beredskaps situasjoner slik problemstillingen fremfører. Et eksempel på krisesituasjon hvor et slikt WLAN har vært et viktig avlastningsnett, er NYCWireless og den tidligere nevnte 11. september katastrofen [Flickenger June 2003].

1.1.3 – Hva er sikret aksess

Når det diskuteres hvilke krav sikret aksess for et utvalg autoriserte personer til teleressurser under nød og beredskap har, kommer man ikke utenom kriterier som:

- Data rater
- Sikkerhet
- QoS
- Mobilitet
- Hvilke tjenester
- Rekkevidde på nettet
- Hvilke myndighet som setter situasjonsstatusen

I denne prosjektoppgaven vil sikret aksess bety at et utvalg autoriserte mennesker alltid vil kunne ha tilgang på teleressursene, i dette tilfellet WLAN ressursene i aksessnettet, ved behov og etter at en erklært beredskapssituasjon har blitt satt i nettet. Kriteriene nevnt ovenfor er også nødvendig å diskutere for en fullverdig nød tjeneste. Avhengig av hvilke omfang WLAN nettet skal integreres mot andre typer nettverk, avgjør det også om kriterier som hvordan prioritet holdes gjennom de ulike nett burde diskuteres.

1.2 – Lover, regulativer og status i dag

Etter avmonopoliseringen og gjennom konsesjonen av 02. mars 1999 [Telenor 2006], var Telenor pålagt å videreføre de ”spesielle samfunnspålagte oppgaver” (SSO) som blant annet innebærer oppgaver innen teleberedskap jf. e-koml. § 2-10. Dette fordi Telenor som tilbyder

blir ansett å ha en sterk markedsstilling. Øvrige operatører har ikke vært pålagt spesielle krav/oppgaver innen telesikkerhet og beredskap.

Imidlertid er praksisen med denne typen konsesjons og registreringsordning endret for å øke forutsigbarheten, lette markedsadgangen, redusere administrative kostnader og tilfredsstille EUs nye reguleringer i henhold til harmoniserende metode for konsesjonering av markedstilgang for tilbydere. ”Den nye metoden innebærer at alle nett og tjenester skal omfattes av en generell tillatelse, dvs. et rettslig rammeverk og sikrer rett til å tilby elektronisk kommunikasjonsnett og tjenester. Individuelle tillatelser begrenses til å omfatte frekvenstillatelser og nummer innenfor nasjonal nummerplan.” [Odelstinget 4. april 2003] Telenors konsesjon som følge av konsesjonen jf. avsnittet over, blir dermed opphevet. Leveringspliktige tjenester og samfunnspålagde oppgaver vil da i stedet bli ivaretatt på en annen måte, enten som følge av avtale eller ved pålegg.

Tidligere har tanken om teleberedskap involvert ett aksessnett og en tjeneste. Ettersom markedet i dag består av et mangfold aktører som tilbyr aksess med ulike teknologier, blir det derfor en utfordring å finne en harmoniserende løsninger. Dette for eksempel på hvordan en kan sikre aksess under den enkelte teknologi som WLAN, og ikke minst hvordan prioritet skal bli beholdt mellom de ulike nettene og teknologiene.

Nød og beredskap er et dagsaktuelt tema. Flere prosjekter tar sikte på å diskutere og finne en løsning innenfor de ulike teknologien og ikke minst finne harmoniserende løsninger. Se for eksempel på http://www.projectmesa.org/.

1.2.1 – Interessenter

Post og Teletilsynet (NPT) er et forvaltningsorgan som regulerer og overvåker telekommunikasjonssektoren i Norge. I tillegg til nød etatene og de grupper mennesker som nevnt i seksjon 6.1.1, kan NPT være interessert i en slik utredning. Betydningen av problemstilingen vil dessuten være til nytte der hvor WLAN vurderes å innlemmes i nød og beredskapssammenheng.

1.3 – Trådløse Trondheim

Startskuddet som skal gjøre Trådløse Trondheim til en forskningsarena ble i januar 2006 satt i gang. Innstillingen for prosjektet fastslår at IT-funksjonene skal fremme samhandling vertikalt og horisontalt i organisasjonen. IT skal forene primærprosesser, som er undervisning og forskning, og sekundærprosesser administrasjon og stab. Konklusjonen fra utvalget er at den faglige ekspertise i primærprosessen må trekkes sterkere med når universitetet anskaffer og utvikler nye IT-løsninger. Trimaks er i denne sammenheng et eksempel på denne utviklingen.

Visjonen er at byen blir et storskala trådløst utvikling og testlaboratorium for forskning og utvikling av mobile datatjenester. Ved å sette i gang med dette prosjektet, skal det gi faglig nytte for NTNUs egen IT-utvikling. [Asphjell 15. Mars 2006]

Således ønsker Trådløse Trondheim å gi alle privatpersoner i Trondheim mulighet til trådløs tilgang. Prosjektet vil være en katalysator for at Trondheim og NTNU blir mer attraktivt for studenter og teknologibasert næringsliv. Dette oppnåes ved å skape et miljø med spisskompetanse på trådløse teknologier og mobile tjenester. På denne måten vil tredjeparts tjenesteleverandører få mulighet til å utvikle tjenester og testet på et levende nett. Mål gruppen er med andre ord FoU miljøet, tjenesteleverandører, studenter og privatpersoner i Trondheim.

Trimaks som blir fundamentet for Trådløse Trondheim, har tre komponenter:

- Trondheim BredBåndsAllmenning (Trondheim BBA) - et eksperimentelt trådløst bredbåndsnett som i første fase dekker Trondheim Midtby og utearealer ved NTNU. Kommunen, fylket og næringsforeningen er partnere.
- Trimaks Nettlaboratorium for fullskala utprøving av nye kommunikasjonsteknologier for trådløst bredbånd.

- Trimaks Informasjonstjenester er et prosjekt for utvikling av nye informasjonstjenester i tilknytning til trådløst bredbåndsnett.

Trådløse Trondheim blir nødt til å realiseres i flere faser med ulike teknologier. I første fase vil NTNU som en hovedaktør vil med dette prosjektet gi 100 prosent trådløsdekning, både inne og ute, til alle campuser innen utgangen av 2006. Dette blir da sammenlignet en 80 prosent økning kun på innendørs dekning fra i dag. Kapasiteten og dekningen er variabelt mellom ulike områder og avhenger av tjenesten. De gule feltene på bildet til høyre illustrerer Wi-Fi dekningen per. 15. Mars 2006 [Asphjell 15. Mars 2006]. Den fullstendig dekningskartet for første fase Wi-Fi finnes i Appendiks C.

I tillegg til campusene vil busstrasene mellom sentrum og Dragvoll, studentboligene, Solsiden, deler av Øya og Midtbyen blir dekket av trådløst Wi-Fi nett basert på 802.11 a/b/g. Prosjektet har dog ingen ambisjoner om å være konkurrent til eksisterende trådbaserte aksess som xDSL, kabel og lignende. NTNU har videre heller ikke ønske om å være operatør av et kommersielt trådløst nett i midtbyen. [Trådløse-Trondheim 13. Juni 2005]

I fase to er målet å gjøre Trondheim fullstendig trådløst. Det er lagt opp til at dette blir realisert med en kombinasjon av Wi-Fi soner og andre teknologier som WiMAX, CDMA, UMTS/HSPDA og WiBRO. Den antatte store utfordringen er å skape sømløs ”roaming” eller såkalt sesjonsmobilitet. [Jelle 21. Oktober 2005]

I Trådløse Trondheimsprosjektet er andre aktører som er involvert Sør-Trønderlag fylkeskommune, Trondheim kommune, UNINETT, Q-Free, Telenor og NextGenTel. Det er forslått at prosjektet er under et konsortium under NTNU de første 2-3 årene, for så å eventuelt ”outsource” driften. ISP-ene blir da ansvarlig å tilby aksess til privatbrukere.

Dette prosjektet sikter mot å bruke Trådløse Trondheim konseptuelt som et eksempel på hvordan å sikre aksess for en autorisert bruker basert på IEEE 802.11 a/b/g.

1.4 – Målsetning og ambisjonsnivå

I forbindelse med problemstillingen i kapitel 1.1, utredes det mulige løsninger på hvordan det er mulig å sikre aksess for autoriserte personer ved bruk av WLAN. Prosjekt rapporten har

ingen ambisjoner om å diskutere de politiske spørsmålene bundet til ansvarsområdet til de ulike aktørene og myndigheter under nød og beredskap i Norge. Likeså fult er dette dagsaktuelt tema som burde diskuteres, men utenfor denne rapporten.

Problemstillingen om et totalforsvar som nevnt i TIFKOM rapporten og teleberedskap i seg selv, er stor og mangfoldig. Av ulike hensyn har for eksempel nød etatene tatt i bruk separate telenett som er uavhengig av de allmenne telenettet. Eksempler på dette er TETRA nettet og GSM-R. Dette prosjektet er ikke ment som et altomfattende løsning på spørsmålene stilt i den TIFKOM rapporten.

Denne prosjektrapporten vil altså utelukkende fokusere på tilstrekkelig ressurs allokering i form av tilgang til aksessnettet, for å sikre aksess under nød og beredskap. Dette betyr at det ikke er i denne oppgavens hovedinteresse å diskutere eller karakterisere: mobilitet, data rater, og rekkevidde på nettverket. Etter samtale med faglærer ble det enighet om at QoS, og hvordan prioritert beholdes gjennom flere ulike nett teknologier, unnlates fra denne oppgaven. Heller ikke sikkerhet som ikke direkte angår sikring av aksess vil bli vurdert noe ytterligere. Hvilke personer som trenger å være innefor det utvalg av autoriserte brukere vil bli antydet, men er heller ikke emnet som blir viet stor oppmerksomhet. Således vil denne prosjektrapporten se på de teknologiske mulighetene IEEE 802.11 spesifikasjonene gir i forhold til problemstillingen, og altså diskutere i forhold til mulige realisasjoner. WLAN sikkerhet vil da være en naturlig del å innlemme i diskusjonen da problemstillingen i storgrad hører med i dette feltet.

Trådløse Trondheim, som i første omgang blir realisert med WLAN dekning, vil konseptuelt bli et eksempel å vurdere opp mot. Et mulig trussel bilde mot et slikt WLAN nettverk, vil dermed være naturlig. Dette prosjektet kan så videre kanskje senere inngå som et bidrag i diskusjonen om totalforsvaret og ikke minst nød og beredskapsdiskusjonene.

Masteroppgaven blir en litteratur studie hvor Post og Teletilsynet bidrar med synepunkter, og hvor er ment som en diskusjon på ulike muligheter.

1.4.1 - Problemvinkling

Målsetningen beskrevet er av en overordnet art. Det er derfor hensiktsmessig å konkretisere problemstillingen. Vi ønsker svar på følgende:

I. Se om og hvordan det er mulig å gi sikret aksess
II. Om IEEE 802.11 er egnet til slikt bruk
III. Hvordan kan dette realiseres i WLAN nett likt Trådløse Trondheim

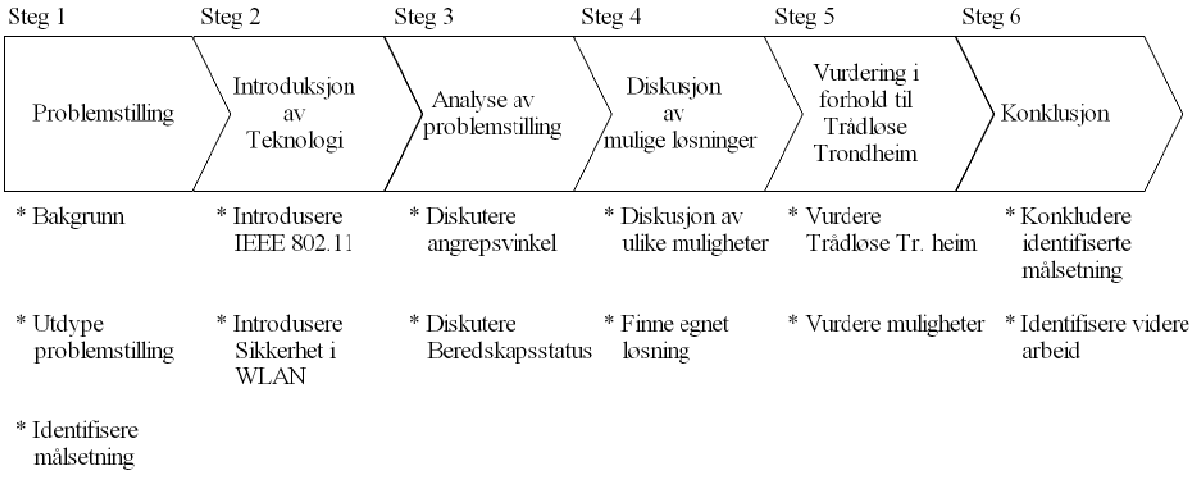
1.5 – Metode

Denne prosjektrapporten vil først og fremst bli en litteratur studie som leder ut til en diskusjon om ulike løsninger. Videre vil problemstillingen bli konseptuelt diskutert opp mot Trådløse Trondheim.

Første fase vil derfor være gi problemstillingen en bakgrunn. Deretter vil det være hensiktsmessig å utdype problemstillingen, målsetning og hva vi ønsker å finne ut av. I andre fase introduseres IEEE 802.11 standarden for å gi en forståelse av teknologien. Sikkerhetsaspektet er her også en naturlig del å introdusere.

Disse to overnevnte fasene vil så lede ut i en ytterligere diskusjon og analyse av problemstillingen i forhold til de muligheter som ligger til grunn i WLAN sammenheng. Dette fører videre til en studie og diskusjon av ulike muligheter for å sikre aksess under nød og beredskap. Resultatet av dette ønskes så å diskuteres konseptuelt i forhold til Trådløse Trondheim.

Stegene for de ulike fasene er illustrert nedenfor:



Figur 1 - Metodesteg

2.0 - Introduksjon av Wi-Fi og IEEE 802.11

IEEE 802.11 er en omfattende samling med spesifikasjoner. Det er derfor hensiktsmessig å gi en introduksjon av WLAN og IEEE 802.11 spesifikasjonen før en diskusjon om løsning. Kapitlet vil gi en introduksjon til teknologien, slik at det også blir en felles forståelse av akronymer og forkortelser. Dette vil også gi et grunnlag for forståelse av virkemåte, og senere hvilke utfordringer som ligger til grunn for problemstillingen.

Historien begynner med at ”The Federal Communications Commission”(FCC) I 1985 godkjente det første ulisensierte ”Spread Spectrum”, og var den utløsende faktor for utvikling av Wi-Fi og Blåtann. Wi-Fi ble oppfunnet av NCR Corporation/AT&T i 1991 og var opprinnelig laget for kassesystemer. De første produktene gikk under navnet ”WaveLAN.” Dette utviklet seg videre til det som senere ble IEEE 802.11 standarden. Radio teknologisk baserer Wi-Fi seg på et ”Direct Sequence Spread Spectrum” (DSSS), og er en del av en større familie med ”spread spectrum” teknologier.

2.1 – Forholdet IEEE og Wi-Fi alliansen

Når det prates om trådløse nett, er det vanskelig å unngå å lese om Wi-Fi og IEEE. Det er heller ikke uvanlig at akronymene gis ulike betydninger. Derfor er det hensiktsmessig å kort fortelle hvilket forhold disse to gruppene har til WLAN.

2.1.1 - Hva er Wi-Fi

Wi-Fi alliansen har komplementær rolle i forhold til IEEE, og lager ikke nye standarder. Fokuset i Wi-Fi gruppen er å sikre sømløshet og kompabilitet ved sertifisering og merkevarenavn bygging. Deres nettsider angir en rekke betingelser for å kunne sertifisering og benytte seg av Wi-Fi logoen [Wi-Fi.Alliance 2006].

Det har hersket forvirring rundt Wi-Fi ordet siden uttrykket ”Wi-Fi - The standard for Wireless Fidelity” oppsto. Ordet har dessuten blitt brukt så mangfoldig at ordets betydning og omfang er blitt uklart. Den generelle misforståelsen er at Wi-Fi er et akronym eller forkortelse for ordet ”Wireless Fidelity.” Dette er imidlertid blitt avvist av Wi-Fi gruppen selv, da ordet ikke har noen som helst meningen utover et merkenavn. [Fleishman November 2005]

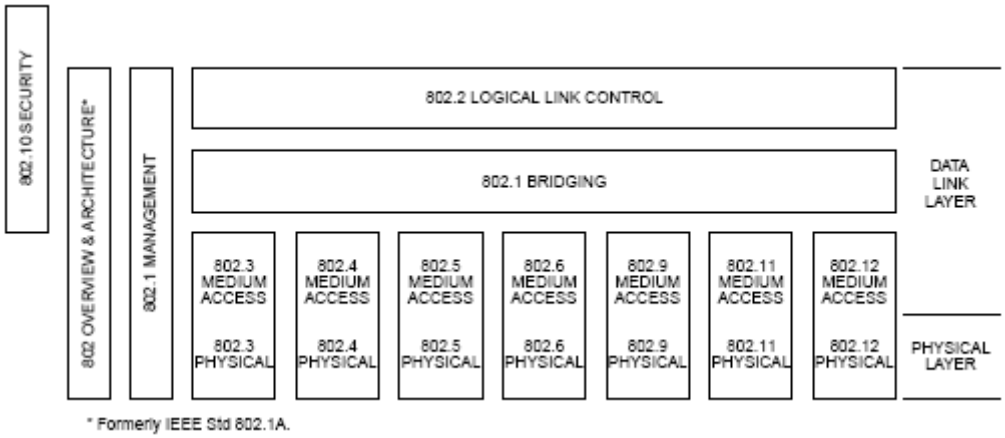
Kort fortalt er Wi-Fi det opprinnelige merkenavnet lisensiert under ”The Wi-Fi Alliance” for å beskrive den underliggende teknologien for trådløs lokalnetteverk basert på IEEE 802.11 spesifikasjonene og kompabiliteten til denne standarden [Wi-Fi.Alliance 2006] [ANSI/IEEE802.11-1999(R2003) 12 Juni 2003].

2.1.2 - The Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE) har en gruppe kalt ”the Standard Association,” som er en underavdeling av IEEE ansvarlige for blant annet IEEE 802 familien: ”Local Area and Metropolitan Area Networks.” IEEE 802 er igjen delt inn i arbeidsgrupper som hver jobber med en spesifikk områder under standarden.

2.2 - IEEE 802.11 familien

IEEE 802.11 familien angir et sett av trådløse LAN/WLAN standarder utviklet av arbeidsgruppe 11 av ”IEEE LAN/MAN standard komiteen.” I litteraturen brukes også IEEE 802.11x til å angi den samme samling standard, altså ikke de enkelt bestående elementene i standarden [ANSI/IEEE802.11-1999(R2003) 12 Juni 2003]. Videre er det viktig å merke seg at bokstaven etter standard revisjonen er av betydning. Liten bokstav indikerer standard avhengighet, hvorav stor bokstav viser at det er en fullt uavhengig standard.



Figur 2 - IEEE 802.11 familie tre [ANSI/IEEE802.11-1999(R2003) 12 Juni 2003]

Per i dag tar 802.11 familien for seg seks modulasjonsteknikker over radio. Den samme protokollen er benyttet ved bruk av disse seks teknikkene. De mest brukte teknikkene er definert i IEEE 802.11a, IEEE 802.11b og forbedringene til den originale standarden i IEEE

802.11g. Videre så var de sikkerhetsmessige sidene også revidert i IEEE 802.11i. De andre standardene i familien som c-f, h-j og n, er tjeneste forbedringer og forlengelser eller feilkorrigeringer for tidligere utgaver. Når dette er nevnt, var IEEE 802.11b den standarden som var første bredt aksepterte trådløse standarden. Deretter kom IEEE 802.11a og IEEE 802.11g.

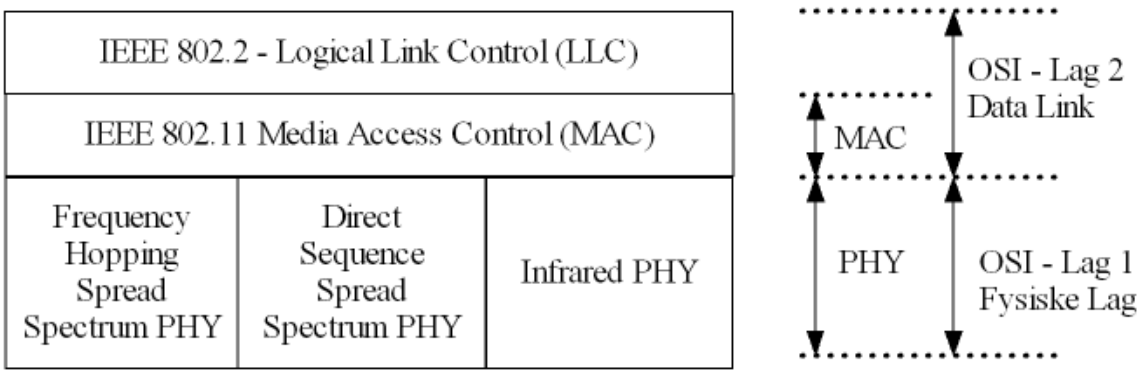
Både IEEE 802.11b og g bruker det samme frekvensbåndet på 2.4 GHz. I Norge er dette et fritt frekvensbånd, men dette varierer mellom de ulike kontinenter som for eksempel mellom USA og Europa. USA har en mer restriktive frekvensinndeling. Andre produkter i dag som opererer på samme frekvensbånd er for eksempel Blåtann, mikrobølgeovner, enkelte trådløse telefoner og andre trådløse video og audio sendere. Således kan det oppstå interferens med disse produktene. IEEE 802.11a benyttes derimot 5 GHz båndet og vil derfor ikke ha interferens med de samme produktene/teknologiene.

Tabell 1 – radiogrensesnittene ved IEEE 802.11 på PHY laget

Grensesnitt	**802.11a (OFDM)**	**802.11b (DSSS)**	**802.11g (OFDM&DSSS)**
Frekvensbånd	**5GHz**	**2.4GHz**	**2.4GHz**
Hastighet	**54 Mbit**	**11 Mbit**	**54 Mbit**

2.4 - IEEE 802.11 protokoll design

IEEE 802.11 protokoll stakken kan sees i sammen heng med OSI modellen som vist i figur 3. Dette er hensiktsmessig da OSI modellen stort sett er en kjent og akseptert referansemodell. På samme måte som OSI modellen, deler modellen funksjoner i protokollen i en serie med lag. Et enkelt lag har alltid den egenskap å kun bruke funksjoner i laget under, mens det kun eksporterer funksjonalitet til laget ovenfor seg selv. Figur 3 viser også at det refereres til link og det fysiske lag når WLAN og IEEE 802.11 omtales.



Figur 3 - IEEE 802.11 i sammenheng med OSI referansemodellen

PHY laget refererer til det fysiske lag og til trådløse elektromagnetiske forbindelsen. Her behandles modulasjon, kollisjonskontroll og andre lavnivå funksjoner. Denne vil da betjene tjenesteforespørsler fra MAC sub laget.

MAC sub laget på sin side avgjør hvem som har tilgang på det fysiske mediet til enhver tid og fungerer som et grensesnitt mellom sub laget LLC og nettverkets PHY lag. Med andre ord så kontrollerer MAC laget tilgang til det fysiske transmisjons medium.

Over MAC sub laget befinner LLC sub laget seg. Den gjenkjenner blant annet hvor rammer begynner og slutter i bit strømmen fra det fysiske lag, avgrenser rammer, oppdager transmisjonsfeil, setter inn kilde og destinasjons MAC adresser i hver enkelt ramme, filtrerer ut rammene som er tiltenkt den mobile stasjonen. LLC laget tar seg også av multipleksingen.

2.5 - IEEE 802.11 nettverkskomponenter

IEEE 802.11 arkitekturen består av flere komponenter som samhandler med hverandre. Hovedkomponentene i arkitekturen er den mobile stasjonen (STA), aksesspunktet (AP) og det trådløse mediet (WM)

- **Stasjon (STA)**. En komponent i IEEE 802.11 arkitekturen, er den trådløse klienten eller den såkalte stasjonen (STA). En stasjonsenhet er en vilkårlig enhet som støtter funksjonene i IEEE 802.11. Således kan denne stasjonen være en bærbar, en håndholdt, et aksesspunkt og være mobile, portable eller stasjonære. Fellesnevneren er altså at de alle støtter IEEE 802.11 stasjonstjenester som autentifikasjon, avautentifikasjon, fortrolighet og dataleveranse.

- **Aksesspunkt (AP)**. Wi-Fi nettet består av en sender og mottaker kalt et aksesspunkt (AP), som fungerer som et koordinasjonspunkt for stasjonene. Dette aksesspunktet radio kringkaster sin ”Service Set Identifier” (SSID), altså nettverksnavnet, i pakker kalt ”beacons.” Denne utsendelsen skjer hver 100 ms med en rate 1 Mbit/s, men er allikevel en så liten pakke at det ikke påvirker total ytelsen. 1 Mbit/s er også den minste hastighetsraten som Wi-Fi tillater [Velayos and Karlson April 2003].

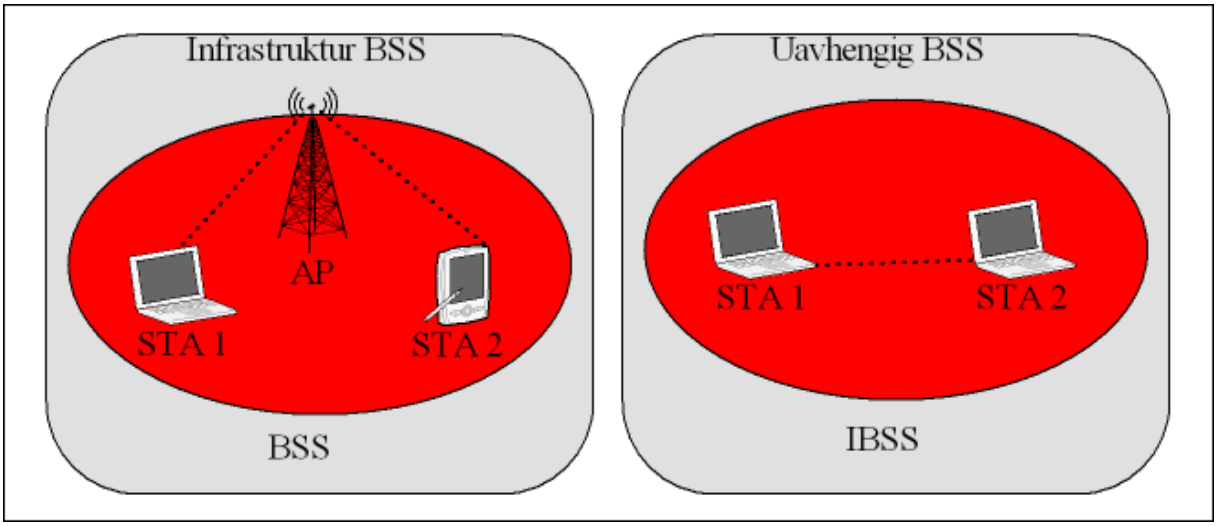
- **Trådløse Mediet (WM)**. Når en STA skal kommunisere med en annen AP eller STA, brukes det trådløse mediet. Data rammene beveger da altså seg over dette mediet.
Standarden definerer videre to typer WLAN design konfigurasjoner: Begge modusene er beskrevet med flere detaljer i kapitel 2.6.

2.6 – Arkitektur struktur

IEEE 802.11 standarden definerer to typer WLAN design strukturer. Enten ved at to eller flere stasjoner kobler seg mot hverandre uten et sentralt styringsobjekt, eller at stasjonene kobler seg opp mot et aksesspunkt.

- **Ad hoc modus**. I ad hoc modus benyttes ikke aksesspunkter og blir ofte referert til som infrastrukturløs eller ”Independent Basic Service Set” (IBSS). Dette fordi at det kun er ”peer-to-peer” stasjoner er involvert i en eventuell kommunikasjon.

- **Infrastruktur modus**. I infrastrukturmodus vil et aksesspunkt forbinde de ulike trådløse stasjonene sammen, eller til et distribusjonssystem. Dette er også den mest vanlige formen modus for WLAN og blir i spesifikasjonen referert til som ”Basic Service Set” (BSS). Distribusjonssystemet er beskrevet i seksjon 2.6.3.



Figur 4 - Infrastruktur BSS og Uavhengig BSS

2.6.1 – BSS

Et BSS er etter IEEE 802.11 definert som den mest grunnleggende byggeklossen i et trådløst 802.11 nettverk i infrastruktur modus. Den består av minst en STA som er koblet opp mot AP i tillegg til aksesspunktet i seg selv. Dekningsområde som et aksesspunkt gir, blir kalt for ”Basic Service Area” (BSA). Venstre siden av Figur 4 viser to enkelte stasjoner og et aksesspunkt som til sammen danner et BSS. Når en STA beveger seg uten for dekningsområdet for BSA-et, skissert som en rød ellipse, vil ikke stasjonen lenger kunne kommunisere med andre medlemmer av det BSS-et.

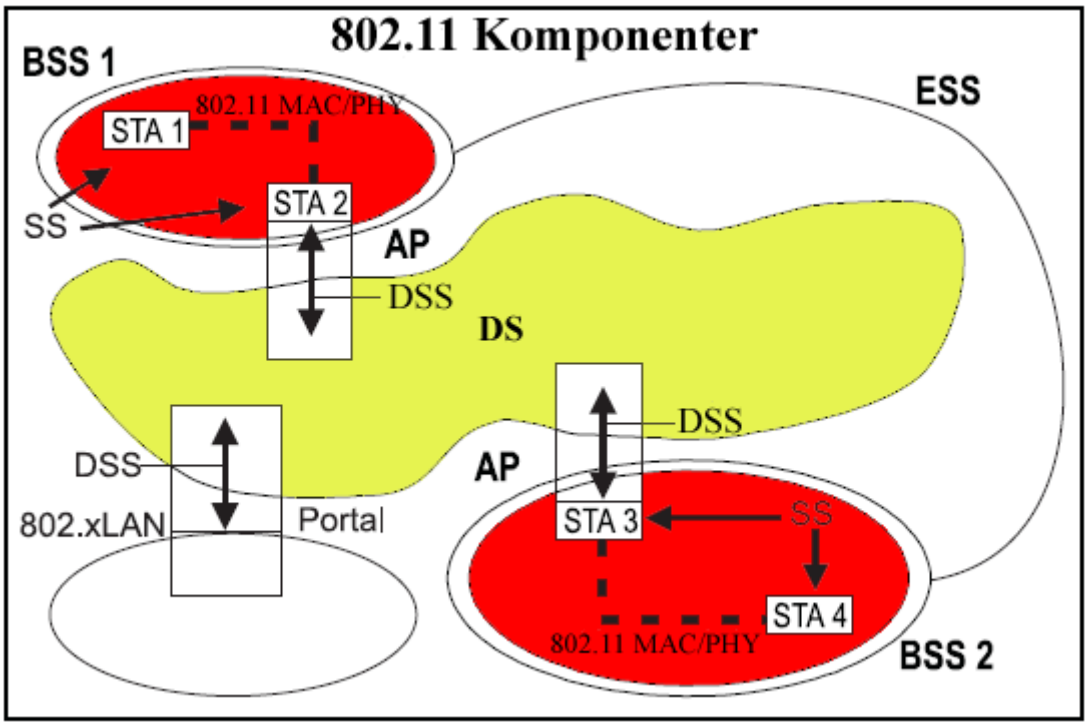
2.6.2 – Uavhengig BSS

Når en eller flere STA er koblet sammen uten et sentralt styringsobjekt, blir det ofte referert til som et ad hoc nettverk. Dette ad hoc nettverket blir i 802.11 sammenheng kalt et IBSS og består i sin mest grunnleggende form av minimum to STA som er sammenkoblet. Figur 4 illustrerer dette.

2.6.3 – Distribusjonssystemet (DS)

Når flere aksesspunkt er koblet sammen for å tilby et større dekningsområde, må det kommuniseres med hverandre for å holde orden på bevegelsene til de mobile stasjonene. Distribusjonssystemet er en logisk komponent i 802.11 brukt til å videresende rammer ditt de skal. Videre er det ingen spesifikk teknologi er angitt for realisere distribusjonssystemet, men er som regel implementert som et såkalt ”bridge engine” og DS medium. Dette blir også kaldt for ”Backbone”.

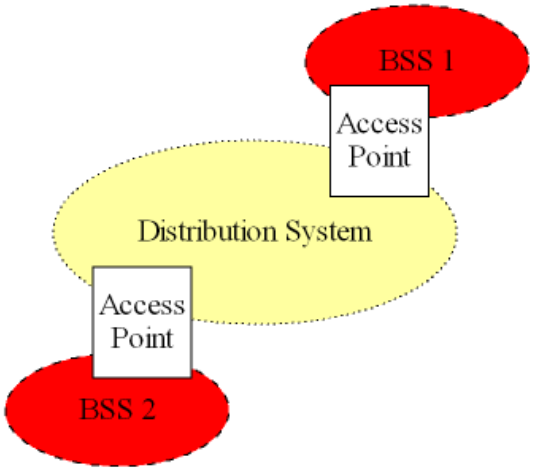
Figur 5 illustrerer den fullstendige IEEE 802.11 arkitekturen. Fra figuren ser vi at en BSS kan innlemmes som en komponent av et større nettverk bestående av flere BSS. Komponenten som brukes for å koble de ulike BSS med hverandre, kalles for ”the distribution system” (DS) og er illustrert som det gule feltet. Tjenestene som DS komponenten gir er kjent som ”the distribution system service.” Dette er i figur 4 betegnet med piler innenfor AP som indikerer at tjeneste er brukt for å krysse medier og logiske grenser.



Figur 5 - Den fullstendig IEEE 802.11 arkitekturen [ANSI/IEEE802.11-1999(R2003) 12 Juni 2003]

2.6.4 – ”Extended Service Set” (ESS)

IEEE 802.11 tillater også ved hjelp DS og BSS å lage trådløse nett med vilkårlige størrelse og kompleksitet. Dette realiseres ved å sette sammen flere BSS sammen med et backbone nettverk. Slike nettverk er referert til som et ”extended service set” (ESS) og er illustrert i figur 6. Videre vil alle aksesspunkter i et ESS ha samme SSID, nettverknavn, for brukeren



Figur 6 - Extended Service Set [ANSI/IEEE802.11-1999(R2003) 12 Juni 2003]

2.6.5 – Multi-SSID

Tidligere var det nok å la brukerne koble seg opp mot et enkelt logisk nettverk. Ettersom WLAN modnet og stadig større aktører viste interesse, viste det seg at dette ikke holdt når spesielt brukerne begynte å bli mange. Det er i dag vanlig å håndtere flere virtuelle aksesspunkter, hvor de deler radiogrensesnittet og den fysiske infrastrukturen. Ved denne måten er det for eksempel mulig å sortere ulike brukergrupper i hvert sitt logiske nettverk. Klient enheten vil da i tilfellet oppdage to separate nettverk i det domenet og kan koble seg opp mot den ønskelige. [Geier 24. April 2003]

2.7 – Nettverkstjenester

Nettverksteknologi vil ikke være mye verdifullt uten netteverkstjenester. Dette underkapittelet presenteres de ulike tjenestene 802.11 tilbyr. I spesifikasjonene er disse tjenestene klart definert og vil dermed gjøre det mulig for utstyrsleverandører å implementere de nødvendige tjenester.

2.7.1 - Distribusjonstjenesten

Denne tjenesten blir benyttet av STA-ene, i et nettverk i infrastrukturmodus, hver gang det skal sendes data. Med engang en ramme har blitt akseptert av et aksesspunkt, vil den bruke distribusjons tjeneste til å levere rammene til destinasjonen. All kommunikasjon som bruker et aksesspunkt vil bevege seg gjennom distribusjonstjenesten. Dette er inkludert kommunikasjon mellom to STA assosiert med det samme aksesspunktet.

2.7.2 - Integrasjon

Distribusjonstjenesten tilbyr en tjeneste kaldt integrasjons. Denne tjeneste muliggjør forbindelser fra distribusjonssystemet til et ikke IEEE 802.11 nettverk. Således er dette en funksjon spesifikk for distribusjonssystemet og er ikke definert i 802.11 annet enn i hva tjenestene må inneholde

2.7.3 – Assosiasjon

Avlevering av rammer til STA er først mulig etter at STA har registrert seg mot aksesspunktet. Denne registreringen kalles i 802.11 sammenheng for assosiasjon. Distribusjonssystemet kan dermed bruke assosieringsinformasjonen for å bestemme hvilket aksesspunkt som skal brukes for enhver STA. En STA som ikke er assosiert mot en AP vil heller være å regne med som å være på nettverket. I praksis vil en assosiasjon føre til at aksesspunktet allokerer ressurser for STA og synkronisere seg mot hverandre.

Om RSN protokollen er tatt i bruk, vil assosiasjonen være et forstadium til autentifiseringen. Før en fullføring av autentifiseringen, vil et aksesspunkt droppe all nettverksprotokolltrafikk fra en STA.

2.7.4 - Gjenassosiasjon

Gjenassosiasjonstjenesten er en DS tjeneste og benyttes for å flytte nåværende assosiasjon fra en AP til en annen. Tjenesten er viktig for å støtte mobilitet ved BSS overganger. Når en STA beveger seg mellom BSA innenfor et ESS, hender det at den må assosiere seg mot et annet AP. Eksempel på dette er når signalstyrken tilsier at det er hensiktsmessig å bytte til en annen AP. Denne gjenassosiasjonen blir alltid initiert av STA selv og aldri av AP.

Denne tjenesten kan også benyttes til å forandre eksisterende assosiasjonsattributter mens STA stadig er forbundet mot samme AP.

2.7.5 – Avassosiasjon

Denne tjenesten kan både bli initiert av AP og STA. Når en eksisterende assosiasjon skal avsluttes, eller av andre grunner trenger å avslutte, påkalles avassosiasjonstjenesten som er en DS tjeneste. Mobilitetsdata som er lagret i distribusjonssystemet blir da fjernet. Når da avassosiasjonen er fullstendig, vil ikke STA lenger være en del av nettverket. En STA som for eksempel forlater et nettverk eller som avslutter, skal avassosiere. MAC protokollen tar

allikevel høyde for at dette kan skje uten å formelt avassosiere. Avassosiasjon er en kunngjøring og ikke en forespørsel. Således kan kunngjøringen heller ikke avvises av verken AP eller STA.

2.7.6 - Autentifikasjon

Trådløse nettverk har ikke de samme barrierer satt av fysisk medium. Derfor vil det være vanskelig å gjennomføre noen fysiske sikkerhetstiltak for å hindre uønsket aksess. IEEE 802.11 gir mulighet for LAN aksesskontroll ved hjelp av denne autentifikasjonstjenesten. Verdt å merke seg er at IEEE 802.11 støtter flere ulike autentifikasjonsmetoder og angir ikke en spesifikk autentifikasjonstype.

Tjenesten er brukt av alle STA til å gi seg tilkjenne overfor andre de kommuniserer med og en nødvendig forutsetning før en assosiasjon. Før assosiasjon vil dermed STA utveksle identitet, sin egen MAC adresse, med den kommuniserende part. En STA kan for øvrig være autentifisert mot mange andre STA samtidig.

2.7.7 - Avautentifikasjon

Avautentifikasjon er også en STA tjeneste og blir påkalt når det er behov for at en eksisterende autentifikasjon skal avsluttes. Siden autentifikasjon er nødvendig for tilgang til et nettverk, vil en avautentifikasjon føre til en avassosiasjon til gjeldende ESS.

2.7.8 - Konfidensialitet

I spesifikasjonene for IEEE 802.11 blir denne tjenesten kalt for fortrolighetstjenesten. Der angis det også bruk av ”Wireless Equivalent Privacy” (WEP) for å sikre fortrolighet ved det trådløse mediet. WEP er i dag ikke regnet som en sikker metode i dag.

2.7.9 - MSDU leveranse

Et nettverk består av sammenkoblete enheter. Dette nettverket har verdi når den kan levere data fra et punkt til et annet. MSDU leveransetjenesten er den tjenesten som er ansvarlig for å levere data til den riktige mottaker.

2.7.10 - Sendekraft kontroll

Rekkevidde av radiobølger er en funksjon av sendekraft. En STA med høy sendekraft vil sannsynligvis føre til interferens med tilstøtende nabonettverk. Derfor spesifiserer 802.11h denne tjenesten for å gi mulighet til å regulere sendekraften til riktig nivå. Opprinnelig

2.7 – Mobilitetstyper i IEEE 802.11

Mobilitet er en av hovedmotivasjonene for trådløse nettverk. IEEE 802.11 tilbyr mobilitet på link laget mellom ulike BSA. I spesifikasjonene defineres tre ulike typer overganger for å beskrive stasjonsmobiliteten mobiliteten innenfor et nettverk.

a) Ingen transisjon

Det er to sub klasser i denne typen som ikke er mulig å skille.

- Statisk hvor det ikke er noen bevegelse
- Lokal bevegelse hvor bevegelsen er innenfor rekkevidden til PHY av de kommuniserende stasjonene. Det vil som regel bety innefor ”Basic Service Area” (BSA).

b) BSS transisjon

Denne transisjonen er definert som bevegelse av en stasjon fra en BSS i en ESS til en annen BSS, men innenfor samme ESS.

c) ESS transisjon

Stasjonsbevegelse fra en BSS i en ESS til en BSS i et annet ESS. Denne transisjonen er kun støttet ved at STA har lov til å flytte på seg, men det er ingen garantier i IEEE 802.11 for at forbindelsen mellom de øvre lag vedlikeholdes. Dermed er det sannsynelig for tjenesteavbrudd. [ANSI/IEEE802.11-1999(R2003) 12 Juni 2003]

2.8 – Hvordan en STA melder seg på en eksiterende BSS

Hver gang en STA ønsker å koble seg til en AP og sende data, gjennomføres det en sekvens av prosedyrer:

1. Skanning og/eller mottak av synkroniseringsinformasjon
2. Autentifisering
3. Assosiering

En stasjon trenger synkroniseringsinformasjon fra aksesspunktet, eller andre noder, for å kunne koble seg til aksesspunktet. Denne informasjonen kan bli mottatt på to ulike måter: passiv skanning og aktiv skanning.

2.8.1 - Passiv skanning

Ved passiv skanning venter STA på å motta ”Beacon” rammer fra AP. En ”Beacon” er en administrasjonstype ramme, som STA mottar ved å lytte til ulike kanaler. Denne rammen blir periodisk sendt ut av AP, og innholder synkroniseringsinformasjon som:

- SSID
- AP egenskaper (datarater)
- ”Beacon” perioder
- ”Traffic Indication Map” (TIM)
- MAC adresse til AP og tidsstempel

Under store nettverk kan det dukket opp mange flere ulike aksesspunkter under denne skanneprosessen. Stasjonen er da nødt til å bestemme hvilke aksesspunkt den vil koble seg imot. Dette kan da for eksempel være bestemt av signalstyrke eller andre parametere satt opp.

2.8.2 - Aktiv skanning

I denne fasen vil STA være aktiv for å lokalisere et aksesspunkt. STA forsøker dette ved å sende ut ”Probe Request” rammer. Deretter venter stasjonen på ”Probe Response” rammer fra aksesspunktet.

2.8.3 - Autentifisering

Etter at stasjonen har lokalisert et aksesspunkt, og har ønsker å melde seg inn i lokaliserte BSS, gjennom går STA en autentifikasjonsprosess. Det blir sendt ut en ”Authenticate Request” melding mot valgte AP. AP svare denne henvendelsen med et svar om godkjennelse. Dermed har STA fått tillatelse til å koble seg mot den valgte AP.

2.8.4 - Assosiering

Når STA er autentifisert starter assosieringsprosessen. Dette er en informasjons utvekslingsprosess om STA og BSS egenskapene. STA sender en assosiasjons melding til AP, hvor AP svarer med et assosiasjonssvar som indikerer om forbindelsen er godkjent. Det er først etter at assosieringsprosessen er fullbyrdet at STA har mulighet til å sende og motta datarammer. Etter dette vil data som er sendt fra STA gjennom AP bli videresendt til nettverket hvor AP er forbundet.

2.9 – Oppsummering

Dette kapitelet introduserer det mest grunnleggende i IEEE 802.11 standarden. WLAN blir vanligvis implementert som en forlengelse av det trådbaserte nettverket, og da vanligvis innenfor en begrenset rekkevidde. Da de første IEEE 802.11 spesifikasjonene ble vedtatt, var WLAN utstyr basert på IEEE 802.11b det mest vanlige. Denne standarden skulle gi trådløse forbindelse med ytelse og sikkerhet sammenlignbart med kablet Ethernet. Etter den tid har WEP (ref til WEP) ikke vist seg og gi tilstrekkelig god sikkerhet. Dette har senere blitt adressert med IEEE 802.11i og blir omtalt mer i kapitel 6.0.

Kapitelet har ellers forklart ulike konsepter som:

- Stasjon (STA)
- Aksesspunkt (AP)
- Trådløse mediet (WM)
- Ad hoc modus eller ”Independent Basic Service Set” (IBSS)
- Infrastrukturmodus modus eller ”Basic Service Set” (BSS)
- Distribusjonssystemet (DS)
- ”Extended Service Set” (ESS)
- Multi-SSID
- Ulike nettverkstjenester
- Mobilitetstyper
- Innmelding mot eksisterende BSS

Neste kapitel vil ta for seg MAC laget, da dette vil være av interesse for problemstillingen.

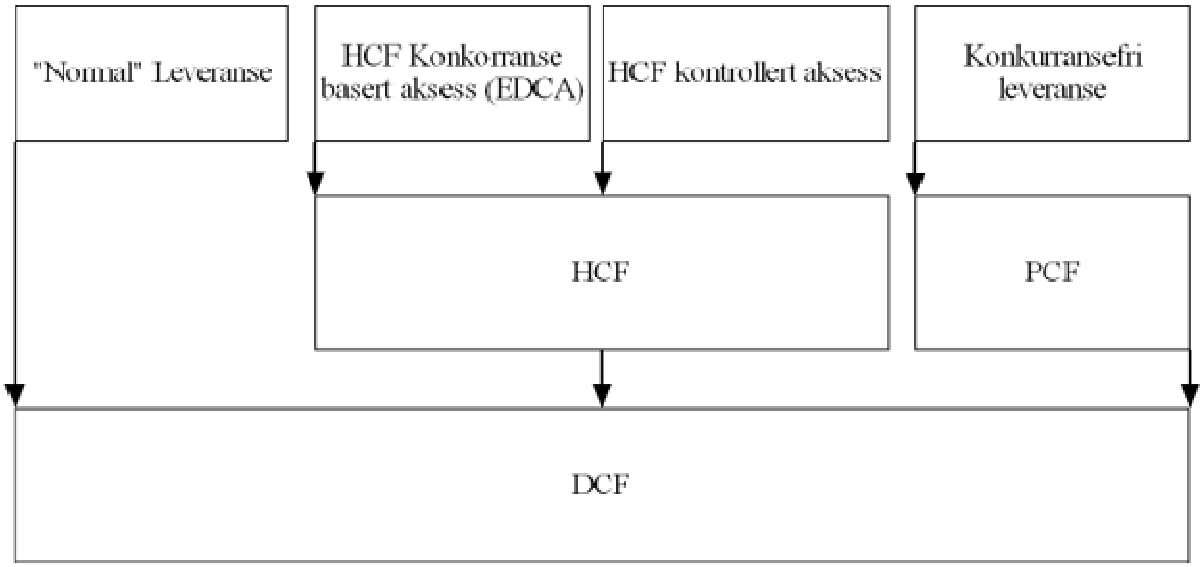
3.0 – Koordineringsfunksjoner på MAC laget

Forrige kapittel ga en oversikt over grunnleggende introduksjon til IEEE 802.11. Dette kapitelet vil enkelt beskrive MAC koordineringsfunksjonene som på mange måter er nøkkelen til å forstå hvordan WLAN teknologien fungerer. Ytterligere forklaringer av laget og funksjonene nevnt under vil være beskrevet i ”802.11 Wireless Networks: The definitive guide” kapitel 3.

IEEE 802.11 MAC laget gir delt aksess til den trådløse kanalen og tilbyr to ulike operasjonsmoduser: DCF og PCF. DCF er obligatorisk i forhold til protokollen, og definerer en distribuert type aksess for et ad hoc nettverk. PCF på sin side er ikke obligatorisk og definerer en sentralisert aksess for infrastruktur nettverk.

De fleste aksesspunkter bygger på en delt buss topologi slik at bare en melding kan bli behandlet om gangen. Derfor er aksesskontrollsteknikker til medier nødvendig. Tilgang til det trådløse mediet er kontrollert av koordineringsfunksjoner. Både DCF og PCF bruker på samme måte som Ethernet ”Carrier Sense Multiple Access” (CSMA) for å kontrollere aksess til transmisjonsmediet. Mens Ethernet forsøker å detektere kollisjoner med CSMA/”Collision Detection” (CD), prøver IEEE 802.11 å heller unngå kollisjoner med CSMA/”Collision Avoidance” (CA). Dette for å unngå å oppta for mye transisjonskapasitet.

En av bakdelene ved IEEE 802.11 MAC er mangelen på QoS støtte for realtime applikasjoner og tjeneste differensiering. IEEE 802.11e forsøker å rette å på dette ved å innføre HCF og er å finne i IEEE 802.11e spesifikasjonene. Figur 6 gir oversikt over koordineringsfunksjonene på MAC laget.



Figur 6 – MAC koordinasjonsfunksjoner [Gast 2005]

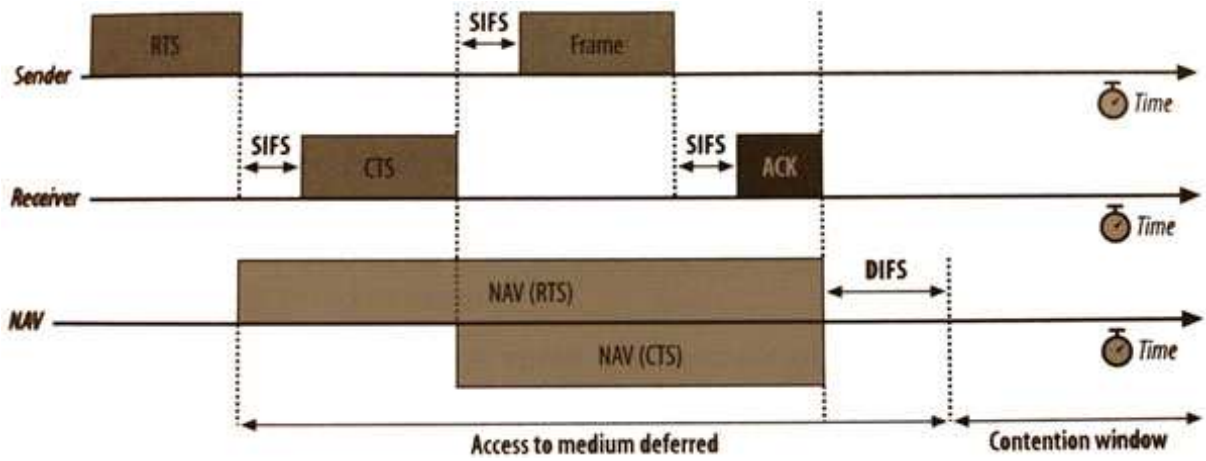
3.1 – "Distributed Coordination Function" (DCF)

Vanlig tilgang til mediet er gitt av "Distributed Coordination Function" (DCF). Hovedoppgaven til DCF er å sjekke mediet før eventuelle transmisjoner, og dermed unngå at flere STA sender på samme tid. Enkelt summert betyr det å lytte før snakke.

Parallelle transmisjoner av flere STA på samme tid, fører til kollisjoner og korresponderende forsøk på å sende på nytt. For å unngå kollisjoner benyttes en "random backoff" funksjon. STA sjekker om mediet er ledig for en spesifisert periode. Er den opptatt vil den avvente sendingen med en tilfeldig tidsperiode. Denne "backoff" funksjonen kan være liten, derfor har DCF innlagt en obligatorisk tidsmellomrom mellom to etterfølgende datarammer. Dette mellomrommet blir kalt for "Data Inter Frame Spacing" (DIFS). Videre vil DCF for hver vellykkede mottatte unicast dataramme, generere en positiv bekreftelse på mottakelse.

Sannsynligheten for kollisjoner ytterligere reduseres ved å benytte CTS/RTS teknikk. Skjemaet for denne teknikken er illustrert nedenfor i figur 7. Teknikken bygger på at en STA sender RTS til destinasjonsnoden. Destinasjonsnoden sender CTS, etter en "Short Inter Frame Spacing" (SIFS) periode, for å gi tillatelse for STA å sende. Både RTS og CTS inneholder begge felt som forteller hvor lang varighet det tar å sende datarammen inklusive ACK bekreftelsen som følger.

Videre vil alle nodene i nærheten av sender STA oppdatere sin egen ”Network allocator vector” (NAV), og avvente sin egen transmisjon. Tilsvarende skjer på mottaker siden hvor alle nærliggende noder hører CTS meldingen. NAV lagrer varigheten hvor mediet er opptatt og rapporterer til det fysiske laget at mediet er opptatt på det tidspunktet. Hele denne prosessen blir referert til som den virtuelle kollisjonsdeteksjonsmekanismen. Kort fortalt vil RTS/CTS allokere mediet for en gitt periode, noe som reduserer kollisjonsfaren.



Figur 7 – NAV for virtuell bærer deteksjon [Gast 2005]

3.2 – ”Point Coordination Function” (PCF)

”Point Coordination Function” (PCF) bruker DCF som basis, og gir en relativt uutviklet form for QoS i infrastrukturmodus. Når tidssensitiv informasjon skal sendes, vil PCF fungerer som en koordinator for den enkelte AP. PCF bevilger en konfliktfri kanal til hver individuell node, ved å forespørre hver enkelt node for transmisjoner.

Aksesspunktet start av en PCF periode ved å kringkaste en spesial ”beacon” type ved hjelp av DCF form for aksess. Etter dette overtar AP kontroll over mediet, referert til som den konkurransefrie periode eller ”Contention Free Period” (CFP). I denne perioden, vil AP spørre hver STA forbundet. STA svarer denne forespørselen med en ACK bekreftelse. Har STA data å sende vil STA svare spørringen med en dataramme. Skulle det oppstå kollisjon, vil STA gjensende datarammen i samme eller neste CFP periode.

For å unngå at klienter med kun DCF fra og forstyrre PCF trafikk, innføres ”Priority Inter Frame Spacing” (PIFS) som har kortere varighet enn DIFS i DCF. Dette fører til at PCF STA

vil sende tidligere og at en DCF stasjon da oppfatter mediet som opptatt. Dermed vil den avvente til PCF STA er ferdig med sendingen.

Videre er PCF en valgfri egenskap for aksesspunkter og er ikke obligatorisk i forhold til spesifikasjonene. Mye på grunn av dårlig markedsmottakelse, ble PCF lite brukt. Således er det få kommersielle aksesspunkter som implementerer denne funksjonen [Gast 2005].

3.3 – Hybrid Coordination Function (HCF)

”The Hybrid Coordination Function” (HCF) blir definert i IEEE 802.11e spesifikasjonene, og utbedrer IEEE 802.11 MAC ved å tilby QoS og tjeneste differensiering. HCF består av to metoder for kanalaksess: ”HCF Controlled Channel Access” (HCCA) og ”Enhanced DCF Channel Access” (EDCA). Begge metoder definerer trafikk klasser for ulike applikasjoner.

IEEE 802.11e protokollen og QoS blir ikke et videre tema i denne prosjektrapporten etter avtale med faglærer.

3.4 - ”Interframe Spacing”

”Interframe Spacing” har en stor rolle vedrørende koordinering av tilgang til mediet. WLAN benytter seg av fire forskjellige mellomromsperioder. På grunn av CSMA/CA mekanismen vil kortere mellomromsperioder gjøre at andre klienter oppfatter mediet som opptatt [Gast 2005]. Ytterligere detaljer om ”Interframe spacing” refereres det videre til ”802.11 Wireless Networks: The definitive guide” kapitel 6.

- **”Short interframe space” (SIFS)**. Benyttes ved høyprioritets transmisjoner som RTS/CTS rammer.
- **”PCF interframe space” (PIFS)**. Denne benyttet av PCF under konkurransefrie perioder.
- **“DCF interframe space” (DIFS)**. Denne benyttes av DCF under perioder hvor det er konkurranse om mediet.
- **”Extendet interframe space” (EIFS)**. Denne benyttes når det er en feil i rammetransmisjonen., perioden har heller ingen fast varighet.

3.5 – Oppsummering

Kapitelet har gitt en oversikt over koordineringsfunksjonene i MAC laget, som kontrollere tilgangen til det trådløse mediet.

- DCF
- PCF
- HCF

IEEE 802.11 benytter seg av CSMA/CA mekanismen for å styre tilgangen til mediet. Ved DCF vil en STA lytte til mediet for å se om det er opptatt. Ved PCF er det aksesspunktet som etter hvert styrer tilgangen til mediet. AP vil her spørre hver enkelt STA om de har datarammer som de ønsker skal bli sendt.

4.0 – IEEE 802.11 rammetyper

Det er hittil beskrevet de grunnleggende funksjoner og operasjoner i IEEE 802.11. For å gi en videre forståelse på IEEE 802.11, vil dette kapitelet gi en introduksjon til ulike ramme typer. Hensikten er å gi en oversikt over trafikken som går mellom nettkomponentene. For en beskrivelse av strukturer og ytterligere bruk, henvises det til IEEE 802.11 spesifikasjonene eller for eksempel ”802.11 Wireless Network: The Definitive Guide” kapitel 4.0 av O’reilly.

IEEE 802.11 standarden definerer ulike rammetyper når nettverkskomponentene kommuniserer. Innenfor spesifikasjonene er det definert tre typer rammer: Data, administrasjon og kontroll rammer. Datarammer innholder protokollinformasjon og data fra høyere lag. Administrasjons og kontrollrammer brukes for å administrere og kontrollere den trådløse forbindelsen. Felles for alle disse rammetypene er at alle inneholder felt med: kontroll felt som forteller om protokollversjon, rammetype, MAC adresser for kilde og destinasjon, ramme sekvensnummer, rammesjekk sekvenser for feilsjekk, felt som forteller om strømsparing er aktiv og enkelte andre indikatorer som om WEP brukes eller ikke.

4.1 - Administrasjonsrammer

Administrasjonsrammer gjør at nettkomponentene klarer å etablere kommunikasjonskanaler og ikke minst opprettholde dem. [ANSI/IEEE802.11-1999(R2003) 12 Juni 2003]

- **Autentifikasjonsrammer**. Autentifikasjon er beskrevet i seksjon 2.7.6. Denne rammetypen blir brukt når en AP aksepterer eller nekter identiteten av et radiogrensesnitt. Nettverkskomponenten begynner denne prosessen ved å sende en autentifikasjonsramme til AP, AP vil svare med en tilsvarende autentifikasjonsramme som indikerer om autentifikasjonen er godtatt eller avslått. Rammen inneholder felt som: Autentifikasjonsalgoritme nummer, transaksjonssekvensnummer, statuskode og utfordringsteksten om delt nøkkel metoden er brukt. [Gast 2005]

- **Avautentifikasjonsramme**. En avautentifikasjonsramme blir sendt til AP eller STA om den ønsker å avslutte kommunikasjonen. Rammen inneholder blant annet en årsakskode og kontrollfelt hvis sub type indikerer ulike administrasjonsrammer.

- **Assosiasjonsramme**. Assosiasjon er beskrevet i seksjon 2.7.3. Prosessen begynner ved at en STA forespør om å assosiere seg mot et AP. Denne forespørselsrammen inneholder informasjonsfelt som indikerer hvilket nettverk STA ønsker å melde seg inn i, SSID og hvilke datarater som er støttet. Disse feltene vil bli verifisert av AP for å sikre at parametrene stemmer mot nettverket.

- **Assosiasjonssvarramme**. Denne rammetypen benyttes som respons på foregående ramme. Ved en godkjennelse av assosiasjonen tildeles assosiasjonen en assosiasjons ID. Hvordan en assosiasjons ID tildeles er ikke spesifisert i IEEE 802.11 standarden. [ANSI/IEEE802.11-1999(R2003) 12 Juni 2003]

- **Gjenassosiasjonsramme**. Gjenassosiasjon er beskrevet i seksjon 2.7.4. Ulikheten mellom denne rammen og assosiasjonsrammen, er at forespørselsrammen inneholder adressen til stasjonens nåværende aksesspunkt. Dette bidrar til at det nye AP kokntakter den gamle AP og overfører assosiasjonsdataene. Gamle bufrede rammer ved en gamle AP vil også da bli overført. [ANSI/IEEE802.11-1999(R2003) 12 Juni 2003]

- **Gjenassosiasjonssvarramme**. Denne rammen er lik assosiasjonssvarrammen. Ulikheten er at sub type feltet i kontrollfeltet er annerledes enn hos assosiasjonsrammen.

- **Avassosiasjonsramme**. Avassosiasjon er beskrevet i seksjon 2.7.5. Om forbindelsen ønskes avsluttes, vil en denne rammetypen benyttes. Rammen er lik avautentifikasjonsrammen. Ulikheten er at rammekontroll feltet er forskjellig siden sub typen skiller mellom ulike typer administrasjonsrammen.

- **Avassosiasjonssvarramme**. Denne rammen er bare ulik assosiasjonssvarrammen, ved at sub type feltet i rammekontrollfeltet. Alle felt i denne rammen er obligatoriske.

- **”Beacon” ramme**. Et aksesspunkt vil periodisk sende ut denne typen rammer for å annonsere nettverkets tilstedeværelse. Dette muliggjør for STA å finne og identifisere et nettverk, ikke minst og synkronisere parameterne nødvendig for å melde seg på nettverket. Alle feltene er i denne rammen ikke obligatorisk, men blir tatt i bruk når nødvendig. [Gast 2005]

- **”Probe request” ramme**. Denne rammetypen blir benyttet når en STA ønsker å motta informasjon fra en annen STA. Dette for eksempel når STA ønsker å finne eksisterende 802.11 nettverk. Rammen innholder to felt: SSID og dataratene som avsender støtter.

- **”Probe response”** ramme. En STA vil svare med en slik ramme etter mottakelse av en ”probe request” ramme, og at de parametrene stemmer overens med nettverket. Videre vil en slik svarramme bære med seg parameterne i en ”Beacon” ramme. Dette muliggjør for STA å synkronisere seg til og melde seg på et nettverk. Herav så vil de samme reglene for ”Beacon” rammer, gjelde for ”probe response” rammer.

4.2 - Kontrollrammer

Kontrollrammer hjelper til ved leveranse av datarammer, ved å administrere tilgangen til det trådløse mediet.

- **”Request to send” (RTS) ramme**. Både RTS og CTS funksjonen reduserer eksisterende kollisjoner. RTS rammen blir benyttet til å ta kontroll av mediet for å sende store rammer. Størrelsen for hva som er stort, blir definert av RTS terskelen satt i nettverksdriveren. RTS rammen inneholder felt som: rammekontroll, varighet, mottaker og avsender adresser.

- **”Clear to send” (CTS) ramme**. Dette er responsrammen til RTS og gir tillatelse til den forespørrende part for å sende data ramme. Etter IEEE 802.11g ble ratifisert, ble CTS rammen også brukt som en beskyttelsesmekanisme for å unngå forstyrrelser for andre eldre STA. (REF IEEE 802.11g). Feltene er like som for RTS.

- **“Acknowledgement” (ACK) ramme**. Etter å ha mottatt en vilkårlig gyldig dataramme, vil mottakene part sende en positiv bekreftelse tilbake på datarammen. Dette for å detektere eventuelle feil. ACK rammer er for øvrig obligatorisk fra MAC laget for hver dataramme, annet enn de tilfeller hvor QoS forbedringer senker denne terskelen. Rammen inneholder felt for rammekontroll, varighet og mottaker adresse.

4.3 - Datarammer

Intensjonen bak WLAN er å transportere data. Datarammer bærer protokoll data fra høyere lag innenfor rammestrukturen. Hvilke felt som blir brukt avhenger av dataramme typen. Ulik data vil her bli kategorisert i forhold til funksjon. Det skilles her mellom fire ulike kategorier data for ulike tjenester: konfliktfri tjenester, konkurranse basert tjeneste, bærer av data og ikke bærer av data.

4.4 – Oppsummering

I dette kapitelet har vi gitt en oversikt over de mest vanlige rammetypene innenfor IEEE 802.11. Da altså ramme typer innefor:

- Administrasjonsrammer
- Kontrollrammer
- Datarammer

Hensikten er å gi et inntrykk over trafikktypene som går over et WLAN, og med hvilke typer rammer som administrerer og kontrollerer nettet.

5.0 – Sikkerhet i IEEE 802.11

Sikkerhet i WLAN er et emne som stadig diskuteres. Begrepet sikkerhet har hatt ulike tolkninger basert på tidsepoke og teknologisk fremgang. Under dataalderen ble det snakket om å bevare data, beskytte det og holde dataene hemmelig. I nyere tid har foretningskontinuitet og tilgjengelighet blitt en viktig diskusjon. Dette involverer å håndtere eventuelle avbrudd tjenester og at tjenesten faktisk er tilgjenglig for bruk.

Sikret aksess for utvalgte autoriserte personer, er et emne sterkt knyttet til sikkerhetstemaet i form av autentifisering, autorisering, aksesskontroll og tilgjenglighet. Derfor kommer dette kapitelet til å introdusere etablerte pilarer sikkerhetsdiskusjoner ofte er bygd opp rundt, for så å diskutere svakheter med WLAN sikkerhet. Videre introduseres enkelte scenarioer som er relevant til problemstillingen.

5.1 – Sikkerhet pilarer

Det er ikke i oppgavens hensikt å formelt beskrive data og nettverkssikkerhet. Baktanken er å gi en introduksjon til de pilarer som sikkerhetsdiskusjonene er bygd rundt. Dette tilfører en felles forståelse for begrepene når det senere diskuteres i sammenheng med WLAN.

5.1.1 – Integritet

Informasjon og data beveger seg gjerne over et åpent nettverk fritt for innsyn. For å sikre disse dataene er sikret mot manipulasjon, er en stor oppgave som gjerne er mer utfordrende når det kommer til trådløse nett. Data integritet i informasjonssikkerhet referer til følgende: ”Selve sikringen av at mottatt data er eksakt lik det som sendt av en autorisert entitet” [Stallings 28. November 2002].

5.1.2 – Konfidensialitet

Begrepet konfidensialitet referer til å sikringen av sendt data fra uønskede tredjepart. Altså: ”Data konfidensialitet er beskyttelse av data fra uautorisert innsyn.”[Stallings 28. November 2002].

5.1.3 – Ikke fornektelse

Etter at en bruker er autorisert og autentifisert vil det noen ganger være behov for et mekanisme som hindrer situasjoner hvor disputt kan oppstå. ”Ikke fornektelse gir beskyttelse mot at en av entitene i en kommunikasjon fornekter å ha deltatt i deler eller hele kommunikasjonen.” [Stallings 28. November 2002]. Kort fortalt vil dette bety av avsender ikke kan nekte å ha sent en gitt melding.

5.1.4 – Tilgjenglighet

Når det diskuteres sikkerhet i forhold til kommunikasjonsressurser, er intensjonen gjerne å sikre at tjenesten er pålitelig og har de nødvendige sikkerhetstiltak. Tilgjengelighet angår i hvilken grad ressursene er fungerende og i brukendes tilstand. Dette vil naturligvis være viktig siden det ikke er behov for å sikre aksess til ressurser som ikke oppfyller dets mening.

5.1.5 – Datavern

Datavern er ikke alltid en selvsagt emne å diskutere i sikkerhet. Datavern omhandler vern av innholdet dataene.

5.1.6 – Autentifisering

Oppgavens ordlyd sier ”Sikre enkelte autentifiserte personer...” Identifisering parten som ønsker sikret aksess vil derfor være viktig. ”Autentifisering er sikring av at den kommuniserende entitet faktisk er den han utgir seg for å være.” [Stallings 28. November 2002]. Hovedtjenesten autentifisering tar seg av, er å forsikre mottaker om at det mottatte data fra kilden er autentisk. IEEE 802.11 støtter flere ulike løsninger for sikker autentifisering ved hjelp av IEEE 802.1X.

5.1.7 - Autorisering

Når en entitet har autentifisert seg vil nest steg være å bli autorisert for ønsket ressurs. Det er her viktig å forstå den sterke forbindelsen mellom autentifisering og autorisering, og fortsatt se at det er to ulike tilstander. Autentifikasjon har med hvem du er, mens autorisering har med hva du har autoritet til å gjøre.

5.2 – Autentifikasjon og aksesskontroll

Et IEEE 802.11 nettverk vil annonsere seg til vilkårlige STA som kan lytte og motta ”Beacons” rammer. For å beskytte dette nettverket mot uønsket aksess, vil det være nødvendig med autentifikasjon og aksesskontroll. I WLAN vil det være fire ulike faser hvor det er naturlig å sikre aksesskontroll på.

- **STA autentifikasjon**. Kapitel 2.8 viste hvordan en STA melder seg på et BSS. Det første steget for å koble seg til et IEEE 802.11 nettverk, er å gjennomføre et STA autentifikasjon. Denne autentifikasjonsprosessen gjøre enten ved ”open system” autentifikasjon, delt nøkkel autentifikasjon eller ved MAC filtrering. Først nevnte er standard autentifikasjonsmetode for 802.11. STA sender en autentifikasjonsrammer til AP med sin egen ID, AP svarer med en ramme som indikerer om den gjenkjenner identiteten til STA. Denne metoden tilbyr nærmest ingen autentifikasjon. Administrasjonsrammene vil her bli sendt ut i klartekst selv om også WEP blir brukt. Delt nøkkel autentifikasjon avhenger av bruk av WEP som er beskrevet senere. MAC autentifikasjon dreier seg om å filtrere uautoriserte klienter ved bruk av MAC adresser. [Arbaugh and Shankar 30. Mars 2001]

- **Assosiasjon**. Etter overnevnte autentifikasjon, vil STA forsøke å tilknytte seg mot et aksesspunkt og etablere et virtuell nettverksport. I denne fasen eksisterer det ingen spesielle sikkerhetskomponenter, annet enn mulighet for MAC adresse filtrering.

- **Linklaget**. Når både autentifikasjon og assosiasjonen er blitt gjennomført, vil det være mulighet for å bruke linklag protokoller som 802.1X for å sikre autentifikasjon på det laget. Brukere som da ikke blir autentifisert, vil da bli kastet av nettverket.

- **Nettverk eller transportlaget**. Autentifikasjon og aksesskontroll på disse to lagene vil være på høyere nivå på OSI stakken. IP nettverk har en mengde ulike metoder å sikre autentifikasjon og aksesskontroll. Blant annet er det brannmur produkter og løsninger basert på VPN.

Når det dreier seg om WLAN og sikret aksess, diskuteres det for det mest på det fysiske og linklaget som beskrevet i kapitel 3.4. Sikkerhet burde også vurderes på høyere lag enn de to laveste nivåene når for eksempel en applikasjonstjeneste skal vurderes. Allikevel er det mest

interessant å prate om de to nederste lagene når sikret aksess på WLAN nettet er problemstillingen. Sikkerhetsarbeidet i WLAN har videre de siste årene stort sett dreid seg om å lage en sterke sikkerhetsmekanismer på linklag.

Per i dag, vil metodene under være de mest aktuelle for å sikre nettverket:

- **WEP autentifikasjon**. Ved delt nøkkel autentifikasjon, vil klienten søke nettverkstilgang ved å svare på en utfordring gitt av et aksesspunkt. Utfordringen vil da bestå av denne delte nøkkelen. En mer eksakt beskrivelse av WEP i ”802.11 Wireless Networks: The definitive guide” kapitel 5.0. WEP og WEP2 tilbyr liten sikkerhet etter at de ble påvist som usikker [Mishra and Arbaugh 6. Februar 2002].

- **MAC adresse filtrering**. De fleste aksesspunkter er i dag levert med mulighet for å skjerme mot ønskede klienter ved MAC adresse filtrering. Problemet med MAC adresse filtrering binder seg til at de både er enkelt å forfalske og administrasjonen av filtreringsadressene er vanskelig å vedlikeholde. Både denne og WEP autentifikasjon nevnes siden det er mange apparater i dag som ikke støtter noe sterke autentifikasjonsmetoder.

- **WPA/WPA2 ”Personal”**. Etter 2001 hvor WEP viste seg å være svært usikker, ble det arbeidet med forbedrede metoder. WPA ble laget som intermediær løsning under utviklingen av IEEE 802.11i, hvorav WPA2 implementerer den fullstendige IEEE 802.11i. Begge gir ved ”WPA og WPA2 personal” en forhånddelt nøkkel, som lar STA autentifisere seg mot et nettverk ved å angi kun et passord. Ved ”WPA og WPA2 Enterprise” benyttes EAP protokollen med flere ulike metoder innenfor den som: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PAEPv1/EAP-GTC og EAP-SIM.

- **802.1X protokollen (WPA/WPA2 ”Enterprise”)**. IEEE 801.1X krever autentifikasjon før brukeren slippes inn på nettverket. Denne identifikasjonen og autentifikasjonen baserer seg på ”Extensible Authentication Protocol” (EAP), og benytter seg av metodene som går over denne. De ulike metodene som går over EAP blir vist i tabell 2 kapitel 5..3.

5.2.1 – Skjuling av SSID

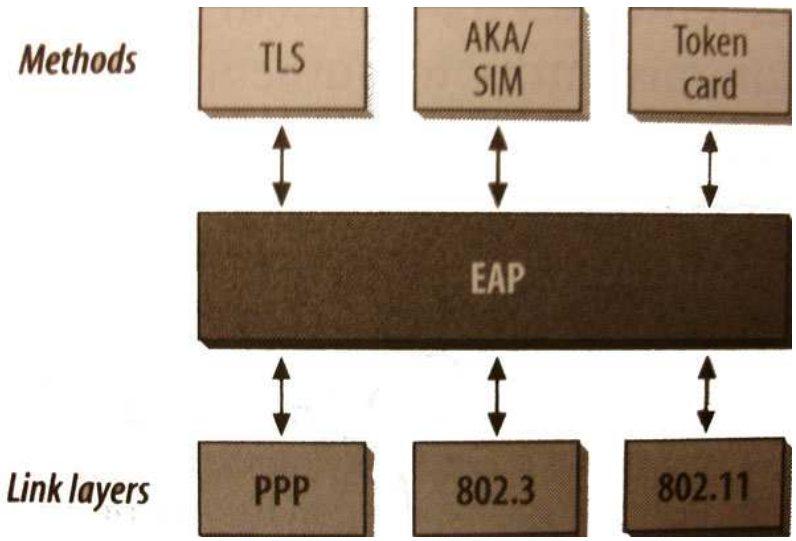
SSID skjuling av ”Beacons” rammer har tidligere vært et tiltak for aksesskontroll. Eldre IEEE 802.11 stasjoner var såpass primitive at de trengte å skanne eteren for ”Beacons” for en gitt

nettverksnavn før de kunne assosiere seg. Hensikten bak gjemmingen var da var at klienten ikke ville motta ”Beacons” fra aksesspunktet, og på den måten lukke nettverket for utenforstående. STA som ønsket å koble seg på, måtte sende ”Probe Requests” som inkluderte den riktige SSID. Denne metoden viser seg og ikke noen form for sikkerhet, først og fremst fordi ”Probe Request” ikke er kryptert og dermed blir lett å plukke opp fra eteren. [Gast 2005]

5.3 – 802.1X og 802.11i

WEP skulle tilby autentifikasjon og datavern, men viste seg å ikke kunne tilby noen av delene. Hovedproblemet med autentifiseringstrafikk er flere. Blant annet at rammer kan bil manipulert, autoriserte sesjoner kan bli kapret, og en tredjepersoner kan utgi seg for å være en del av nettverket å dermed stjele nettverksakkrediteringer.

IEEE 801.1X krever autentifikasjon før brukeren slippes inn på selve nettverket, og benytter seg av EAP metoder. De ulike metodene vises i tabell 2. 802.1X tilbyr en sterkere, bedre og mer fleksibel autentifikasjonsform, da det gjennomføres en brukerautentifikasjon fremfor maskinautentifikasjon som WEP. En slik løsning vil være langt bedre da brukerrettighetene følger brukeren og ikke maskin. Ikke minst så vil dette tillate en finere form for aksesskontroll siden brukere kan bli klassifisert og begrenset før nettverkstilgangen blir godkjent. Autentifikasjon ved EAP over IEEE 802.1X befinner seg for øvrig på MAC laget, som vist av illustrasjon i appendiks F.



Figur 8 – EAP arkitekturen [Gast 2005]

Autentifikasjonsprotokoll	Beskrivelse
MD5 utfordring	Autentifikasjon som CHAP i EAP
GTC	Tiltenkt brukt med token kort som ”RSA SecureID”
EAP-TLS	Gjensidig autentifikasjon med digitale sertifikater
TTLS	TLS med tunnel, beskytte svakere autentifikasjons metoder med TLS kryptering.
PEAP	Beskyttet EAP, beskytte svakere EAP metoder med TLS kryptering
EAP-SIM	Autentifikasjon ved mobil telefon og ”Subscriber Identity Module” (SIM)
MS-CHAPv2	Microsoft kryptert passord autentifikasjon

Tabell 2 – EAP metoder [Gast 2005]

Rammeverket for IEEE 802.1X blir nærmere i ”802.11 Wireless Networks: The definitive guide” kapittel 6 og i spesifikasjonene IEEE 802.1X rev.

Siden de fleste organisasjoner har en sentralisert brukerdatabase, benyttes en RADIUS server på baksiden av autentifikasjonsmekanismen for IEEE 802.1X. Denne RADIUS kan binde sammen flere brukerkonto systemer, og presentere det i en enkelt oversikt. Noe som vil være en fordel om organisasjonen har flere avdelinger, eller at flere ulike brukerkonto systemer må knyttes sammen for å sikre autentifikasjon.

IEEE 802.11i, også kjent som WPA2 ”Enterprise” bruker 802.1X som basis. Denne tilføyer flere sikkerhetsmekanismer for trådløse nettverk. Arkitekturen for denne standarden inneholder følgende komponenter:

- 802.1X for autentifikasjon. Er allerede beskrevet over og under kapitel 5.2.

- ”Robust Security Network Association” (RSNA). RSN blir definert som et nettverk som implementerer autentifikasjon og konfidensialitetsmetodene i IEEE 802.11i. Denne støtter

ikke bruk av WEP. RSNA etablerer en prosedyre for gjensidig autentifikasjon og nøkkel administrasjon. RSNA orden på assosiasjonene mot aksesspunktet.

- AES basert CCMP. ”Cipher Block Chaining Message Authentication Code Protocol” (CCMP), er en krypteringsprotokoll under IEEE 802.11i og ble utviklet for å erstatte WEP. Nøkkel administrasjon og meldingsintegritet blir tatt hånd om av CCMP. Videre så benytter CCMÅ seg av ”Advanced Encryption Standard” (AES) algoritmen. Verdt å merke seg at CCMP ikke krypterer eller autentifiserer administrasjons og kontrollrammer.

Disse komponentene er beskrevet i spesifikasjonene IEEE 802.11i og vil ikke bli noe videre utredet i dette dokumentet. Dette fordi det først og fremst er interesse for autentifikasjonsdelen, IEEE 802.1X, for å eventuelt sikre aksess for enkelte autoriserte brukere.

5.4 – Sikkerhetsproblemer i WLAN

Da de første IEEE 802.11 spesifikasjonene ble fremlagt, dreide sikkerhetsdiskusjonen seg rundt diskresjon av data som ble sendt over eteren. Det hadde da med feil krypteringsprotokollene som var brukt, og mangelen på en sterk metode for å gjennomføre bruker autentifikasjon [Gast 2005]. Tidligere har det blant annet vært for enkelt for en tredjepart å tyvlytte og eventuelt injisere et WLAN med uønsket trafikk. Mye har blitt forbedret med nyere protokoller som 802.11i og 802.1X. Allikevel er det flere andre svakheter som fører til problemer, deriblant mangelen på ramme autentifikasjon [He and Mitchell Februar 2005]. Mangelen på autentifikasjon på administrasjon og kontrollrammer fører til at det er vanskelig å sikre seg mot DOS angrep [Gavrilenko, Mikhailovsky et al. 28. Juni 2004].

Sikret aksess ved WLAN henger, som nevnt, i stor grad sammen med sikkerhetsdiskusjonen. En adekvat metode for å sikre aksess fordrer til at konfidensialitet, integritet og tilgjenglighet blir ivaretatt. Hvilke trusler som eksisterer vil således være interessant. ”…fra linklaget av et WLAN, er det tre mulige typer rammer: administrasjonsrammer, kontrollrammer og datarammer. Enhver manipulasjon av disse rammene som direkte eller potensielt utsetter data konfidensialitet, integritet, gjensidig autentifikasjon og tilgjenglighet vil være og regnet som en trussel.” [He and Mitchell Februar 2005]

Tabell 3 – Trusler mot trådløse nett [He and Mitchell Februar 2005]

Trussel	Trussel	Engelske begrep	Trusselen angår
1	**Passiv tyvlytting**	**Passive eavesdropping**	**Alle 3 rammer på linklag**
2	**Meldingsinjeksjon**	**Message injection**	**Alle 3 rammer på linklag**
3	**Meldingssletting og oppsnapping**	**Message deletion and interception**	**Alle 3 rammer på linklag**
4	**Maskrade og ondsinnet AP**	**Masquerading and malicious AP**	**Tilintetgjør gjensidig autentifikasjon**
5	**Sesjonskapring**	**Session Hijacking**	**Tilintetgjør gjensidig autentifikasjon**
6	**Mann i midten angrep**	**Man-in-the-middle-attack**	**Tilintetgjør gjensidig autentifikasjon**
7	**Tjeneste fornektelse**	**Denial of Service – DOS**	**Tilgjenglighet**

Fra artikkelen fra Stanford viser at bruk av 802.11i adresserer de truslene angitt i tabellen, minus tilgjenglighetsproblemet. Blant annet blir ikke kontroll og administrasjonsrammer krypterte eller autentifiserte av krypteringsalgoritmen på linklaget. Dette fører til sårbarhet, for eksempel, overfor ulike former for DoS angrep.

Konklusjonen til artikkelen er at det mulig å sikre integritet, data konfidensialitet og mot ”replay” angrep ved hjelp av CCMP på trussel 1,2 og 3. Det er ikke gjeldende for administrasjons og kontrollrammer siden de ikke blir kryptert eller autentifisert. Gjensidig autentifikasjon kan bli ivaretatt av EAP-TLS og en fireveis ”handshake.” Siden tilgjenglighet ikke er adressert i 802.11i foreslår artikkelen å faktisk autentifisere administrasjonsrammene [He and Mitchell Februar 2005].

5.5 – Tilgjenglighet av ressurser og WLAN sikkerhet

Det er nevnt flere ganger at det er løsninger på hvordan autentifisering, autorisering og konfidensialitet kan vedlikeholdes i WLAN ved hjelp av eksisterende protokoller. Et tema som hører med i diskusjonen og som ingen løsninger håndter fullt, er spørsmålet om

tilgjengelighet. En tjeneste har ikke noen videre verdi så lenge den ikke får fullføre sin påtenkte funksjon. Derfor er dette et emne viktig å diskutere i lys av problemstillingen.

Hindre tilgjengligheten av WLAN, er ikke spesielt komplisert. Trådløse nett bygger på radiogrensesnitter. På dette nivået, vil interferens være en naturlig del av miljøet den er ment å betjene. Dette kan være naturlige elementer fra naturens side som legger begrensninger eller mer kunstige som andre sterke radiosendere. Uansett vil dette påvirke tilgjengeligheten av nettet og kan i verste tilfeller fullstendig hindre tilgang. Dette karakteriseres som ”Denial of Service” og heretter DoS.

Mange av disse elementene må taes hensyn til og er kanskje mer av interesse under selve utbyggingsprosessen. I tillegg til mulige DoS fra aksesspunktets naturlig miljø, har sikkerhetsmiljøet bekymret seg over hvor svakt IEEE 802.11 er mot DoS angrep. De fryktet dermed ondsinnede forsøk på å hindre tilgjengeligheten av WLAN og hva det fører med seg. Det er avdekket flere måter på hvor enkelt DoS angrep kan utføres [Gohring 18. Mai 2004].

Bakgrunnen et DoS angrep kan være mangfoldig. Ofte utføres slike angrep som et ledd i en større inntregningsplan. Andre baktanker kan være av nysgjerrighet, ønske om teste sikkerheten, hevn fra en angriper for å ikke klare å komme inn på nettet, kommersielle årsaker eller politiske grunner. IEEE 802.11 kjerneprotokollen og radiogrensesnittet gjør det vanskelig å sikre seg mot lag 1 og enkelte lag 2 angrep.

I sammenheng med nød og beredskap kan det være kritisk at ressursene er tilgjengelig.
Når sikret aksess vurderes realisert med 802.11 nettforbindelser, kan det være hensiktsmessig å beskrive problemene å til slutt konkludere hvilke implikasjoner det har.

5.5.1 – PHY Laget

Blokkering på det PHY laget er som nevnt over ikke spesielt vanskelig. Det er lite å gjøre med blokkeringer forårsaket av for eksempel mikrobølgeovner annet enn å detektere dette, spore opp og løse problemet. Dette gjelder også utstyr som hjemmeprodusert spesifikt med hensikt å blokkere tilgang ved å spy ut fiktivtrafikk med høyeffekt over kanalene. Denne oppsporingen kan i flere tilfeller også være svært vanskelig [Gavrilenko, Mikhailovsky et al. 28. Juni 2004]. Sistnevnte type angrep med hjemmelaget utstyr er dessuten tidkrevende, kan være kostnadsmessig dyrt for en angriper.

Videre viser det seg at implementasjon med IEEE 802.11 DSSS har noen flere noen fundamentale problemer når det kommer til DoS angrep [Bellardo and Savage August 2003]. ”The Clear Channel Assessment” (CCA) benyttes av DSSS protokollen for å sjekke om en WLAN kanal er ledig. ”Et angrep mot denne svakheten utnytter CCA funksjonen på det fysiske lag og fører til at alle WLAN noder innenfor rekkevidde, både klienter og aksesspunkter, venter med å sende data for perioden angrepet varer. Under angrep vil enheten oppføre seg som om kanalen alltid er opptatt over det trådløse nettverket” [AUSCERT 13. Mai 2004].

Problemet har vært diskutert og enkelte leverandører indikerer at eneste løsning vil være å gå over til 802.11a som benytter en annen modulasjonsteknikk [Brewin 17. Mai 2004]. ”Uavhengige leverandører har bekreftet at det ikke er noen forsvar mot denne type angrep for DSSS baserte WLAN” [Brewin 17. Mai 2004].

Det interessante med dette angrepet er at den gjelder for alle implemtasjoner som benytter DSSS. Dette vil bety ved bruk av 802.11b og ved mikssituasjoner hvor 802.11b og g i miks situasjoner. 802.11g vil også være affektert av dette problemet når den benytter DSSS i hastigheter under 20 Mbit/sek. I forhold til høyeffekt sendere som er dyre, vil dette la seg gjennomføre med billig utstyr funnet i butikken og lamme WLAN utstyr innefor det typiske rekkevidden for slikt utstyr. Således vil det lett være mulig å øke denne rekkevidden ved bruk av antenneforsterkere.

Alvorlighetsgraden av et slikt angrep på PHY laget kan også diskuteres. Siden dette først og fremst rammer aksesspunkter innenfor rekkevidden av blokkeringsutstyr, vil ikke hele nettverket falle ned. Allikevel kan det være alvorlig nok når det kommer til kritiske tjenester som nød og beredskap og brukte aksesspunktene er angrepet. Dette er dermed et problem som må taes høyde for og videre vurdere om det er akseptabelt.. En løsning kan være å detektere og fjerne slike angrep. Deteksjonen vil da være nødt å bli gjort av sensorer som er separate fra aksesspunktet for å kunne registrere signalene sendt fra en angripende part. Dette fordi aksesspunktet ikke vil kunne registrere slik angrepstrafikk. [Gohring 18. Mai 2004].

5.5.2 – MAC laget

Sikkerhetsarbeid opp mot IEEE 802.11 protokollen har som nevnt ikke hatt fokus tilgjenglighetstemaet. IEEE 802.11i mangler for eksempel kryptering og autentifikasjon på kontroll og administrasjonsrammer. Dette fører til vanskeligheter å sikre tilgjengelighet på dette laget.

Blant de mer kjente DoS angrepene her er falske avassosiasjons og avautentifikasjonsmeldinger. Slike angrep fører til at STA som er assosiert og autentifisert til en AP blir droppet fra AP og dermed nettverket. Problemet var oppe til diskusjon under utviklingen av IEEE 802.11i, men løsningen med å autentifisere autentifikasjons og avassosiasjonsmeldinger ble aldri innlemmet i den endelige standarden.

Videre er et annet kjent angrep å forfalske innholdsfeil i autentifikasjonsrammer. Dette angrepet er basert på at en angriper utgir seg å være en annen klient for å sende en forfalsket autentifikasjonsramme med feil i innholdet. En autentifikasjonsramme type 2 blir sendt til AP med destinasjonsadresse til gjelden AP og kilde adresse til den forulempede STA. Sekvens nummer og statuskode blir begge satt til 0xffff. Resultatet er at AP sender den forulempede klienten en ramme med feilmeldingen: ”Received an authentication frame with authentication sequence transaction sequence number out of expected sequence.” [Gavrilenko, Mikhailovsky et al. 28. Juni 2004] Dette fører til at den aktuelle klienten avassosierer seg og oppfører seg deretter ustabilt ved å skape problemer med gjenassosiering og vilkårlige kanal hopping. [Gavrilenko, Mikhailovsky et al. 28. Juni 2004]

Andre DoS angrep som ofte blir nevnt er: overbelaste buffere og autentifikasjonsbuffere i AP, DoS angrep baserte på enkelte konfigurasjoner i WLAN og angrep på 802.11i implementasjoner. Disse angrepene er går inn for å være av mer teoretisk art. Uansett illustrerer disse eksemplene at det er vanskelig å sikre tilgjengligheten i WLAN med de eksisterende protokoller.

5.6 – Oppsummering

I dette kapitelet har vi sett på sikkerheten i WLAN. Det er gitt grunnleggende introduksjon til begreper innenfor klassisk sikkerhet som:

- Integritet
- Konfidensialitet
- Tilgjenglighet
- Ikke fornektelse
- Datavern
- Autentifikasjon
- Autorisering

I sammenheng med denne prosjektrapporten ønsker vi først og fremst å se på nettverkssikkerhet opp mot WLAN. I dette tilfellet vil det så være opp mot sikret aksess for utvalgte autoriserte brukere. Med andre ord vil vi først og fremst være interessert i mulige metoder for å autentifisere brukerne og hvilke faser det er viktig å autentifisere. Det har også vært fokus på hva eksisterende sikkerhetsløsninger per i dag ikke bidrar med, fremfor å utrede hver enkelt sikkerhetsprotokoll og metodene under dem. Allikevel vil det være verdt å nevne at en fullverdig tjeneste for nød og beredskap, vil kreve en mer fullstendig sikkerhetsutredning hvor de klassiske begrepene over også er dekket.

Det viser seg ellers at sikkerhet ved STA autentifikasjonsfasen er veldig svak. Sikkerhetsmekanismene på dette stadiet er faktisk ikke sterkt overhodet. Det er strengt tatt to muligheter bestående av WEP og MAC filtrering. Ingen av metodene er ideelle siden WEP siden 2001 har vært påvist å være usikkert, og MAC filtrering fordrer til administrative utfordringer i tillegg til at det kan forfalskes. Disse er allikevel tatt med i vurderingen siden enkelte av dagens klientapparater, som enkelte IP telefoner, ikke støtter noe sterkere metoder. En kombinasjon av begge disse metodene blir også vurdert til svakt. Uansett så vil en autentifikasjon ved begge disse typene være en form for maskin og ikke bruker autentifikasjon.

Videre viser det seg at linklag autentifikasjon ser ut til å være en langt sterkere løsning. Dette tilatter at brukeren blir identifisert, og en fullverdig tilgang på nettverket blir heller ikke gitt før brukerautentifiseringen er gjennomført. En identifikasjon av brukerne i stedet for maskin, vil dessuten tillate en større gradering mellom ulike brukere. Et slikt linklag autentifikasjons protokoll er IEEE 802.11i.

I kapitel 5.4 viser det seg at IEEE 802.11i adresserer en rekke problemer med WLAN sikkerhet. Allikevel har ikke fokuset vært rettet mot tilgjenglighet under utviklingen av IEEE 802.11i. Mangelen på autentifikasjon og kryptering av administrasjons og kontrollrammer, fører til problemer med å sikre tilgjengligheten. Dette gjør WLAN svakt i forhold til DoS angrep, noe som vil være svært viktig i forhold til sikret aksess. Muligheten for et alternativt kommunikasjonsnett vil være null, så fremt det ikke er tilgjengelig. Derfor har kapitelet beskrevet problemet videre med tilgjenglighet i WLAN.

En oversikt over IEEE 802.11 sikkerhetselementer vil være å finne i appendiks F.

6.0 – Diskusjon og analyse av problemstillingen

Tidligere kapitler har gitt en oversikt over IEEE 802.11, MAC laget, rammetypene og sikkerhet bundet til WLAN. I dette kapittelet diskuterer en rekke punkter problemstillingen gir. Et gjenblikk på problemstillingen vil være på sin plass.

"Under unormale situasjoner kan det være nødvendig å sikre et utvalg autoriserte personer tilgang til teleressurser. Dette kan f.eks. ordnes ved at disse har terminaler med spesielle id-er som gir prioritert tilgang i visse tilfelle.

I oppgavene skal man diskutere og studere forskjellige løsninger for slike problemer i en WLAN sammenheng. Man kan ta utgangspunkt i et nett likt det som skisseres for Trådløse Trondheim (basert på IEEE 802.11 standarden) og vurdere hvordan viktige personer/terminaler kan gis sikret aksess under f.eks. alminnelige nødssituasjoner og erklærte beredskapssituasjoner[2] - I samarbeid med faglærer kan oppgaven eventuelt utvides til også å dekke WiMAX og/eller UMTS(inkl. GSM)."

Av problemformuleringen ønsker vi å finne en eller flere løsning som diskuteres i forhold til å sikre aksess for et utvalg autoriserte personer. I henhold til dette kommer dette kapitelet til og diskuterer og analysere problemstillingen noe videre fra det som allerede er gitt av kapitel 1. Målet er å gi et grunnlag for hvilke type løsninger som blir valgt å se nærmere på.

Kapittel 1.4 snevret problemstillingen inn mot sikret tilgang på WLAN aksessnettet. Videre definerte seksjon 1.1.4 tre ulike målsetninger for denne prosjektrapporten.

I. Se om og hvordan det er mulig å gi sikret aksess
II. Om IEEE 802.11 er egnet til slikt bruk
III. Hvordan kan dette realiseres i WLAN nett likt Trådløse Trondheim

[2] Med en erklært beredskapssituasjon menes en situasjon som er definert av en myndighet, f.eks. politimesteren i en by (studenten behøver ikke detaljere hvem som skal definere denne situasjonen). I dette tilfelle kan det gå en melding til nettverksoperatøren som kan iverksette (via " Network Management" funksjoner en omlegging av nettets funksjoner)

6.1 – Hensikt

Hensikten er som nevnt i problemstillingen, å sikre autoriserte personer tilgang til kommunikasjonsressurser under nød og beredskap. Det disktures mulige løsninger for hvordan dette kan oppnås ved hjelp av IEEE 802.11 i senere kapitler. Gevinsten ved en slik mulighet, er en større sikkerhet under krisesituasjoner. Ved brudd på mobiltelefonisystemet eller kopperkabler, vil dette nettverket være uavhengig av de tradisjonelle infrastrukturene og dermed fortsatt være operativt. Personer som betjener viktige samfunnsmessige posisjoner, for eksempel ordfører osv., vil da ha mulighet til å benytte WLAN nettet som et alternativt kommunikasjonsnett hvor de er sikret aksess under nød og beredskap.

6.1.1 – Hvem har behov for å være autoriserte brukere

Dagens separate radiosamband i politiet, brannvesenet og helsevesenet bygger i dag på gammel analog teknologi som i liten grad tilfredsstiller operative og sikkerhetsmessige krav [Nødnett 13. Oktober 2005]. Derfor initierte Justisdepartementet Nødnett prosjektet som skal gjøre nødnettet digitalt og landsdekkende [Halvorsen 27. Februar 2006].

Politi, brannvesen og helsevesen har bruk for sikret aksess til teleressurser. Disse representerer en andel hvor det er kostnadsmessig bærekraftig å realisere et eget separat landsdekkende nødnett. Noe Nødnett prosjektet i seg selv viser. Andre etater med lignende behov er for eksempel Jernbaneverket som realiserer nødnettet sitt ved GSM-R.

Selv med nødnettene, med separat infrastruktur fra alminnelig offentlig mobiltelefoni, kan det i de mest ekstreme situasjonene være behov for alternativ aksess til teleressurser. Eksempler på dette er om infrastrukturen til nødnettene er satt ut av spill. Derfor vil det være hensiktsmessig å koordinere og vurdere andre kommunikasjonsnett, slik de eventuelt kan inngå i et bredere dekningsnett for nød og beredskap.

WLAN har begrenset med dekningsområde, og er som oftest begrenset lokalt til en by. Eksempler på dette er Trådløse Trondheim og andre ”Community Networks.” Hensikten med problemstillingen i dette prosjektet er ikke å erstatte noen av de nevnte nødnettene, men derimot være et bidrag og klarlegging av nød og beredskap ved bruk av WLAN. Mulighet for sikret aksess med WLAN kan være et alternativ der hvor det ikke er like kostnadsmessig bærekraftig med eget nødnett, men allikevel ha behov for sikret aksess. Dette er gjerne mennesker som betjener viktige lokaleposisjoner under krise og unntakstilstander. Eksempler

på slike, er mennesker innefor grupper som kommunen, Statens Veivesen, kommunale vannverket, trafikksentraler, fylkesmenn, bilbergningstjenester, Statens strålevern, offentlige transportmidler osv. Videre vil en slik mulighet åpne for at WLAN nettet kan integreres i nød og beredskapsnett i bredere forstand.

Siden det først og fremst dreier seg om mennesker som innehar viktige posisjoner i samfunnet, vil ikke det bli tatt hensyn til sikret aksess for ordinære nødsamtaler til nødnumre.

6.2 – Hvorfor er det problematisk med sikre aksess i WLAN

IEEE 802.11 standarden baseres på rekkevidde og signal for valg av hvilke aksesspunkt som den tilknyttes. Standardene angir ikke noen metode for klienten å skille mellom hvilke AP som har nettverkskapasitet ledig. I et trådbasert nettverk, vil det være mulig å kontrollere hvor mange klienter som faktisk er knyttet til en svitsj. På standard IEEE 802.11 basert nettverk, vil ikke det ikke være mulig å kontrollere hvor mange klienter som forsøker å bruke en gitt aksesspunkt. Dette fører til problemer når mange brukere forsøker å bruke det samme aksesspunktet samtidig.

WLAN er per i dag begrenset stort sett begrenset til 54 Mbit/sek. I tillegg til dette vil man være avhengig av atmosfæriske og siktforhold. Dersom mange brukere benytter det samme aksesspunktet på samme gitt tid, vil de oppleve en voldsom hastighets redusering i tillegg at nettet ikke responderer til tider.

Tjeneste differensiering med IEEE 802.11e, tilbyr tjenesteklassifisering og QoS. Dette kan til en viss grad sikre kapasitet blant tilkoblede brukere. Allikevel tilbyr ikke denne noen styring i forhold til antall klienter som kan påkobles aksesspunktet. QoS vil heller ikke bli diskutert noe videre da dette etter avtale med veileder ble enighet om å droppe.

Underkapitel 1.1 forteller at under krise og beredskapssituasjoner, kan oppstå press på kommunikasjonsressurser. Dette vil dermed gjelde spesielt for WLAN som kommunikasjonsnett. For å oppfylle mulig metode for sikret aksess, er det dermed nødvendig å se på metoder å begrense antall klienter tilkoblet et aksesspunkt. Klientene som tillates å være tilkoblet i en nød og beredskapssituasjon, vil da tilhøre et utvalg autoriserte personer i kraft av deres posisjon i samfunnet. Dette vil altså bety å skape løsninger som sikrer

autentifikasjon og aksesskontroll på fysiske og linklag, for å sikre at de nødvendige brukerne får tilgang.

6.3 – Beredskapsstatus – Hvorfor

En hendelse må kunne identifiseres som nød eller beredskap, for at resten av omverden skal reagere på situasjonen deretter. WLAN nettverket er avhengig å vite om situasjonstilstanden, før det blir prinsipielt riktig å differensiere mellom de ordinære og utvalgte autoriserte brukere. ”Sikret aksess” burde dermed kun være tilgjengelig i de tilfeller hvor situasjonen tilsier at det nødvendig. Når en nød og beredskapsstatusen blir erklært i nettet, vil det på en eller annen måte forstyrre for vanlige WLAN brukere. For eksempel ved at allmenne brukere har lite eller ingen tilgang. Således vil det være hensiktsmessig at en myndighetsinstans, som har mulighet til å anerkjenne situasjonen og behovet, er det organet som forespør netteier om nød og beredskapsstatus blir satt i det aktuelle nettverket.

Radiogrensesnittet til IEEE 802.11 har ikke et spesielt stor dekningsområde, typisk en hundre meter med standardutstyr og i frisikt. Dette kan kompenseres ved enten et såkalt ”Mesh nettwork” eller kombinere flere aksesspunkter i et ESS. WLAN bruker allikevel ikke å dekke over store avstander. Den korte rekkevidden per. AP gjør det ikke spesielt kostnadseffektivt å dekke større områder med en mengde Wi-Fi aksesspunkter.

Trådløse Trondheim vil i første omgang få WLAN dekning i sentrum, campuser og enkelte traseer. Myndighetsinstansen som eventuelt forespør at status blir satt i nettet, vil som nevnt være nødt til å kunne identifisere situasjonen og behovet for sikret aksess. I tilfellet lik Trådløse Trondheim, vil det nødvendigvis være en instans med nærhet til situasjonen. En lokal myndighet som politi vil da være nærliggende, da de allerede har en utøvende myndighet fra før. I tilfeller hvor det er en storkrise, kan det være nødvendig at en enda høyere instans har mulighet til å ta over dette ansvaret fra den lokale myndighet. Hvilke myndighetsinstans som ivaretar denne oppgaven er allikevel ikke i fokus i denne omgang og vil dermed ikke bli diskutert noe videre.

I innledende kapitler ble det fastslått at det allikevel var flere grupper personer i kraft av sin funksjon, som kan ha behov for sikret aksess. Nød og beredskap eksisterer i ulik grad av

alvorlighet. Av den grunn, vil det være lite optimalt å ekstingvere alle teleressurser ved en liten hendelse. Således vil det være hensiktsmessig å dele nød og beredskap inn i flere båser.

6.3.1 – Nød og beredskapsnivåer

I den mest ekstreme grad kan det være nødvendig å gi eksklusiv tilgang til autoriserte personer for å ha mulighet til å løse de oppståtte problemene. En krisesituasjon fører til enorm press på eksisterende ressurser og det dermed ikke er ønskelig at vanlige WLAN bruk skal forstyrre pågående arbeid for å løse krisen. I slike situasjoner vil det sannsynligvis være et større antall personer som ønsker seg mulighet for sikret aksess. Disse må ha mulighet for eksklusiv tilgang så lenge infrastrukturen til nettet fortsatt eksisterer og er operativt.

Det hører med sjeldenheten at slike ekstreme situasjoner oppstår. Ofte vil situasjoner enten være lukket rundt et enkelt område eller at krisen generelt er begrenset. Da er det verken nødvendig, økonomisk eller optimalt at alle ressursene blir forbeholdt. Dette siden det sannsynligvis vil være kapasitet ledig. I tilfeller hvor nødssituasjonen er begrenset, burde det derfor være mulighet for ordinære brukere fortsatt kan være tilkoblet. Dog kanskje ha tilgang i noe mindre grad. De utvalgte autentifiserte brukerne vil også her ha første prioritet aksess.

Denne rapporten foreslår da i tilfeller to ulike grader for nød og beredskap:

- Erklært beredskapssituasjon. Full krise – Eksklusivt tilgang og sikret aksess. Dette betyr at ordinære brukere som er tilkoblet aksesspunktet ønskes ut av nettet. Situasjoner likt dette er store naturkatastrofer, terrorhandlinger og krig.

- Forhøyet nødssituasjon. Ingen stor krise, men allikevel behov for sikret aksess. Her vil vanlige brukere fortsatt være tilkoblet, men tilgang til nettet vil på så måte være begrenset. Situasjoner som kan kreve denne tilstanden, er for eksempel større ulykker.

Ytterligere lavere nivåer ansees foreløpig ikke som nødvendig, siden en helt ordinær nødssituasjon antageligvis ikke involverer gruppene nevnt 61.1. Det taes allikevel forebehold, slik at flere nivåer kan være nødvendig. Allikevel er det disse to nivåene som vil bli diskutert og forsøkt løst i senere kapitler.

6.4 – Autentifikasjon ved IEEE 802.1X tilstrekkelig?

Seksjon 6.2 viser at det er fire faser hvor det er naturlig å føre autentifikasjon og aksesskontroll ved: STA autentifikasjon/assosiasjon, linklaget og nettverkslaget. Det er allikevel slik at sikkerhet på høyere lag er avhengig av sikkerhet på lavere lag. I tilfellet WLAN er det først og fremst interessant med autentifikasjon og aksesskontroll på de to nederste lagene. Dette vil bety STA autentifikasjons/assosieringsfasen og linklaget.

Ved første fase viser seg det seg at det kun eksisterer tre ulike metoder: ”Open System”, delt nøkkel og MAC filtrering. Ingen av disse er adekvate i en autentifiseringsprosess, men kan mulig inngå som et ledd i en større autentifikasjonsprosess.

På linklaget, er det i tidligere kapitler beskrevet at autentifikasjon, kan bli ivaretatt av IEEE 802.1X og ulike EAP metoder. Valg av EAP metoder ved eksisterende løsninger, må basere seg på hvilke type klienter som skal tilknyttes nettverket fremfor metode. Det viser seg at de fleste operativsystemer og klientapparater støtter IEEE 802.1X, minus enkelte eldre IP telefoner. Hvilke EAP metoder som støttes er allikevel svært annerledes apparat til apparat.

På bak enden av autentifikasjonen, benyttes en RADIUS server for å binde sammen brukerkonto systemet.

6.5 – Tilgjenglighet en nødvendighet?

Kapitel 6 viser at autentifikasjon av brukeren i seg selv ikke er tilstrekkelig for å sikre aksess. For å oppnå mulighet for sikret aksess må nødvendigvis hensynet til tilgjenglighet vurderes. Dette siden det ikke er mulig å sikre aksess til et WLAN, så fremt nettet ikke er tilgjenglig.

På det fysiske nivået, vil interferens fra naturlige omgivelser er det vanskelig å ta høyde for. Radiobølger lar seg lett forstyrre av andre sterke signaler. Dette kan forstyrre så mye at det i praksis kan kategoriseres som DoS angrep. Støykilder kan også bli generert av en tredjepart som beskrevet i seksjon 5..5.1. Samme seksjon beskriver en metode som utnytter CCA funksjonen ved DSSS protokollen.

Ingen av de nevnte problemene er selvsagt ønsket i noen form når det kommer til tilgjenglighetsspørsmålet. For at nettet skal ha verdi som nød eller beredskapsnett, vil det derfor være nødvendig og kalkulere om dette er akseptabelt. Løsningen for problemene kan være å detektere mulige støykilder, og løse dem fortløpende med egne sensorer som regisserer slike støykilder eller forsøk på bruk av CCA. For støykilder i miljøet vil det også være mulig å identifisere faste støykilder allerede ved implementasjon.

Videre skulle IEEE 802.11i representerer en sikkerhetsmekanisme for MAC laget, og som skulle sikre integritet, konfidensialitet og tilgjenglighet. Riktignok tilbyr standarden integritet og konfidensialitet, men tilgjenglighetsspørsmålet viser seg å ha blitt utelatt. Noe ulike undersøkelser viser [He and Mitchell Februar 2005]. Seksjon 5.5.2 beskriver mulige DoS angrep som det også burde taes høyde for.

6.6 – Andre generelle egenskaper

Tidligere i dette kapitelet har gitt en dypere forståelse av problemstillingen og hvilke utfordringer som ligger til grunn. Seksjonene under vil angi andre egenskaper som er ønsket i en mulig løsning.

Rapporten her dreier seg i all hovedsak om å sikre autoriserte personer tilgang til ressurser allerede ved aksessnettet. Rapporten forutsetter at det allerede eksisterer en velfungerende backbone eller et annet netteverk som tar for seg den videre forbindelsen ut av aksessnettet. Det vil derfor være viktig at det trådløse aksessnettet integreres godt mot eksisterende nettverk, og at dette aksessnettet lar seg administrerer eller styre av et sentralt styringsobjekt. Ikke minst så må sikkerheten være i varetatt. Videre må styrkene ved trådløst aksess være ivaretatt slik at de ikke blir lidende ved ønsket om sikret aksess.

6.6.1 – Mobilitet og portabilitet

Trådløse nett og bevegelsesfrihet er sterkt knyttet sammen. Portabilitet gir brukeren mulighet for tilgang til nettkobling fra flere lokasjoner og de fysiske barrierer mellom terminal og nettet. Dette gjør det enkelt for brukere å flytte på terminalen mellom flere ulike lokasjoner. Derimot gir ikke portabilitet muligheten til å beholde forbindelsen når terminalen er under bevegelse. Mobilitet fjerner på sin side enda flere barrierer og gjøre det mulig å holde nettverksforbindelsen aktiv under flytting.

Portabilitet og mobilitet er to sentrale funksjoner som under diskusjonen i størst mulig grad bør være tilstede.

6.6.2 - Integrasjon mot eksisterende nettverk

Løsningene som diskuteres burde kunne integreres mot eksisterende nettverk. Dette er viktig av flere årsaker, blant annet at det ikke er spesielt hensiktsmessig å måtte redesigne hele nettverkstopologien på bakgrunn av problemstillingen. I motsatte tilfellet vil løsningen være vanskelig å få innført i eksisterende nett. Videre er det dessuten mer hensiktsmessig å kunne administrere et integrert nettverk.

I forhold til Trådløse Trondheim prosjektet, vil nødvendigvis ha mange aktører som tilbyr tjenester. Aktørene har sine egne nettverkselementer eller nettverk. En løsning vil derfor være mulig å kunne integreres opp mot disse aktørene.

6.6.3 - Klientstøtte

Aksessnettet må kunne ta imot alle typer klienter uavhengig av operativsystem, så lenge den støtter 802.11 grensesnittet.

6.6.4 - Administrasjonsmuligheter

Når det oppstår en nød og beredskapssitasjon, må status kunnes settes i nettverket. Dette må kunne bli administrert fra sentralt hold. Det samme må gjelde bruker administrasjonen.

6.6.5 - Nettnøytralitet

Det amerikanske organet ”The Federal Communications Commission” (FCC), det norske ekvivalente Post og teletilsynet, ustedet et ”policy statement” som en veiledning på hvordan nettnøytralitet kan beholdes. Dette for å oppmuntre til bredbåndsdekning og ivareta samt fremme den åpne og kontaktfremmede natur som det offentlige Internett har, gir man sin tilslutning til at følgende prinsipper følges:

1. Forbrukerne skal sikres aksessrett til lovlig innhold på Internett etter eget ønske

2. Forbrukerne har rett til å bruke programvare og tjenester etter eget ønske, under hensyntagen til legale krav om begrensninger eller virkemåte.

3. Forbrukere skal ha fritt valg med hensyn på hvilke terminalutstyr de bruker, så lenge dette ustyret er lovlig (i følge gjeldende regelverk) og ikke forårsaker skade i nettet.

4. Forbruker har rett til (å erfare) konkurranse mellom nettoperatører, applikasjons- og tjenesteytere og innholdsleverandører.

I problemstillingen diskuteres det å sikre aksess på kommunikasjonsresurser på et WLAN. WLAN representerer en type aksessnett, og disse prinsippene burde derfor bli tatt i følge i en løsning. I appendiks E er det referanse til original dokumentet.

6.7 – Oppsummering

Dette kapitelet har sett på ulike sider ved problemstillingen og gitt enkelte retningslinjer på hva vi ønsker å finne frem til. Emner som:

- Hvem har behov for å være blant de utvalgte autoriserte brukerne
- Sikret aksess i forhold til WLAN
- Hvorfor sette beredskapsstatus og hvilke nivåer
- Om det er tilstrekkelig med autentifisering for å sikre aksess
- Generelle egenskaper som ønskes innlemmet i en løsning

Del konklusjonen for kapitelet er at IEEE 802.1 tilbyr adekvat sikkerautentifisering på linklaget. IEEE 802.1X er dessuten relativt vidt støttet blant dagens operativsystemer. Dessverre så tilbyr ikke IEEE 802.11i god nok sikkerhet i forhold til tilgjenglighetsproblemet. Sikret aksess har liten verdi så fremt nettverket i seg selv ikke er tilgjenglig. Således vil det være nødt til å diskuteres hvordan tilgjenglighet kan vedlikeholdes i nød og beredskapssammenheng.

Når det kommer til å sette status i nettet, blir to tilstander definert. Erklærte beredskapssituasjoner og forhøyet nødssituasjoner. En løsning vil være nødt til å antyde hvordan tilstandene kan settes.

Videre nevner kapitlet andre generelle egenskaper som burde vurderes i en løsning. Dette er egenskaper som:

- Integrasjon mot eksisterende nettverk
- Mobilitet og portabilitet
- Klientstøtte
- Administrasjonsmuligheter
- Nettnøytralitet

Neste kapitel vil således se på mulig løsninger for å begrense hvilke klienter apparater som får lov til å koble seg til aksesspunktet. Dette vil da muliggjøre sikret aksess til selve aksesspunktet.

7.0 - Mulige løsninger for autentifikasjon og aksesskontroll

IEEE 802.11 tilbyr ingen metode å kontrollere hvor mange eller hvilke klienter som kan aksesspunktet. Sett i lys av problemstillingen, kategoriseres alternativene i inn i tre: Det spesialiserte alternativ, eksisterende alternativ og standardisere alternativer. Grunnlaget for å dele mulighetene inn i kategorier, er å få en mer presis struktur for diskusjonen.

Det proprietære alternativ vil eksempelvis være en spesial produsert apparat. Apparatet vil ha en eller flere egenskaper som gjør at den klarer og identifiserer brukeren eller enheten, og som dermed gir sikret aksess. Det eksisterende alternativet, vil da bygge på eksisterende utstyr og muligheter som allerede foreligger ved standarder. Den siste delen som kan være interessant, vil være å sette krav til eksisterende spesifikasjoner som tillatter å sikre aksess på en standardisert måte.

Problemstillingen uttrykker at ulike løsninger ønskes studert og diskutert. Først og fremst vil rapporten se på muligheten av sikre aksess ved å bruke eksisterende løsninger eller modifikasjoner av denne. Videre diskuteres også mulige proprietære løsninger. Resultatet fra disse diskusjonene vil skape et grunnlag for en konklusjon hvor det eventuelt spesifiserer om mulige krav som kan fremsettes til et standardiserings arbeid.

7.1 - Proprietære løsninger

Spesial produserte enheter har fordeler nettopp ved at den er spesialisert i forhold til funksjon. Således vil det være mulig å spesifisere og realisere enkelte funksjoner som ellers er vanskelig. Gitt av hvordan WLAN teknologisk fungerer, vil dette nødt til å være støttet av både AP og STA.

Ulempene knyttet generelt til en proprietærløsning kan være mange. Norge med sin begrensede befolkning kan det å produsere spesialapparater i lite antall være dyrt. Om en slik løsning skal være økonomisk bærekraftig, må nedslagsfeltet for bruk av denne løsningen være større enn kun gjelde i Norge eller et spesifikt WLAN nett. I bruk for nød og beredskap vil situasjonen å vurdere nytte i forhold til kost.

7.1.1 – Bruke apparater som operer utenfor vanlig frekvenser i WLAN

Det er her for eksempel mulig å skissere en løsning hvor en enhet opererer som alle andre enheter til vanlig, men har en ekstra kanal tilgjenglig i tillegg til de kanalene og frekvenser som er vanlige for WLAN apparater. Når unntakstilstand blir satt i nettet, de vanlige kanalene sperret og den ekstra kanalen åpnet, vil apparatet ha mulighet til å bruke den ekstra kanalen som de vanlige enhetene ikke har. På denne måten vil kun enheter, som har den spesifikke kanalen, fortsatt ha aksess. Dette gir også en mulighet til å kaste ut de vanlige brukerne under krisesituasjoner.

En slik løsning krever blant annet at aksesspunktet må kunne operere i denne nye kanalen. Noe som vil være en svært tiltaksrikk og dyr affære når nettet blir dekket av en mengde aksesspunkter.

WLAN ustyr operer i område fra 2400 – 2483.5 MHz og 5470 – 5725 MHz [NPT 20. desember 2000]. Dette er å regne som frie frekvensområder. Ordinært WLAN nett tilbyr som regel dets tjenester over IEEE 802.11b/g og da altså 2.4GHz båndet. Ut fra kanallisten for WLAN utstyr i appendiks C viser at en eventuelt bruk av ny kanal innefor 2.4 GHz, da må eksistere som et mellom steg innefor eksisterende kanaler. Således vil enhver bruk av frekvenser innenfor 2.4GHz området, medføre til overlappende kanaler med de eksisterende. Egen interferens mellom kanalene er da svært uønsket, da det allerede er nok interferens å ta hensyn til ved tilgjenglighetsspørsmålet.

Ved utnyttelse av løsningen under nød og beredskap, kan det dog hende at myndighetene ser blidere på bruk utenfor nevnte frekvensområder. Allikevel er ikke dette ønskelig i WLAN sammenheng, siden det både bryter med eksiterende praksis og frekvensbåndet da blir dårlig utnyttet.

Videre er diskusjonen om hvilke personer som burde være autentifiserte for sikret aksess, blitt tatt med bakgrunn av funksjonen personen representerer. En løsning som beskrevet over vil være å autorisere aksess i egenskaper av apparatet. Kun en identifikasjon av apparatet, vil heller ikke bety det samme som en identifikasjon av brukeren. Dette vil skape et sikkerhetsproblem om apparatet blir stjålet og tyveriet ikke blir registrert i tide. Kjennskap til

hvilken kanal som benyttes, vil da også gi tilgang til nettet. Derfor er det ved en slik løsning viktig å også autentifisere brukeren ved bruk av for eksempel IEEE 802.1X.

Det vil videre alltid være et spørsmål om det er bærekraftig å realisere en slik proprietær løsninger på grunn av administrasjon, vedlikehold, oppdateringer av slike spesialapparatene kontra en standard apparat. I sammenheng med problemstillingen i denne rapporten, vil sannsynligvis de utvalgte autentifiserte brukerne allikevel kreve en viss administrasjon, vedlikehold og oppdateringstjeneste. Allikevel ansees løsninger av denne art som lite realiserbart blant annet fordi aksesspunktene da også må modifiseres.

7.2 – Standardisere alternativer

Et siste alternativ som er mulig er å bidra til standardarbeidet innefor den riktige gruppen. I tilfellet hvor det ikke er en tilsynelatende løsning med eksisterende spesifikasjoner, kan det være hensiktsmessig å stille krav og foreslå endringer eller tilføyelser til eksiterende standarder. Arbeidet frem til at en tilføyelse blir vedtatt er krevende, og det vil også gå en periode før leverandører og kunder både gjør seg kjent og implementert de nye spesifikasjonene.

Dette kan være av akademisk interesse å se på hvordan dette lar seg løse. Slikt arbeid er som nevnt tidkrevende og tidsperspektivet til denne rapporten blir for kort til å fullføre et slikt prosjekt. Prinsippet er allikevel at noen må sette krav for at muligheten for at en standardisert løsning noen gang skal la seg realisere. Konklusjonen for denne prosjektrapporten vil antagelig gi en indikasjon om dette er nødvendig. Det er uansett viktig å ha denne muligheten åpen, da dette kan være en god mulighet.

7.3 – Eksisterende alternativer

En annen mulighet er å benytte eksisterende sikkerhetsløsninger til å realisere muligheten for sikret aksess under nød og beredskap. Ettersom WLAN teknologien har modnet, har det kommet på plass flere sikkerhetsløsninger som adresserer svakhetene ved de tidlige IEEE 802.11 spesifikasjonene. Det eksisterer i dag ulike kombinasjoner av sikkerhetsløsninger som i grader kan løse autentifisering og sikkerhetsproblemer knyttet til sikret aksess. Blant annet

adresserer IEEE 802.11i og IEEE 802.1X i grader dette. Aksesskontrollen er allikevel et tema som forblir problematisk.

Dette underkapitelet ønsker å se på mulige løsninger i forhold til å gi AP kontroll på hvilke apparater som får lov til å koble seg til aksesspunktet.

7.3.1 - Bruke ubenyttede kanaler

Et alternativ er å bruke standardapparater som kan operere i en kanal eller frekvens som ikke brukes i Norge og Europa. En slik løsning vil da unngå enkelte ulemper knyttet til eksempelet gitt under det proprietære alternativ, og benytte seg av eksisterende utstyr. På samme måte vil det her også være nødvendig å autentifisere brukerne av samme årsaker.

I frekvenstabellen for IEEE 802.11 i appendiks C, viser at IEEE 802.11b/g ustyr i Norge og Europa opererer på kanal 1 til 13. Japan benytter derimot en kanal 14 på 2484 MHz i tillegg til de vanlige kanalene. Dokumentet fra NPT, viser også at bruk på 2484 MHz i Norge er å regne som fritt frekvensbånd [NPT 20. desember 2000]. Muligheten er å benytte utstyr som støtter kanal 14 og unytte denne ekstra kanalen. Det er her også å forstå at europeisk utstyr har mulighet til å ”firmware” oppgraderes til å støtte kanal 14.

Løsningen er allikevel lite aktuell siden aksesspunkter som er organisert som i Trådløse Trondheim, hvor det er flere aksesspunkter som kan overlappe, har behov for å operere på ulike kanaler. Dette fordi at det vil oppstå egeninterferens i de områder hvor det benyttes like frekvenser og hvor aksesspunktdekningen overlapper hverandre. Dermed vil det være behov for to kanaler som er ulike og ikke overlappende. Etter gjeldende standard vil det da være nødvendig å skape en ny og ikke eksisterende kanal i tillegg til å ta i bruk kanal 14. Dermed vil diskusjonen havne i samme spor som på det proprietære alternativet.

7.3.2 - MAC adressefiltrering/WEP/SSID i kombinasjon med IEEE 802.1X

I kapitel 5.2 beskrev at både at WEP var regnet som usikkert etter 2001, skjuling av SSID og MAC adressefiltrering ikke ga noen stor sikkerhetsgevinst. Allikevel vil en kombinasjon av disse tre gi det beste et grunnlaget, basert på eksiterende løsninger, for sikkerhet på PHY laget

Det antaes at et WLAN nett likt Trådløse Trondheim, baserer autentifisering på andre metoder enn WEP, skjult SSID og MAC adressefiltrering. Om alle tre inkorporeres avhenger av valg gjort i forhold til konfigurasjon og struktur på nettet i sammenheng med nød og beredskap. Det er her mulig at det er nødvendig å lage et eget parallelt nett spesifikt for nød og beredskapssammenhenger. Eventuelt at et eksisterende nett setter på de tre sikkerhetsmekanismene ved endret status fra normal til nød eller beredskap.

Sikkerheten ved WEP og skjult SSID er lav, og ikke minst kronglete å benytte. Dette fordi brukeren eventuelt må huske på en WEP nøkkel som må inntastes, det samme gjelder SSID. Det ønskes helst at en slik løsning unngåes. Dermed vil det gjenstå en mulighet for MAC adresse filtrering som aksesskontroll og benyttelse av IEEE 802.1X som autentifikasjonsprotokoll.

De fleste aksesspunkter leveres i dag med mulighet å MAC filtrere adresser ved STA autentifikasjon og assosiasjon. Det vil si at det gir en mulighet for å programmere hver AP med en liste over MAC adresser som er tillatt nettverksaksess. I utgangspunktet er dette en lite brukt metode siden MAC adresser er enkelt og forfalske og kopiert. Som beskrevet i kapitel 5.2, binder det seg også administrative utfordringer ved vedlikehold av slike lister. Nyere WLAN svitsjer tillater dog en sentralisert form for MAC adressefiltrering. Således vil det være mulig å vedlikeholde MAC adresselister fra sentralt hold.

Ved erklærte beredskapssituasjoner vil netteier ha mulighet til å be alle aksesspunkter å koble inn MAC adressefiltreringen etter å ha avassosiert eksisterende allmenne brukere. Således vil kun de apparatene med gyldig MAC adresser fortsatt ha tilgang eller mulighet for aksess til WLAN nettet.

Som nevnt over og i kapitel 5.2, tilbyr ikke MAC adressefiltrering noen god sikkerhet. Derfor er det nødvendig å autentifisere og benytte eksisterende sikkerhetsmekanismer på linklaget, for å sikre ytterligere tilgang.

7.3.3 - Apparater med eget ID

Et apparat med eget ID som nevnt i problemstillingen, kan også være et alternativ. På samme måte som MAC så kan denne identifikasjonen være en del av apparatet, eller som en tredjepartssikkerhetsløsning som RSA SecurID.

RSA SecurID i sammenheng med EAP ikke tilby noen kontroll på PHY laget, da EAP metodene befinner seg på MAC laget. Spørsmålet vil være om det er mulig å bruke en slik ID for å identifisere apparatet på PHY laget. Uansett vil en slik identifikator, tredjeparts eller inkorporert i apparatet, være relativt lett å kopiere og forfalske på samme måte som MAC adressen. En angriper kan tvinge en STA å avassosiere, slik at STA under autentifisering og assosiering må utveksle denne identifikatoren. Dette er mulig siden verken administrasjons og kontrollrammene blir kryptert på dette nivået. Således vil det ikke være noen hensikt og utrede dette alternative noe videre. Dette siden MAC adressefiltrering vil tilby en ekvivalent form for sikkerhet. MAC adresser har den fordelen at alle nettverkskort har det innprentet i seg fra fabrikk.

Derimot vil en spesiell identifikator på apparatet være en mulig løsning på datalinklaget. Uansett vil det på dette laget, ha flere andre metoder som kan være interessante. Valg av EAP metode ved bruk av IEEE 802.11 vil eventuelt være avhengig av hvilke klient apparater og tjenester som blir tatt i bruk. Ved mobiltelefon, er det da også mulig å benytte EAP-SIM som identifikator. Valg av apparat eller spesifikk tjeneste, som IP telefoni eller video, er ikke en del av denne prosjektrapporten.

Uansett vil en implementasjon av IEEE 802.1X være lik her som i 7.3.2. Gevinsten ved den spesielle identifikatoren, er at den kan benyttes slik at brukeren slipper å manuelt identifisere seg. På denne måten kan denne løsningen kombineres med løsningen nevnt i 7.3.2.

7.4.4 - Modifisert PCF

I en forhøyet nødssituasjon ønskes det at brukerne fortsatt skal ha mulighet til å være tilkoblet et aksesspunkt, men allikevel at utvalgte autoriserte brukere skal kunne ha første prioritet. Derfor kan PCF funksjonen interessant å se på siden den tilbyr en sentralisert styringsfunksjon som beskrevet i underkapitel 3.2, og samtidig gir mulighet for konkurransefri levering. PCF funksjonen er ikke spesielt hyppig implementert i aksesspunkter, og vil derfor være av teoretisk interesse. Det antaes derfor at aksesspunktene, og apparatene til de som skal ha sikret aksess, har denne funksjonen implementert.

Et mulig scenario er at PCF funksjonen tiltrer i det den forhøyet nødssituasjonen blir satt i nettet. For at dette skal skje, må alle STA tilknyttet aksesspunktet oppdatere sin NAV på

begynnelsen av en CFP. CFP perioden blir satt i gang når Alle STA vil adlyde denne orderen. Dette vil alle STA gjøre siden PCF reglene baserer seg på DCF. Aksesspunktet blir konfigurert til kun å spørre stasjoner som støtter PCF. For oppnå mulighet til at kun de autoriserte brukerne skal sende under CF periodene, vil aksesspunktet måtte tildele ekstra lange perioder hvor datarammer suksessivt kan sende fra den enkelte STA.

En løsning av denne slag avhenger av at aksesspunktet må vite hvilke STA den skal forespørre. I vanlig PCF modus vil dette være tilfeldig fra en listen aksesspunktet holder oden på. Etter endt PCF periode, hvor STA ikke har mer og sende. Sendes det en ramme som avslutter CF perioden, noe som fører til at vanlige brukere igjen vil ha tilgang.

7.4 – Oppsummering

I dette kapitelet har vi diskutert mulige løsninger innenfor proprietære løsninger og mulige metoder ellers. Proprietære løsninger, så vidt denne rapporten ser det, tilføyer få sikkerhetsgevinster annet enn om de skulle operere på egne kanaler. En løsning hvor et apparat har mulighetene til å operere på egne kanaler er ikke spesielt egnet av flere årsaker.

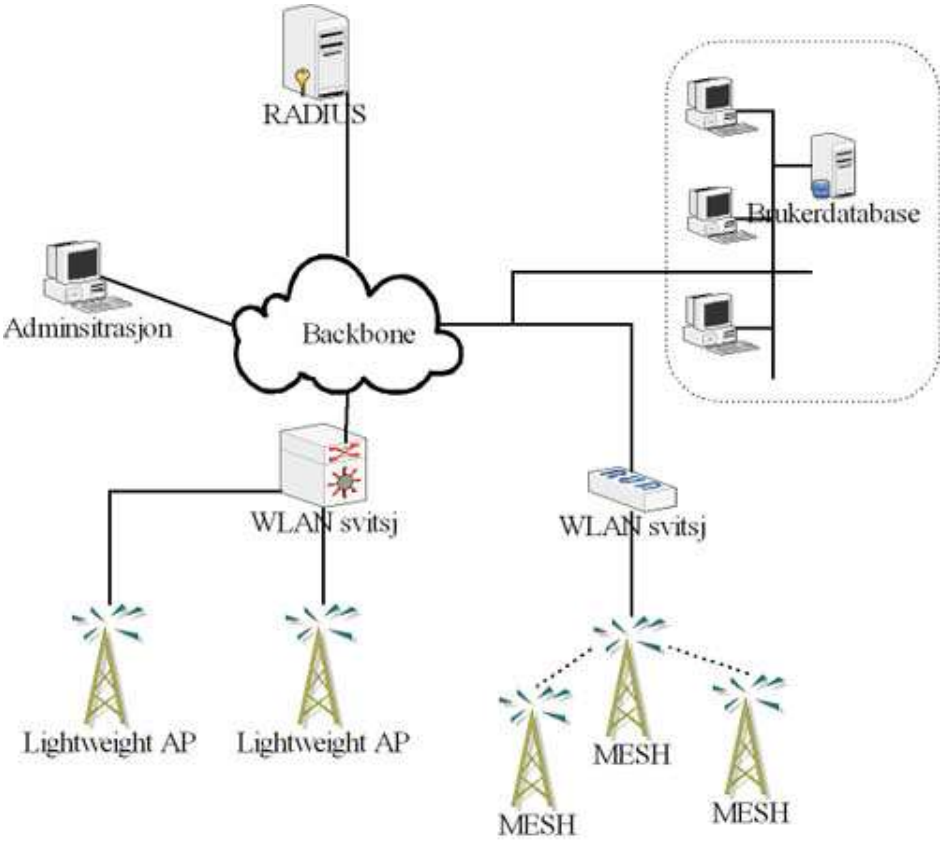
Andre mulige løsninger kan involvere en kombinasjon av MAC adressefiltrering, WEP og skjult SSID. WEP og SSID skjuling er av både praktiske årsaker og at de ikke tilbyr store sikkerhetsgevinster, unnlatt. MAC adressefiltrering gjenstår da som et mulig alternativ i kombinasjon med IEEE 802.1X.

Heller ikke apparater med spesielle identifikatorer som problemformuleringen foreslår, gir noen gevinst i forhold til aksesskontroll på PHY laget. Derimot kan en slik løsning være aktuelt på datalinklaget og muligens kombineres med MAC adressefiltrering. Løsningen er såpass lik MAC løsningen, at bruken vil så å si tilsvare hverandre.

8.0 – Løsningene i et nett likt Trådløse Trondheim

Dette kapitelet ønsker å se hvordan det er mulig å implementere løsningene diskutert i kapitel 7, og realisere sikret aksess ved WLAN nettet, i et nett likt Trådløse Trondheim.

Trådløse Trondheim er pågående prosjekt hvor Midtbyen, busstraseene opp til Dragvoll og alle campuser får WLAN dekning innen 15. august 2006. Dekningskartet finnes i appendiks D. På grunn av at det er et pågående prosjekt og at det eksisterer veldig få arbeidsdokumenter, kan WLAN nettet som vurderes i forhold til sikret aksess avvike ganske kraftig fra faktiske utførsel. Et mulig alternativ er som vist på figur 9.



Figur 9 – Mulig arkitektur

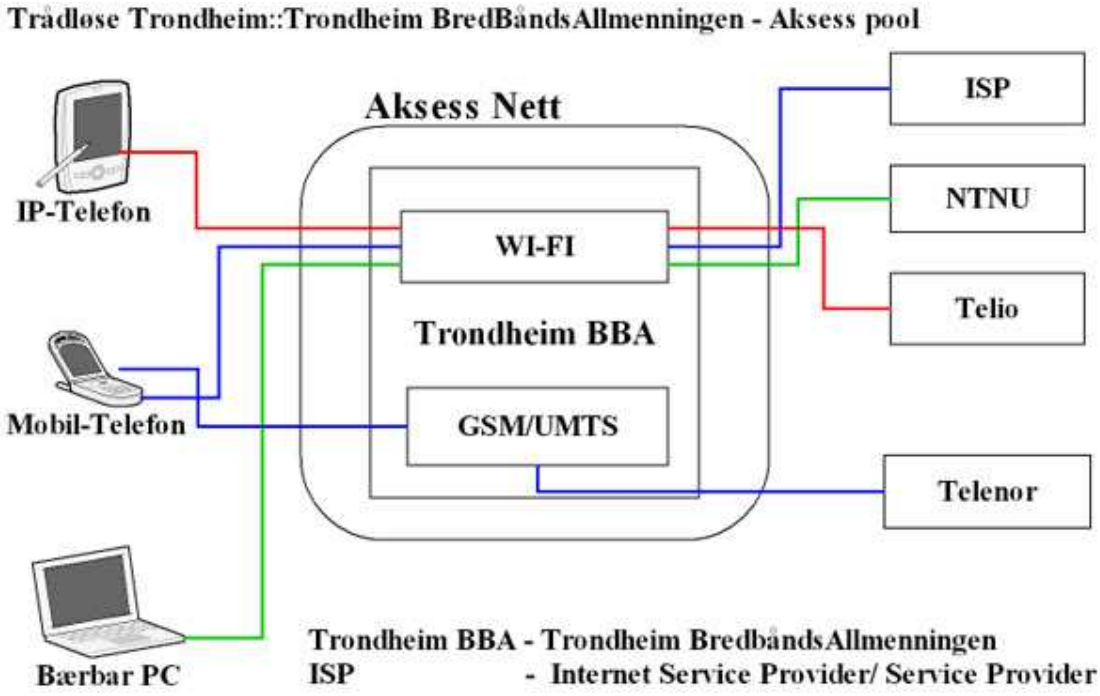
Figuren 4 viser et WLAN nettverk, hvor ene er basert på to tynnklienter som er tilknyttet en WLAN svitsj. Videre er det et mesh nettverk hvor to aksesspunkter er trådløstbundet til et aksesspunkt med forbindelse til backbone. Nettverket administreres av en sentralt objekt og autentifikasjon skjer ved hjelp av en RADIUS server. Backbon-et er også tilknyttet et eksternt nett hvor en brukerkontosystem er tilknyttet.

8.1 - Logisk arkitektur

En logisk arkitektur vil alltid ha styrker og svakheter. Valg av arkitektur burde derfor gjenspeile eventuelle ønsker. Videre vil det være naturlig at WLAN nettet har flere ulike klasse brukere med forskjellige behov og ønsker. Dette vil være nødvendig å ta hensyn til.

Kapitel 1.3 gir bakgrunn for hvorfor og hvilke ønsker som oppnåes ved å realisere Trådløse Trondheim. Dette er grunnleggende ønsker som skal gjøre Trådløse Trondheim til en forskerarena i kombinasjon hvor kommersielle aktører kan tilby sine tjenester. Utfordringen ved et slikt nett er store.

Trondheim BredBåndsAllmenningen (Trondheim BBA) er en av komponentene i Trådløse Trondheim. Dette er et eksperimentelt trådløst bredbåndsnett bestående av flere teknologier, hvorav WLAN nettet er en. Trondheim BBA kan dermed tenkes på som en aksesspool, hvor brukerne får tilgang til ulike tjenester avhengig av kundeforholdet. Her involveres det altså brukere fra ulike ISP-er. En oversikt på et slikt arkitektur vises i figur 10. Denne arkitekturen vil således gi mulighet å ta hensyn til nettnøytralitet, da ISP selv eventuelt ikke eier aksessnettet.



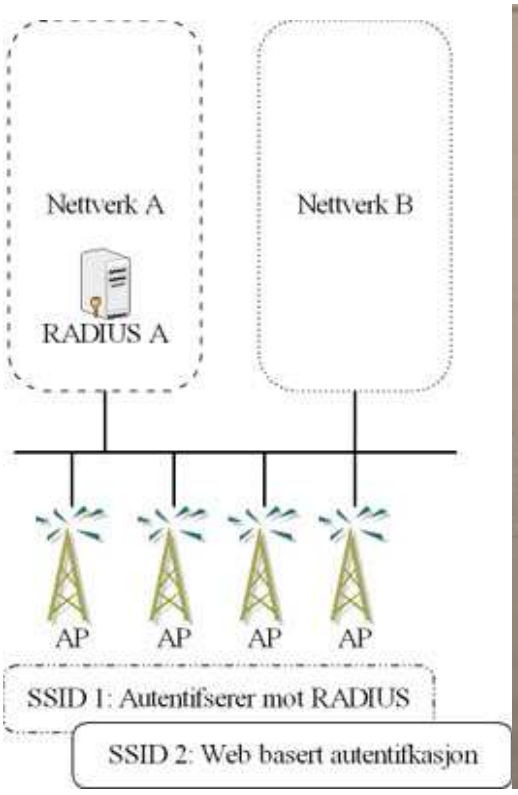
Figur 10 – Trondheim BredbåndsAllmenningen

Innenfor aksesspoolen finner vi WLAN nettet. Dette nettet vil være bestående av en mengde aksesspunkter som på en eller annen måte er sammenknyttet via et backbone. Fra dette backbone vil det eventuelt gå ut til forskjellige ISP-er.

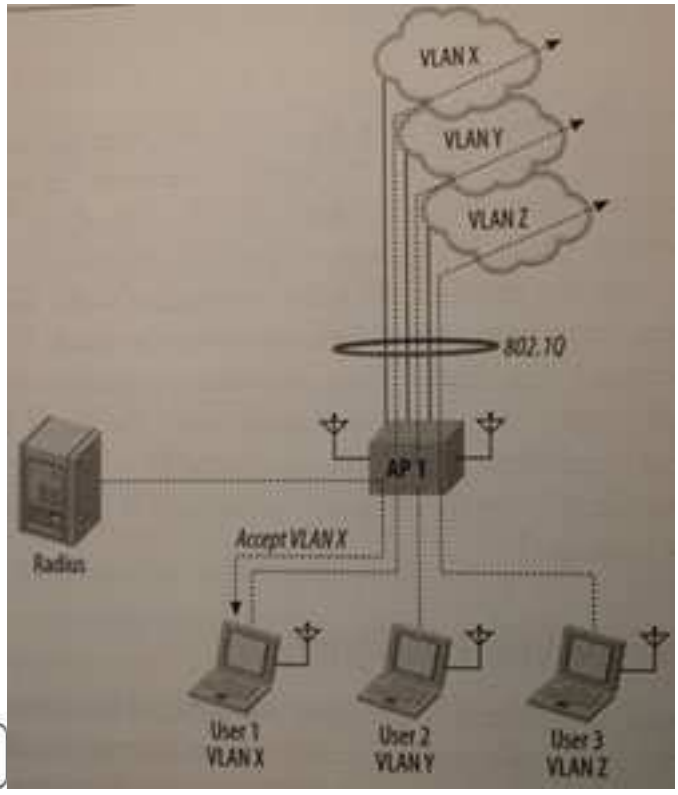
For å skille mellom forskjellige operatører i aksesspoolen, krever det at flere logiske arkitekturer blir lagt parallelt. Dette kan oppnåes ved å benytte seg av virtuelle aksesspunkter for å simulere flere fysiske nettverk, som illustrert i figur 11. På denne måten vil netteier fungere som felles bærer og transittnettverk mot andre nettverk tilknyttet.

Innfor dette det enkelte nettverk vil det være mulig å skille forskjellige brukerklasser med ulike behov ved hjelp av EAP over IEEE 802.1X og dermed la ulike brukerklasser få tilgang til ulike VLAN. Eksempel på dette er illustrert i figur 12. Figur 13 eksempel på EAP over IEEE 802.1X

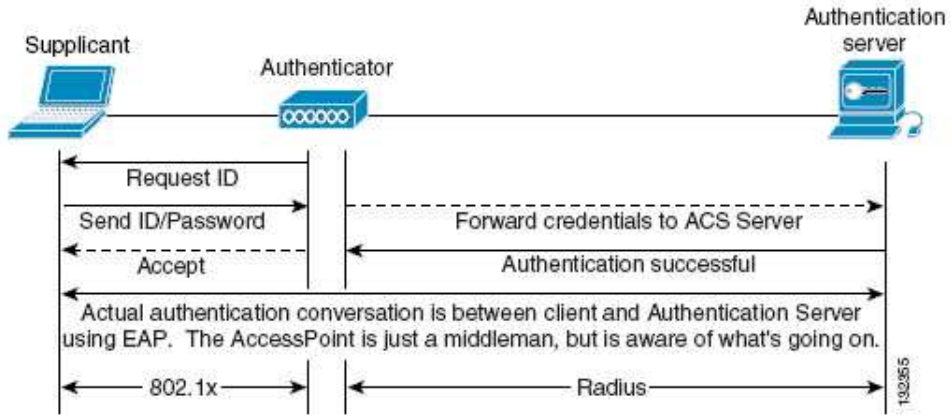
Benyttelse VLAN på denne måten bidrar også til øket mobilitet siden STA ikke lenger fysisk trenger å være bundet mot samme subnett.



Figur 11 – Virtuelle aksesspunkter [Gast 2005]



Figur 12 – Dynamisk VLAN [Gast 2005]

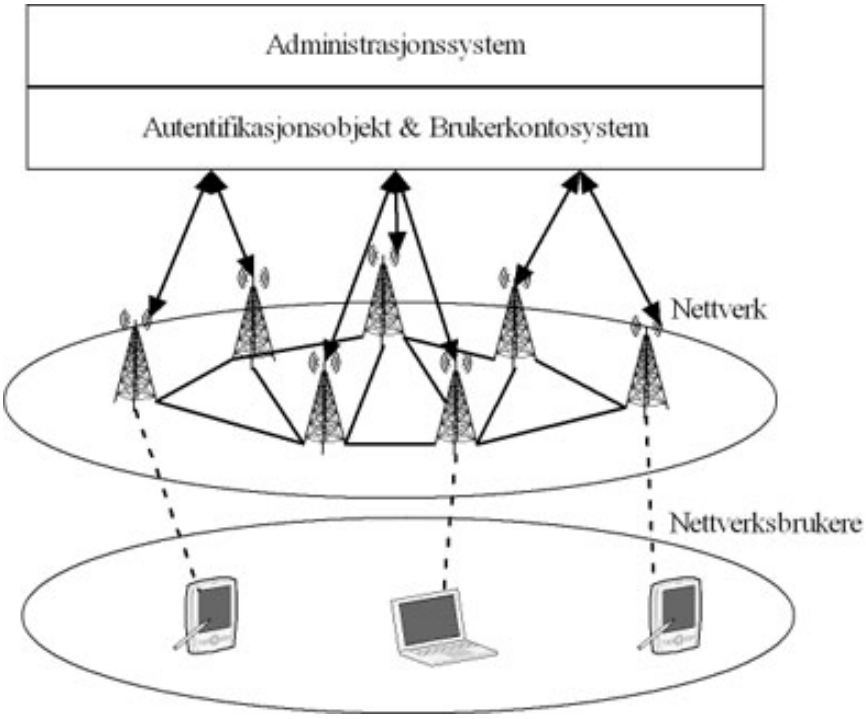


Figur 13 – IEEE 802.1X/EAP autentifikasjon [Cisco 2005]

8.2 – Hvordan sette status i nettet

Felles for alle løsningene diskutert i kapitel 7, er at status i nettet må settes før noen kan benytte seg av sikret aksess til WLAN nettet. En mulighet for å realisere dette, kan være å ha et sentralt administrasjonsobjekt som kontrollerer hele WLAN nettet. Fra dette objektet hos netteier, vil det være mulig å definere de to ulike statusene: Erklært beredskap og forhøyet nødssituasjon. Figur 8 illustrerer dette konseptet.

Når statusen er satt i administrasjonssystemet, vil objektet være nødt til konfigurere alle aksesspunkter til å følge de operasjoner som blir gitt under de ulike løsningene. Siden beredskapsstatusen er noe som blir definert i denne oppgaven, vil eventuelle løsninger bli programmert opp mot administrasjonsgrensesnittet. En manuell konfigurasjon av basestasjonene vil ikke være spesielt effektivt.



Figur 14 – Dynamisk styringsobjekt for beredskapsstatus og administrasjon

8.3 – Autentifisering

En arkitektur kan tillate at forskjellige brukere ved hjelp av IEEE 802.1X ka bli tilknyttet ulike VLAN. For hver av disse vil det også være mulig å benytte ulike EAP metoder[Gast 2005].

I forhold til autentifisering, foretrekkes EAP over IEEE 802.1X og en RADIUS server på baksiden. Dette er fordi dette er den mest brukte autentifiseringsmetoden i WLAN, og dermed er problemer god kjent. Hvilken EAP metode som benyttes vil avhenge av både hvilke muligheter klienter tillater.

Om det i denne rapporten antar at en ”Smartphone” med støtte for IEEE 802.1X benyttes, vil EAP-SIM kanskje være en mulighet å benytte. Denne løsningen vil i så tilfellet basere autentifiseringen på SIM kortet/smart chip-en.

Ulempen med slike smart chip/SIM løsning, vil nok være at SIM kortet kan bli stjålet eller mistet mens telefonen er pålogget. Således vil det være mer hensiktsmessig å benytte en EAP metode som autentifiserer ved brukernavn og passord. Klassiske problemer bundet til det er at passordet er for kort og enkelt. Ikke minst vil et stadig bytte av passordet, for eventuelt å

opprettholde høyest mulig sikkerhet, føre til at brukeren ikke husker passordet når behovet melder seg.

Andre muligheter er å bruke kombinasjoner av sertifikater og supplere med brukernavn og passord. Dette fordrer til at en god ”Public Key Infrastructure” (PKI) blir opprettet. Om en slik PKI struktur kan opprettes for kun nød og beredskapsnett, kan dette være en meget god løsning. Nøkkeldistribusjonen vil da som alltid være en utfordring.

8.3 – MAC adressefiltrering i kombinasjon med IEEE 802.1X

Under erklært beredskap ble det ønsket å føre aksesskontroll med MAC adresser for å filtrere ut klienter som ikke var ønsket assosiert. For å få til dette burde MAC adressene være kjent på forhånd, og lagt inn i et brukerkontosystem for de utvalgte personene som skal være autoriserte. Dette vil være mulig å gjennomføre siden brukerne i et slikt nett må gjennom gå opplæring. Således vil antagelig apparatene være innkjøpt for formålet, noe som øker sannsynligheten for at en vist administrasjonsdel eksisterer uansett.

Etter at beredskapssituasjonen blir erklært i nettet, vil aksesspunktet gå fra normal modus, uten MAC adressefiltrering, til beredskapsstatus med MAC filtrering på. Et nett likt skissert som i kapitel 8.1, vil statusen virke for de virtuelle aksesspunkter og således VLAN nettet også.

En parallellprosess med dette, er at alle STA som ikke har MAC adressen inne hos autentifikasjonsserveren vil bli avassosiert fra aksesspunktet. I de tilfeller hvor STA allerede er assosiert og autentifisert, vil forbindelsen holdes såfremt MAC adresselisten er tilgjenglig fra selve aksesspunktet. Ved motsatte tilfeller og hvor en STA ønsker å koble seg opp mot aksesspunktet, vil MAC adressen bli sjekket mot det lokale registeret før det eventuelt blir henvist videre til autentifikasjonsserveren.

Antagelig vil det være vanskelig for en bruker å beholde assosiasjonen når MAC adresselisten aktiveres. Listen vedlikeholdes og lagres sentralt i denne løsningen, og dermed vil det eventuelt være en distribusjonsfunksjon som kan lage duplikater av denne listen ute hos aksesspunktet. Dette på sin måte vil ikke være ressursøkonomisk eller en god måte, da listen vil lett være tilgjenglig om aksesspunktet for eksempel blir stjålet. Uansett vil sannsynligvis

ikke en sjekk hos autentifikasjonsserveren ta minimalt tid og sannsynligvis ha en levelig varighet.

Ved autentifikasjon av brukeren benyttes IEEE 802.1X og en EAP metode. Hvilke metode blir ikke definert noe videre annet enn at EAP-TTLS, EAP-PEAP, EAP-SIM og EAP-MSCHAP-v2 i kombinasjon med TTLS/PEAP sikrer alle en god måte å autentifisere på.

Videre vil denne løsningen enten gi sikret aksess eller ikke. Det er ingen intermediært nivå, det er mulig å implementere på denne måten. Muligheten er å kombinere dette med den modifiserte PCF, slik at forhøyet nødssituasjon også blir dekket.

8.5 - Tilgjenglighet

Det har blitt repetert gjennom denne prosjektoppgaven at sikret aksess, ikke vil gi sikret aksess så fremt ikke nettet er tilgjenglig. Kapitel 6.5 viser at naturlige støykilder må løses eller taes høyde for ved plassering av aksesspunkter.

Falske avassosiasjoner og avautentifiseringsrammer er det derimot vanskelig å ta høyde for. Riktignok vil disse angrepene ha begrenset med rekkevidde og problemområde, men er allikevel ikke spesielt gunstig. I Nød og beredskapssammenhenger kan det meste skje, og derfor der det viktig at nettverket er best mulig sikret.

Da eksisterende standarder ikke løser tilgjenglighetsspørsmålet ved slike DoS angrep, burde det derfor diskuteres hva som er mulig å gjøre. Problemet binder som nevnt seg til at administrasjons og kontrollrammer ikke autentifiseres eller krypteres. Den mest vanlige foreslåtte metoden, er faktisk å autentifisere disse rammene. Bakgrunnen for at dette ikke allerede er gjort, er tilsynelatende fordi aksesspunktene ikke har kapasitet til behandle autentifikasjon av administrasjon og kontrollrammer.

Et annet alternativ er å la aksesspunktet bufrer alle administrasjons og kontrollrammer i et gitt periode. IEEE 802.11 er spesifisert slik at en STA aldri vil sende en vanlig dataramme etter at den har sendt en avassosiasjonsramme. En bufring av denne administrasjonsrammen vil muliggjøre for aksesspunktet å forstå avassosiasjonsrammen er falsk og dermed forkaste gjeldende administrasjonsramme. Tilsvarende er mulig å gjøre for autentifikasjonsrammen.

En slik løsning krever dog at alle radiogrensesnittene må firmware oppgraderes. [He and Mitchell Februar 2005]

8.6 – Oppsummering

Dette kapitelet gir en indikasjon på hvordan et WLAN likt Trådløse Trondheim, kan realiseres og viderefører løsningene fra forrige kapitel inn i dette nettet. Her er det kommet frem til at MAC adressefiltrering i kombinasjon med EAP over IEEE 802.1X kan være et alternativ for å sikre aksess i et nød nett. Allikevel er dette en enten eller løsning. Ved situasjoner hvor det ikke er behov for å oppta alle ressurser, tilbyr ikke løsningen noen intermediær metode for å sikre aksess. En noe modifisert utgaven PCF på MAC laget kan være en løsning i disse tilfellene.

Andre emner berørt i kapitelet er:

- Hvor styringsobjektet kan plasseres
- Hvordan tilgjenglighet kan ytterligere trygges

9 – Konklusjon

Trådløse aksesspunkter blir implementert av ulike organisasjoner fordi transmisjonsområdet til trådløse LAN gir en langt større frihet enn trådbaserte nettverk. At radiobølger ikke på samme måte som trådbaserte er hindret av fysiske barrierer, er både positivt og negativt. Radiobasert aksess gjør blant annet sikkerhetsarbeidet mer krevende. På en annen side vil FoU ha stor interesse for muligheten til å utvikle nye innovative tjenester basert på denne trådløse trenden. Denne forskningen vil til syvende og sist gi brukerne nye muligheter og tjenester, da i tillegg til de muligheter Internett allerede tilbyr. Ikke minst vil sannsynligvis sikkerhet i trådløse nett utvikle seg etter hvert som nye krav oppstår og med tiden. Adekvat sikkerhet for trådløse nett vil være nødvendig for at tjenester skal være interessant for noe mer alvorlig bruk.

I lys av at WLAN stadig i større grad blir organisert i det offentlige rom, som Trådløse Trondheim og andre ”Community Networks,” dukker problematikken om det faktisk er mulig å bruke dette nettet som nødnett. Viktigheten av slike alternative aksessnett for kommunikasjon viser seg spesielt når andre kommunikasjonsnett har falt ned. 11 september i New York viste at NYCWireless fungerte som et slikt alternativ. Allikevel er det en rekke store utfordringer når det bevisst skal legges opp til å bruke WLAN i nød og beredskapssammenhenger. Sikret aksess under nød og beredskap for et utvalg autoriserte brukere vil da være et av de interessante punktene.

Enkelte parametere som normalt ville vært med i en slik vurdering, er ikke denne gang vurdert. Etter samtale med veileder, er det enighet om at problemstillingen dreier seg om å sikre aksess inn til WLAN nettet og diskutere muligheter å gjøre dette med 802.11. Således er QoS diskusjonen ikke innlemmet i denne diskusjonen. Ressurs allokering innenfor det trådløse nettet og ”Community Networks,” vil sannsynligvis være omfattende nok til et eget studie. Videre vil det da være interessant å diskutere hvordan WLAN QoS prioriteringer kan beholdes mellom og gjennom flere ulike teknologier. Dette vil være spesielt interessant siden Trådløse Trondheim er planlagt realisert ved WLAN, WiMAX, WiBRO og HSDPD.

9.1 - Målene i forhold til problemstilling

I denne prosjektrapporten ønsket vi å finne svar på følgende:

I. Se om og hvordan det er mulig å gi sikret aksess
II. Om IEEE 802.11 er egnet til nød og beredskap
III. Diskutere dette i lys av et WLAN nett likt Trådløse Trondheim

Under denne prosjektrapporten har vi diskutert og studert ulike løsninger på hvordan et utvalg autentifiserte personer kan sikres aksess under nød og beredskapssituasjoner.

9.1.1 - Hva er oppnådd

I løpet av dette prosjektet har vi forsøkt og løse problemstillingen og målsetningen angitt i kapitel 1. Per i dag ekstierer det lite utviklede løsninger som tar høyde for sikret aksess under nød og beredskap. Allikevel har det blitt gjort forsøk på å finne metoder for å muliggjøre dette. Det ble her delt inn i tre ulike alternativer: det proprietære alternativ, eksisterende alternative og standardisere alternativer.

Det proprietære alternativ vil eksempelvis være en spesial produsert apparat. Apparatet vil ha en eller flere egenskaper som gjør at den klarer og identifiserer brukeren eller enheten, og som dermed gir sikret aksess. Det eksisterende alternativet, vil da bygge på eksisterende utstyr og muligheter som allerede foreligger ved standarder. Den siste delen som kan være interessant, vil være å sette krav til eksisterende spesifikasjoner som tillatter å sikre aksess på en standardisert måte.

Ved det proprietære alternative viser seg ikke å være en fullverdig metode. Dette spesielt siden en spesialløsning må støttes av både aksesspunktet i tillegg til STA. Dette fører med seg store kostnader, samtidig som en løsning skissert med å benytte en ny kanal ville ha fungert dårlig i et WLAN likt Trådløse Trondheim. Dette på grunn egen interferens ved overlappende kanaler av nærliggende aksesspunkter. Aksesspunkter som overlapper hverandre i dekningsområde, burde operere på ulike frekvenser.

Det er mulighet for å sikre aksess ved hjelp av eksisterende løsninger. En kombinasjon av MAC adressefiltrering og EAP over IEEE 802.1X, gir mulighet for å kaste allmenne brukere

ut av nettet. Denne løsningen tilbyr dog ingen intermediær løsning under de situasjoner hvor ikke det er full krise, og det ikke er nødvendig å allokere alle ressurser. Derfor vil denne løsningen kun dekke ene av to definerte statusene for nød og beredskap.

For å dekke dette siste beredskapsnivået, introduseres en modifisert versjon av PCF funksjonen på MAC laget. Denne funksjonen tilbyr i utgangspunktet en sentralisert styring av hvilke stasjoner til enhver tid får sende. Aksesspunktet vil her forespørre hver enkelt stasjoner for trafikk og på den måten skape en konkurransefri tilgang på mediet. Ved en forhøyet nødssituasjon vil den modifiserte utgaven kunne gi autentifiserte brukere tilgang på mediet over en litt lenger periode enn den ordinære PCF funksjonen. Således vil de autoriserte personene alltid ha ressurser tilgjenglig uten å kaste de allmenne brukerne ut av nettet. Dog vil de oppleve at tilgangen til tider blir noe begrenset.

Til spørsmålet om IEEE 802.11 er spesielt egnet til å sikre aksess under nød og beredskap, er svaret flerfoldig. IEEE 802.11 representerer en peer-to-peer form for nettverk og tilbyr ingen sentralisert styring. Dermed blir det også vanskelig å styre hvilke klienter som til enhver tid har mulighet å koble seg til et aksesspunkt. Løsningen skissert i denne oppgaven, er ikke optimale og sikkerhetsmekanismene på det fysiske lag er heller svake.

Sikkerhetsmessig klarer protokoller som IEEE 802.11i å sikre integritet og konfidensialitet. Protokollen mangler dog mulighet til å autentifisere og eventuelt kryptere administrasjons og kontrollrammer. Dette gjør WLAN svært utsatt for DoS angrep. Videre er det skissert en løsning som tar for seg falske avautentifisering og avassosiasjonsrammer. Dette er dog en teoretisk løsning som det ikke er gjort noen forsøk på under dette prosjektet.

IEEE 802.1X tilbyr ellers flere brukendes metoder for autentifisering. Bruk av EAP over denne protokollen er en av de mest brukte autentifikasjonsmetodene over WLAN i dag. Standarden er godt støttet av dagens operativsystemer, og vil derfor være et naturlig valg under autentifiseringsprosessen.

Videre har de mulige metodene blitt sett i sammenheng med et nett likt Trådløse Trondheim. Da det eksiterer lite skrevne dokumenter som hvordan WLAN nettet er tenkt løst eller spesifikasjoner på brukt utstyr, har det vært vanskelig å ta høyde for en skikkelig

sammenligning. Allikevel er det gitt enkelte indikasjoner som hvor styringsobjektet som setter beredskapsstatus kan ligge og sett på mulige nett arkitektur for å realisere de metodene diskutert i foregående kapitler.

Som en siste avslutende ord på denne seksjonen, så har en del av oppgaven vært å se på om IEEE 802.11 er modent nok til bruk under nød og beredskap. Om et svar må bli avkrevd, vil nok svaret blitt at IEEE 802.11 heller har vanskelig å være egnet til denne typen bruk. Men allikevel vil utbredelsen av WLAN nett representere et alternativ kommunikasjonsnett som kan være nyttig. Eksempler på dette er 11. september i New York, hvor NYCWireless bidro som nød nett. Derfor vil konklusjonen på være at WLAN kan inngå som et bidrag til nød og beredskapsnett, men for seg selv tilby for lite mekanismer for at dette skal være adekvat.

Med svarene svært sammenfattet:
I. Det er mulig, men ingen ideell løsning har kommet frem under prosjektperioden
II. Det er etter min mening at IEEE 802.11 ikke er skapt til slik bruk, men det er allikevel muligheter.
III. Dette har delvis blitt gjort i kapitel 8, men mangel på mer håndfaste dokumenter gjorde også denne vurderingen vanskelig.

9.1.2 - Fremtidig arbeid

Det har tidligere vært antydet at en mulighet er å setet krav endringer av eksisterende standard eller til ny standard kan være et alternativ. Etter å ha sett nærmere på det, så er IEEE 802.11 en vanskelig teknologi og arbeide med når det kommer til sikret aksess. Om tilgjenglighetsspørsmålet skal besvares, må administrasjons og kontrollrammer autentifiseres eller krypteres på et vis. Dette helst uten å belaste aksesspunktet for mye og eventuelt tappe mobile stasjoner for alt batteri. Videre er det nødt til å komme mekanismer på det fysiske lag som i sterkere grad kan sikre en aksesskontroll. Det er nok her også et eventuelt arbeid burde legges.

For fremtidig arbeid av nød og beredskap vil det også være interessant å vurdere QoS inn i nød og beredskapssammenheng. Dette spesielt hvordan eventuelle prioriteringer kan bli holdt gjennom ulike nett basert på ulike teknologier. Trondheim BredBåndsAllmenningen vil på så måte være en god case.

9.2 – Avsluttende ord

Prosjektet har vært spennende og lærerikt. Gjennom perioden har det vært mye frustrasjoner med tanke på at IEEE 802.11 familien er svært omfangsrik og teknologier på så måte ikke er spesielt egnet i forhold til problemstillingen. Allikevel føler jeg det har vært en nyttig opplevelse. Mye kunne nok ha blitt inkludert i vurderingen og mye kunne nok ha vært unnlatt. Men slik er det med prosjekter.

Appendiks - Literaturliste

ANSI/IEEE802.11-1999(R2003). (12 Juni 2003). "PART 11: Wireless LAN Medium Access Controll (MAC) and Physical Layer (PHY) Spesifications."

Arbaugh, W. A. and N. Shankar. (30. Mars 2001). "Your 802.11 Wireless Network has no Clothes."

Asphjell, A. (15. Mars 2006). "Trådløse Trondheim er operativ." from http://www.universitetsavisa.no/ua_lesmer.php?kategori=nyheter&dokid=44183db7819e21.47668965.

AUSCERT. (13. Mai 2004). "AA-2004.02 -- Denial of Service Vulnerability in IEEE 802.11 Wireless Devices." from http://www.auscert.org.au/render.html?it=4091.

Bellardo, J. and S. Savage. (August 2003). "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions." from http://www.cse.ucsd.edu/~savage/papers/UsenixSec03.pdf.

Brewin, B. (17. Mai 2004). "'Indefensible' Wi-Fi flaw discovered in 802.11b network protocol The flaw could be used to jam wireless networks." from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=93221&pageNumber=1.

Cisco. (2005). "Cisco Enterprise Distribuded Wireless Solutions Reference Network Desing V.2.5."

Fleishman, G. (November 2005). "Wi-Fi Stands for.Nothing (and Everything)." from http://wifinetnews.com/archives/006029.html.

Flickenger, R. (June 2002). Building Wireless Community Networks.

Flickenger, R. (June 2003). Building Wireless Community Networks, O'Reilly.

Gast, M. S. (2005). 802.11 Wireless Networks - The Definitive Guide, O'Reilly.

Gavrilenko, K. V., A. A. Mikhailovsky, et al. (28. Juni 2004). Wi-Foo: The Secrets of Wireless Hacking, Addison Wesley Professional.

Geier, J. (24. April 2003). "Implementing Multiple SSIDs." from http://www.wi-fiplanet.com/tutorials/article.php/2196451.

Gohring, N. (18. Mai 2004). "DoS Attack Nothing New." from http://wifinetnews.com/archives/003348.html.

Halvorsen, F. (27. Februar 2006). "Tetra-teknologi i nødnettet." from http://www.tu.no/nyheter/ikt/article48357.ece.

He, C. and J. C. Mitchell. (Februar 2005). "Security Analysis and Improvements for IEEE 802.11i." from www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/NDSS05-1107.pdf.

Jelle, T. (21. Oktober 2005). "Teknoport: Trådløse Trondheim - En moderne utviklingsarena for ideskapning, forskning og produktutvikling."

Mishra, A. and W. A. Arbaugh. (6. Februar 2002). "An initial Security Analysis of the IEEE 802.1X Standard."

NPT. (20. desember 2000). "Merknader til forskrift 20. desember 2000 om tillatt bruk av frekvenser."

Nødnett. (13. Oktober 2005). "Hvorfor nytt landsdekkende nødnett?" from http://www.nodnett.no/default.asp?pubid=549.

Odelstinget. (4. april 2003). "Ot.prp. nr. 58." Odelstingproposisjoner, from http://odin.dep.no/sd/norsk/dok/regpubl/otprp/028001-050026/ind-nn.html.

PT. (9.mai 2005). "Det norske telemarkedet 2004." from http://www.npt.no/pt_internet/venstremeny/publikasjoner/telestatistikk/statistikk2004/telemarked2004.pdf.

Stallings, W. (28. November 2002). Network Security Essentials (International Edition), Prentice Hall.

Telemuseum, N. "Telefonen i verden - Telehistorie." from http://telemuseum.no/mambo/content/blogcategory/90/150/.

Telenor. (2006). "Samfunnspålagte oppgaver i Norge." from http://www.telenor.no/om/samfunnsansvar/produkter/oppgaver/.

TIFKOM. (20 mars 2000). "Teleberedskap i fritt konkurransemarked." from http://www.npt.no/pt_internet/venstremeny/publikasjoner/div_rapporter/tifkom/.

Trådløse-Trondheim. (13. Juni 2005). "Trådløse Trondheim - Workshop."

Velayos, H. and G. Karlson. (April 2003). "Techniques to reduce IEEE 802.11b MAC layer handover time." from http://web.it.kth.se/~hvelayos/papers/TRITA-IMIT-LCN R 03-02 Handover in IEEE 802.pdf.

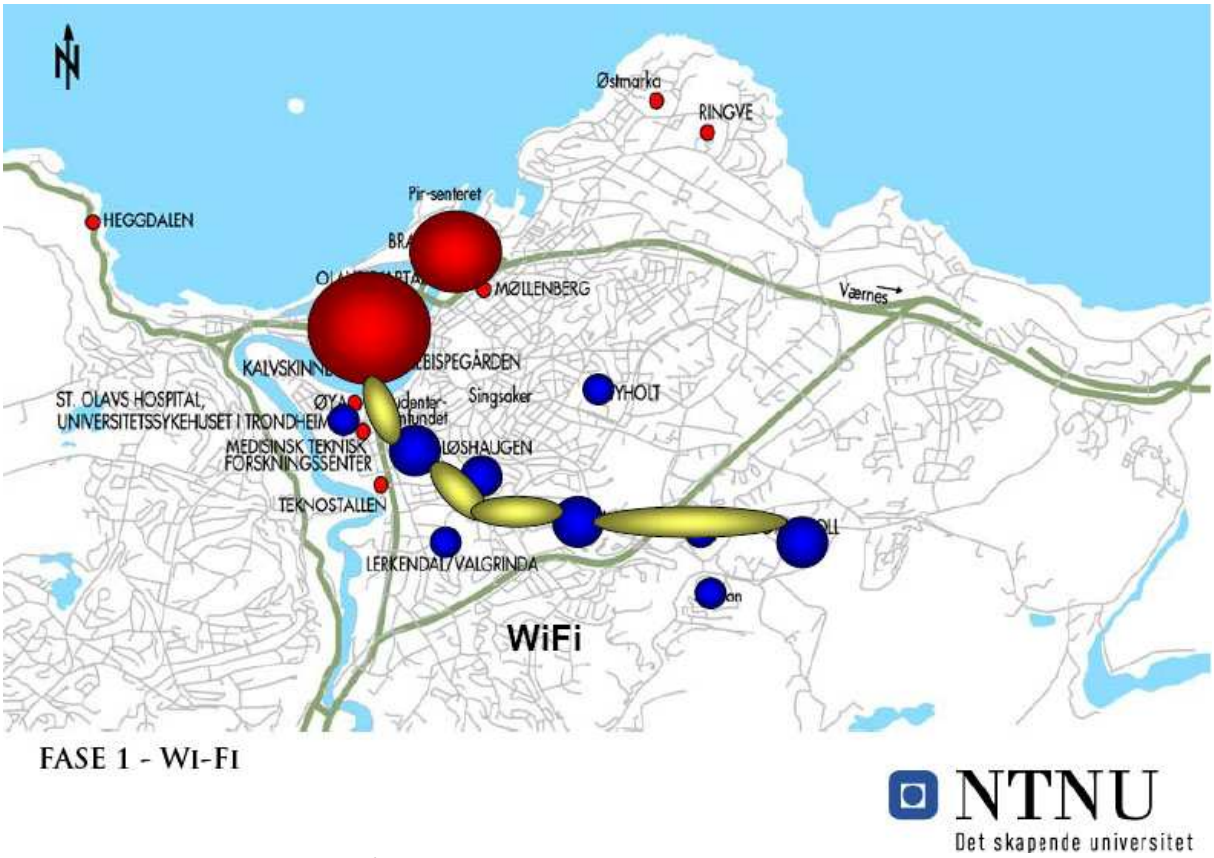
Wi-Fi.Alliance. (2006). "About the Wi-Fi Alliance." from http://www.wi-fi.org/about_overview.php.

Wi-Fi.Alliance. (2006). "Our Brand." from http://www.wi-fi.org/brand_usage.php.

Appendiks - Wi-Fi Kanaler

Wi-Fi Channels				
Channel	**Center Frequency (GHz)**	**USA & Canada**	**Europe (ETSI)**	**Japan**
1	2.412	Y	Y	Y
2	2.417	Y	Y	Y
3	2.422	Y	Y	Y
4	2.427	Y	Y	Y
5	2.432	Y	Y	Y
6	2.437	Y	Y	Y
7	2.442	Y	Y	Y
8	2.447	Y	Y	Y
9	2.452	Y	Y	Y
10	2.457	Y	Y	Y
11	2.462	Y	Y	Y
12	2.467		Y	Y
13	2.472		Y	Y
14	2.484			Y

Appendiks – Dekningskart for Trådløse Trondheim



[Trådløse Trondheim – Workshop 13. Juni 2005]

Appendiks – FCC-s ”Policy Statement” - Nettnøytralitet

Nettnøytralitet, bredbåndsutfordring - 4 Prinsipper:

(fra FCC i USA - anvendes blant annet av ”NYC Wireless”, se http://www.nycwireless.net).

For å oppmuntre til bredbåndsdekning og ivareta samt fremme den åpne og kontaktfremmende natur som det offentlige internett har; gir man sin tilslutning til følgende prinsipper:

1. Forbrukerne skal sikres aksessrett til lovlig innhold på Internett etter eget ønske
2. Forbrukerne har rett til å bruke programvare og tjenester etter eget ønske, under hensyntagen til legale krav om begrensninger eller virkemåte.
3. Forbrukere skal ha fritt valg med hensyn på hvilke terminalutstyr de bruker, så lenge dette ustyret er lovlig (i følge gjeldende regelverk) og ikke forårsaker skade i nettet.
4. Forbruker har rett til (å erfare) konkurranse mellom nettoperatører, applikasjons- og tjenesteytere og innholdsleverandører.

Opprinnelig tekst (hentet fra FCC **POLICY STATEMENT**
Adopted: August 5, 2005 Released: September 23, 2005

Appendiks – IEEE 802.11 Sikkerhetsoversikt

[Gast 2003]