NTNU
Det skapende universitet

Evaluerings- og testkriterier for trådløse datanettverk

Rune Vedvik

Master i kommunikasjonsteknologi
Oppgaven levert: Juli 2006
Hovedveileder: Steinar Andresen, ITEM
Biveileder(e): Thomas Jelle, ITEM

Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Oppgavetekst

Studenten skal vurdere eksisterende og foreslå nye test og evalueringskriter for trådløse "citywide" bredbåndsnettverk. Dette kan være kriterier knyttet til opplevd brukerkvalitet for både tale og data, roaming, posisjonering og andre parametre som neste generasjons trådløse bredbåndsnett bør ha støtte for. Videre skal disse testkriteriene prøves ut i en pilotutbygging av Trådløse Trondheim. Målsetningen med oppgaven er å komme frem til generelle parameter som kan brukes for å evaluere trådløse datanettverk og hvordan disse skal måles. Oppgaven forutsetter en del praktiske målinger i felt og studenten vil få være med å evaluere/teste en planlagt pilot av Trådløse Trondheim.

Oppgaven gitt: 16. januar 2006
Hovedveileder: Steinar Andresen, ITEM

"A test specification is particularly important for 802.11 given the complexity of the protocol and the challenges of wireless test. Standard test-methodology guidelines can help the end-user community evaluate product specifications and performance."

– Paul Nikolich, formann i IEEE 802-komiteen

Forord

Denne rapporten er et resultatet av arbeidet med min masteroppgave ved Norges teknisk-naturvitenskaplige universitet (NTNU) i Trondheim. Arbeidet har pågått fra januar til juni 2006 og avslutter fem hektiske og innholdsrike år som student ved Instituttet for Telematikk.

Jeg ble presentert for oppgavens problemstilling av prosjektleder for Trådløse Trondheim, Thomas Jelle. Han har også fungert som min veileder under arbeidet. Veiledningsmøter med han har, under hele prosessen, gitt ekstra motivasjon og giv til videre arbeid med oppgaven.

I tillegg til Thomas Jelle vil jeg takke Jardar Leira ved Uninett for testsamarbeid, veiledning og tekniske forklaringer. Det er veldig lærerikt å samarbeide med personer som har så mye kunnskap om sitt fagfelt og entusiasme for jobben sin.

Jeg håper at denne rapporten vil komme til nytte, og jeg er åpen for alle tilbakemeldinger, innspill og spørsmål.

Trondheim, 27. juni 2006

Rune Vedvik

Sammendrag

Den økte utbredelsen av trådløse datanettverk har ført til en rekke forskjellig trådløst nettverksutstyr på markedet. Det blir produsert utstyr både til hjemmemarkedet og bedriftsmarkedet, og utstyret er tilpasset og utviklet med forskjellig kompleksitet og til forskjellige nettverksstørrelser.

For at brukere skal kunne velge det mest egnede utstyret til sitt nettverk, trengs det en felles test- og målemetode for utstyrsegenskaper. For trådløse nettverk finnes det ingen standard for slik testing. Sammenlignet med trådbundne nettverk er testing av utstyr for trådløse nettverk mer kompleks og involverer flere faktorer som det må tas hensyn til. Fordi signalutvekslingen utføres over luftmediet, kan utenforliggende faktorer og støy forstyrre kommunikasjonen. Derfor trengs det andre evaluerings- og testmetoder for trådløse nettverk enn det gjør for trådbundne nettverk.

Utviklingen av trådløse nettverk har gått fra sammenkoblinger av enkeltstående klienter som sendte radiosignaler mellom hverandre, til store city-wide trådløse nettverk med sentrale kontrollere som styrer kommunikasjonen. Kontrollerne innehar mye av den kompleksiteten som autonome aksesspunkt har. Den nye typen nettverk kan betjene større og flere brukergrupper, og har et stort geografisk dekningsområde. De nye funksjonalitetene og skaleringsegenskapene gjør at det stilles andre krav til nettverkene enn det som er tilfelle for tidligere trådløse nettverk. Det trengs derfor nye måleparametre og nye evalueringsmetoder for utstyr som er utviklet for den nye typen nettverk.

Gjennom testing av nettverksutstyr i laboratorium og evalueringer i piloten til Trådløse Trondheim på Solsiden i Trondheim, har en kunnet finne ut hva som kreves av nettverksutstyret og hvilke kriterier som må ligge til grunn for et city-wide trådløst nettverk. På grunnlag av slik testing er det mulig å finne generelle parametre som kan brukes for å beskrive utstyr fra forskjellige produsenter.

Cisco Systems og Meru Networks leverer nettverksutstyr som egner seg for city-wide trådløse nettverk. I piloten til Trådløse Trondheim er det benyttet utstyrsløsningen Airespace fra Cisco, og i laboratorium har det vært mulig å teste egenskapene til dette nettverksutstyret opp mot nettverksutstyret fra Meru Networks. Sammenligningen mellom utstyret fra de to produsentene har vært utført ved å måle grunnleggende egenskaper og innebygd funksjonalitet. For å kunne utføre slike tester og målinger er det avgjørende å ha gode testverktøyer og gode testplaner. Under laboratorietestene har programvaren IxChariot fra Ixia, som er utviklet for testing av nettverkskomponenter, vært benyttet. Resultatet av testingen viser hvilket av de to aktuelle produktene som best støtter de egenskapene som et city-wide trådløst nettverk krever.

For å kunne vite hva som kan forventes av trådløst nettverksutstyr, må en før testingen ha klart hva som teoretisk er mulig for utstyret. De forskjellige standardene for trådløse nettverk støtter ulike overføringshastigheter og har forskjellig maksimal overføringskapasitet. Utregninger viser en teoretisk forskjell på 21,7 Mbit/s for standarden med størst overføringskapasitet av nyttedata i forhold til standarden med minst overføringskapasitet. Testresultater viser derimot at denne forskjellen er noe mindre i praksis. Det er likevel nyttig å vite hva en kan forvente av utstyret tatt i betraktning teoretiske hindringer. For å finne nødvendige kriterier for en bestemt type nettverk, er det også nødvendig å vite hvilken type tjenester som skal tilbys brukerne av nettverket. Kravet til nettverksegenskapene må samsvare med tjenestebehov til for eksempel overføringskapasitet, roaming og posisjonering.

I denne oppgaven brukes testresultatet og målingene som er gjort i laboratorium og i piloten til å foreslå generelle parametre som kan brukes for å beskrive nettverksutstyr. Dette kan benyttes til å sammenligne ulike produkter ut i fra hva som kreves i city-wide trådløse nettverk. Målet er at disse parametrene skal kunne brukes under testing for å gi nyttig informasjon om egenskapene til nettverksutstyr fra forskjellige produsent.

Teorien bak den trådløse nettverksteknologien er grunnleggende for å konfigurere riktige tester, og er grunnlaget for å kunne bruke testverktøyet. Resultatene av testene benyttes for å finne grunnleggene beskrivelsesparametre og for å finne hvilke krav og funksjonaliteter som er ønskelig i trådløse city-wide datanettverk.

Akronymer

ACK	Acknowledgment Packet
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AIFS	Arbitration Interframe Space
AP	Aksesspunkt
BPSK	Binary Phase Shift Keying
BSS	Basic Service Set
CAPWAP	Control and Provisioning of Wireless Access Points
CCK	Complementary Code Keying
CCMP	Counter Mode with CBC-MAC Protocol
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DFS	Dynamic Frequency Selection
DIFS	Distributed Inter Frame Space
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authenticatio Protocol
EIFS	Extended Inter Frame Space
ERP	Extended Rate PHY
ESS	Extended Service Set
FCS	Frame Check Sequence
FHSS	Frequency Hopping Spread Spectrum
GSM	Global System for Mobile Communication
HEC	Header Error Check
HS/DSSS	High Rate Direct Sequence Spread Spectrum
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
ITU	International Telecommunication Union
LAN	Local Area Network
LLC	Logical Link Control
LWAPP	Light Weight Access Point Protocol
MAC	Medium Access Control
MIC	Massage Integrity Check
MOS	Mean Opinion Score
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit

OFDM	Orthogonal Frequency Division Multiplex
OSI	Open Systems Interconnection
PHY	Physical Layer
PIFS	Point Coordination Inter Frame Space
PLCP	Physical Layer Convergence Procedure
PMD	Physical Medium Dependent
PoE	Power Over Ethernet
PPDU	PLCP Protocol Data Unit
PSDU	Physical Sublayer Service Dataunits
PT	Post- og Teletilsynet
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial In User Service
RRM	Radio Resource Management
RSSI	Received Signal Strength Indication
RTP	Real Time Protocol
RTS	Request To Send
RTT	Round Trip Time
SDU	Service Data Unit
SIFS	Short Inter Frame Spaces
SIR	Spredt Infrared
SLAPP	Secure Light Access Point Protocol
SNAP	SubNetwork Access Protocol
SNR	Signal/Støyforhold
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TPC	Transmit Power Control
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VCS	Virual Carrier Sense
VoIP	Vioce over IP
VoWIP	Voice over Wireless IP
WAP	Wi-Fi Protected Access
WCS	Wireless Control System
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

Innholdsfortegnelse

FORORD ..... **III**
SAMMENDRAG ..... **V**
AKRONYMER ..... **VII**
FIGURLISTE ..... **XIII**
TABELLISTE ..... **XIV**
1 INNLEDNING **1**
1.1 BAKGRUNN 1
1.2 PROBLEMSTILLING 2
1.3 OPPBYGNING AV OPPGAVEN 2
1.4 AVGRENSING 3
1.5 KILDEKOMMENTAR 3
2 NETTVERKSARKITEKTUR OG FYSISKE PARAMETRE **5**
2.1 WLAN-DESIGN OG TERMINOLOGIER 5
2.2 REKKEVIDDE 9
2.3 FREKVENSER 9
2.4 INTERFERENS 9
2.5 LISENSBELAGTE OG FRIE FREKVENSBÅND 10
2.6 SIGNAL-/STØYFORHOLD 10
2.7 KAPASITETEN TIL RADIOSIGNALER 11
2.8 OPPSUMMERING 11
3 TRÅDLØSE NETTVERKSSTANDARDER **13**
3.1 IEEE 802.11-STANDARDEN 13
3.2 SPREAD SPECTRUM RADIO 22
3.3 IEEE 802.11a 23
3.4 IEEE 802.11h 26
3.5 IEEE 802.11b 27
3.6 IEEE 802.11g 29
3.7 IEEE 802.11e 32
3.8 SIKKERHET I TRÅDLØSE NETTVERK 33
3.9 IEEE 802.1X 34
3.10 IEEE 802.11i 37
3.11 OVERSIKT OVER STANDARDER I IEEE 802.11-FAMILIEN 38
3.12 WI-FI 39
4 TRÅDLØSE TRONDHEIM **41**
5 TESTING OG EVALUERING **45**
5.1 TESTUTSTYR 46
5.2 THROUGHPUT 47
5.3 ROAMING 62
5.4 VOICE OVER WIRELESS IP 64
5.5 POSISJONERING 73
5.6 ADMINISTRATIVE VERKTØY 78
6 HVILKE PARAMETRE TRENGS FOR Å BESKRIVE CITY-WIDE WLAN? **83**
6.1 ROAMINGTID 84
6.2 THROUGHPUT 85
6.3 POSISJONERINGSNØYAKTIGHET 85
6.4 VOIP EGENSKAPER 86

6.5 SKALERINGSEGENSKAPER 86
6.6 ADMINISTRATIVE VERKTØY 87
6.7 SIKKERHET 88
6.8 TEKNISKE SPESIFIKASJONER 88
7 KONKLUSJON 89
REFERANSER 91
APPENDIKS 93
APPENDIKS A 93
APPENDIKS B 94
APPENDIKS C 95
APPENDIKS D 97
APPENDIKS E 100

Figurliste

FIGUR 2.1: AD-HOC NETTVERK 5
FIGUR 2.2: TRADISJONELT WLAN MED AKSESSPUNKT 6
FIGUR 2.3: WLAN MED LETT AKSESSPUNKT, KONTROLLER OG AUTENTISERINGSSERVER 6
FIGUR 2.4: TRANSPORT HEADEREN FOR EN CAPWAP-PAKKE 8
FIGUR 2.5: CAPWAP-INNKAPSLINGEN AV DATAPAKKER 8
FIGUR 2.6: SNR-NIVÅ 11
FIGUR 3.1: IEEE 802.11-PLASSERING I FORHOLD TIL OSI-MODELLEN 14
FIGUR 3.2: ALTERNATIVER PÅ DET FYSISKE LAGET 14
FIGUR 3.3: HIDEN NODE-PROBLEMET 15
FIGUR 3.4: KLARERING MED RTS/CTS 16
FIGUR 3.5: OPPDELINGEN AV EN RAMME SOM DEFINERT I IEEE 802.11-STANDARDEN 18
FIGUR 3.6: DEN GENERELLE RAMMESTRUKTUREN FOR IEEE 802.11 19
FIGUR 3.7: MAC-DATAFELTET 19
FIGUR 3.8: FRAME CONTROL FELTET 19
FIGUR 3.9: FRAME BODY-OPPBYGGINGEN I IEEE 802.11 20
FIGUR 3.10: MELLOMRAMMEAVSTANDER 21
FIGUR 3.11: RAMMEFORMAT FOR OFDM PLCP 25
FIGUR 3.12: SIGNALFELTDELEN AV PLCP-HEADEREN 25
FIGUR 3.13: INNKAPSLINGEN I EN IEEE 802.11b-DATARAMME 28
FIGUR 3.14: DATARATESPESIFIKASJONER FOR IEEE 802.11b 29
FIGUR 3.15: REALISERINGSTEKNIKKER FOR DE FORSKJELLIGE DATARATENE I IEEE 802.11g 29
FIGUR 3.16: RAMMEFORMATET I ERP-OFDM 32
FIGUR 3.17: WEP-KRYPTERING 33
FIGUR 3.18: AUTENTISERINGSPROSESSEN I IEEE 802.1X 35
FIGUR 3.19: MELDINGSUTVEKSLING VED AUTENTISERING MED 802.1X 36
FIGUR 4.1: AKSESSPUNKT I TRÅDLØSE TRONDHEIM PILOTEN 41
FIGUR 4.2: DEKNINGSOMRÅDET FOR FØRSTE FASE I UTBYGGINGEN AV TRÅDLØSE TRONDHEIM 42
FIGUR 5.1: SENDING AV ET TCP/IP-DATAGRAM 49
FIGUR 5.2: SENDING AV ET TCP/IP-DATAGRAM MED CTS 52
FIGUR 5.3: SENDING AV ET TCP/IP-DATAGRAM MED RTS/CTS 54
FIGUR 5.4: THROUGHPUTRESULTATER FOR AIRESPACE 56
FIGUR 5.5: THROUGHPUTMÅLINGER FOR AP1010 OG AP1030 58
FIGUR 5.6: THROUGHPUT FOR AIRESPACE OG MERU FOR IEEE 802.11a 59
FIGUR 5.7: THROUGHPUT PER KLIENT FOR AIRESPACE MED 1 KLIENT OG MED 16 KLIENTER FOR IEEE 802.11a 60
FIGUR 5.8: THROUGHPUT PER KLIENT FOR MERU MED 1 KLIENT OG MED 16 KLIENTER FOR IEEE 802.11a 60
FIGUR 5.9: THROUGHPUT FOR AIRESPACE MED 4 KLIENTER 61
FIGUR 5.10: RSSI VED KLIENTROAMING 63
FIGUR 5.11: REPRESENTATIVT RESULTAT FOR RESPONSTID VED ROAMING 63
FIGUR 5.12: VOIP-PROTOKOLLSTAKK 65
FIGUR 5.13: RTP-HEADERFORMAT 65
FIGUR 5.14: FORHOLDET MELLOM R-FAKTOR OG MOS-VERDI 68
FIGUR 5.15: MOS-VERDIER FOR TRE VOWIP-SAMTALER OG EN SAMTIDIG DATAPAKKESTRØM MED NETTVERKSUTSTYR FRA AIRESPACE 71
FIGUR 5.16: ENVEISFORSINKELSE OG JITTER I TESTEKSEMPELET 72
FIGUR 5.17: MOS-VERDI FOR 16 SAMTIDIGE SAMTALER MED IEEE 802.11a FOR AIRESPACE 72
FIGUR 5.18: MOS-VERDIER FOR FIRE KLIENTER MED IEEE 802.11g OG FIRE KLIENTER MED IEEE 802.11b FOR AIRESPACE TIL VENSTRE OG MERU TIL HØGRE. 73
FIGUR 5.19: CISCO WCS-KART MED POSISJONERT KLIENT 74
FIGUR 5.20: KLIENTPLASSERING OG TILHØRENDE POSISJONERING GJORT AV WCS-EN 76
FIGUR 5.21: POSISJONERING AV STASJONÆR KLIENT 77

Tabelliste

TABELL 3.1: KODEDE BITS PER SYMBOL I FORHOLD TIL DATABITS PER SYMBOL FOR DE ULIKE OVERFØRINGSHASTIGHETENE I IEEE 802.11a 24
TABELL 3.2: IEEE 802.11-STANDARDER 39
TABELL 5.1: UTREGNING AV TOTAL OVERFØRINGSTID FOR EN TCP-PAKKE MED TCP ACK FOR IEEE 802.11b ... 49
TABELL 5.2: UTREGNING AV TOTAL OVERFØRINGSTID FOR EN TCP-PAKKE MED TCP ACK FOR IEEE 802.11a ... 50
TABELL 5.3: UTREGNING AV TOTAL OVERFØRINGSTID FOR EN TCP-PAKKE MED TCP ACK FOR IEEE 802.11g-ONLY 52
TABELL 5.4: UTREGNING AV TOTAL OVERFØRINGSTID FOR EN TCP-PAKKE MED TCP ACK FOR IEEE 802.11g MED CTS-BESKYTTELSE 53
TABELL 5.5: UTREGNING AV TOTAL OVERFØRINGSTID FOR EN TCP-PAKKE MED TCP ACK FOR IEEE 802.11g MED RTS/CTS-BESKYTTELSE 54
TABELL 5.6: NYTTEDATAKAPASITET FOR DE ULIKE FYSISKELAG-TEKNOLOGIENE 55
TABELL 5.7: GJENNOMSNITTLIG THROUGHPUT MED EN KLIENT FOR AIRESPACE 57
TABELL 5.8: SAMMENLIGNING AV THROUGHPUT MELLOM AUTONOME AIRONET AP1131AG OG AIRESPACE AP1010 58
TABELL 5.9: TESTRESULTATER FOR THROUGHPUT 59
TABELL 5.10: R-FAKTOR OG SAMTALEKVALITET 68
TABELL 5.11: VOIP-KODEKSER 69

1 Innledning

1.1 Bakgrunn

Sommeren 2005 ble det tatt et initiativ ved Norges teknisk-naturvitenskaplige universitet (NTNU) til å bygge et city-wide trådløst nettverk i Trondheim. Det geografiske omfanget av et slikt nettverk ville bli mye større enn det som allerede fantes på sporadiske steder i form av enkeltstående hotspots. Arkitekturen og oppbyggingen av et slikt nettverk ville derfor bli annerledes enn for de tradisjonelle uavhengige aksesspunktene. Dette prosjektet skulle ha overlappende aksesspunktdekning med muligheter for roaming mellom de ulike aksesspunktene og posisjonering av klienter.

Den nye arkitekturen for city-wide trådløse nettverk fører med seg muligheter for nye nettverkstjenester og dermed nye muligheter for brukerne av systemet. Arkitekturen i denne typen trådløse nettverk, har gitt nye krav til funksjonalitet. Dette har skapt et behov for nye testmetoder for utstyrstesting. For å kunne avgjøre hvilke produsenter og leverandører som bør benyttes i utbygging av et city-wide trådløst nettverk, trengs det testparametre og testmetodikk for å sammenligne de ulike alternativene. Sammenligningen bør bygge på parametre som er relevante for den aktuelle typen nettverk. Siden oppbyggingen av Trådløse Trondheim vil være forskjellig fra oppbyggingen av tradisjonelle trådløse nettverk, vil det være andre kriterier og andre parametre som er avgjørende ved testing av nettverksutstyr i dette prosjektet.

For å komme frem til hva som er avgjørende parametre for et vellykket city-wide trådløst nettverk, er det satt opp en testpilot av Trådløse Trondheim på Solsiden i Trondheim. I tillegg er det gjort tester på utstyr fra forskjellige produsenter i testlaboratorium hos Uninett. Pilotutbyggingen og utstyrstestingen er gjort for å tilegne seg kunnskap om hva som kreves av denne type nettverk og hvilke krav som må stilles til utstyr og administrasjon. Dette vil igjen kunne legge grunnlaget for å finne generelle parametre for testing av utstyr for city-wide trådløse nettverk.

1.2 Problemstilling

I denne oppgaven er det overordnede målet å finne generelle parametre som kan brukes for å evaluere city-wide trådløse datanettverk. For å komme frem til disse parametrene vil det bli gjennomført praktiske tester på relevant nettverksutstyr, og det vil utføres målinger i en pilot av Trådløse Trondheim-prosjektet. Testresultatene og evalueringen vil lede frem til hva som er viktig for et city-wide trådløst nettverk og hvordan utstyr fra forskjellige utstyrsprodusenter skal testes. Ved å ha generelle test- og evalueringskriterier, vil det bli enklere å sammenligne utstyr på tvers av produsenter. Spørsmålet som denne oppgaven tar sikte på å finne svar på er: Hvilke parametre trengs for å beskrive et city-wide trådløst nettverk?

1.3 Oppbygning av oppgaven

Oppgaven er delt inn i 7 kapitler, hvor kapittel 1 er innledning og kapittel 7 er konklusjon. Hoveddelen av oppgaven er kapittel 2 til kapittel 6 som er oppdelt på følgende måte:

- Kapittel 2 og kapittel 3 tar for seg den teoretiske oppbyggingen av trådløse nettverk. I kapittel 2 er det en kort beskrivelse av de vanligste trådløse nettversarkitekturene og fysiske forhold rundt denne nettverksteknologi. Kapittel 3 er hovedsakelig satt av til beskrivelse av de mest relevante trådløse nettverksstandardene fra IEEE.
- Kapittel 4 inneholder en kort beskrivelse av Trådløse Trondheim prosjektet og prosjektpiloten.
- I kapittel 5 er resultater fra det praktiske arbeidet med oppgaven beskrevet. Her er det også tatt med en del teori som ligger til grunn for den teknologien som er benyttet.
- I kapittel 6 vil det, på bakgrunn av kapittel 5, diskuteres hvilke parametre som er nødvendige for å kunne beskrive egenskapene til trådløst nettverksutstyr.

Oppgaven har også 5 vedlegg:

- Appendiks A gir en oversikt over frekvensplan og hoppsekvenser ved bruk av Frequency Hopping Spread Spectrum.
- Appendiks B gir en oversikt over frekvensplan ved bruk av Direct Sequence Spread Spectrum.
- Appendiks C er testresultater fra posisjoneringstestingen i piloten på Solsiden.
- Appendiks D er testresultater fra utstyrstestingen med IxChariot.
- Appendiks E viser tekniske spesifikasjoner for utstyrsløsningen til Airespace.

I tillegg har oppgaven følgende elektroniske vedlegg:

- HTML-fremstilling av posisjoneringstester.
- HTML-fremstilling av resultater fra testing med IxChariot.
- Tilgjengelige elektroniske kilder.

1.4 Avgrensing

Oppgaven er todelt med en teoridel og en del med praktiske målinger og evalueringer av utstyr. Teorien i denne oppgaven er tatt med for å gi en forståelse av de ulike oppbygningene og løsningene for trådløse nettverk. Den skal gi forståelse for de resultatene som fremkommer av utstyrstestingen som er gjort i den praktiske delen av oppgaven. Noe av denne teorien kunne ha vært lagt i vedlegg til oppgaven, men er tatt med fordi forståelse for grunnleggende tekniske detaljer er nødvendig for å konfigurere de utførte testene på riktig måte.

I den teoretiske beskrivelsen av teknologien er det likevel ikke tatt med detaljer rundt moduleringsteknikker på det fysiske laget for de ulike IEEE standardene eller beskrivelser av de forskjellige VoIP kodeksene og teknologiens protokoller. Dette er utelatt fordi det ikke er relevant for oppgavens resultater eller konklusjon. Oppgaven tar heller ikke for seg oppbyggingen av nettverkstjenester for den nye trådløse nettverksarkitekturen og hvordan disse kan integreres i den trådløse løsning som er beskrevet i oppgaven.

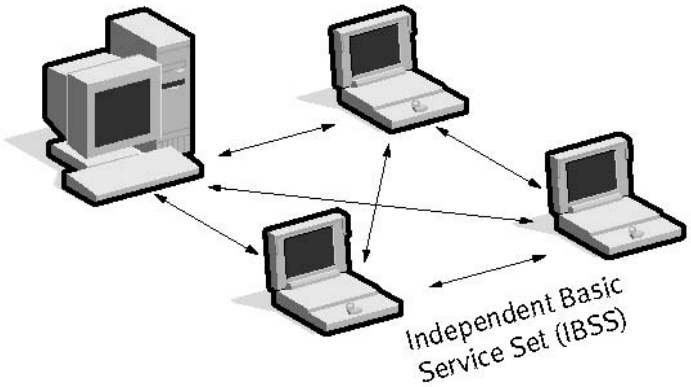
1.5 Kildekommentar

I oppgaven er det benyttet bakgrunnskilder fra ulike oppslagsverk, faglitteratur og fra Internett. Teorien i denne oppgaven er i hovedsak bygget på standarddokumentene til IEEE og nettsidene til organisasjonen. I tillegg er Matthew Gasts *802.11 Wireless Networks*, utgitt av O'Reilly, brukt for å få en oversikt over nettverksarkitekturer og sammenhengen mellom de ulike IEEE-standardene for trådløse nettverk. Tall og tidsluker i utregningene av throughput for nyttedata er hentet fra standardpapirene for de ulike fysiskelag-teknologiene. Kapittelet om Trådløse Trondheim er bygget på dokument *Trådløse Trondheim 1:2006*, samt samtaler med prosjektleder Thomas Jelle. I testdelen av denne oppgaven er det meste av bakgrunnsstoffet hentet i tekniske papirer fra de forskjellige utstyrsprodusenter og fra softwaredokumenter til testprogramvaren IxChariot. Kilder som er hentet fra Internett er vedlagt som elektroniske vedlegg. En meny over elektroniske kilder fremkommer ved å åpne filen index.html i en nettleser. Viser til referanselisten for mer detaljert oversikt over kilder.

2 Nettverksarkitektur og fysiske parametre

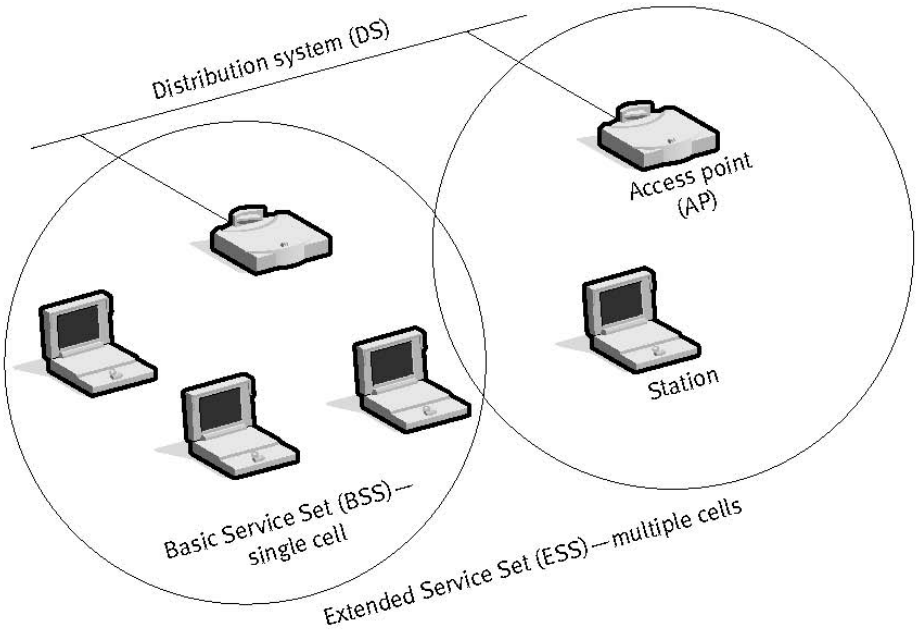
2.1 WLAN-design og terminologier

Oppsettet av trådløse nettverk kan gjøres med forskjellig kompleksitet og med ulik arkitektur. Den enkleste måten er gjennom peer-to-peer oppkoblinger der data sendes direkte mellom klienter, uten bruk av aksesspunkt. Denne typen trådløse nettverk er mest vanlig i tilfeller der to klienter utveksler informasjon med hverandre. En utvidelse av dette er å koble flere maskiner sammen på samme måte i et ad-hoc nettverk. Ad-hoc nettverk støtter mer eller mindre tilfeldig oppkobling mellom trådløse klienter, som vist i figur 2.1. Disse nettverkene er gjerne ustrukturerte og inneholder ingen faste nettverksenheter. Vanligvis kan alle klientene i et slikt nett kommunisere med alle de andre klientene i nettverket, dersom rekkevidden på radiosignalene tillater det.



Figur 2.1: ad-hoc nettverk

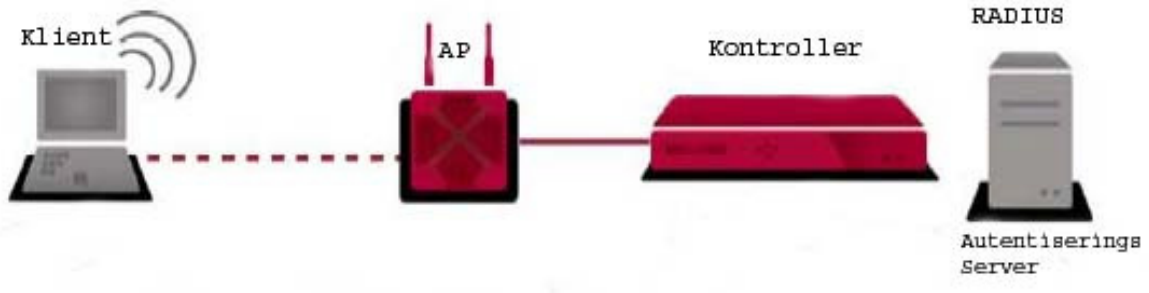
En annen måte å sette opp et Wireless Local Area Network (WLAN) på, er å benytte et aksesspunkt til å styre informasjonsflyten i nettverket, som vist i figur 2.2. Et slikt aksesspunkt har minst to forskjellige grensesnitt, et mot det trådløse nettverket og et mot et kablet nettverk. Aksesspunktet kan også fungere som en bro til andre nettverk. En av oppgavene til aksesspunktet er å tilpasse informasjonen fra de trådløse enhetene til fastnettet og omvendt. I tillegg fungerer det som en router for riktig routing av informasjon som sendes til nettverket og internt i det trådløse nettet. En kan også sette opp flere overlappende nettverk som dekker forskjellige celler. Da kan en støtte roaming mellom de trådløse aksesspunktene, dersom aksesspunktene samarbeider med å koordinere forflyttningen. Et Aksesspunkt (AP) og de mottakerne som finnes i dekningsområdet til AP, kalles et Basic Service Set (BSS). Et Extended Service Set (ESS) er en samling av to eller flere BSS. I denne typen trådløse nettverk finnes det fire hovedkomponenter: Distribusjonssystemet, det trådløse mediet, aksesspunkt og trådløse terminaler.



Figur 2.2: Tradisjonelt WLAN med aksesspunkt

Når flere aksesspunkt er koblet sammen for å få et stort dekningsområde, kan håndtering av klienter foregå ved utveksling av informasjon mellom aksesspunktene, eller ved at klientene selv tar seg av roaming mellom ulike BSS. Det distribuerte systemet i figur 2.2 er en grunnleggende komponent i et IEEE 802.11-nettverk. Det brukes i overføringen av pakker mot deres destinasjon. IEEE 802.11-standarden spesifiserer ingen bestemt teknologi for distribusjonssystemet, men i de fleste kommersielle tjenester er Ethernet brukt som backbone nettverksteknologi.

Den nyeste formen for trådløs nettverksarkitektur er en oppbygging der en bruker kontrollere for å styre aksesspunktene. Figur 3 viser et trådløst nettverk med en sentral kontroller.



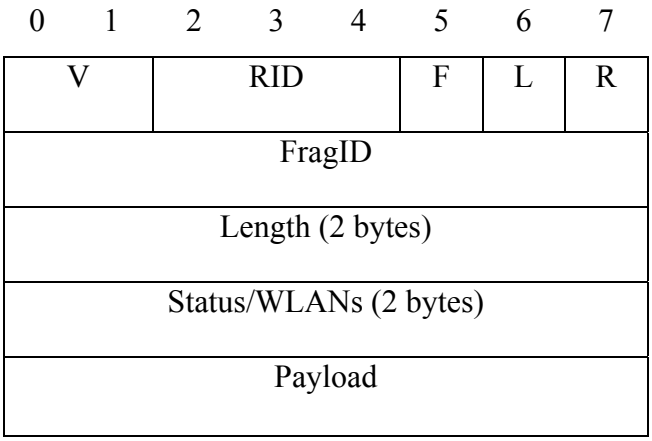
Figur 2.3: WLAN med lett aksesspunkt, kontroller og autentiseringsserver
Figuren er hentet fra [22]

Denne oppbyggingen av trådløse nettverk er best egnet for store campus, kontorlandskaper eller i city-wide trådløse nettverk, der flere aksesspunkt skal samarbeide om å tilby aksess i et større begrenset geografisk område. Det meste av funksjonaliteten i slike nettverk har blitt

flyttet fra aksesspunktet til kontrolleren, og de ”lette” aksesspunktene blir derfor mindre komplekse enn autonome aksesspunkt. Produsenter av utstyr for slike nettverk benytter ulike tunnelleringsprotokoller for tunnellering av data mellom aksesspunktene og kontrolleren. Alle data i nettverket går gjennom denne tunnelen til eller fra aksesspunktet. Det Cisco-eide Airespace benytter Light Weight Access Point Protocol (LWAPP), mens andre kommersielle aktører som Trapeze og Aruba benytter en Secure Light Access Point Protocol (SLAPP) [27]. Dette er de mest brukte protokollene for tunnellering i dagens kommersielle produkter, men det finnes også produsenter, som for eksempel Meru, som benytter en egenutviklet protokoll for denne tunnelleringen. En arbeidsgruppe i The Internet Engineering Task Force (IETF) kalt Control and Provisioning of Wireless Access Points (CAPWAP) har vurdert de vanligste tunnelleringsprotokollene opp mot hverandre og nylig valgt LWAPP som grunnlag for en ny standard for bruk i trådløse nettverk med kontroller. [11]

Ved å fjerne det meste av funksjonaliteten fra aksesspunktene og samle den i sentrale kontrollere, kan en få nettverk som er lettere å administrere og billigere å bygge. Det gir også mulighet til å benytte utstyr fra forskjellige produsenter. Dette forutsetter at kommunikasjonen mellom aksesspunktene og kontrolleren følger de samme standardene hos de ulike utstyrsprodusentene. Det er derfor CAPWAP har laget en standard for tunnellering mellom aksesspunkt og kontroller. Med CAPWAP vil en kunne ta i bruk utstyr fra tredjeparts produsenter i trådløse nettverk med lette aksesspunkt.

Aksesspunktene blir strippet for funksjonalitet og fungerer som fjernstyrte radiofrekvensgrensesnitt for kontrolleren. Ved oppstart av aksesspunkt og kontrollere blir det gjennomført en versjonsutveksling og synkronisering. Etter at denne informasjonen er utvekslet, blir CAPWAP-protokollen brukt for å innkapsle de trådløse datarammene som sendes mellom aksesspunkt og kontroller. CAPWAP vil fragmentere lag 2-rammene dersom størrelsen av den innkapslede trådløse datapakken eller protokollkontrollrammen er så store at den endelige CAPWAP-pakken blir større enn Maximum Transmission Unit (MTU) som er satt mellom aksesspunktene og kontrolleren. Fragmenterte CAPWAP-pakker blir satt sammen igjen for å rekonstruere den originale innkapslede nyttelasten hos mottakeren. Om en pakke er en del av en fragmentering eller ikke, kommer fram av F-bitet i CAPWAP-transportheaderen. Dersom dette bitet er satt til 1, må pakken settes sammen med resten av fragmenteringen i den andre enden. [11] CAPWAP-datatransport headeren er vist i figur 2.4.



Figur 2.4: Transportheaderen til en CAPWAP-pakke

Alle CAPWAP-pakker inneholder denne transportheaderen som en del av innkapslingen. Den angir følgende:

V er et to bit felt som angir versjonsnummeret for CAPWAP-innkapslingen.
RID angir radioID-nummeret til pakken.
F-bitet sier om pakken er en del av en fragmentering.
L-bitet forteller om dette er siste fragmentet i en fragmentering.
R-bitet er reservert og satt til 0.
FragID angir fragmenteringsidentifikasjonen.
Length er et 16 bit felt som gir antall bytes i nyttedatafeltet. [11]

CAPWAP-datapakkene er bygget opp som vist i figur 2.5. Wireless Payload er her hele IEEE 802.11-datarammen (beskrevet i kapittel 3). LWAPP pakker inn hele MAC protocol data unit med unntak av Frame Check Sequence (FCS) som blir behandlet av aksesspunktene. Dette gjør at aksesspunktene kan bekrefte gyldigheten til en ramme før det skal sende rammen til kontrolleren. Når kontrolleren skal sende en ramme til en klient, blir FCS kalkulert og lagt til hos aksesspunktene.

Figur 2.5: CAPWAP-innkapslingen av datapakker

CAPWAP-datapakkene består av en 20 byte IP-header, en 8 byte UDP-header, en 48 byte CAPWAP-header og en nyttelast som består av et TCP/IP-datagram pluss IEEE 802.11 MAC-headeren på 30 byte.

Motivasjonen for å lage et nytt system for trådløse nettverk som inneholder en sentral kontroller, er at det ved skalering av trådløsnettet vil forenkle administrasjonsjobben. Oppgraderinger eller endringer hos aksesspunktene i et trådløst nettverk kan styres fra kontrolleren, slik at man slipper å utføre endringene på hvert enkelt aksesspunkt. En

kontroller gjør det også enklere å overvåke det trådløse dekningsområdet. Aksesspunktene rapporterer til kontrolleren om alle IEEE 802.11 b-, g- eller a-kilder som de oppdager. Dette kan benyttes for å få en kortere roamingtid mellom forskjellige aksesspunkt, til posisjoneringsbestemmelser for klienter, og for å unngå interferens mellom ulike enheter i det trådløse nettverket.

2.2 Rekkevidde

Rekkevidden i et WLAN varierer etter utgangseffekt, valg av antenner og hvilken radiotype som velges. Ved lengre avstander går kapasiteten ned på grunn av svakere signaler. I fri sikt, med de beste antennene, kan rekkevidden være på flere kilometer. Begrensningene i Norge ligger i at det, etter forskriftene om tillatt bruk av frekvenser, er spesifisert en maksimal grense på 100 mW utstrålt effekt for 2,4 GHz frekvensområdet [12]. For 5 GHz frekvensområdet er den maksimale utstrålte effekten satt til 200 mW [12]. I tillegg er det mange hindringer og problemer som kan redusere effekten og nytten i dagens WLAN. Støy og interferens oppstår når andre kilder sender på de samme radiofrekvensene som det trådløse nettverket. I trådløse radionettverk er vegger, mennesker og andre fysiske gjenstander eksempel på hindringer som kan forårsake reduksjon i signalstyrken.

2.3 Frekvenser

Informasjonen i trådløse nettverk blir sendt ved hjelp av bølger ved gitte elektromagnetiske frekvenser. Frekvenser i det elektromagnetiske spekteret spenner fra ingen til uendelig mange svingninger per sekund. Den elektromagnetiske strålingen fremkommer ved at en utstråler energi i form av elektromagnetiske bølger. Frekvensen til et signal betegnes som antall svingninger per sekund og oppgis med måleenheten Hertz (Hz). Frekvensutbredelsen til et signal spenner over et større frekvensområde, men kjernefrekvensen settes til frekvensverdien der signalet er på sitt sterkeste. For et signal vil det, med andre ord, være avtagende stråling for frekvenser både høyere og lavere enn kjernefrekvensen, helt til strålingen etter hvert forsvinner. Frekvensområdet som spenner over den delen av frekvensspekteret der signalet har stråling, deles ofte opp i kanaler der kjernefrekvensen befinner seg midt i kanalens totale frekvensområde. Dersom slike kanaler har så stor båndbredde at et signal kan sendes uten å bruke frekvenser som tilhører nabokanalene, vil ikke signaler forstyrre hverandre, selv om de sendes samtidig.

2.4 Interferens

Interferens oppstår når to eller flere signal møter hverandre med overlappende frekvenser. De enkelte signalenes bidrag adderes og danner et nytt signal med ny amplitude og ny frekvens. Det blir da vanskelig for mottakeren å skille det ene signalet fra de andre, og vi får det vi kaller for interferens. Dersom signalene sendes med forskjellig styrke, vil det sterkeste

signalet overdøve de andre og gjøre det enda vanskeligere for mottakeren av de svakeste signalene å skille dem fra hverandre.

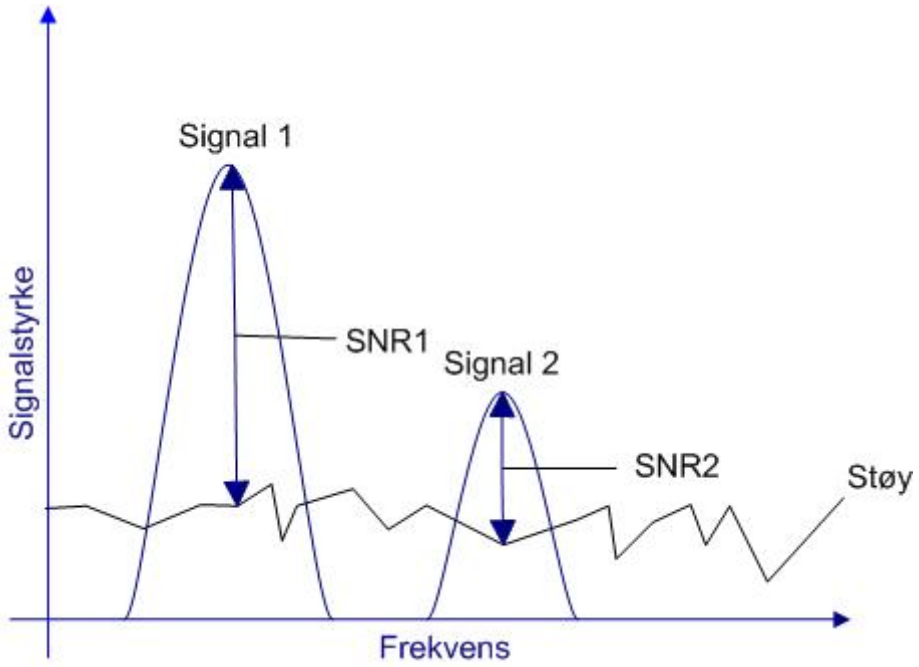
2.5 Lisensbelagte og frie frekvensbånd

For å unngå interferens og konkurranse om luftmediet, har myndigheter i de forskjellige land innført strenge konsesjoner og regler for bruk av radiosignal. De elektromagnetiske frekvensene deles opp i ulike bånd som fordeles ved å tildele konsesjoner for bruk av signaler med gitte frekvenser. På denne måten kan myndighetene avgrense konkurranse i luftmediet og tildele konsesjoner for å gi et best mulig tilbud til innbyggerne i landet. I tillegg til de lisensbelagte frekvensområdene er det frigjort en del frekvensbånd som ikke er konsesjonsbelagte. Disse frekvensbåndene kan fritt disponeres av hvem som helst, innenfor gitte lover og regler. I Norge er det Post- og Teletilsynet (PT) som forvalter bruken av radio og tildeler konsesjoner på vegne av myndighetene. Det er også PT som håndhever og overvåker bruken av elektromagnetiske bølger i landet. For trådløse datanettverk er det frekvensbåndene 2,4 – 2,4835 GHz og 5,15 – 5,725 GHz som er tatt i bruk. Disse frekvensområdene er ulisensierte og kan derfor brukes av de som måtte ønske det. Lisensfrie frekvensbånd fører til at teknologien blir lettere tilgjengelig, men det vil samtidig øke faren for interferens og støy fra andre elektroniske radiosendere. Ved hjelp av regler om blant annet maksimalt utstrålt effekt, vil PT begrense den geografiske rekkevidden til hver enkel radiosender i disse frekvensbåndene. Signaleffekten er en betegnelse på styrken til signalet som igjen bestemmer rekkevidden. [1] [12]

2.6 Signal-/støyforhold

Signal-/støyforhold er et forholdstall som beskriver signalkvaliteten. Det er valgt å benytte et forholdstall for å beskrive dette, fordi kraftig signalstyrke tillater mer støy en det som er tilfellet ved svake signaler. Støyforhold måles i dBm fra -100 til 0, der det er mest gunstig med lave verdier. For eksempel er -80 bedre enn -70. Signalstyrken måles også fra -100 til 0, men her er det beste signalforholdet uttrykt med høyere verdier. En signalstyrke på -30 er et sterkere signal enn -50.

Fordi desibel er logaritmisk, er forholdet mellom signal- og støystyrke (SNR) i dB differansen mellom signal og støy, dersom de er oppgitt i samme dB-enhet. SNR finner vi altså ved å trekke støyverdien fra signalverdien [13]. Dette måltallet sier noe om opplevd signalkvalitet. Jo høyere SNR er, jo bedre er opplevd signalkvalitet.



Figur 2.6: SNR-nivå

Figur 2.6 viser støy og signal i samme graf. Avstanden mellom støygulvet og maksimumstoppen til signalet gir SNR-verdien.

2.7 Kapasiteten til radiosignaler

Kapasiteten til en kanal i frekvensbåndet er gitt ved hjelp ev Shannon Limit som ble utviklet av Claude Shannon i 1948 [13]. Teoremet gir den maksimale grensen for kapasiteten C i bits per sekund som en funksjon av båndbredden W i Hertz og det absolutte SNR-nivået. Funksjon (1) uttrykker maksimal kapasiteten for et gitt frekvensbånd W, der SNR er gitt i desibel. [13]

$$C <= W \log_2 (1 + 10^{(0,1 \times SNR)}) \quad (1)$$

Dette er et teoretisk maksimum for kapasitet i trådløse datanettverk. Med de kanalbåndbreddene som populære standarder for trådløse datanettverk opererer med, vil ikke Shannon Limit sette noen begrensning under normale SNR-forhold.

2.8 Oppsummering

Tradisjonelt har trådløse nettverk blitt satt opp som sammenkoblinger mellom enkeltmaskiner eller som små private hjemmenettverk med et enkelt aksesspunkt. Etter hvert som nettverksutstyr har blitt mer utbredt, har det dukket opp enkelte hotspots der universiteter, bedrifter, restauranter, eller andre kommersielle aktører tilbyr nettaksess til sine brukere eller kunder. De nyeste typene trådløse nettverk er bygget opp med kontrollere som styrer og administrerer aksesspunktene. I slike nettverk er det mulig å oppnå sømløs roaming og

posisjonering av klienter. Med denne arkitekturen kan en tilby nettaksess i store geografiske områder. Hele byer kan bygges ut med nettaksess, og universiteter kan gi studenter og ansatte aksess til et sammenhengende trådløst nettverk over hele campus. Den grunnleggende teknologien bak de forskjellige arkitekturene er den samme. Alle er bygget på internasjonale standarder for trådløse datanettverk. De mest populære standardene er beskrevet i kapittel 3.

De samme utfordringene med å benytte luftmediet til transport av data gjennom radiosignaler gjelder for alle arkitekturene. Utviklingen innen trådløs nettverksteknologi har vært drevet for å takle disse utfordringene best mulig, samt for å kunne tilby en stadig større brukermasse best mulige tjenester over det trådløse nettverket. Nye bruksområder, nye trådløse nettverkstjenester, og nye standarder for trådløse datanettverk vil være med på å utvikle den trådløse nettverksteknologien videre.

3 Trådløse nettverksstandarder

Institute of Electrical and Electronic Engineers (IEEE) har publisert standarder for trådløse datanettverk som benytter de lisensfrie frekvensbåndene som er nevnt i kapittel 2.5. Det er disse standardene som blir benyttet i de fleste av dagens kommersielle WLAN. Den første arbeidsgruppen for trådløse nettverk ved IEEE ble opprettet i 1990 og publiserte IEEE 802.11-standarden for WLAN i juni 1997. Senere har IEEE publisert flere tilleggsstandarder til IEEE 802.11.

3.1 IEEE 802.11-standarden

Den første publiserte IEEE 802.11-standarden var kraftig påvirket av teknologi i produkter som allerede eksisterte på markedet for trådløst datakommunikasjonsutstyr. Standarden beskriver funksjoner og tjenester som kreves av en enhet som skal operere i ad-hoc nettverk eller i trådløse infrastrukturnettverk. I tillegg definerer den aspekter rundt mobilitet. IEEE 802.11 beskriver Medium Access Control (MAC) prosedyrene for å støtte den asynkrone MAC Service Data Unit (MSDU) leveringstjenesten, flere fysiskelag (PHY) signaleringsteknikker, og grensesnittfunksjoner som er kontrollerte av IEEE 802.11 MAC. Målet med arbeidet rundt denne standarden var å finne en spesifikasjon for MAC og PHY for trådløse forbindelser til stasjonære, flyttbare og bevegelige enheter innen et lokalt nettverk [2]. En av målsetningene til IEEE 802.11 var å kunne håndtere mobile klienter, i tillegg til flyttbare klienter. En flyttbar klient er her definert som en klient som blir flyttet fra lokasjon til lokasjon, men som kun blir benyttet som en stasjonær klient. Mobile klienter er derimot tilknyttet LAN mens de forflytter seg. IEEE 802.11 benytter, på det fysiske laget, radiobølger av typen Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) eller Spread Infrared (SIR) [4]. FHSS og DSSS er nærmere beskrevet i kapittel 3.2.1 og 3.2.2.

3.1.1 Protokollhierarkiet

Standarden er definert for de to laveste lagene i OSI-modellen, det fysiske laget og MAC-laget. Sammenhengen mellom OSI-modellen og IEEE 802.11 er vist i figur 3.1. De blå feltene viser de trådløse spesifikasjonene. De overliggende OSI-lagene er de samme som i alle andre IEEE 802-standarder. Det betyr at det i de høyere lagene ikke er forskjell mellom kablede og trådløse medier.

<table>
<tr><td>Lag 7
Applikasjonslaget</td><td rowspan="3">Application Layer</td></tr>
<tr><td>Lag 6
Presentasjonslaget</td></tr>
<tr><td>Lag 5
Sesjonslaget</td></tr>
<tr><td>Lag 4
Transportlaget</td><td>Transport Layer (TCP)</td></tr>
<tr><td>Lag 3
Netverkslaget</td><td>Network Layer (IP)</td></tr>
<tr><td rowspan="2">Lag 2
Datalinklaget</td><td>IEEE 802.2 Logical Link Control (LLC)</td></tr>
<tr><td>IEEE 802.11 Medium Access Protocol (MAC)</td></tr>
<tr><td rowspan="2">Lag 1
Fysiskelag (PHY)</td><td>Physical Layer Convergence Procedure (PLCP)</td></tr>
<tr><td>Physical Medium Dependent (PMD)</td></tr>
</table>

Figur 3.1: IEEE 802.11-plassering i forhold til OSI-modellen

På det fysiske laget er IEEE 802.11, som sagt, definert med flere radioalternativer. Det kan benyttes DSSS, FHSS eller SIR. Figur 3.2 viser hvordan disse alternative valgene opprinnelig er utformet for IEEE 802.11 i forhold til OSI-modellen. Alle de tre radioteknologiene støtter overføring med en datarate på 1 og 2 Mbit/s. De to spread spectrum spesifikasjonene opererer i 2,4 – 2,4835 GHz frekvensområdet, mens SIR PHY opererer i 300 – 428,000 GHz området. Selv om SIR i trådløse nettverk er en teknologi som er sikrere en de to andre med tanke på tredjepersons inntrenging, har denne teknologien liten utbredelse. Dette skyldes i hovedsak at SIR trenger fri sikt fra sender til mottaker, og at SIR kan ødelegges eller påvirkes av sollys. SIR på det fysiske laget, som beskrevet i IEEE 802.11, har ikke blitt implementert i noen kommersielle produkter i stor skala. SIR-teknologien vil derfor ikke bli videre diskutert i denne oppgaven.

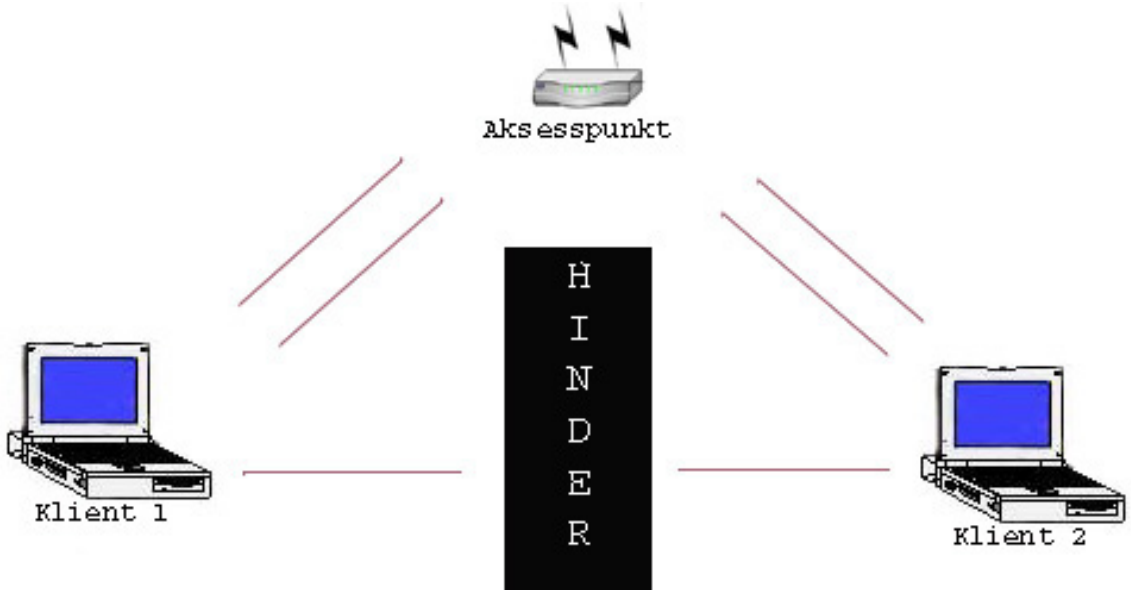
Den opprinnelige IEEE 802.11-standarden spesifiserer en 11-bit chipping metode, kalt Barker Sequence. Denne benyttes for å kode all data som sendes gjennom luften. Hver 11-chip sekvens representerer et enkelt databit som blir konvertert til bølgeform, og som igjen kalles symbol. Disse symbolene blir sendt med en hastighet på en million symboler per sekund (MSps) ved hjelp av en teknikk som heter Binary Phase Shift Keying (BPSK). Når IEEE 802.11 opererer med en datarate på 2 Mbit/s, brukes en annen teknikk som kalles Quadrature Phase Shift Keying (QPSK). Denne metoden dobler dataraten som oppnås med BPSK ved å forbedre effektiviteten på radiobåndet. [1]

<table>
<tr><td colspan="3">IEEE 802.2</td><td rowspan="2">Datalink-
laget</td></tr>
<tr><td colspan="3">IEEE 802.11 MAC</td></tr>
<tr><td>FH</td><td>DS</td><td>IR</td><td>PHY-Laget</td></tr>
</table>

Figur 3.2: Alternativer på det fysiske laget

3.1.2 Aksessmetode

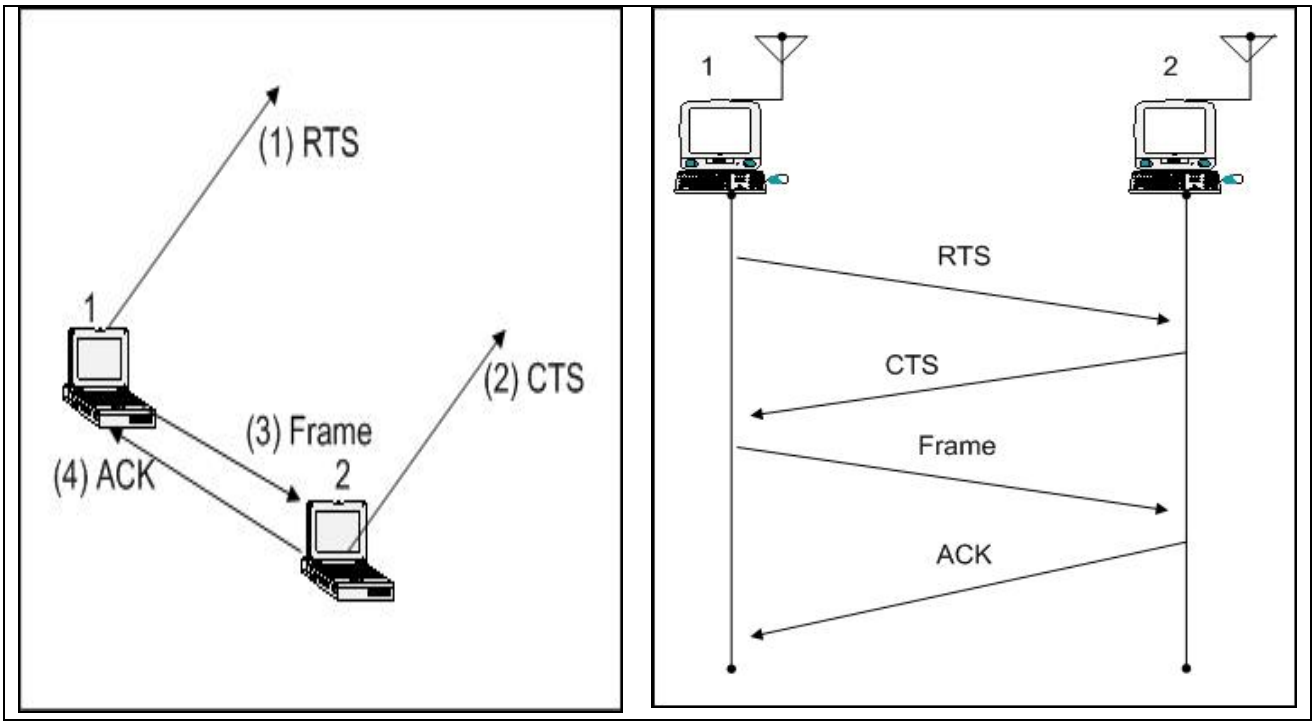
Den grunnleggende aksessmekanismen i IEEE 802.11 blir kalt Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). I en CSMA lytter avsenderen til transmisjonslinjen for å finne ut om den er ledig. Dersom linjen er opptatt, vil avsenderen vente med å sende sine pakker. Når linjen er ledig, starter sendingen. I tilfeller der flere avsendere registrerer at sendekanalen er ledig samtidig og begge starter transmisjonen, vil det likevel kunne oppstå kollisjoner. Disse kollisjonene må kunne detekteres, slik at MAC-laget kan retransportere de ødelagte eller forsvunne datapakkene. Dette gjøres i Ethernet ved bruk av en Collision Detection mekanisme. I WLAN kan ikke denne metoden benyttes fordi det ville ha krevd en full duplex radio som kunne sende og motta samtidig. I tillegg oppstår problemet i et WLAN med at ikke alle enhetene hører hverandre, et såkalt Hidden Node Problem. Dette problemet er vist i figur 3.3. Her har ikke klient 1 mulighet til å kommunisere direkte med klient 2, men begge er tilknyttet det samme aksesspunktet. I dette tilfellet kan ikke klient 2 se pakker som klient 1 sender. I en slik situasjon er klient 1 og 2 skjulte for hverandre. Dersom en transmisjonsprotokoll uten noen form for kollisjonsmekanismer hadde blitt benyttet i et slikt tilfelle, kunne en risikere at både 1 og 2 sendte til aksesspunktet samtidig, og det ville oppstått interferens mellom signalene.



Figur 3.3: Hiden Node-problemet

For å forhindre eventuelle kollisjoner i systemer som beskrevet i figur 3.3, er det utviklet en mekanisme som benytter Request To Send (RTS) og Clear To Send (CTS) signaler. Denne metoden kalles Virtual Carrier Sense (VCS) mekanismen og er illustrert i figur 3.4. Her har klient 1 en pakke som den ønsker å sende. Den gir beskjed om dette ved å sende en RTS. Denne sendingsforespørselen reserverer radiolinken for sending av data og beretter alle klienter som ser RTS om sendingen som skal komme. Når klient 2 mottar RTS, svarer den med å sende ut en CTS. I likhet med RTS varsler denne pakken alle nærliggende klienter om dataoverføringen som kommer. Når RTS/CTS-utvekslingen har funnet sted, kan klient 1

sende datapakken uten fare for innblanding fra skjulte klienter. RTS varsler alle klienter i dekningsområdet til klient 1, mens CTS gjør det samme for alle klienter i dekningsområdet til mottakeren av pakkene. I praksis utføres dette ved at alle klienter som ser en RTS eller en CTS setter VCS-indikatoren lik varigheten til den aktuelle overføringen. Når RTS/CTS blir benyttet, må alle datapakker bekreftes med en Acknowledgment Packet (ACK).



Figur 3.4: Klarering med RTS/CTS
Figuren er laget ut i fra [4]

Sending av RTS/CTS og ACK for hver datapakke genererer ekstra overlast i nettverket. Dette gjør at overføringen av nyttedata blir kraftig redusert. Det er derfor ikke lønnsomt å ha RTS/CTS i nettverk der kapasiteten er lav. Da vil overlasten bruke så mye kapasitet at det vil være bedre å sette opp nettverket uten denne mekanismen, med de risikoer dette medfører når det gjelder skjult klient-problematikken. I den senere tid har i tillegg skjult klient blitt et mindre problem i trådløse nettverk. Enkeltstående aksesspunkt med få tilknyttet klienter har liten sannsynlighet for at klienter som er skjult for hverandre skal starte sending samtidig. Her er det også mye kapasitet for eventuelle retransmisjoner dersom dette skulle skje. Større trådløse nettverk kan settes opp slik at aksesspunktene overlapper på en måte som gjør at alle klienter assosiert til samme aksesspunktet kan kommunisere med hverandre [4]. Utviklingen har derfor gått mot at det er mer vanlig å forsøke å unngå RTS/CTS i trådløse nettverk.

Som en erstatning for RTS/CTS er det tatt i bruk en nyere metode. At alle enhetene hører hverandre er et grunnleggende prinsipp for Collision Detection. For å løse dette bruker IEEE 802.11 Collision Avoidance (CA) som en erstatning. Denne mekanismen kan brukes for å unngå kollisjoner i stedet for den kapasitetskrevende RTS/CTS. Ved bruk av CA lytter avsenderne til transmisjonskanalen for å detektere trafikk. Dersom linjen er opptatt, vil

avsendere avvente sendingen av pakker. Om linjen er ledig i en spesifisert periode kalt Distributed Inter Frame Space (DIFS), kan sendingen starte. Mottakeren vil undersøke Frame Check Sequence (FCS) feltet i headeren til pakken og sende en Acknowledgment Packet (ACK) som bekreftelse på mottatt pakke, etter en Short Inter Frame Space (SIFS). Mottagelse av ACK-meldingen vil være en bekreftelse på at ingen kollisjon oppstod. Dersom mottakeren ikke får en ACK-melding, vil den sende pakken på nytt inntil den får en ACK-melding, eller kaste meldingen etter et visst antall forsøk på retransmisjon. Kapittel 3.1.6 forklarer mer detaljert om mellomrammeavstander i IEEE 802.11. [2] [4]

IEEE 802.11-standarden definerer også en Exponential Backoff algoritme som skal hjelpe til med å redusere muligheten for kollisjon. Denne algoritmen brukes etter at transmisjonen er avsluttet og etter en DIFS. Backoff fungerer ved at hver klient velger et tilfeldig tall (n) mellom 0 og et gitt tall, og venter deretter n antall sloter før den sender over transmisjonslinjen, etter igjen å ha sjekket om den er ledig. Exponential Backoff betyr at for hver gang en klient velger en slot der det kan oppstå en kollisjon, vil maksimumstallet i det tilfeldige utvalget av tall øke eksponentialt. [2]

3.1.3 Oppkobling og Sikkerhet

For å koble seg opp i et BSS må klienten synkronisere seg mot aksesspunktet. Dette kan gjøres på to forskjellige måter [1]:

- Passiv scanning: Klienten venter til den mottar den periodiske rammen, Beacon Frame, med synkroniseringsinformasjon fra AP.
- Aktiv scanning: Klienten forsøker å finne et AP ved å sende ut Probe Request Frames, og venter deretter på Probe Response fra et AP.

Når klienten har funnet et AP som den ønsker å koble seg opp mot, må den gjennom en autentiseringsprosess der den utveksler godkjenningsinformasjon med AP. IEEE 802.11 definerer to autentiseringsmetoder, Open System og Shared Key. Open System er default autentiseringsmetode. Den tilfører egentlig ikke noe sikkerhet til systemet, fordi en oppkoblingsenhet har tillatelse til å koble seg opp mot alle enheter som er innstilt med Open System. Shared Key-autentisering er en mer sikker metode. Den krever at alle enhetene som ønsker å benytte nettverket må ha en delt nøkkel. De som ikke er i besittelse av denne nøkkelen, vil ikke kunne koble seg opp mot nettverket. Oppkoblingsprosessen som blir utført etter dette, består av utveksling av kapasitetsinformasjon. Etter at dette er utført, kan AP begynne med å sende eller motta datarammer på vegne av klienten.

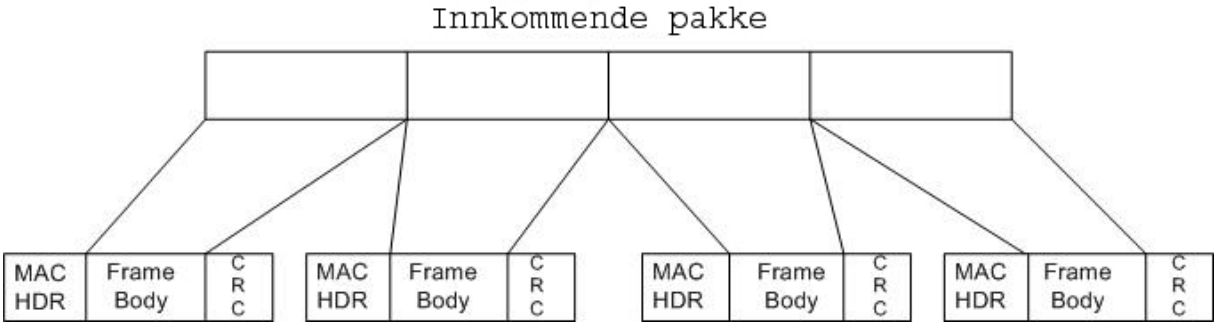
IEEE 802.11 bruker Wired Equivalent Privacy (WEP) algoritmen for å tilby kryptering av data over det trådløse nettverket. WEP bruker hemmelige nøkler for å kryptere data som skal sendes etter at autentiseringen har blitt utført. Denne løsningen er langt i fra sikker mot

angrep, og skaper kun en sikkerhet mot brukere uten angrepskunnskap. WEP-kryptering er nærmere beskrevet i kapittel 3.8.1.

3.1.4 Fragmentering og sammensetting av informasjonsenheter

Fragmentering forekommer når størrelsen på datapakker fra et høyere OSI-lag er større enn en terskel satt av nettverksadministrator. Denne terskelen blir kalt Maximum Transmission Unit (MTU) og settes ofte til 1500 bytes fordi det er den maksimale rammestørrelsen på Ethernet. Trådløse nettverk må kunne håndtere pakkestørrelser som er større enn det som er maksimalt tillatte pakkestørrelser i det trådløse nettverket. Det trengs derfor en metode for å dele opp og sette sammen de store pakkene for å tilpasse dem et WLAN. Dette er gjort i IEEE 802.11 ved å legge til en mekanisme på MAC-laget som kan dele opp og sette sammen informasjonsenheter. Fragmenter av samme pakke har alle det samme rammesekvensnummeret, og har stigende fragmentnummer for å hjelpe til med å sette sammen pakken igjen. Fragmentering er nyttig for å begrense påvirkningen av interferens og andre signalforringende kilder, og dermed øke overføringskapasiteten av nyttedata i nettverket. Dersom pakkene hadde vært større i trådløse nettverk, ville sannsynlighet vært større for at en pakke inneholdt feil. Jo større pakker, jo større sannsynlighet for pakkefeil. Når pakkefeil forekommer, er overlasten mindre dersom pakkestørrelsene er små.

Oppdelinger av rammer gjøres som i figur 3.5. Den store rammen splittes opp i mindre pakker og det blir lagt til en MAC-header og et Cyclic Redundancy Check (CRC) bit i hver av de nye pakkene.



Figur 3.5: Oppdelingen av en ramme som definert i IEEE 802.11-standarden
Figuren er hentet fra [1]

3.1.5 Rammeformater

IEEE 802.11 definerer tre hovedtyper med rammer:

- Datarammer med nytteinformasjon
- Kontrollrammer (for eksempel RTS, CTS og ACK)
- Administrative rammer (for eksempel Beacon rammer)

Alle rammer har den generelle strukturen som vist i figur 3.6.

Preamble	PLCP Header	MAC Data	CRC

Figur 3.6: Den generelle rammestrukturen for IEEE 802.11

Preamble: Innholdet er avhengig av hvilken fysiskelag-teknologi som er brukt. Feltet inneholder alltid synkroniseringsinformasjon som er en 80 bits sekvens med vekslende 0 og 1 bit. I tillegg er rammestartflagget (0000 1100 1011 1101) en del av dette feltet. Dette flagget blir også brukt for timing. [1]

Physical Layer Convergence Procedure (PLCP) Header: Dette feltet er logisk informasjon som brukes av PHY-laget for å dekode MAC datafeltet. Dette er informasjon om hastigheten på overføringen, lengden til pakken og Header Error Check (HEC). [4]

MAC-Data: Figur 3.7 viser den generelle MAC-Data strukturen. [2]

bytes: 2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS
←	MAC Header					→		

Figur 3.7: MAC-datafeltet

Frame Control feltet i figur 3.7 inneholder informasjonen som er vist i figur 3.8. En del av bitene her brukes i fragmenteringen beskrevet i kapittel 3.1.4.

0 | 1	2 | 3	4 | 5 | 6 | 7	8	9	10	11	12	13	14	15
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	Protected Frame	Order
Bits: 2	2	4	1	1	1	1	1	1	1	1

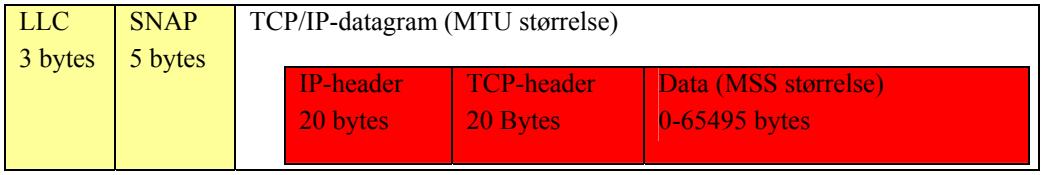
Figur 3.8: Frame Control feltet

- Protocol Version feltet i denne rammen er brukt for å gjenkjenne mulige fremtidige versjoner av IEEE 802.11-standarden. I den originale standarden er dette feltet satt til 0.
- ToDS feltet er satt til 1 dersom rammen er adressert til et AP for videresending til Distribution System (DS). Bitet er satt til 0 i alle andre tilfeller.
- FromDS er satt til 1 dersom rammen kommer fra DS.
- MoreFrag er satt til 1 når det finnes flere fragmenteringer som tilhører samme rammen og kommer etter det gjeldende fragmentet.

- Retry indikerer at dette fragmentet er en retransmisjon av et tidligere sendt fragment. Denne informasjonen vil bli brukt av mottakeren for å finne duplikater.
- Pwr Mgt bitet forteller hvilken Power Management-innstilling mottakeren er i etter transmisjonen.
- More Data brukes både til Power Management og av AP for å fortelle at det er flere rammer i bufferet klar til sending til denne mottakeren.
- WEP-bitet forteller om dataen er kryptert i henhold til WEP-algoritmen.
- Order-feltet forteller om rammen er sendt ved hjelp av Strictly-Ordered service class.

MAC-datafeltet i figur 3.7 blir videre benyttet til:

- Duration/ID er stasjonsID eller varighetsverdien som benyttes av VCS for varighetskalkulasjoner og blir satt ved RTS/CTS som beskrevet i kapittel 3.1.2.
- Address angir mottaker, avsender og en del spesialtilfeller.
- Sequence Control-feltet brukes for å angi rekkefølgen til fragment som tilhører den samme rammen. Informasjonen i dette feltet kan også brukes for å detektere duplikater.
- Frame Body består av innkapslet overføringsdata. Et eksempel på oppbygning av denne er vist i figur 3.9. Den røde delen er TCP/IP-datagrammet som er nyttedata innkapslet i en TCP-header og en IP-header. Fremfor dette datagrammet blir det lagt til en Sub-Network Access Protocol (SNAP) som er en del av IEEE 802.2-standarden. Sammen med Logical Link Control (LLC) er de nødvendige for at IEEE 802.11-pakker skal kunne transportere de forskjellige nettverklagsprotokollene.
- FCS er et 32 bit stort felt som inneholder en 32-bit Frame Check Sequence.



Figur 3.9: Frame Body-oppbyggingen i IEEE 802.11

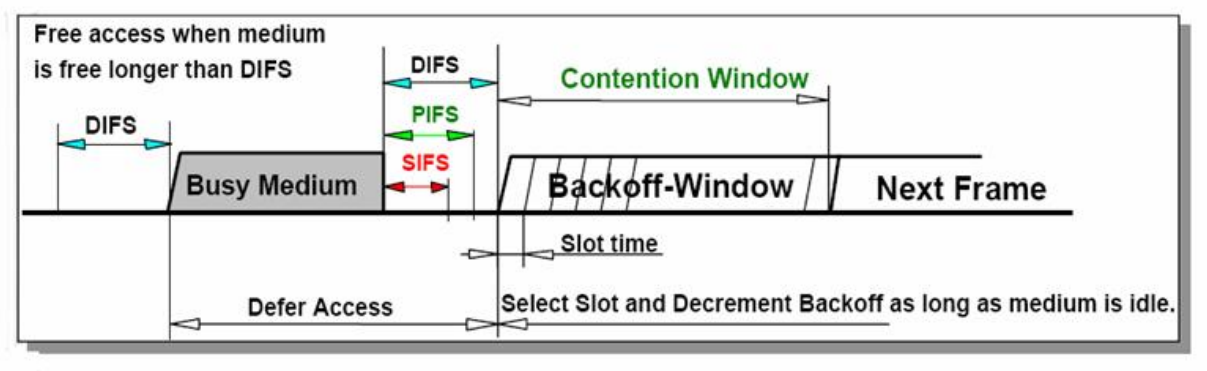
For mer detaljert forklaring av de forskjellige feltene i MAC-datafeltet med underhierarki, vises det til [2].

3.1.6 Prioriteter [2]

Det er definert 4 typer med mellomrammeavstander som brukes for å sette forskjellige prioriteter i IEEE 802.11:

- Short Inter Frame Spaces (SIFS) er minimum mellomrammestørrelse. Størrelsen er definert ut i fra fysiske parametre og er forskjellig for de ulike PHY. SIFS blir brukt for administrasjons- og kontrollpakker.

- Point Coordination Inter Frame Space (PIFS) er SIFS pluss en tidsluke. AP bruker denne mellomrammeavstanden for å få tilgang før noen av de andre enhetene i nettverket.
- Distributed Inter Frame Space (DIFS) er SIFS pluss to tidsluker. Dette er mellomrammeavstanden for en klient som ønsker å starte en ny transmisjon.
- Extended Inter Frame Space (EIFS) er en lenger mellomrammeavstand som brukes av klienter som har mottatt en pakke den ikke forstår. EIFS brukes i dette tilfellet for å unngå at kommende pakke skal bli misforstått av mottakeren.



Figur 3.10: Mellomrammeavstander
Figuren er hentet fra [17]

Figur 3.10 er hentet fra Cisco sine nettsider og illustrerer bruken av de forskjellige mellomrammeavstandene SIFS, PIFS og DIFS. Contention Window i figuren er verdimengden som backoff-tiden kan ha.

3.1.7 Synkronisering

I et strukturert trådløst nettverk er det til en hver tid viktig at enhetene er synkroniserte med AP. Dette blir gjort i IEEE 802.11-standarden ved at alle nettverksklientene oppdaterer klokkene sine mot klokken i AP. AP sender ut periodiske rammer som kalles Beacon Frames. Disse rammene inneholder verdien til klokken i AP ved utsendingstidspunktet. Mottakerne sjekker egen klokke i det de mottar en Beacon Frame og justerer den for å holde seg synkronisert mot AP. Beacon Frames inneholder også informasjon til nye klienter som vil koble seg opp i det trådløse nettverket.

3.1.8 Roaming

I den opprinnelige IEEE 802.11-standarden er det ikke definert noen metode for å utføre roaming. Det er derimot beskrevet noen grunnleggende verktøy for å utføre dette, som for eksempel aktiv og passiv scanning, og gjenoppretting av forbindelse [4]. Scanning er prosessen der en klient identifiserer tilgjengelige trådløse nettverk i området. Forskjellen på passiv og aktiv scanning etter tilgjengelige aksesspunkt er beskrevet i kapittel 3.1.3.

3.2 Spread spectrum radio

Spread spectrum teknologier er fundamentet for å tilpasse ISM-bandet for transmisjon av data. ISM er en fellesbetegnelse for de ulisensierte frekvensbandene og er en forkortelse for industrial, scientific and medical. Som navnet tilsier er spread spectrum en teknologi som sprer signalet over et gitt spektrum, for så å sette det sammen igjen i den andre enden. I IEEE 802.11 er det definert to typer spread spectrum radioteknologier på det fysiske laget, Frequency-Hopping Spread Spectrum (FSSS) og Direct Sequence Spread Spectrum (DSSS). I senere standarder for trådløse nettverk fra IEEE, er det også tatt i bruk en spredd spektrumsteknologi som kalles Orthogonal Frequency Division Multiplex (OFDM). Denne ble først introdusert i IEEE 802.11a, men er senere brukt også i IEEE 802.11g. Her blir den ofte kalt Extended Rate PHY (ERP), men den er vesentlig det samme som OFDM, bortsett fra at den opererer i et lavere frekvensbånd. De forskjellige spektrumsteknologiene definerer bruken av frekvensområdet og hjelper til med å forhindre interferens mellom forskjellige trådløse nettverk.

3.2.1 Frequency-Hopping Spread Spectrum

FHSS sender med stor effekt i et relativt smalt frekvensbånd. Teknologien bruker hele frekvensområdet ved å dele det opp i 79 kanaler på 1 MHz som det kontinuerlig blir hoppet mellom i et gitt mønster [28]. Det finnes totalt 78 slike hoppmønster som aldri lander på den samme kanalen samtidig [28]. Rekkefølgen på hvordan en hopper mellom frekvensbånd gir en koding for signalet som mottakerne vet på forhånd, og som de synkroniserer seg i forhold til. Hoppmønstrene er ortogonale, noe som betyr at ved valg av mønster vil frekvensen som brukes ikke kollidere med et annet hoppmønster. Appendiks A gir en nærmere oversikt over hoppmønsteret i FHSS. Hoppingen mellom frekvensbåndene skjer etter gitte tidsintervall. FHSS definerer en maksimal sendetid på hver kanal. Denne har størrelsesorden 400 ms som default-verdi, men hopping kan foregå i ulike hastigheter. [2] I systemer med mye støy vil det være en fordel å hoppe raskt mellom frekvensbåndene. Dersom støyen er liten, vil det gi mest effektiv dataoverføring når hoppene utføres sjeldnere. I praksis vil de ofte være en del støy i det lisensfrie frekvensområdet som de fleste WLAN benytter. Det er derfor vanlig å hoppe ofte, noe som krever nettverksutstyret som kan takle den raske skiftingen mellom frekvensbåndene. [28]

3.2.2 Direct Sequence Spread Spectrum

DSSS er en enklere spread spectrum radio teknologi som deler opp hele frekvensområdet slik at det er 22 MHz mellom hver frekvenskanal [4]. Denne oppdelingen skaper 14 kanaler som dekker hvert sitt frekvensområde. Oppdelingen av signalet er vist i appendiks B. Signalet spres over et stort frekvensområde, men med lav effekt i hele området. Den lave effekten gjør at flere systemer kan dele samme frekvensområde. Maksimalt kan det være 3 rivaliserende aksesspunkt i det samme området ved bruk av DSSS, uten at det skaper ødeleggende interferens og gjensidige problemer. I DSSS blir hvert databit kodet med en sekvens av sub-

bit, såkalte chip, som kun er kjent av senderen og mottakeren. For alle andre potensielle mottakere vil signalet se ut som tilfeldig støy. Den som skal motta signalet må kjenne til koden, være synkronisert til riktig fase og ha riktig chip-rate for å motta signalet korrekt. I slik asynkron kommunikasjon må hver DSSS-pakke starte med synkroniseringsinformasjon. Deteksjon av slik synkroniseringsinformasjon gjøres ved å sammenligne bitstrømmer med forventede bitmønster. [4] [28]

3.2.3 OFDM

OFDM er en tredje form for utnyttelse av frekvensområdet som har blitt tatt i bruk av trådløse nettverksteknologier, og som har blitt standardisert etter den første IEEE 802.11-standarden. OFDM ble første gang standardisert av IEEE i 802.11a-publikasjonen. Den har som prinsipp at dersom en kanal ikke er nok for å oppnå ønsket overføringshastighet, bruk flere kanaler [4]. Når en ser bort i fra alle de matematiske aspektene med OFDM, er det i enkelhet en metode for å dele opp en stor frekvenskanal i mindre subkanaler. Subkanalene blir så brukt parallelt for å øke overføringskapasiteten. Frekvenskanalen blir delt inn i 8 kanaler som hver er på 20 MHz. Hver av disse kanalene er en multiplekset sum av 48 separate datastrømmer. Hver kanal kan yte 54 Mbit/s i overføringskapasitet og teknologien har derfor større nettverkskapasitet en ved bruk av DSSS eller FHSS. OFDM splitter opp signalene, sender dem parallelt via de forskjellige kanalene, og setter dem sammen igjen. I tillegg til å øke kapasiteten i nettverket, skjermer OFDM-signalene bedre mot interferens. [4] [8]

3.3 IEEE 802.11a

IEEE 802.11a-standarden kom som det første tillegget til IEEE 802.11 i 1999. Den støtter teoretisk dataoverføring på opptil 54 Mbit/s på 5 GHz frekvensbåndet og bruker OFDM som moduleringsteknikk på det fysiske laget. 2,4 GHz frekvensbåndet er hyppig brukt, og faren for interferens er ikke like stor på det mindre benyttede 5 GHz båndet. I tillegg til å forsøke å lage en standard som støttet høyere overføringshastighet, var dette motivet for å lage en tilleggsstandard på et nytt frekvensbånd. Det er kun på det fysiske laget at IEEE 802.11a skiller seg vesentlig fra den opprinnelige IEEE 802.11-standarden.

3.3.1 Forandringer på PHY laget

Radiospekteret blir ved bruk av OFDM delt inn i kanaler på samme måte som for DSSS. Størrelsen på hver av disse kanalene er på 20 MHz. IEEE 802.11a kan tilby flere kanaler som ikke overlapper hverandre enn det standarder på 2,4 GHz frekvensbåndet kan. IEEE 802.11a har derfor store fordeler i miljøer med mange brukere og der applikasjoner med høy datagjennomstrømning er i bruk. Hver av de 20 MHz kanalene er oppbygd av 52 subkanaler der 48 blir brukt til å overføre data. Disse subkanalene har en frekvensavstand på 0,3125 MHz [8]. For å transportere data ved hjelp av subkanaler, bruker IEEE 802.11a en moduleringsteknikk som kalles Quadrature Amplitude Modulation (QAM) på hver subkanal.

Den totale kapasiteten for en radiokanal fremkommer ved å multiplisere antall subkanaler med antall bits per kanal. Dersom en kanal bruker moduleringsteknikken 64-QAM på hver subkanal, kan den transportere seks bits per kanal. [4] Når IEEE 802.11a har 48 slike underkanaler for å transportere data, vil den ha en kapasitet på 288 bits per kanal. Hver kanal i denne standarden har 48 slike subkanaler. De 48 kanalene er derfor en multipleks av 48 separate datastrømmer. De kodede bitene blir sendt til de riktige subkanaler ved hjelp av gitte forutbestemte regler. [4]

OFDM systemet tilbyr et trådløst nettverk med teoretisk overføringskapasitet på 6, 9, 12, 18, 24, 36, 48 og 54 Mbit/s. Støtte for sending og mottaking av data med en rate på 6, 12 og 24 Mbit/s er påkrevd av alle operative enhetene i et slikt nettverk [8].

IEEE 802.11a bruker forskjellige moduleringsteknikker for de forskjellige overføringshastighetene som standarden støtter. Det fysiske laget benytter en symbolrate på 250 000 symbol per sekund over de 48 subkanaler [4]. Forskjellen mellom antall kodede bits per symbol og databits per symbol i tabell 3.1, viser overlast som følge av redundante bit som blir benyttet til feilretting i overføringen. Tabellen viser også de ulike moduleringsskjemaene ved de forskjellige overføringshastighetene. For høyere overføringsrater benytter IEEE 802.11a forskjellige variasjoner av QAM. [8]

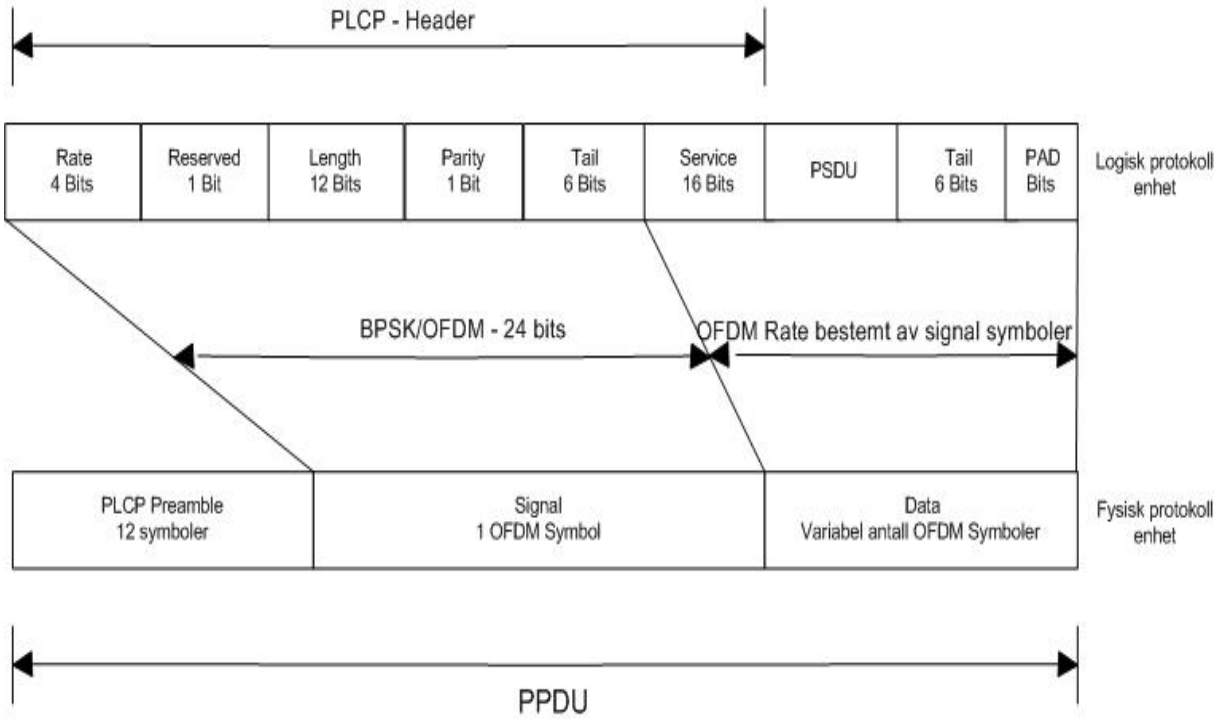
Overføringshastighet	Moduleringsskjema	Kodede bits per subkanal	Kodede bits per symbol	Databits per symbol
6	BPSK	1	48	24
9	BPSK	1	48	36
12	QPSK	2	96	48
18	QPSK	2	96	72
24	16-QAM	4	192	96
36	16-QAM	4	192	144
48	64-QAM	6	288	192
54	64-QAM	6	288	216

Tabell 3.1: Kodede bits per symbol i forhold til databits per symbol for de ulike overføringshastighetene i IEEE 802.11a

Tabellen er hentet fra [4]

3.3.2 Rammeformat

I likhet med alle andre fysiskelag-standarder for trådløse nettverk, inkluderer OFDM PHY en egen Preamble og en egen PLCP. Rammeformatet til alle IEEE 802.11-standardene er lik den som er vist i figur 3.6, men med ulike variasjoner i Preamble og i PLCP. IEEE 802.11a legger til en egen Preamble, PLCP og avslutningsbits som hjelper det aktuelle kodingsskjemaet. Figur 3.11 viser OFDM PLCP-rammeformatet. Vi ser at overlasten i denne pakken, som tidligere nevnt, er Preamble og PLCP. I tillegg kommer også avslutningsbitene.



Figur 3.11: Rammeformat for OFDM PLCP
Figuren er hentet fra [8]

Preamble: OFDM-protokollen starter med en 12 OFDM symbol Preamble. Denne synkroniserer mottaker og avsender og utfører enkelte administrative oppgaver mellom dem.

PLCP header: PLCP-headeren er transportert i hele signalfeltet på det fysiske laget og inkluderer også serviceblokken i datafeltet. Figur 3.12 viser signalfeltdelen av PLCP-headeren.

0 | 1 | 2 | 3	4	5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16	17	18 | 19 | 20 | 21 | 22 | 23
Rate	Reserved	Length	Parity	Signal Tail
Bits: 4	1	12	1	6

Figur 3.12: Signalfeltdelen av PLCP-headeren

- Rate bruker de 4 bitsene til å oppgi hvilken datarate som er brukt.
- Reserved er ment for fremtidig bruk og er satt til 0.
- Lenght feltet forteller hvor mange byte som er i den påfølgende MAC-rammen.
- Parity bitet brukes for å sikre mot datakorrupsjon.
- Signal Tail er seks nuller som er brukt for å avvikle innkapslingen.
- I tillegg består PLCP-headeren av en 16 bits serviceblokk i datafeltet. De første 6 bitene her er satt til 0 for å markere starten til den påfølgende

MAC-sammensetningen. De resterende bitene i dette feltet er satt til 0, men kan bli benyttet i fremtidige bruksområder.

Data: Kodingsskjemaet som er brukt for dataen er avhengig av dataraten. Før transmisjon er dataen sammensatt på samme måte som for andre fysiskelag-teknologier. Denne delen forandrer seg ikke for de forskjellige IEEE 802.11-standardene på det fysiske laget. Serviceblokken til PLCP-headeren er innlemmet i datafeltet for å markere starten til rammesammensettingen. Datafeltet slutter med en hale, eller en Trailer, som består av en 6 bits Trail og en Pad av variabel lengde. De 6 Trail-bitene markerer slutten på rammesammensettingen, mens Pad blir brukt for å gjøre den totale rammestørrelsen lik rammestørrelsen definert i IEEE 802.11a. [8]

I likhet med andre fysiskelag-standarder krever IEEE 802.11a at det sendes en ACK-melding etter at en datapakke er mottatt. Denne ACK-meldingen må sendes med en rate som støttes av alle klienter i nettverket. Det vanligste er at enheter sender denne ACK-meldingen med en hastighet på 24 Mbit/s fordi dette minimerer overlasten i nettverket. [4]

3.4 IEEE 802.11h

5 GHz frekvensbåndet, som blir brukt av IEEE 802.11a-standarden, har i mange land tradisjonelt vært benyttet til militært utstyr, radarer og satellitter. International Telecommunication Union (ITU) har derfor foreslått regler som gjør at IEEE 802.11a-standarden kan operere på 5 GHz frekvensbåndet uten å ødelegge eller forstyrre den eksisterende trafikken på dette båndet. I oktober 2003 ble standarden IEEE 802.11h publisert av IEEE. Den definerer mekanismer som gjør at IEEE 802.11a-produkter kan benyttes i henhold til anbefalingene fra ITU. Hovedmekanismene som brukes i standarden er Dynamic Frequency Selection (DFS) og Transmit Power Control (TPC).

DFS brukes for å detektere andre enheter som benytter den samme radiokanalen. Dersom den oppdager tilfeller av sammenfallende radiokanalvalg, vil den skifte trafikken over til andre kanaler. Det kan derfor sies at denne mekanismen har ansvaret for å unngå interferens med andre aktører på frekvensbåndet.

TPC brukes også for å redusere faren for interferens. Denne mekanismen styrer signalstyrken som det sendes med i det trådløse nettverket. Aksesspunktene informerer klientene i nettverket om maksimum tillatt signalstyrke og om gjeldende signalstyrke i nettverket.

I tillegg til at DFS og TPC brukes for å tilfredsstille de ulike krav fra myndigheter, kan de også benyttes til små administrative oppgaver i trådløse nettverk på 5 GHz båndet [31].

3.5 IEEE 802.11b

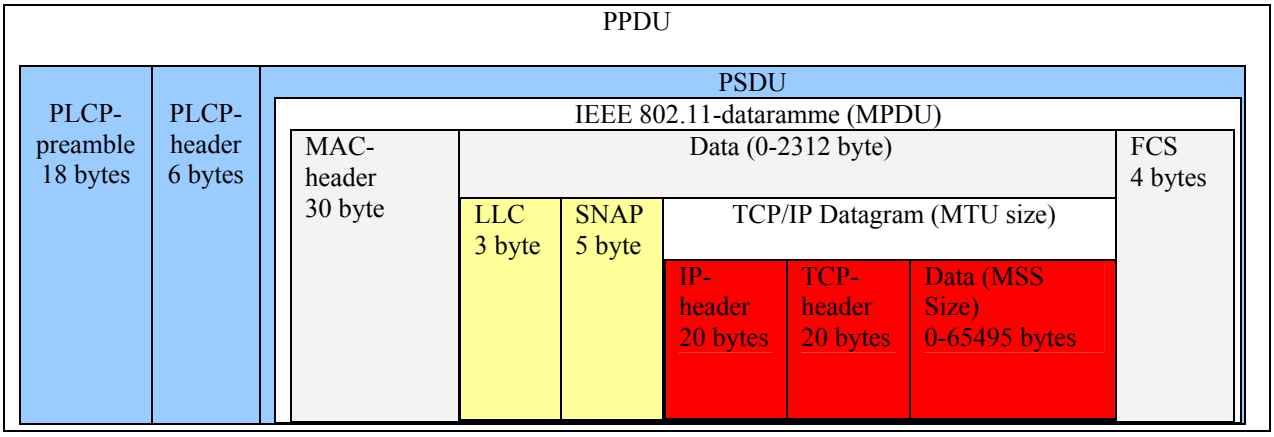
I den originale IEEE 802.11-standarden er det definert to spread spectrum teknologier på det fysiske laget. DSSS og FHSS opererte med de samme overføringshastighetene på 1 og 2 Mbit/s. Det tok imidlertid ikke lang tid før DSSS ble brukt i en ny standard med mye større overføringsrater enn det som var tilfellet med den originale standarden. I juli 1999 kom IEEE med en ny standard for det fysiske laget som tok i bruk DSSS. Den maksimalt teoretiske overføringskapasitet for IEEE 802.11b er på 11 Mbit/s, og standarden tar i bruk det lisensfrie 2,4 GHz båndet. Det var med dette tillegget at utbredelsen av trådløse nettverk for alvor nådde det kommersielle markedet. Selv om IEEE 802.11a ble ferdig standardisert tidligere enn IEEE 802.11b, tok det forholdsvis lang tid før 5 GHz frekvensbåndet ble fristilt til allmenn bruk i alle de store kommersielle markedene. I tillegg brukte IEEE 802.11b det samme frekvensbåndet som originalstandarden, slik at det var enklere å oppgradere eksisterende utstyr til denne standarden. Disse faktorene var avgjørende for at det var IEEE 802.11b-produkter som først ble kommersielt masseprodusert. Det ble etter hvert vanlig med trådløst utstyr i bærbare og håndholdte datamaskiner, og antall private WLAN og offentlige ”hotspots” eksploderte.

3.5.1 Kapasitetseffekt

Med IEEE 802.11b ble den opprinnelige standarden utvidet til en båndbredde på 11 Mbit/s i 2,4 GHz frekvensbåndet ved bruk av DSSS. For å oppnå dette ble en såkalt Complementary Code Keying modulering tatt i bruk. Det nye tillegget brukte likevel den samme CSMA/CA-protokollen på MAC-laget som den opprinnelige standarden, som medfører en overføringskapasitet for nyttedata som er langt mindre enn den fysiske overføringskapasiteten. For IEEE 802.11b er overlasten ved sending av datapakker i form av PLCP Preamble, PLCP-header, MAC-header, LLC/SNAP-header og TCP/IP-header. I tillegg kan vi få ekstra nettverksoverlast på grunn av pakkekollisjoner, fragmenteringer, RTS/CTS og ACK-meldingsutveksling.

3.5.2 Dataramme

Datarammen i IEEE 802.11b er bygd opp som vist i figur 3.13. Den røde delen er TCP/IP-datagrammet som består av nyttedata innkapslet i en TCP-header og en IP-header på 20 byte hver. Fremfor dette datagrammet blir det lagt på en Sub-Network Access Protocol (SNAP) som er en del av IEEE 802.2-standarden. Sammen med Logical Link Control (LLC) er de nødvendige for at IEEE 802.11-pakker skal kunne transportere de forskjellige nettverkslag-protokollene. Alt dette, sammen med en 30 byte MAC-header og en 4 byte FCS, utgjør IEEE 802.11-datarammen eller det som kalles MAC Protocol Data Unit (MPDU). Til slutt er dette pakket inn i en PLCP-header på 6 byte og en PLCP-preamble på 18 bytes. Preambelen blir brukt som en start på datapakken for at mottakeren skal vite at det kommer en datapakke. Den inneholder informasjon som aksesspunkt og klienter trenger for å sende og motta pakker. [9] PLCP Preamble kan være en 18 bytes long preamble eller en 9 bytes short preamble [4].



Figur 3.13: Innkapslingen i en IEEE 802.11b-dataramme

Short preamble gir mindre overlast enn long preamble. Ulempen med short preamble er at det kan være enkelte klienter i nettverket som ikke støtter denne preamble. IEEE 802.11b introduserte short preamble som en valgfri tilleggsfunksjonalitet for å øke overføringshastigheten av nyttedata. Dersom det er klienter i nettverket som ikke støtter short preamble, blir long preamble benyttet av alle enheter.

3.5.3 Forandringer på PHY-laget

Forandringene i IEEE 802.11b-standarden i forhold til den originale standarden, ligger på det fysiske laget. For å kunne tilby høyere datarate bruker IEEE 802.11b DSSS. Det medfører at IEEE 802.11b er kompatibelt med den originale standarden kun dersom den originale standarden benytter DSSS for hastighetene 1 og 2 Mbit/s. For å skille den nye DSSS teknologien fra DSSS i den originale standarden, betegnes IEEE 802.11b-versjonen som High Rate Direct Sequence Spread Spectrum (HS/DSSS).

Den opprinnelige IEEE 802.11-standarden spesifiserte en 11-bit stor Barker Sequence chipping metode som bruker BPSK eller QPSK som transportprotokoller. For å øke dataraten i IEEE 802.11b tilføres avansert koding på det fysiske laget. I stedet for de to 11-bit Barker sekvensene brukes Complementary Code Keying (CCK) som består av et sett med 64 8-bit kodeord. Disse kodeordene har unike matematiske egenskaper som gjør at de kan skilles fra hverandre av en mottaker. 5,5 Mbit/s bruker en CCK for å kode 4 bits per sending, mens 11 Mbit/s bruker dobbelt så mange bit. Tabell 1 viser de forskjellige dataratespesifikasjonene som er definert for IEEE 802.11b. [6]

For å kunne støtte tilfeller der støy og andre påvirkninger ødelegger for overføringshastigheten, definerer IEEE 802.11b en metode for å skifte datarate automatisk. Under ideelle forhold vil en bruker kunne sende med 11 Mbit/s. Dersom forholdene blir dårligere, vil IEEE 802.11b kompensere for dette ved å justere dataraten ned til 5.5, 2 eller 1 Mbit/s. Blir forholdene bedre igjen, vil dataraten justeres trinnvis opp.

Datarate	Kodelengde	Moduleringsskjema	Symbolrate	Bits/Symbol
1 Mbit/s	11 (Barker Sequence)	BPSK	1 MSps	1
2 Mbit/s	11 (Barker Sequence)	QPSK	1 MSps	2
5,5 Mbit/s	8 (CCK)	QPSK	1.375 MSps	4
11 Mbit/s	8 (CCK)	QPSK	1.375 MSps	8

Figur 3.14: Dataratespesifikasjoner for IEEE 802.11b
Tabellen er hentet fra [6]

3.6 IEEE 802.11g

I juni 2002 kom IEEE med en ny standard for trådløse nettverk, IEEE 802.11g. Den nye standarden har en teoretisk overføringskapasitet på 54 Mbit/s i det lisensfrie 2,4 GHz frekvensområdet. IEEE 802.11g-standarden er kompatibel med radioutstyr bygget på 802.11b-standarden, og bruker på lik linje med IEEE 802.11a, OFDM som modelleringsteknikk på det fysiske laget. I tillegg støtter den altså DSSS for å være kompatibel med tidligere standarder, og for å kunne tilby flere datarater. [10] Tabell 3.15 viser en oversikt over hvilke teknologier som er definert i IEEE 802.11g for de forskjellige dataratene. Kompatibiliteten med b-standarden gjør at IEEE 802.11g-nettverk kan brukes av den store brukergruppen som allerede har investert i utstyr som bygger på IEEE 802.11b. Dette ga standarden et stort fortrinn i forhold til IEEE 802.11a når det gjaldt byttekostnader for de eksisterende brukerne av trådløs nettverksteknologi.

Datarate (Mbit/s)	Overføringsteknologi	Moduleringsskjema
54	OFDM	64 QAM
48	OFDM	64 QAM
36	OFDM	16 QAM
24	OFDM	16 QAM
18	OFDM	QPSK1
12	OFDM	QPSK
11	OFDM	CCK2
9	OFDM	BPSK3
6	OFDM	BPSK
5,5	DSSS	CCK
2	DSSS	QPSK
1	DSSS	BPSK

Figur 3.15: Realiseringsteknikker for de forskjellige dataratene i IEEE 802.11g
Tabellen er hentet fra [10]

3.6.1 Kapasitet og dekningsgrad

I likhet med IEEE 802.11b kan denne standarden tilby tre ikke-overlappende kanaler. Kapasiteten til et IEEE 802.11g-nettverk er bestemt av en rekke påvirkninger fra miljøet nettverket er satt opp i. Den viktigste av disse er om det finnes enheter som benytter IEEE 802.11b-standarden i nettverket eller ikke. IEEE 802.11b bruker CSMA/CA som ikke klarer å detektere OFDM-overføringer. Disse pakkene forekommer kun som støy for b-enheter, noe som gjør at de ikke kan dekode datapakker, administrative pakker, eller kontrollpakker som er sendt med OFDM. For at standarden skal være kompatibel med b-standarden og støtte samkjøring, har IEEE 802.11g definert beskyttelsesmekanismer. Den sikreste av disse beskyttelsesmekanismene tar i bruk Request to send/Clear to send (RTS/CTS). Når IEEE 802.11b-enheter kobler seg opp i et IEEE 802.11g-nettverk, kobles RTS/CTS inn. Klienter må da først spør etter aksess til aksesslinjen med RTS, for så å vente på CTS fra AP før den kan starte sending av data. Dette er nærmere beskrevet i kapittel 3.6.2. Beskyttelsesmekanismene er utviklet for å unngå at IEEE 802.11b-enheter sender samtidig med IEEE 802.11g-enheter og forhindrer derfor kollisjoner. Den skaper imidlertid en del ekstra overlast i nettverket og resulterer dermed i en lavere effektiv dataoverføring. I tillegg må IEEE 802.11g tilpasse seg backoff-metodene som brukes i IEEE 802.11b for å støtte kompatibiliteten. Denne gir en lavere ytelse en hva som er tilfelle med IEEE 802.11a-standarden sin backoff-metode, som også blir brukt av g-standarden dersom det ikke er b-komponenter i nettverket. [10] Selv om IEEE 802.11g har nesten samme effektive dataoverføring som IEEE 802.11a, har den, som sagt, bare tre ikke-overlappende kanaler. Det betyr at IEEE 802.11a er mindre utsatt for interferens og er mer velegnet i miljøer der det er mange aksesspunkt.

3.6.2 Forandringer på det fysiske laget

IEEE 802.11g er en sammensmelting av mange ulike fysiskelag-teknologier, alt etter hvilke forhold som råder. Extended Rate PHY Direct Sequence Spread Spectrum (ERP-DSSS) og Extended Rate PHY Complementary Code Keying (ERP-CCK) brukes i IEEE 802.11g for å støtte kompatibilitet med den originale DSSS på 1 og 2 Mbit/s, og med IEEE 802.11b-hastighetene 5,5 og 11 Mbit/s. Extended Rate PHY Orthogonal Frequency Division Multiplex (ERP-OFDM) er hovedteknologien for IEEE 802.11g. Dette er omtrent den samme teknologien som IEEE 802.11a bruker, bortsett fra at ERP-OFDM sender på 2,4 GHz frekvensbåndet. De små endringene i forhold til IEEE 802.11a er gjort for at teknologien skal være kompatibel med tidligere standarder på det samme frekvensbåndet. IEEE 802.11g støtter, i likhet med IEEE 802.11a, teoretiske hastigheter på 6, 9, 12, 18, 24, 36, 48 og 56 Mbit/s. I tillegg til ERP-DSSS og ERP-CCK nevner standarden to valgfrie teknologikombinasjoner for IEEE 802.11g. Disse er imidlertid ikke ofte implementert i trådløst nettverksutstyr. [4]

Da IEEE 802.11g ble standardisert, ble det tatt i bruk allerede eksisterende teknologier på det fysiske laget. Endringer på disse teknologiene ble gjort for å gjøre standarden kompatibel med eksisterende standarder på 2,4 GHz frekvensbåndet. IEEE 802.11b støtter både DSSS fra den

originale standarden og HR/DSSS med CCK. IEEE 802.11g inneholder begge disse teknologiene med noen små endringer, i tillegg til ERP-OFDM som baserer seg på IEEE 802.11a. Fordi IEEE 802.11g er utviklet for å være kompatibel med IEEE 802.11b, må den ha mekanismer som gjør at de forskjellige fysiskelag-teknologiene kan samkjøre i et nettverket. Produkter med g-standarden har ingen problemer med å motta pakker fra b-standard-produkter. Utfordringen er imidlertid at IEEE 802.11b-produkter ikke klarer å forstå informasjon som er sendt med høyere hastigheter med IEEE 802.11g-standarden. Dersom et aksesspunkt skal betjene trafikk fra både IEEE 802.11b og IEEE 802.11g, må det sende ut Beacon frames med en overføringsrate som ikke overstiger 11 Mbit/s. I tillegg må der være en mekanisme som kan informere IEEE 802.11b-enheter om at der er IEEE 802.11g-trafikk i nettverket. Dette kan gjøres på to forskjellige måter:

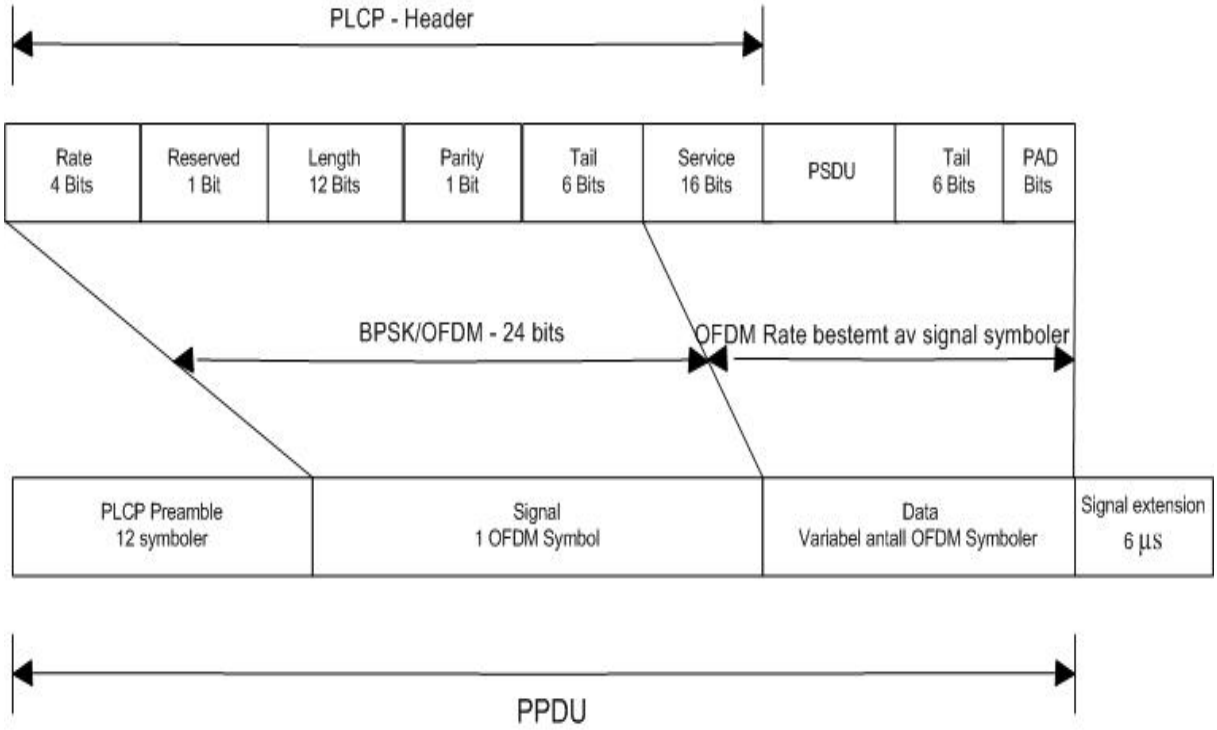
- Den ene metoden er at IEEE 802.11g-klienter bruker CTS for å beskytte sin egen trafikkstrøm. Når klienten har en pakke som den ønsker å sende, vil den først sende en CTS med sin egen MAC-adresse som mottaker. I denne CTS-meldingen vil klienten opplyse andre assosierte klienter om at den vil bruke radiolinken i den tidsperioden det tar å overføre CTS, OFDM-rammene og ACK-meldingene. Ved å sende CTS til seg selv på denne måten, er en sikret at klienter på nettverket har fått oppdatert sin informasjon om hvor lenge nettverket er opptatt. CTS sendes med en hastighet og en dekoding som gjør at alle klienter kan lese den. Dette medfører naturligvis en betraktelig reduksjon i overføringskapasitet av nyttedata for nettverket.
- Den andre beskyttelsesmetoden for samtrafikk er en sikrere metode for at også skjulte klienter skal kunne registrere reserveringen av transmisjonsmediet. Den oppnår samkjøring av trafikken fra de to standardene ved å utføre en full RTS/CTS-utveksling. Denne mekanismen er mer robust og sikrere enn den første, men medfører samtidig et enda større ytelsestap i overføringskapasitet.

Beskyttelsesmekanismene og det ekstra overlast de medfører, blir aktivert med en gang en IEEE 802.11b-klient kobler seg opp i et IEEE 802.11g-nettverk. ERP-informasjonen i Beacon frames blir da satt ved hjelp av et informasjonsbit. Når dette bitet er satt, må klienter bruke beskyttelsesmekanismen for å forhindre interferens med IEEE 802.11b-klienter. I nettverk med et aksesspunkt er det aksesspunktet som bestemmer når beskyttelsesmekanismer skal aktiveres. I den nyeste trådløse nettverksarkitekturen med sentrale kontrollere, blir denne avgjørelsen gjort av kontrolleren. Konsekvensene disse beskyttelsesmekanismene har for overføringskapasiteten i nettverket er kalkulert i kapittel 5.2.1.3.

3.6.3 Dataramme

De forskjellige fysiskelag-teknologiene som er nevnt i dette kapittelet, har ulike rammeformater. Som nevnt er ERP-OFDM hovedteknologien i IEEE 802.11g. Det er denne teknologien som må støttes av alle IEEE 802.11g-produkter. Rammeformatet til ERP-OFDM er nesten identisk med rammeformatet i IEEE 802.11a. Den eneste forskjellen er at det bak

rammen er satt inn en 6 µs Idle tid, kalt signal extension [4]. Dette oppholdet er satt inn for å gjøre tidsberegninger og hyppigheten til rammeankomstene identisk med IEEE 802.11a. Dette er ulikt fordi IEEE 802.11a bruker 16 µs SIFS, mens IEEE 802.11g bruker 10 µs for å være kompatibel med 802.11b. [8] [20]



Figur 3.16: Rammeformatet i ERP-OFDM
Figuren er hentet fra [20]

Med små endringer er dette rammeformatet identisk med rammeformatet til IEEE 802.11a. Preamble er identisk med 802.11b-preamble og består av et synkroniseringsfelt og et rammestartfelt. Preamble kan være kort eller lang og overføres med en hastighet på 1 Mbit/s [4].

3.7 IEEE 802.11e

IEEE 802.11e er en av de tilleggsstandardene det er knyttet seg størst forventninger til. Den kan vise seg å bli nyttig for utvikling av en rekke nye tjenester over trådløse datanettverk. Standarden ble ferdigstilt i november 2005 og er enda ikke implementert i det meste av dagens nettverksutstyr. IEEE 802.11-WLAN tilbyr best-effor-tjeneste i likhet med Ethernet. I kablet Ethernet har man neglisjert QoS-spørsmålet fordi dataraten er veldig høy, og fordi feilraten er lav på slike kabler. Det samme er ikke tilfellet for IEEE 802.11-nettverk. Her innholder datapakkene en del overlast. Dette fører til at transportkanalen ikke blir utnyttet like bra som i Ethernet. I tillegg gir kontrollrammer dårligere overføringskapasitet for nyttedata. De fleste multimediatjenester er avhengige av garantert QoS for å fungere som de skal. Dersom dataraten de sender med overstiger en viss grense i et WLAN, vil tjenesten lide på

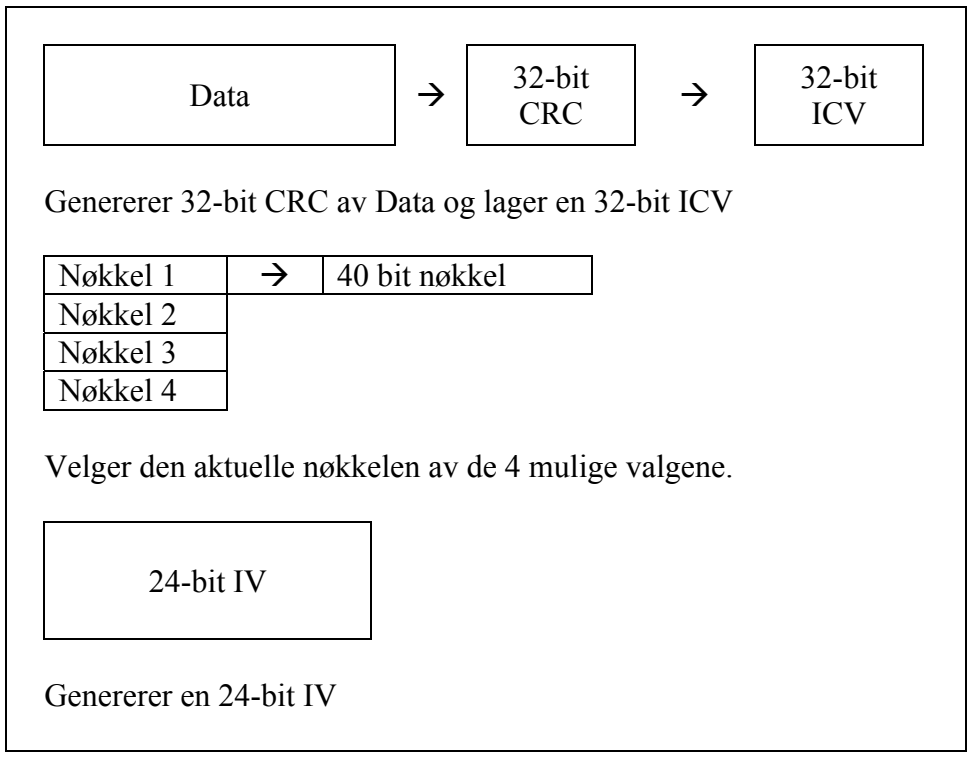
grunn av forsinkelser og pakketap. Dette er en stor hindring ved benyttelse av sanntidsapplikasjoner over trådløse nettverk. IEEE 802.11e har foreslått en del endringer på MAC-laget for å kunne tilby QoS i trådløse nettverk. Sanntidsdata vil med denne standarden få høyere prioritet enn data som ikke er avhengige av konstant pakkestrøm. For eksempel vil applikasjoner som bruker VoIP, lyd- og bildestreaming kunne utnyttes bedre i WLAN med denne tilleggsstandarden.

Den opprinnelige IEEE 802.11-standarden støttet ingen prioriteringsnivåer mellom forskjellige typer trafikk på MAC-laget. Med IEEE 802.11e vil en innføre en forsterkning på MAC-laget som gir åtte prioriteringsnivå for datatrafikk [6]. Klienter forsøker å sende data etter at de har sjekket om transmisjonsmediet er ledig og etter å ha ventet en tidsperiode som er definert av trafikkprotokollen Arbitration Interframe Space (AIFS). De pakkene med høyest prioritet, vi ha kortest AIFS med IEEE 802.11e. På denne måten kan pakker som er avhengig av liten forsinkelse, få prioritet fremfor pakker fra applikasjoner som ikke stiller like strenge krav til pakkeforsinkelse. [4]

3.8 Sikkerhet i trådløse nettverk

3.8.1 WEP

Wired Equivalent Privacy (WEP) er en krypteringsteknikk for trådløse nettverk som tar i bruk Ron's Code 4 Pseudo Random Number Generator (RC4 PRNG) fra RSA Data Security Inc.



Figur 3.17: WEP-kryptering

WEP spesifiserer en 40-bit eller en 104-bit krypteringsnøkkel. Noen produkter har også implementert 232-bit nøkler [4]. Krypteringsnøkkelen blir lagt sammen med en 24-bit initialiseringsvektor (IV), og blir til sammen 64-bit eller 128-bit. WEP-krypteringen genererer 32-bit CRC (Cyclic Reduncdancy Code) av Data og lager en 32-bit Integiry Check Value (ICV). Deretter velges den aktuelle nøkkel ut av 4 mulige, hvor hver nøkkel består av 10 heksadesimale verdier, og genererer en 24-bit IV. Etter det legges den 24-bits IV-en sammen med den 40-bits nøkkelen og kjøres gjennom RC4-algoritmen for å få en nøkkelstrøm. ICV blir lagt til datapakken som skal sendes og utført XOR med nøkkelstrømmen. Resultatet blir en ferdig kryptert datapakke. Etter å ha lagt til IEEE 802.11-headeren og en 24-bit IV, kan pakken sendes kryptert over nettet. [23] Denne krypteringen er vist ved hjelp av figur 3.17.

Når mottakeren skal dekryptere pakken, utføres den reverserte prosessen. Den 24-bits IV-en og den samme 40-bits nøkkelen som ble brukt av senderen, blir kjørt igjennom RC4 for å generere en nøkkelstrøm. Den krypterte pakken blir tatt XOR på mot nøkkelstrømmen, og resultatet blir den dekrypterte datapakken og ICV. Mottaker utfører så en CRC på dataen, og resultatet blir sammenlignet med ICV-en som ble sendt sammen med datapakken. Pakken blir kastet dersom disse to verdiene ikke er identiske. [23]

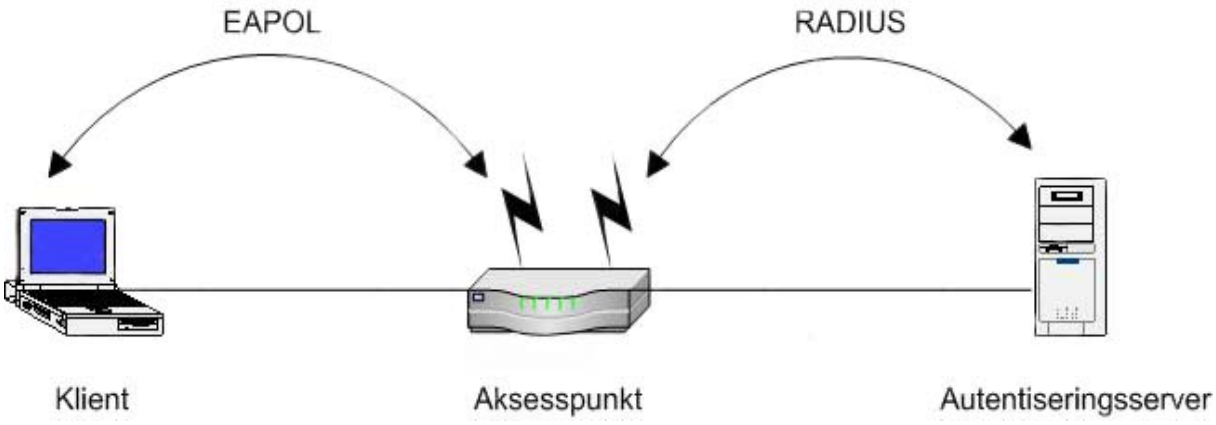
WEP ble i utgangspunktet utviklet som en sikkerhetsmekanisme på trådbundne nettverk. Ved å ta den i bruk i trådløse nettverk, var en klar over at sikkerhetsmekanismen ville få svakheter. For at en klient skal kunne logge seg på det trådløse nettverket, må han manuelt legge inn WEP-nøkkelen. En eventuell hacker har flere muligheter til å finne denne WEP-nøkkelen ved for eksempel å sjekke krypterte pakker for gjentakende mønster, eller sjekke krypterte pakker mot kjent innhold. Det finnes en rekke software som er utviklet for å finne WEP-nøkler i trådløse nettverk. Denne sikkerhetsmekanismen gir kun beskyttelse mot de som ikke har kunnskap om innbrudd i WEP-krypterte trådløse nettverk.

3.9 IEEE 802.1X

IEEE 802.1X er en standard for autentisering på linklaget. I motsetning til tidligere autentiseringsmetoder for trådløse nettverk, kan en ved bruk av denne standarden autentisere personer i stedet for å autentisere maskiner. IEEE 802.1X er et verktøy som benyttes for autentisering og nøkkeldistribuering, noe som tidligere var et sikkerhetsproblem i trådløse nettverk. En av fordelene med denne måten å autentisere brukere på, er at hver enkelt bruker kan gis ulike rettigheter, og at en kan beholde disse rettighetene, selv om man forflytter seg til andre extended service set, eller til tross for at brukeren logger seg på fra forskjellige maskiner.

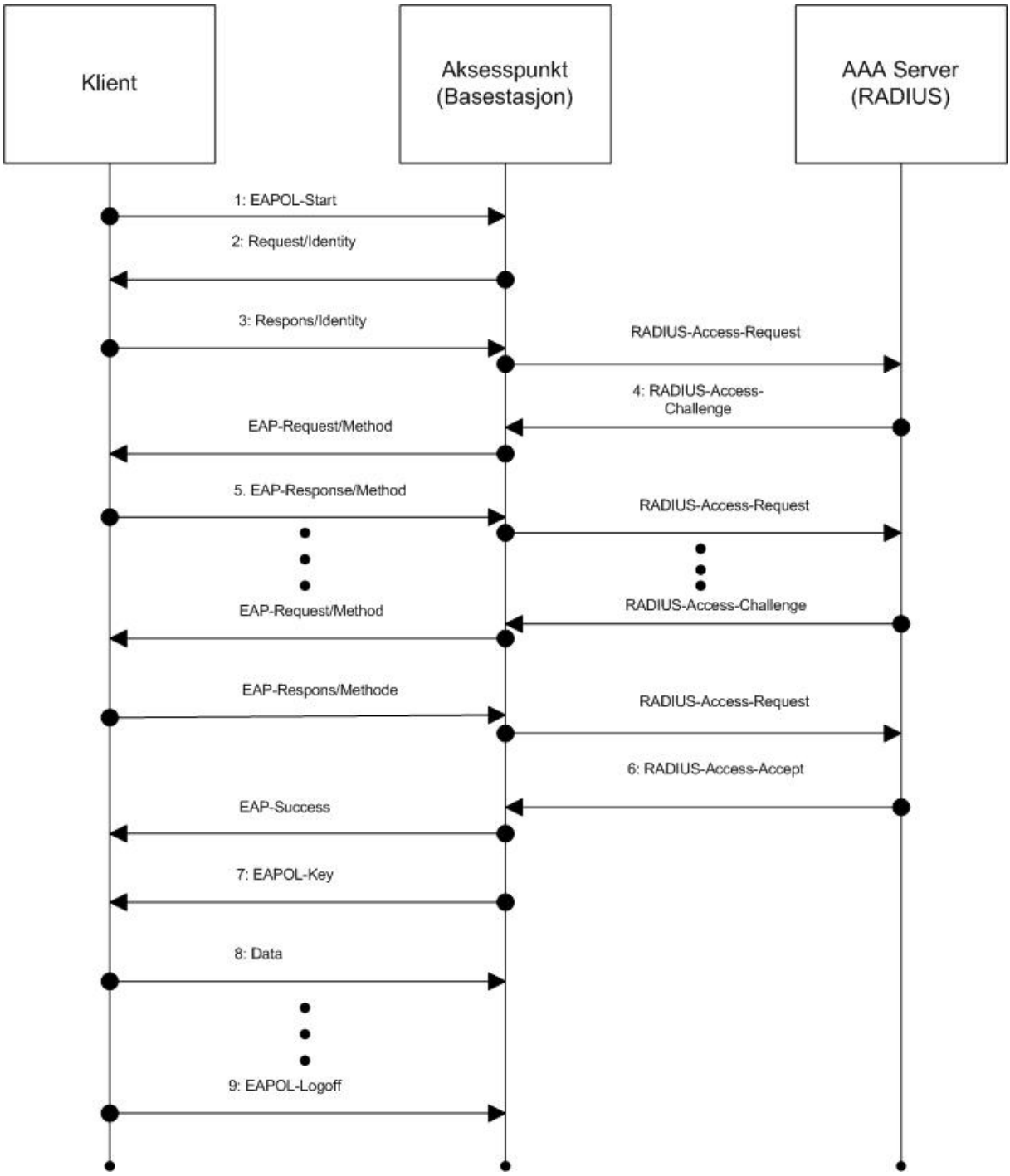
I IEEE 802.1X er det beskrevet tre forskjellige nettverkselementer for å utføre autentiseringen av klienter [4]. Autoriseringssøkeren er klienten som ønsker å koble seg til nettverket. Tilgang til nettverket styres av en autentiserer som videresender alle autentiseringsforespørsler til en

autentiseringsserver som ofte er en RADIUS-server. Figur 3.18 viser nettverkselementene som er involvert i autentiseringsprosessen i et trådløst nettverk. Forkortelsen EAPOL i denne figuren betyr Extensible Authenticatio Protocol (EAP) over LAN. Utvekslingen av autentiseringsinformasjon skjer mellom autentiseringssøkeren og autentiseringsserveren. Autentisereren fungerer kun som en bro i denne prosessen. Klienter som ikke er autentiserte får kun tillatelse til å sende autentiseringsinformasjon i nettverket. All annen trafikk til eller fra klienten blir sperret før autentiseringen er gjennomført. En av fordelene med å bruke RADIUS er at den er fleksibel og kan konfigureres til å benytte mange forskjellige typer brukerdatabaser [4]. I tillegg krever den ingen forandring i nettverksutstyret til klientene.



Figur 3.18: Autentiseringsprosessen i IEEE 802.1X

I trådløse nettverk vil trådløse klienter være de som skal autentiseres, og aksesspunktet vil være broen mellom klient og autentiseringsserveren. IEEE 802.1X tar i bruk EAP som erstatning for autentiseringsmetoden i Point to Point Protokollen som opprinnelig ble brukt for autentisering i WLAN [2]. IEEE 802.1X-standarden definerer innkapsling av EAP-pakker over nettverket. Autentiseringen foregår som vist i figur 3.19. Her ser vi meldingsutvekslingen mellom de tre objektene klient, aksesspunkt og autentiseringsserveren.



Figur 3.19: Meldingsutveksling ved autentisering med 802.1X
Figuren er utviklet på bakgrunn av [4]

1. Meldingsutvekslingen starter med at klienten sender en EAPOL-start til aksesspunktet.
2. Aksesspunktet svarer med en EAP-forespørsel om identitet.
3. Klienten sender EAP-respons-identitetsmelding som aksesspunktet videresender til RADIUS-serveren.
4. RADIUS-serveren bestemmer hvilken type autentisering som er nødvendig og sender en EAP-forespørsel etter autentiseringsopplysninger, innpakket i en Radius-Access-

Challenge-pakke, til aksesspunktet. Når pakken mottas, sendes en EAP-forespørsel videre til klienten.

5. Klienten mottar forespørselen og etterspør autentiseringsinformasjon fra brukeren og sender denne videre til aksesspunktet som en EAP-respons. Denne blir oversatt til en Radius-Access-Request av aksesspunktet og videresendt til RADIUS.
6. RADIUS serveren tillater at klienten får tilgang ved å sende en Radius-Access-Accept pakke til aksesspunktet som sender bekreftelsespakken EAP-vellykket til klienten.
7. Like etter sender aksesspunktet ut nøkler til klienten ved hjelp av EAPOL-nøkkelmelding.
8. Når nøkkelen er installert hos klienten, kan den begynne å sende datapakker over nettverket.
9. EAPOL-logoff melding blir sendt til aksesspunktet når klienten ikke lenger vil ha tilgang til det trådløse nettverket. [4]

3.10 IEEE 802.11i

I juni 2004 var arbeidsgruppen IEEE 802.11i ferdig med sitt arbeid med å standardisere en metode for linklagskryptering av trådløs kommunikasjon. IEEE 802.11i er utviklet for å reparere tidligere svakheter ved kryptering på linklaget. Dette blir gjort ved å innføre to nye krypteringsprotokoller, Temporal Key Integrity Protocol (TKIP) og Counter Mode with CBC-MAC Protocol (CCMP). [26]

TKIP er en forbedring av WEP-krypteringen. Den tar i bruk en delt nøkkel som er kjent av både sender og mottaker. Denne nøkkelen er på lik linje med WEP-kryptering, RC4-basert, men nøkkelen blir byttet ut for hver pakke [4]. Det gir en unik kryptering for hver eneste pakke som sendes. IEEE 802.1X brukes i sammenheng med TKIP for å distribuere hovednøkkelen på en sikker måte. Ved sending av pakker er det i IEEE 802.11i innført en Massage Integrity Check (MIC) for å finne ut om pakker har blitt endret under overføring. Denne sjekken omfatter også en kontroll av adressene til sender og mottaker for å forsikre at disse samsvarer med de opprinnelige adressene [26]. I tillegg omfatter MIC også prioriteringsbitet som er standardisert i IEEE 802.11e. Integritetssjekk er et av de svakeste punktene med WEP-kryptering. Før IEEE 802.11i la fram sitt arbeid, plukket Wi-Fi-alliansen opp TKIP og tok den i bruk sammen med IEEE 802.1X under navnet Wi-Fi Protected Access (WPA). WPA bruker en forbedret MIC, kalt Michael, som sjekker rammer som blir sendt til MAC-laget av overliggende lag. Grunnen til at Michael ble implementert for rammer over MAC-laget, var at den skulle være kompatibel med eksisterende hardware. [4]

CCMP er sikkerhet basert på Advanced Encryption Standard (AES) og er bygd inn på linklaget i IEEE 802.11i. AES-CCMP er et forslag fra IEEE 802.11i til en symmetrisk krypteringsalgoritme som erstatning for TKIP. AES-CCMP bruker en algoritme kalt Rijndael og tar i bruk 128, 192 og 256 bits krypteringsnøkler. For å utføre kryptering og dekryptering med AES-CCMP, bør en ha en egen brikke. Dersom en ikke har det, vil mye av

prosessorkraften bli brukt til kryptering og dekryptering. Dette betyr at AES-CCMP vil være noe mer kostbar, fordi en bør skifte ut aksesspunkt for å oppgradere til denne sikkerhetsstandarden. Wi-Fi (beskrevet i kapittel 3.12) sertifiserer produkter med WPA2 dersom de har full støtte for IEEE 802.11i og kan kjøre AES-CCMP i kombinasjon med IEEE 802.1X. [26]

3.11 Oversikt over standarder i IEEE 802.11-familien

IEEE har publisert flere andre tillegg til IEEE 802.11-standarden. Noen av disse standardiseringsprosessene er avsluttet, mens andre fortsatt er under utvikling. Tabell 3.2 gir en oversikt over alle standardene i IEEE 802.11-familien. Standarder med store bokstaver er standarder som er frittstående fra originalstandarden. Disse er ikke standarder, men en anbefaling. I parentes er det oppgitt årstall for når standardene er publisert.

IEEE-standard	Beskrivelse
802.11	Den originale 1 og 2 Mbit/s standarden fra 1997. Denne spesifiserer MAC-laget og de originale FHSS- og DSSS-moduleringsteknikker på det fysiske laget. På det fysiske laget opererer standarden på 2, 4 GHz frekvensbåndet. (1997)
802.11a	Bruker 5 GHz frekvensbåndet for dataoverføringer med en rate på opp til 54 Mbit/s. Dette var den første publiserte tilleggstandarden, men produkter som støttet denne standarden lot vente på seg før de ble tilgjengelige på det kommersielle markedet. (1999)
802.11b	Den tredje standarden på det fysiske laget. Denne hadde støtte for 5,5 og 11 Mbit/s. Produkter som støttet denne standarden var i salg før produkter for a-standarden var på markedet. (1999)
TGc	Arbeidsgruppe som jobbet frem en korreksjon i 802.11-standarden. Det finnes ikke noe 802.11c, siden det eneste de produserte var en oppdatering av originalstandarden.
802.11d	Denne standarden brukes for å tilfredsstille radiolovgiving i enkelte land. Den brukes av systemer som benytter andre 802.11-standarder for å tilpasse standardene etter nasjonale lover. (2001)
802.11e	Arbeidsgruppe som har fremarbeidet et tillegg på MAC-laget for å støtte applikasjoner som trenger QoS. (2005)
802.11F	Denne standarden kalles Inter-Access Point Protocol, og er en anbefaling som beskriver et valgfritt tillegg til 802.11. Den tar for seg kommunikasjon mellom trådløse aksesspunkt som tilhører forskjellige tjenesteleverandører. (2003)
802.11g	Den nyeste av 802.11-standardene for det fysiske laget. Produkter sender med opp til 54 Mbit/s på 2,4 GHz frekvensbåndet. (2003)
802.11h	Standard for å gjøre 802.11a kompatibel med europeiske radioreguleringer. (2003)
802.11i	Forbedringer av sikkerheten på linklaget. (2004)
802.11j	Forsterkning til 802.11a for å tilpasse seg det japanske radioregulativet. (2004)

802.11k	Dette er en foreslått standard for administrasjon av radioressurser. Sammen med IEE802.11r vil denne standarden bli viktig for å få til sømløs roaming mellom BSS i trådløse nettverk. 802.11k-standarden skaffer informasjon som hjelper til med å finne det beste tilgjengelige aksesspunktet. (Ikke ferdigstilt standard.)
TGm	Arbeidsgruppe for å innlemme 802.11a, 802.11b, 802.11g, og forandringer gjort av TGc i hovedspesifikasjonen for 802.11.
802.11n	Arbeidsgruppe som skal utvikle høyere ytelser. Målet for denne arbeidsgruppen er å oppnå hastigheter på 100 Mbit/s. (Ikke ferdigstilt standard.)
802.11p	Arbeidsgruppe som skal utvikle standarden for bruk i kjøretøy. Denne skal gjøre det mulig å kommunisere mellom kjøretøyer og mellom bil og aksesspunkt i veikanten. (Ikke ferdigstilt standard.)
802.11r	Forbedringer i roaming ved å lage støtte for raske BSS-overganger. Målet er at denne standarden skal være med på å gjøre det mulig med rask sømløs handover fra en basestasjon til en annen. (Ikke ferdigstilt standard.)
802.11s	En standard som tar sikte på å utvikle 802.11 på MAC-laget slik at den støtter kommunikasjon mellom aksesspunkt i et maskenett. (Ikke ferdigstilt standard.)
802.11T	Arbeidsgruppe som utarbeider testmetoder og målspesifikasjoner for 802.11-nettverk. (Ikke ferdigstilt standard.)
802.11u	Arbeidsgruppe som tilpasser 802.11 for å kunne samarbeide med andre nettverksteknologier. (Ikke ferdigstilt standard.)
802.11v	Arbeidsgruppe som jobber med en standard for å konfigurere klienter mens en er tilkoblet et 802.11-nettverk. (Ikke ferdigstilt standard.)
802.11w	Arbeidsgruppe som jobber med å forbedre sikkerheten for administrasjonspakker. (Ikke ferdigstilt standard.)

Tabell 3.2: IEEE 802.11-standarder

Tabellen er utviklet på bakgrunn av [4] og [31]

3.12 Wi-Fi

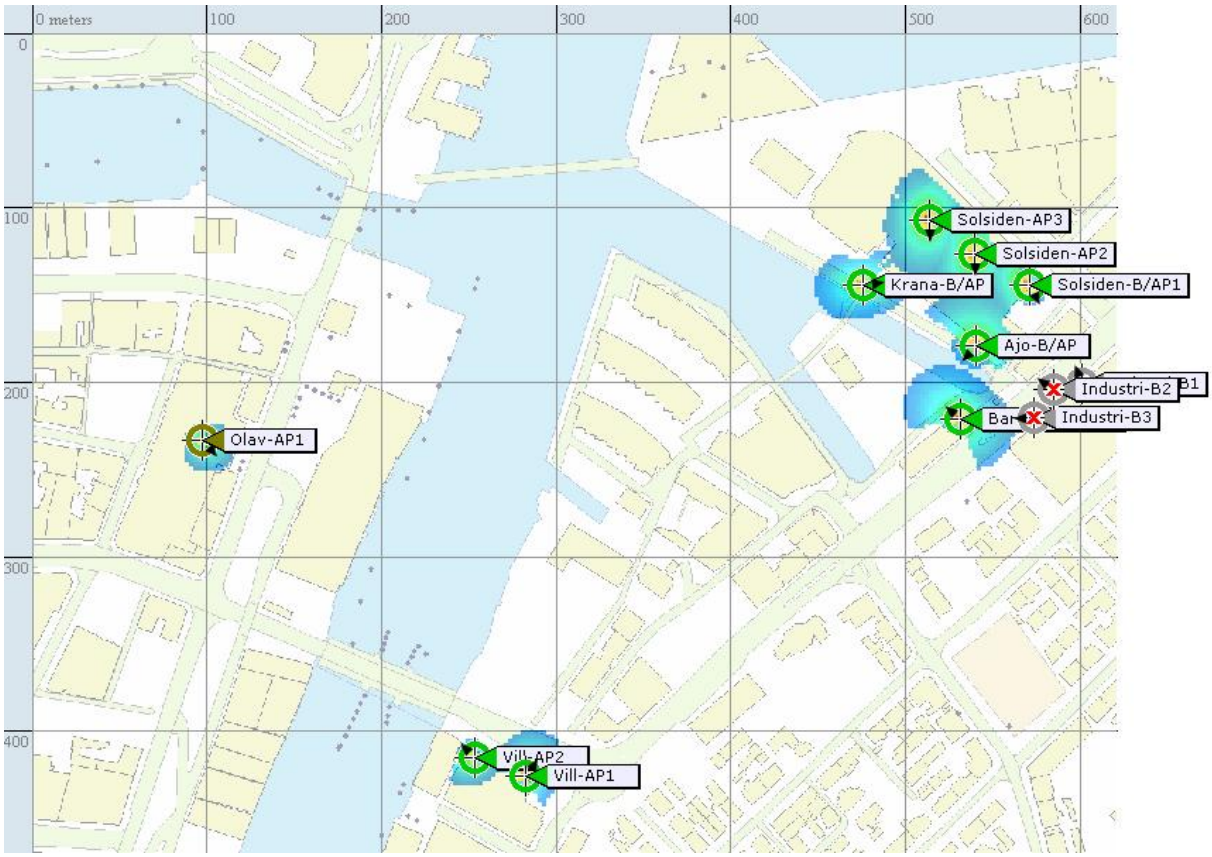
Wi-Fi er en nonprofit, internasjonal organisasjon som består av medlemmer fra over 250 bedrifter. Den ble etablert i 1999 og er et organ for godkjenning av WLAN-produkter som baserer seg på IEEE 802.11-standarder. Målet med Wi-Fi-alliansen er å skape kompatibilitet på tvers av produsenter og dermed øke brukervennligheten gjennom en internasjonalt akseptert godkjenning av produkter. Sertifiseringen startet i mars 2000 for å garantere at produkter som er merket med Wi-Fi faktisk følger den standarden de har oppgitt. Før et produkt kan bruke logoen som forteller at det er Wi-Fi-kompatibelt, må produktet gjennomgå forskjellige tester med tilfredsstillende resultater. Dette gir ingen garanti for produktets funksjonalitet, utover at det tilfredsstiller visse minimumskrav gitt av IEEE-standardene.

4 Trådløse Trondheim

Sommeren 2005 tok NTNU initiativ til et prosjekt som skulle gi trådløs nettverksdekning for forskning og utvikling i sentrum av Trondheim. Andre aktører ble invitert til å delta i prosjektet, og 30. november 2005 stilte Trondheim Kommune, Sør-Trøndelag Fylkeskommune og Næringsforeningen i Trondheim seg positivt til å delta i et samarbeid. I samarbeidsavtalen mellom aktørene forpliktet partene seg til å arbeide sammen for å etablere utendørs bredbåndsnett i Trondheim. [18]

Tidligere har det kun vært mulig å koble seg opp mot utendørs trådløse nettverk på sporadiske steder i Trondheim. Etter at første fase av Trådløse Trondheim-utbyggingen er gjennomført, skal overlappende aksesspunkt kunne dekke store deler av Trondheim sentrum.

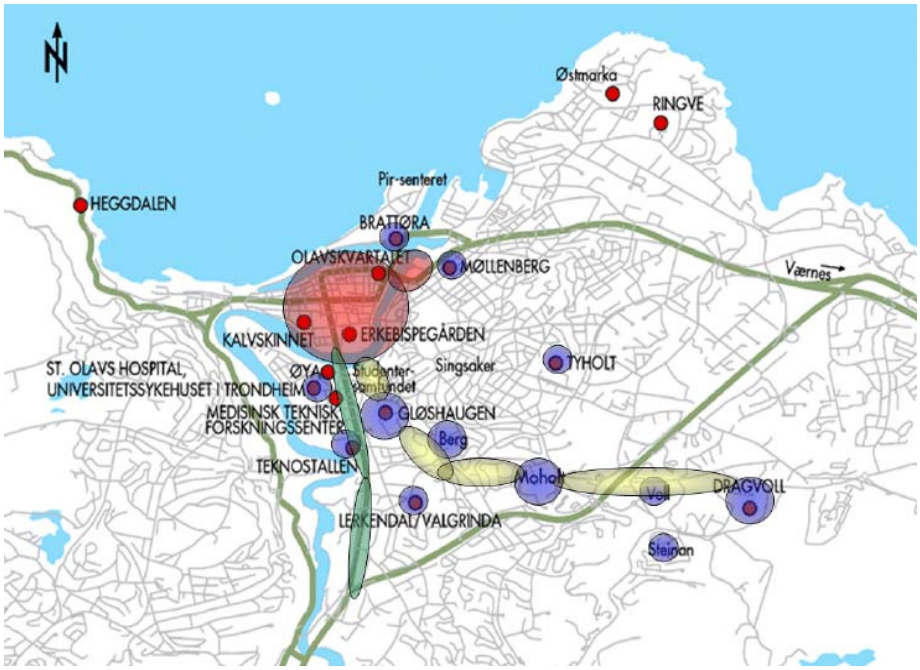
Som et forprosjekt ble det i februar i år satt opp en pilot i området rundt dokken på Solsiden i Trondheim og inne på fellesarealene på Solsiden kjøpesenter. I denne piloten ble det benyttet utstyr fra produsenten Airespace. Piloten har gitt nyttige erfaringer til kommende utbygginger både når det gjelder utstyr, skalering, administrasjon og hvordan en best kan utnytte mulighetene som ligger i et city-wide trådløst nettverk. Figur 4.1 viser en oversikt over aksesspunktene i piloten og kart over området. Her viser de runde sirklene lokasjonen til tilknyttede aksesspunkt.



Figur 4.1: Aksesspunkt i Trådløse Trondheim-piloten

Prosjektets overordnede mål er å bidra til å tilføre norsk næringsliv spisskompetanse innen trådløse teknologier og tjenester. Det skal skape et utviklingslaboratorium i verdensklasse for forskning og utvikling, og prosjektet skal gjøre Trondheim og NTNU mer attraktivt for studenter og teknologibasert næringsliv. [18]

Trådløse Trondheim har som langsiktig plan er å dekke store områder av Trondheim med trådløst bredbånd. Dette skal gjøres gjennom flere faser. Et delmål i utbyggingen er å dekke Midtbyen i Trondheim med omegn, NTNUs campus og busstraseen mellom sentrum, Gløshaugen og Dragvoll. Figur 4.2 viser en oversikt over dekningsområdet for denne utbyggingen. Områdene som på figuren er merket med rødt er dekningsområdet i midtbyen. De blå områdene er NTNU-områder, mens de gule dekningsområdene er busstraseen mellom campus.



Figur 4.2: Dekningsområdet for første fase i utbyggingen av Trådløse Trondheim
Figuren er hentet fra [18]

Trådløse Trondheim vil tilby en plattform for tilleggstjeneste med mobilitet, posisjonering, internettaksess og sikkerhet som innebygde utstyrsfunksjonaliteter. I starten vil nettet åpnes for forsknings- og utviklingsmiljøet i Trondheim, studenter og ansatte ved NTNU, kommunen og fylkeskommunen. Dette vil bidra til å få kontroll på skaleringen av nettverket før det åpnes for kommersielle tjenesteutviklere og andre som ønsker å tilby tjenester over plattformen. Med en slik tjenesteplattform vil det være mulig for andre bedrifter å tilby tjenester, nettaksess og annen funksjonalitet over den trådløse plattformen. [18]

I forhold til eksisterende trådløse soner i Trondheim og andre steder for øvrig, er det posisjonering og mobilitet som gir innovative muligheter i denne nettarkitekturen.

Arkitekturen åpner for større mobilitet i hele dekningsområdet, med klient-roaming mellom alle overlappende BSS. Dersom roamingtiden mellom aksesspunk blir tilfredsstillende lav, kan sanntidstjenester som streaming av lyd og bilder og VoIP utføres samtidig som at klienten roamer mellom BSS. Denne formen for mobilitet blir ofte omtalt som sesjonsmobilitet. I tillegg til roamingmulighetene kan systemet, ved hjelp av signalstyrke fra flere aksesspunkt, posisjonere klienter. Nøyaktigheten på posisjoneringer er avgjørende for hvor nyttig denne funksjonaliteten er for potensielle posisjoneringstjenester.

Aksessnettet i Trådløse Trondheim vil i utbyggingen av første fase være bygget på IEEE 802.11b-, IEEE 802.11g- og IEEE 802.11a-standarden. Hovedgrunnen til å velge denne teknologien er at store brukergrupper allerede har utstyr som støtter disse standardene. Produkter som er godkjent av Wi-Fi er i dag sterkt økende og daglig brukt av store brukergrupper. Teknologi som benytter de lisensfrie frekvensbåndene er derfor valgt som aksessnett, til tross for utfordringene som ligger i lisensfrie frekvensbånd. Aksessnettet vil ha varierende kapasitetsbehov. Enkelte steder er mer populære enn andre, og samtidige brukere vil være størst på de mest folkerike stedene. Kapasitetsbehovet er også avhengig av hvilke tjenester som skal tilbys i nettet. Erfaringer og brukerstatistikker gir grunnlag for å kunne si noe om kapasitetsbehov og gir nyttig informasjon om hvordan nettverkskapasiteten bør være.

Den teknologien som har størst kapasitet som matnett er fibernettverk. Andre aktuelle matnetteknologier er radioteknologi i lisensierte frekvenser, ADSL og ADSL2+. I Trådløse Trondheim vil fibernettverk være den mest aktuelle teknologien på grunn av gode skaleringsegenskaper og flere muligheter for innovativ forskning [32]. Trådløse Trondheim har et mål om 11 Mbit/s dekning over hele aksessnettet. Dette må det taes hensyn til ved valg av matnett. For at nettverket skal kunne benyttes til testing og forskning på for eksempel WiMAX og neste generasjons Wi-Fi, må kapasiteten til matnettet imidlertid være mye større. Slikt arbeid kan foregå på begrensede geografiske områder innenfor nettverket, og en trenger derfor ikke like stor matnettskapasitet frem til alle aksesspunktene. [32]

Utfordringene til Trådløse Trondheim og teknologier som benytter ulisensierte frekvensbånd er først og fremst konkurranse fra andre radiokilder. Det er derfor viktig med gode administrative verktøy for å kunne betjene kontrollerne og velge kanal og effekt for de forskjellige aksesspunktene. Det er også viktig at konkurrerende kilder i dekningsområdet blir detektert for at interferens og forringelse av tjenestekvalitet skal kunne forhindres på best mulig måte.

Trådløse Trondheim vil bli en pioner i forsking og utvikling av city-wide trådløse nettverk. Under utbyggingen og bruken av nettverket vil en få erfaringer som blir verdifulle for lignende nettverksutbygginger i fremtiden. I tillegg vil forsking på innovativ infrastruktur og nettverksteknologi gi mange muligheter for forsknings og utviklingsmiljøet. Bruken av optisk kablet matnett i enkelte deler av dekningsområdet, gjør at nye teknologier som for eksempel nye Wi-Fi-teknologier og WiMAX vil kunne testes ut og forskes på i reelle omgivelser. Nettet

vil også kunne bli en base for utvikling av nye tjenester fra eksterne tjenesteleverandører. Dette vil kunne bidra til at det oppstå nyttige og populære kommersielle tjenester. Spesielt plattformtjenester som mobilitet på tvers av hele dekningsområdet og posisjoneringsmuligheter, vil åpne for utvikling av helt nye tjenester i trådløse nettverk av denne typen. [18]

5 Testing og evaluering

I denne hovedoppgaven er det overordnede målet å finne generelle parametre som kan brukes for å evaluere trådløse city-wide datanettverk. For å komme frem til dette har det vært testet nettverksutstyr fra ulike produsenter i laboratorium hos Uninett i Trondheim og gjort tester og evalueringer i piloten til Trådløse Trondheim. De forskjellige IEEE 802.11-standardene for trådløse datanettverk beskriver ulike parametre og aspekter rundt nettverksteknologien. Mange av disse parametrene kan måles og testes, som blant annet egenskaper rundt overføringskapasitet, roaming og posisjonering. Andre aspekter som sikkerhet, administrative egenskaper og enkelte fysiske spesifikasjoner er det vanskeligere å finne nøyaktige test- og måleverdier for. Gjennom piloten til Trådløse Trondheim har det vært mulig å evaluere egenskapene til et funksjonelt city-wide trådløst nettverk. I tillegg har det vært testet trådløst nettverksutstyr fra forskjellige produsenter i laboratorium. Laboratorietestingen har gitt innsikt i hvordan nettverksutstyret kan brukes og hvilke produsenter som har valgt de beste løsningene. Ved hjelp av testingen har jeg kunnet undersøke hvilke parametre som er viktige for å evaluere trådløst nettverksutstyr, og hvilke kriterier som er viktige i city-wide trådløse nettverk som Trådløse Trondheim.

I laboratorium har jeg testet trådløst nettverksutstyr fra produsentene Airespace og Meru. De leverer begge en arkitekturløsning med sentrale kontrollere og ”lette” aksesspunkt. Testingen har bidratt til å gi et bilde av hvordan en slik nettverksarkitektur er bygget opp, og hvilke fordeler og ulemper arkitekturen medfører. Resultatet av testingen har gjort det mulig å sammenligne utstyret fra de to produsentene for å finne ut hvem som har implementert de beste løsningene i forhold til behovet i city-wide trådløse nettverk.

I piloten på Solsiden har det vært mulig å evaluere et funksjonelt city-wide trådløst nettverk. Her har det blitt utført klientposisjoneringstester og evaluert administrative kriterier for drifting av city-wide trådløse nettverk. Administrative verktøy i slike nettverk skal være gode og funksjonelle. Slike verktøy er en viktig del av et vellykket trådløst nettverk. Det er likevel vanskelig å måle eller teste denne funksjonaliteten. Her er det til en viss grad subjektivt hva som er nyttig og hvilken leverandør som har de beste løsningene. Det er likevel en del administrative funksjonaliteter som systemet må støtte. Fordi dette er så viktig, er det gjort en vurdering av administrativt software basert på erfaringene fra piloten på Solsiden.

5.1 Testutstyr

5.1.1 Hardware

Det trådløse nettverksutstyret som er testet i denne oppgaven er fra produsentene Cisco og Meru. De to produsentene leverer begge trådløse nettverksløsninger med sentrale kontrollere som innehar mye av funksjonaliteten i de tradisjonelle aksesspunktene. Denne arkitekturen er godt egnet for city-wide trådløse nettverk med mulighet for mange aksesspunkt som administreres gjennom en eller flere kontrollere. Fra Cisco har jeg testet utstyret Cisco Airospace Lightweight AP med kontroller som benytter LWAPP som tunnelleringsprotokoll mellom aksesspunkt og kontroller. Her har jeg sett på de ulike alternative aksesspunktene AP1010 og AP1030. I tillegg har jeg foretatt noen sammenligningsmålinger mot Ciscos autonome aksesspunkt, Cisco Aironet AP1131AG. Fra Meru har jeg testet Lightweight AP208 med en MC1000 kontroller som bruker en egenprodusert tunnelleringsprotokoll mellom aksesspunkt og kontroller.

5.1.2 Software

Under laboratorietesting er det benyttet programvaren IxChariot fra Ixia. Denne softwaren kan brukes i testingen av overføringskapasitet, VoIP-kvalitet, roaming, og diverse andre egenskaper i trådløse og trådbundne nettverk. Testene kan utføres med ulike innstillinger av nettverksparametre og med ulike trafikktyper. Programvaren fungerer ved at en installerer IxChariot-konsollen på en server som er tilkoblet et Local Area Network (LAN) med kabel. Denne kommuniserer med Endpoint1 som er en klient tilkoblet det samme LAN med kabel. Den trådbundne tilkoblingen gir nok kapasitet på linken mellom dem til at dette ikke vil være noen flaskehals i testingen av et trådløst system. Endpoint1 kommuniserer med Endpoint2 som er installert på trådløse klienter. Målinger og resultater fra denne kommunikasjonen blir rapportert tilbake til serversoftwaren av Endpoint1.

Når en kjører en enkel test med IxChariot med kun en Endpoint1 og en Endpoint2, vil IxChariot-konsollen sende konfigurasjonsdata og testskriptet til Endpoint1. Testskriptet er et kjørbart skript som endpointene vil kjøre for å utføre testene som IxChariot ber om. Endpoint1 beholder sin del av skriptet og sender resten av skriptet til Endpoint2. Når Endpoint2 sender ACK, varsler Endpoint1 fra om dette til IxChariot konsollen. Konsollen ber da Endpoint1 om å kjøre det aktuelle skriptet. Både Endpoint1 og Endpoint2 utfører skriptkommandoene. Skriptet kjøres gjentatte ganger i løpet av tiden testen bruker. Endpoint1 samler resultatene gjennom testtiden og leverer disse til IxChariot konsollen. Konsollen analyserer resultatene og presenterer de grafisk og analytisk.

Testingen med IxChariot er altså basert på skript som styrer testforløpet og bestemmer parametre for testen. Ved testing av Airespace brukte jeg IxChariot skriptet Response-Timer.src for å teste roamingtid og skriptene filercvl.src og et Meru-utviklet skript for å teste

throughput. Throughput-skriptene simulerer en filoverføring ved bruk av TCP med en lang forbindelse. Ved hjelp av disse skriptene kunne jeg utføre tester for roaming, throughput med forskjellig antall aktive klienter, og VoIP samtalekvalitet i form av MOS-verdier (beskrevet i kapittel 5.4.1).

5.2 Throughput

Bitrate er, i et WLAN, definert som hastigheten en bruker kan sende og motta data mellom en mobil klient og et aksesspunkt. Denne bitraten varierer på forskjellige steder i dekningsområdet til aksesspunktet og kan bli påvirket av forskjellige eksterne faktorer. IEEE 802.11-standarden definerer ulike hastigheter for forskjellige typer WLAN. For IEEE 802.11b og IEEE 802.11g er ratene 1, 2, 5.5 og 11 Mbit/s definert. For IEEE 802.11g og IEEE 802.11a er i tillegg ratene 6, 9, 12, 18, 24, 36, 48 og 54 Mbit/s inkludert. Brukeren opplever imidlertid alltid bitrater som er lavere enn den teoretisk maksimale bitraten. Det finnes forskjellige grunner til hvorfor det er slik, men de viktigste er at hver datapakke inneholder overlast som Preamble, MAC-header, IP-header, TCP-header og Frame Check Sequence. I tillegg minker bitraten på grunn av sending av kontrolldata mellom mottakere og aksesspunkt som vist i figur 3.4. En annen viktig grunn til at den praktiske bitraten blir lavere enn den teoretiske, er at de som skal overføre et signal venter et tilfeldig tidsrom mellom sending av pakker for å gi andre brukere mulighet til å bruke frekvensbåndet, som beskrevet under aksess i kapittelet om IEEE 802.11. I kapittelet 3.6 er det også beskrevet beskyttelsesmekanismene som IEEE 802.11g har innebygd for å unngå interferens i nettverk der det finnes både b- og g-produkter. Når denne beskyttelsesmekanismen er aktivert vil overføringsraten for g-produktene minke betraktelig.

Når en kalkulerer med all rammeoverlasten og mellomrammeavstandene, vil det være en maksimal teoretisk overføringskapasitet for nyttedata ved de forskjellig fysiskelag-teknologiene. Denne vil, som sagt, være lavere enn den teoretiske overføringskapasiteten som produsenter av utstyr oppgir i tekniske spesifikasjoner.

5.2.1 Teoretisk utregning av throughput for nyttedata

For å kunne ha en formening om hva som kan forventes under testing av throughput, må en vite hva som er mulig å oppnå ved de forskjellige fysiskelag-standardene. Den teoretisk maksimale overføringskapasiteten for nyttedata kan regnes ut ved å ta hensyn til de forskjellige innkapslingene og mellomrammeavstandene. For å finne disse verdiene har jeg tatt utgangspunkt i et enkelt TCP-segment etterfulgt av en TCP ACK. TCP-segmentet består av en DIFS, datarammen innkapslet i TCP, en SIFS og ACK-meldingen. TCP ACK består av en DIFS, datarammen som inneholder ACK-meldingen, en SIFS og ACK. Dette er vist langs tidslinjen i figur 5.1. Som MTU har jeg benyttet 1500 bytes, fordi dette er den maksimale rammestørrelsen på Ethernet som de fleste trådløse nettverk er koblet opp mot. Figur 3.7 viser innkapslingen av nyttedata på MAC-laget. I tillegg vil LLC/SNAP-protokollen legge til enda

8 bytes, som vist i figur 3.9, for å identifisere nettverklagsprotokollen. Den totale størrelsen på MAC-innkapslingen for en TCP-pakke og en TCP ACK blir derfor:

TCP-pakker:		TCP ACK:	
MTU:	1500 bytes	TCP/IP:	40 bytes
MAC-header:	28 bytes*	MAC-header:	28 bytes*
LLC/SNAP:	8 bytes	LLC/SNAP:	8 bytes
Total størrelse:	**1536 bytes**	**Total størrelse:**	**76 bytes**

*Figur 3.7 viser en MAC-header på totalt 34 bytes. Det fjerde adressefeltet blir i følge kapittel 7.2.2 i IEEE 802.11-spesifikasjonen fra 1999, kun benyttet i enkelt spesialtilfeller og utelatt i vanlige sender/mottaker-datautvekslinger.

MTU er satt til 1500 bytes, men inkludert i dette er TCP- og IP-header. Dette utgjør til sammen 40 bytes av total MTU som vist i figur 3.9. Den totale mengden nyttedata er derfor 1500 bytes minus 40 bytes, altså 1460 bytes.

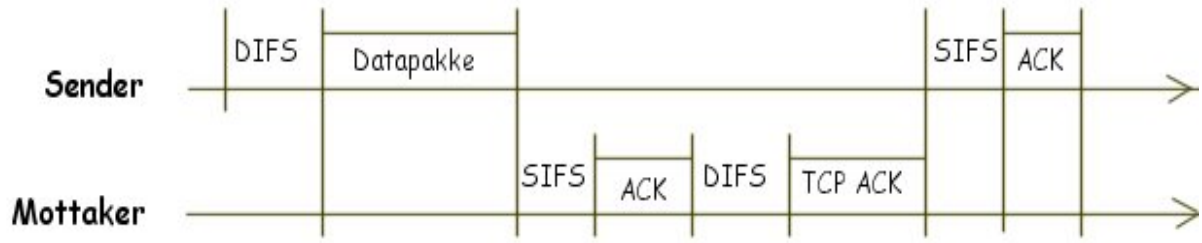
Utregningene og resultatene som er presentert nedenfor gjelder for TCP-pakker sendt med maksimal overføringskapasitet. Tallene vil være forskjellige ved bruk av UDP og med de lavere overføringshastighetene som er spesifisert i de ulike fysiskelag-standardene.

5.2.1.1 IEEE 802.11b

Produkter etter IEEE 802.11b-standarden blir solgt med spesifikasjoner som oppgir en maksimal overføringskapasitet på 11 Mbit/s. For å finne den teoretisk maksimale overføringshastigheten for nyttedata, må en først finne den totale tiden det tar å overføre et TCP-segment, og hvor mye nyttedata som overføres på denne tiden. I IEEE 802.11b er det følgende mellomrammetider og slot-tid [9]:

SIFS:	10 µs	
Slot-tid:	20 µs	
DIFS:	50 µs	(2 x slot-tid + SIFS)

En overføring av TCP-pakken med påfølgende TCP ACK i et IEEE 802.11b-nettverk, foregår som vist langs tidslinjen i figur 5.1. Her er det vist både mellomrammetidene og signalpakkene som sendes over nettverket.



Figur 5.1: Sending av et TCP/IP-datagram

Figur 3.13 viser at IEEE 802.11b bruker en preamble før hver ramme som sendes over radiolinken. Dette kan, som nevnt i kapittel 3.5.2, være enten en long preamble eller en short preamble. En long preamble vil bruke 192 µs, mens en short preamble bruker 96 µs for å overføres [9].

IEEE 802.11b deler data opp i 8-bit kodeord som nevnt i kapittel 3.5.3. Vi får derfor 1536 8-bit datablokker i TCP-segmentet, og 76 8-bit datablokker i TCP ACK. ACK-meldingen har ingen LLC/SNAP og er derfor kun 14 bytes lang [9]. MAC-rammen blir delt opp i en serie av 8-bit kodeord og det sendes 1 375 millioner kodeord per sekund [19].

Tabell 5.1 viser den totale overføringstiden for TCP-pakken med preamble og ACK-meldingen. Pakkestørrelsen er dividert med antall kodeord per sekund for å finne tiden det tar å overføre den aktuelle pakkestørrelsen.

	TCP-pakke	TCP ACK
DIFS	2x slot-tid + SIFS = 2x 20 µs + 10 µs = 50µs	2x slot-tid + SIFS = 2x 20 µs + 10 µs = 50µs
IEEE 802.11-datapakke	192 µs + 1536/1375 Msps = 192 µs + 1118 µs = 1310 µs	192 µs + 76/1375 Msps = 192 µs + 56 µs = 248 µs
SIFS	10 µs	10 µs
IEEE 802.11 ACK	192 µs + 14/1375 Msps = 192 µs + 11 µs = 203 µs	192 µs + 14/1375 Msps = 192 µs + 11 µs = 203 µs
Total rammetid	1 573 µs	511 µs
Den totale rammetiden med ACK	1 573 µs + 511 µs = 2 084 µs	

Tabell 5.1: Utregning av total overføringstid for en TCP-pakke med TCP ACK for IEEE 802.11b

Hver overføring bruker minimum 2 084 µs. Dette betyr at det maksimalt kan gjennomføres (1 000 000 / 2 084) 479 slike overføringer per sekund. Det vil gi en overføringskapasitet for

nyttedata på (1460 bytes x 8 bit x 479 per sekund) 5,6 Mbit/s. Den maksimale overføringskapasiteten for nyttedata ved bruk av 802.11b på det fysiske laget er derfor lik 5,6 Mbit/s. Maksimal nyttedatakapasitet for denne standarden er nesten en halvering av den teoretiske overføringskapasiteten som brukere og produsenter opererer med.

5.2.1.2 IEEE 802.11a

Det er to hovedgrunner til at IEEE 802.11a er raskere enn b-standarden, dersom vi ser bort fra de fysiske kodingene. Mellomrammeavstandene er mindre for IEEE 802.11a, og i tillegg er preamble kortere for denne fysiskelag-teknologien.

I IEEE 802.11a er det følgende mellomrammetider og slot-tid [8]:

SIFS: 16 µs
Slot-tid: 9 µs
DIFS: 34 µs (2 x slot-tid + SIFS)

I likhet med IEEE 802.11b deler også IEEE 802.11a opp data i en serie med kodeord før overføringen. Disse kodeordene kalles symboler. Ved 54 Mbit/s vil hvert symbol kode 216 bits og legge til 6 koding-bits på slutten av rammen [8]. Vi får derfor en total pakkestørrelse på ((1536 x 8) + 6) 12 294 bits som kan kodes i (12 294 / 216) 57 symboler. TCP ACK bruker ((76 x 8 + 6) / 216) 3 symboler, mens IEEE 802.11 ACK trenger ett symbol.

	TCP-pakke	TCP ACK
DIFS	2x slot-tid + SIFS = 2x 9 µs + 16 µs = 34µs	2x slot-tid + SIFS = 2x 9 µs + 16 µs = 34µs
IEEE 802.11-datapakke	20 µs + 57 x 4 µs/symbol = 20 µs + 228 µs = 248 µs	20 µs + 3 x 4 µs/symbol = 20 µs + 12 µs = 32 µs
SIFS	16 µs	16 µs
IEEE 802.11 ACK	20 µs + 1 x 4 µs/symbol = 20 µs + 4 µs = 24 µs	20 µs + 1 x 4 µs/symbol = 20 µs + 4 µs = 24 µs
Total rammetid	322 µs	106 µs
Den totale rammetiden med ACK	322 µs + 106 µs = 428 µs	

Tabell 5.2: Utregning av total overføringstid for en TCP-pakke med TCP ACK for IEEE 802.11a

Hver ramme har en 20 µs preamble for å synkronisere mottakeren. Etter denne synkroniseringsheaderen følger symbolene som hver bruker 4 µs for å overføres. [8] Tidsforløpet i denne overføringen foregår som vist i figur 5.1.

Tabell 5.2 viser utregningen av totaltiden for overføring av en IEEE 802.11a-pakke med TCP ACK. Hver overføring bruker minimum 428 µs. Det betyr at det maksimalt kan gjennomføres (1 000 000 / 428) 2336 slike overføringer per sekund. Dette vil gi en overføringskapasitet for nyttedata på (1460 bytes x 8 bit x 2336 per sekund) 27,3 Mbit/s.

5.2.1.3 IEEE 802.11g

Som nevnt i kapittel 3.6 er IEEE 802.11g oppbygd med forskjellige teknologier på det fysiske laget etter hvilken overføringshastighet som blir benyttet. En utregning av maksimal teoretisk overføringskapasitet for IEEE 802.11g er mer komplisert enn det som er tilfellet for IEEE 802.11a og IEEE 802.11b på grunn av beskyttelsesmekanismene. For IEEE 802.11g blir den maksimale teoretiske overføringskapasiteten forskjellig for tilfellene der produkter som støtter IEEE 802.11g er eneste klientene i nettverket, og der det er både IEEE 802.11b og IEEE 802.11g klienter assosiert. Det siste tilfellet kan også deles opp i to tilfeller, bruk av CTS til selvsending og bruk av RTS/CTS.

I IEEE 802.11g er det følgende mellomrammetider og slot-tider [20]:

SIFS:	10 µs	
Kort slot-tid:	9 µs	(Brukes når IEEE 802.11g-enheter opererer alene)
Lang slot-tid:	20 µs	(Brukes i samkjøring med IEEE 802.11b-enheter)
Kort DIFS:	28 µs	(2 x kort slot-tid + SIFS)
Lang DIFS:	50 µs	(2 x lang slot-tid + SIFS)

IEEE 802.11g alene i BSS

Når IEEE 802.11g-produkter opererer alene innenfor et BSS, brukes en kort slot-tid som genererer mindre overlast. Kalkulasjonen av maksimal overføringskapasitet i denne typen nettverk er lik den som ble gjort for IEEE 802.11a, med små forskjeller i mellomrammeavstandene. Som for IEEE 802.11b og IEEE 802.11a vil overføring i et trådløst nettverk der IEEE 802.11g opererer alene, foregå som vist i figur 5.1. Tabell 5.3 viser utregningen av den totale tiden det tar å overføre en TCP-datapakke med en påfølgende TCP ACK for IEEE 802.11g-only.

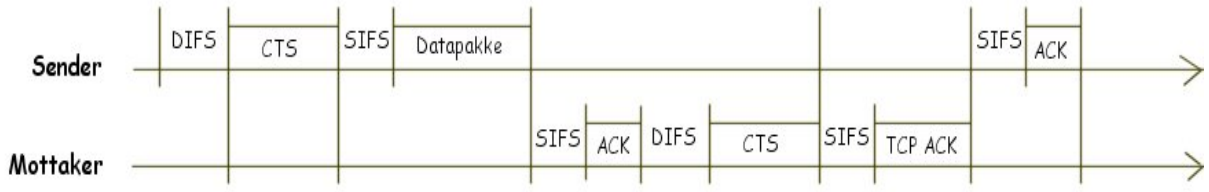
	TCP-pakke	TCP ACK
DIFS	2x slot-tid + SIFS = 2x 9 µs + 10 µs = 28 µs	2x slot-tid + SIFS = 2x 9 µs + 10 µs = 28 µs
IEEE 802.11-datapakke	20 µs + 57 x 4 µs/symbol + 6 µs = 20 µs + 228 µs + 6µs = 254 µs	20 µs + 3 x 4 µs/symbol + 6 µs = 20 µs + 12 µs + 6 µs = 38 µs
SIFS	10 µs	10 µs
IEEE 802.11 ACK	20 µs + 1 x 4 µs/symbol + 6 µs = 20 µs + 4 µs + 6 µs = 30 µs	20 µs + 1 x 4 µs/symbol + 6 µs = 20 µs + 4 µs + 6 µs = 30 µs
Total rammetid	322 µs	106 µs
Total rammetid med ACK	322 µs + 106 µs = 428 µs	

Tabell 5.3: Utregning av total overføringstid for en TCP-pakke med TCP ACK for IEEE 802.11g-only

Som for IEEE 802.11a vil resultatet medføre en overføringskapasitet av nyttedata på (1460 bytes x 8 bit x 2336 per sekund) 27,3 Mbit/s, fordi hver overføring bruker minimum 428 µs. Det kan maksimalt gjennomføres (1 000 000 / 428) 2336 slike overføringer per sekund.

IEEE 802.11g med CTS-beskyttelse

Når en IEEE 802.11b-klient assosierer seg i et IEEE 802.11g-nettverket, blir beskyttelsesmekanismer koblet inn. Dette er illustrert i figur 5.2 og 5.3. Figurene viser at beskyttelsesmekanismene gir mer trafikk på transmisjonslinjen og mer bruk av mellomrammeavstander. Dette vil igjen få konsekvenser for overføringskapasiteten i nettverket.



Figur 5.2: Sending av et TCP/IP-datagram med CTS

I tillegg til at det blir brukt lang slot, og dermed lengre mellomrammeavstander, vil administrasjonspakker ta opp mer kapasitet i nettverket. CTS-pakker sendt til seg selv er den beskyttelsesmekanismen som gir minst overlast av de to vanlige beskyttelsesmekanismene.

CTS-rammene er på 14 bytes og blir overført med 11 Mbit/s som er en hastighet alle klientene i nettverket klarer å dekode.

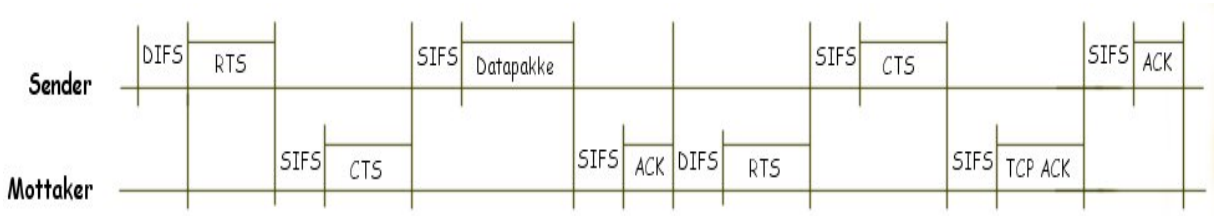
	TCP-pakke	TCP ACK
DIFS	2x slot-tid + SIFS = 2x 20 µs + 10 µs = 50 µs	2x slot-tid + SIFS = 2x 20 µs + 10 µs = 50 µs
CTS	192 µs + 14/1375 Msps = 192 µs + 11 µs = 203 µs	192 µs + 14/1375 Msps = 192 µs + 11 µs = 203 µs
SIFS	10 µs	10 µs
IEEE 802.11-datapakke	20 µs + 57 x 4 µs/symbol + 6 µs = 20 µs + 228 µs + 6 µs = 254 µs	20 µs + 3 x 4 µs/symbol + 6 µs = 20 µs + 12 µs + 6 µs = 38 µs
SIFS	10 µs	10 µs
IEEE 802.11 ACK	20 µs + 1 x 4 µs/symbol + 6 µs = 20 µs + 4 µs + 6 µs = 30 µs	20 µs + 1 x 4 µs/symbol + 6 µs = 20 µs + 4 µs + 6 µs = 30 µs
Total rammetid	557 µs	341 µs
Total rammetid med ACK	557 µs + 341 µs = 898 µs	

Tabell 5.4: Utregning av total overføringstid for en TCP-pakke med TCP ACK for IEEE 802.11g med CTS-beskyttelse

Hver overføring bruker minimum 898 µs, noe som er over dobbelt så mye som uten beskyttelsesmekanismer. Det betyr at det maksimalt kan gjennomføres (1 000 000 / 898) 1113 slike overføringer per sekund. Dette vil gi en overføringskapasitet for nyttedata på (1460 bytes x 8 bit x 1113 per sekund) 13 Mbit/s.

IEEE 802.11g med RTS/CTS-beskyttelse

RTS/CTS er en sikrere beskyttelsesmekanisme for reservering av overføringsmediet enn det CTS sendt til seg selv er. Denne beskyttelsesmekanismen når også skjulte klienter i nettverket. Den vil imidlertid føre til enda mer kontrolldata sendt i det trådløse nettverket, og dermed mindre kapasitet for nyttedata, som vist langs tidslinjen i figur 5.3.



Figur 5.3: Sending av et TCP/IP-datagram med RTS/CTS

Tabell 5.5 viser utregningen av tiden en TCP-pakke og en påfølgende TCP ACK bruker med IEEE 802.11g med RTS/CTS og alle mellomrammeavstandene.

	TCP-pakke	TCP ACK
DIFS	2x slot-tid + SIFS = 2x 20 µs + 10 µs = 50 µs	2x slot-tid + SIFS = 2x 20 µs + 10 µs = 50 µs
RTS	192 µs + 20/1375 Msps = 192 + 15 µs = 207 µs	192 µs + 20/1375 Msps = 192 + 15 µs = 207 µs
SIFS	10 µs	10 µs
CTS	192 µs + 14/1375 Msps = 192 µs + 11 µs = 203 µs	192 µs + 14/1375 Msps = 192 µs + 11 µs = 203 µs
SIFS	10 µs	10 µs
IEEE 802.11 datapakke	20 µs + 57 x 4 µs/symbol + 6 µs = 20 µs + 228 µs + 6 µs = 254 µs	20 µs + 3 x 4 µs/symbol + 6 µs = 20 µs + 12 µs + 6 µs = 38 µs
SIFS	10 µs	10 µs
IEEE 802.11 ACK	20 µs + 1 x 4 µs/symbol + 6 µs = 20 µs + 4 µs + 6 µs = 30 µs	20 µs + 1 x 4 µs/symbol + 6 µs = 20 µs + 4 µs + 6 µs = 30 µs
Total rammetid	774 µs	558 µs
Total rammetid med ACK	774 µs + 558 µs = 1332 µs	

Tabell 5.5: Utregning av total overføringstid for en TCP-pakke med TCP ACK for IEEE 802.11g med RTS/CTS-beskyttelse

TCP ACK med denne metoden bruker lenger tid enn det som er tilfellet i IEEE 802.11b-standarden i tabell 5.1. Overføringen vil derfor bestå av en RTS/CTS-utveksling på 774 µs og en TCP ACK på 511 µs som i den eldre IEEE 802.11b-standarden [19]. Med denne

beskyttelsesmekanismen for samkjøring, vil hver overføring bruke minimum 1285 µs. Dette betyr at det maksimalt kan gjennomføres (1 000 000 / 1285) 778 overføringer per sekund. Det vil gi en overføringskapasitet for nyttedata på (1460 bytes x 8 bit x 778 per sekund) 9,1 Mbit/s.

5.2.2 Sammenligning av utregnet throughput for de ulike standardene

Bitrate for nyttedata kan ikke sammenlignes med linkraten som er oppgitt i spesifikasjonene for de ulike standardene for trådløse nettverk. Tabell 5.6 viser resultatet av kalkulert maksimal overføringskapasitet ved bruk av TCP-segmenter for de ulike fysiskelag-teknologiene. Den viser også hvor effektiv teknologien er i forhold til IEEE 802.11b.

PHY-teknologi	Overføringer per sekund	Nyttedatakapasitet	Nyttedatahastighet i forhold til 802.11b
802.11b	479	5,6 Mbit/s	1,0
802.11a	2336	27,3 Mbit/s	4,9
802.11g alene	2336	27,3 Mbit/s	4,9
802.11g med CTS-beskyttelse	1113	13,0 Mbit/s	2,3
802.11g med RTS/CTS-beskyttelse	778	9,1 Mbit/s	1,6

Tabell 5.6: Nyttedatakapasitet for de ulike fysiskelag-teknologiene

Fra den siste kolonnen i tabell 5.6 kan vi se at det er stor forskjell i overføringskapasitet av nyttedata for de forskjellige teknologiene. Det er derimot ikke så veldig stor forskjell på den eldre IEEE 802.11b-standarden og IEEE 802.11g med RTS/CTS-beskyttelse. IEEE 802.11g uten beskyttelse oppnår samme overføringskapasitet for nyttedata som IEEE 802.11a, men den er kun drøyt en halv gang så rask som IEEE 802.11b med den beste beskyttelsesmekanismen.

De utregnede resultatene for throughput samsvarer med resultater fra tidligere publisert utregningsarbeid. Et eksempel på kalkulasjoner som samsvarer med resultatene i tabell 5.6 er Proxim Corporation White Paper: *A Detailed Examination of the Environmental and Protocol Parameters That Affect 802.11g Network Performance* [33].

5.2.3 Svakheter ved utregningsmodellen

Utregningene som er gjort i kapittel 5.2.1 er gjennomført på en simpel måte som neglisjerer flere faktorer som er gjeldende i praksis. Blant annet blir det antatt en konstant strøm av pakker som ankommer i riktig rekkefølge uten å måtte konkurrere om transmisjonslinjen. IEEE 802.11 bruker CSMA/CA og exponential backoff, slik at det i realiteten vil være lenger

enn en DIFS mellom to rammer. Dette kommer frem av figur 3.10. Ved konkurranse om transmisjonsmediet vil exponential backoff redusere throughputen for nyttedata.

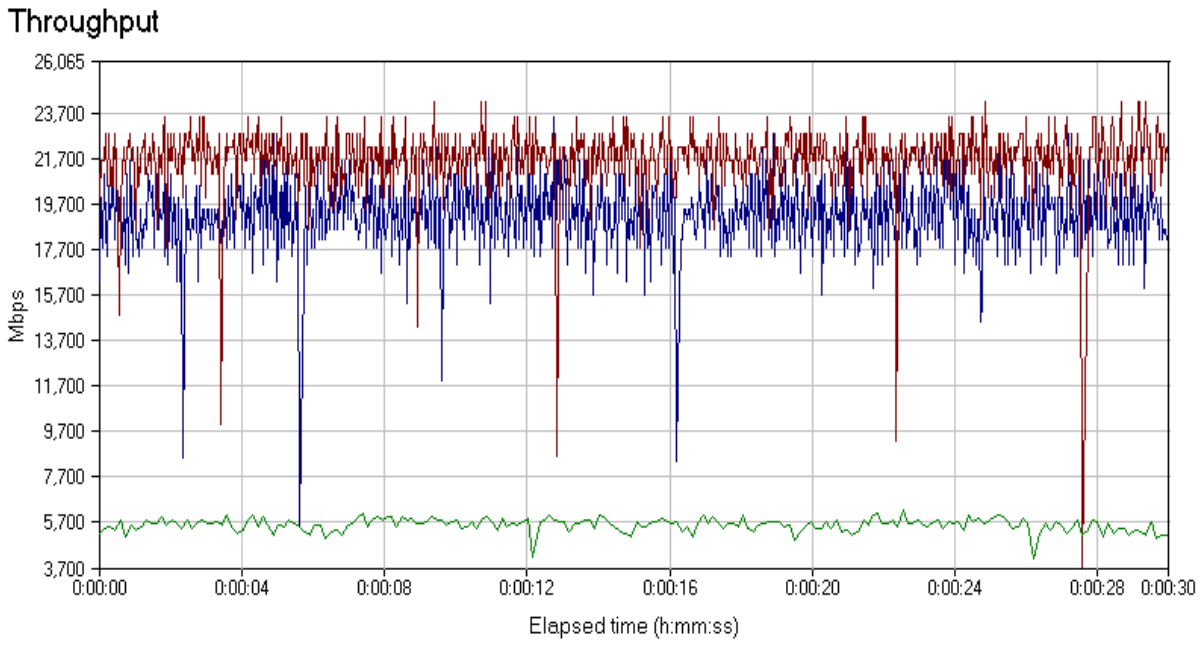
I tillegg er det sett bort i fra muligheten for ”sliding windows”. ”Sliding windows” er en metode som brukes av TCP for flytkontroll mellom sender og mottaker. TCP krever at alle transporterte pakker skal kvitteres av mottakeren med en ACK. Ved bruk av ”sliding wondows” og mottakerbuffer kan flere pakker bekreftes med en enkel ACK. Dette vil redusere overlasten og gi økt throughput.

5.2.4 Testing av throughput med IxChariot

Throughput er, som nevnt, et mål for mengden data som blir transportert fra et sted til et annet i løpet av et spesifisert tidsintervall. Som vist gjennom utregninger, er ikke den spesifiserte overføringskapasiteten på det fysiske mediet det samme som teoretisk overføringskapasitet av nyttedata. Under testing av throughput i laboratorium ble det undersøkt throughput per klient ved bruk av IEEE 802.11b, IEEE 802.11a, IEEE 802.11g-only, og til slutt IEEE 802.11b og IEEE 802.11g i samkjøring. I tillegg ble det testet forholdet mellom antall samtidige klienter og throughput per klient. Her var det interessant å finne den maksimale overføringskapasiteten til det testede utstyret, gitt et best mulig SNR-forhold.

5.2.4.1 Throughputtester og sammenlikning mellom Airespace og Meru

Under testing av ytelse ble skriptet ”filercvl.src” fra IxChariot benyttet. Dette skriptet simulerer, som tidligere nevnt, en lang forbindelse med sending av TCP-pakker på 1500 bytes.



Figur 5.4: Throughputresultater for Airespace

Testen ble utført med en klient tilknyttet aksesspunktet for alle de tre ulike radioteknologiene. Det var ingen annen trafikk gjennom aksesspunktet i løpet av testtiden. Figur 5.4 viser throughput for testtiden på tre minutter med Airespace. Den røde grafen viser IEEE 802.11a med en gjennomsnittlig throughput på 21,2 Mbit/s, den grønne grafen viser IEEE 802.11b med en gjennomsnittlig throughput på 5,6 Mbit/s, og den blå grafen viser IEEE 802.11g med en gjennomsnittlig throughput på 18,8 Mbit/s. I disse testene ble det ikke registrert noe ytelsestap på grunn av tunnelleringen mellom aksesspunktet og kontrolleren. Figur 5.4 viser at grafene får et kort dropp i throughput med tilnærmet faste tidsintervall. Sannsynligvis skyldes dette at aksesspunktet i disse intervallene utfører annet arbeid. Produsenten av utstyret reklamerer med at en ved bruk av kontrollere vil kunne få bedre oversikt over radiospekteret i dekningsområdet til systemet. Det er nærliggende å tro at i de periodene der en ser et dropp i throughput, foretar aksesspunktene en skanning av radiospekteret for å søke etter eventuelle andre radiosignaler og deretter rapportere resultatet tilbake til kontrolleren.

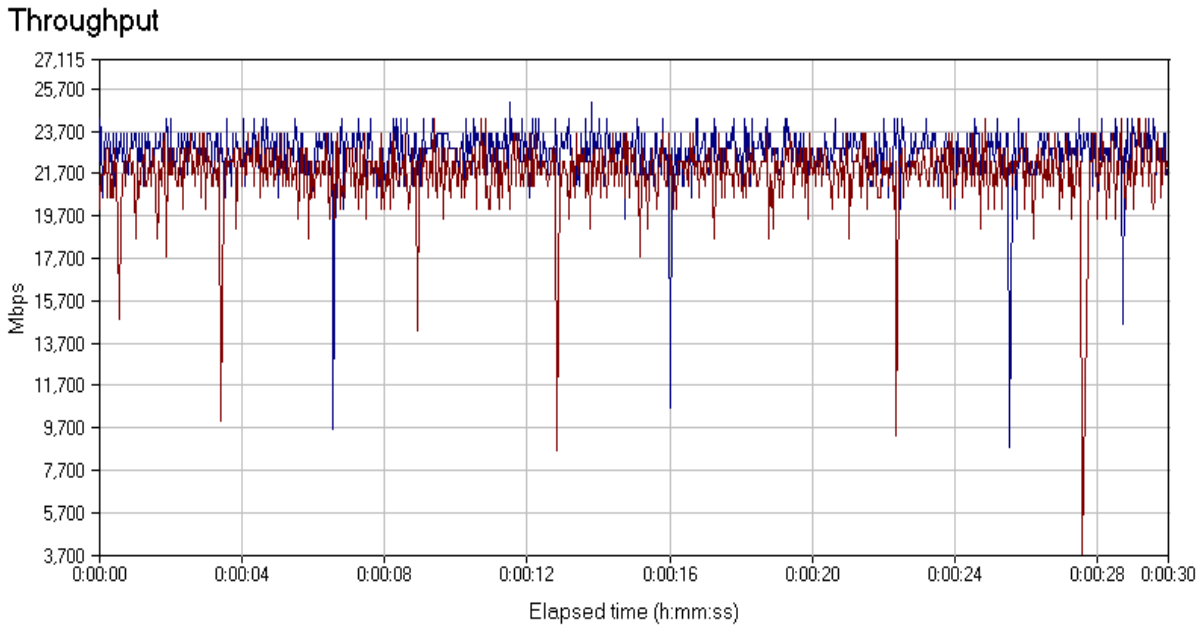
Gjennomsnittlig overføringskapasitet for testene er gjengitt i tabell 5.7. I samkjøring av IEEE 802.11b og IEEE 802.11g er en b-klient assosiert i nettverket der en g-klient fungerer som Endpoint2 (Endpoint2-rollen er beskrevet i kapittel 5.1.2). I forhold til de utregnede verdiene for throughput er de målte verdiene for IEEE 802.11b og IEEE 802.11b/g omtrent som forventet. For IEEE 802.11a og IEEE 802.11g-only, er resultatet imidlertid noe lavere enn de utregnede verdiene. Det er flere faktorer som kan være grunnen til at de to siste standardene ikke oppnådde de utreknede throughputverdiene. I tillegg til svakhetene i utregningsmodellen som er nevnt i kapittel 5.2.3, kan blant annet pakkekollisjoner, et lavt SNR-nivå og retransmisjon av pakker redusere overføringskapasiteten.

Fysiskelag-standard	Målt gjennomsnittlig throughput
IEEE 802.11a	21,2 Mbit/s
IEEE 802.11b	5,6 Mbit/s
IEEE 802.11g	18,6 Mbit/s
IEEE 802.11b/g	9,2 Mbit/s

Tabell 5.7: Gjennomsnittlig throughput med en klient for Airespace

5.2.4.1.1 Kontrollertunnelleringens innvirkning på throughput

Som beskrevet i kapittel 2.1 vil tunnelleringen mellom aksesspunkt og kontrolleren føre til ekstra overlast i form av en ekstra innkapslingsheader. For Airespace er denne tunnelleringsprotokollen en LWAPP-protokoll. Tunnelleringen mellom aksesspunkt og kontroller vil trolig påvirke den faktiske overføringskapasiteten i det trådløse nettverket. For å finne ut hvor mye dette eventuelt utgjør, testet jeg ytelsen med en AP1030. Dette aksesspunktet har støtte for å kjøre i bridge-modus og kan dermed gi klienter direkte adgang til subnettet, på samme måte som en vanlig WLAN-bridge.



Figur 5.5: Throughputmålinger for AP1010 og AP1030

Den røde grafen viser AP1010 som tunnellerer all trafikk gjennom kontrolleren, mens den blå grafen viser AP1030 i bridge-modus. Hardware for de to aksesspunktene er, av produsenten, oppgitt å være helt lik. Figur 5.5 viser at throughput for AP1010 hele tiden ligger litt under det som er tilfellet for AP1030. Gjennomsnittlig throughput for AP1030 i bridge-modus ble målt til 22,3 Mbit/s, mens den gjennomsnittlige verdien for AP1010 var på 21,2 Mbit/s. Denne forskjellen kan være et resultat av LWAPP-tunnelleringen. For å bekrefte at det virkelig var tunnelleringen som skapte forskjellen i throughput, gjorde jeg sammenligninger mellom AP1010 og Cisco Aironet AP1131AG som ikke har noe form for tunnellering. Tabell 5.8 viser resultatet av denne testen. Konklusjonen er at tunnelleringen fører til en lavere throughput, men at forskjellen likevel er så liten at den ikke vil ha noe praktisk betydning.

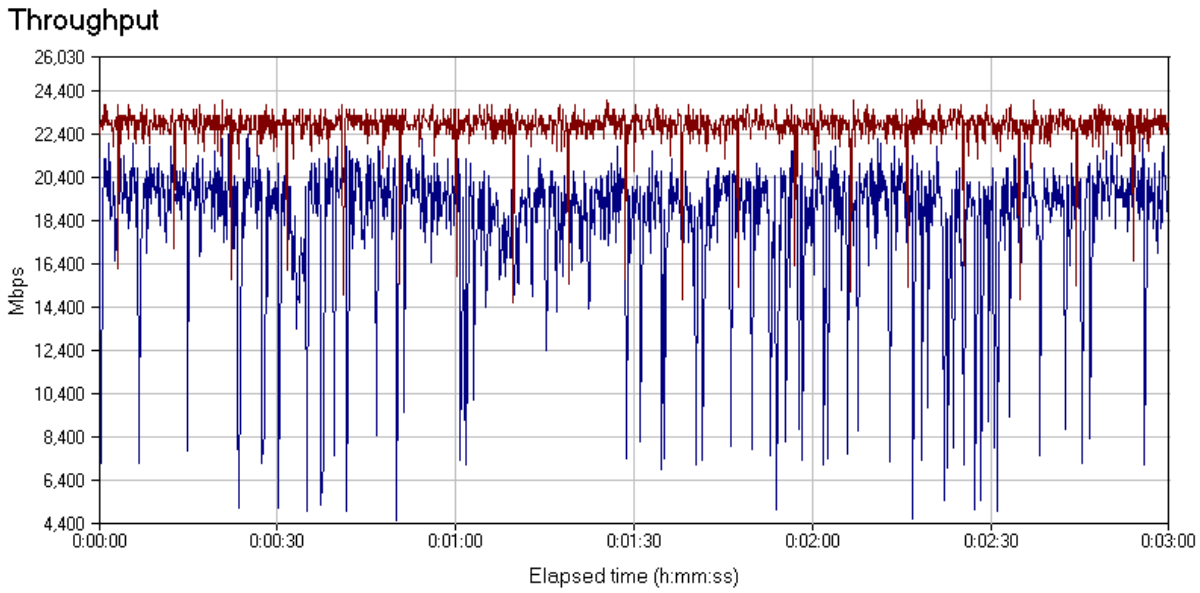
IEEE-standard	Aironet AP1131AG	Airespace AP1010
802.11a	22,7 Mbit/s	21,2 Mbit/s
802.11b	6,3 Mbit/s	5,6 Mbit/s
802.11g	22,2 Mbit/s	18,8 Mbit/s

Tabell 5.8: Sammenligning av throughput mellom autonome Aironet AP1131AG og Airespace AP1010

5.2.4.1.2 Sammenligningstester

IxChariot, konfigurert på den samme måten for alle tester, gjør det mulig å utføre sammenligningstester på forskjellig utstyr. Testresultatene gjør det lettere å vurdere egenskapene til de forskjellige produktene mot hverandre. For å sjekke om der var noe forskjell i throughput for Airespace og Meru, utførte jeg likt konfigurerte tester på de to produktene. Graf 5.6 viser throughput for IEEE 802.11a, der den røde grafen er Airespace

AP1010, og den blå grafen er Meru AP208. Dette resultatet viser en fordel til Airespace over hele testperioden.



Figur 5.6: Throughput for Airespace og Meru for IEEE 802.11a

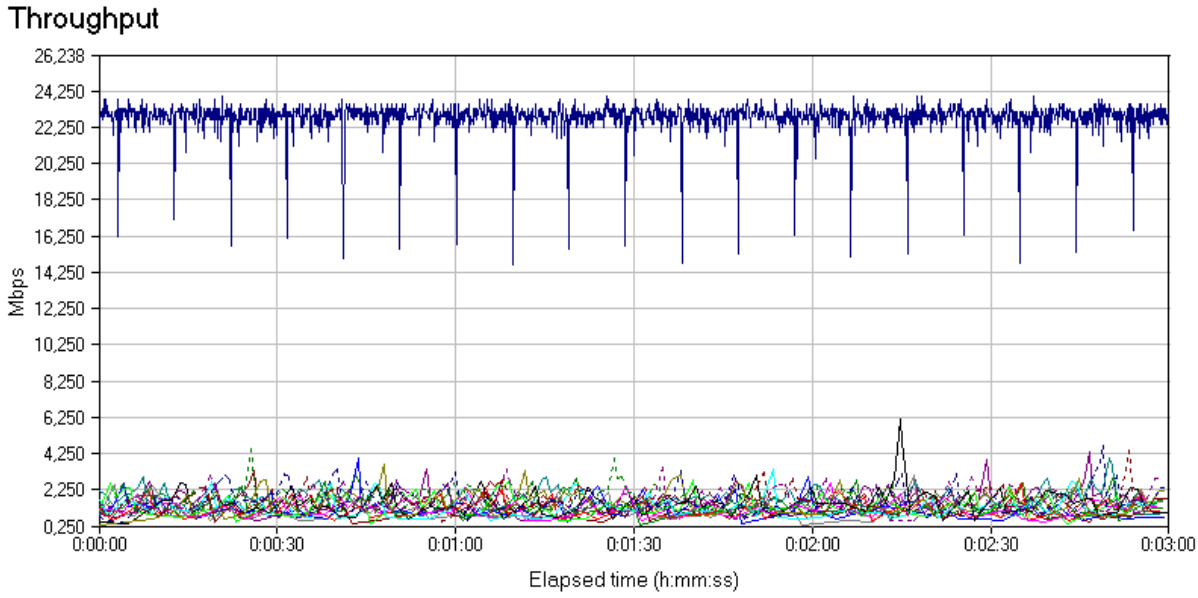
Throughputen for Airespace ligger gjennom hele testtiden høyere enn det som er tilfellet for Meru. I tillegg har grafen til Airespace mindre amplitudeutslag. Det betyr at forholdene vil være mer stabile i et trådløst nettverk som er satt opp med Airespace enn med Meru.

IEEE-standard	Airespace	Meru
802.11b	5,6 Mbit/s	5,5 Mbit/s
802.11g	18,8 Mbit/s	6,2 Mbit/s
802.11a	21,2 Mbit/s	17,9 Mbit/s

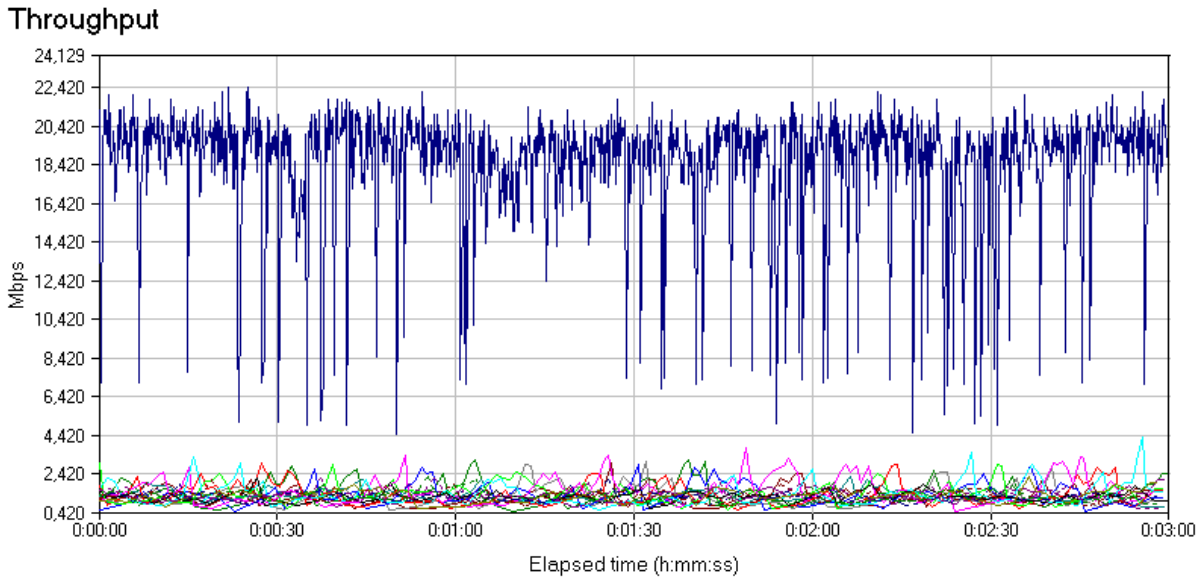
Tabell 5.9: Testresultater for throughput

Tabell 5.9 viser throughputresultatene for de to produktløsningene ved de ulike fysiskelag-teknologiene. Resultatet for IEEE 802.11g med Meru er mye lavere enn forventet. Leverandøren av Meru-utstyret har ikke kunnet finne noen konkrete feil ved denne testingen, men de har likevel foreslått alternative konfigurasjoner som kanskje kan bidra til et bedre testresultat. Disse alternative konfigurasjonene har det ikke vært mulig å teste i denne oppgaven. Skriptet som ble brukt i alle sammenligningstestene er imidlertid laget av Meru og burde derfor gi tilfredsstillende resultater for deres produkter.

Resultatene i tabell 5.9 viser utstyrets throughput ved betjening av en enkelt klient. For city-wide trådløse nettverk er det en viktigere egenskap hvordan totalkapasiteten fordeler seg ved flere klienter. Jeg testet derfor ytelsen på IEEE 802.11a med flere samtidige klienter og sammenlignet resultatet med throughputverdien jeg fant med en enkel klient.



Figur 5.7: Throughput per klient for Airespace med 1 klient og med 16 klienter for IEEE 802.11a

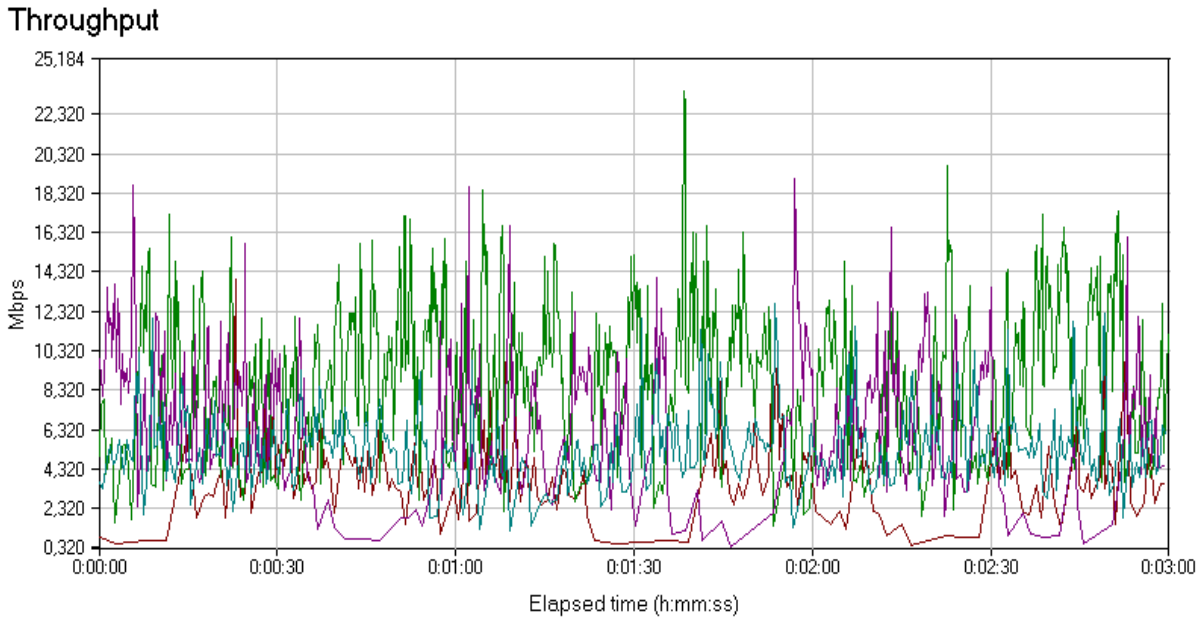


Figur 5.8: Throughput per klient for Meru med 1 klient og med 16 klienter for IEEE 802.11a

Testene som er vist i figur 5.7 og 5.8, er utført med et skript skrevet av Meru. De er kjørt over 3 minutter og sammenligner ytelsen dersom aksesspunktet betjener en IEEE 802.11a-klient og 16 IEEE 802.11a-klienter. Resultatene for Airespace viser en gjennomsnittlig throughput på 22,8 Mbit/s med kun en IEEE 802.11a-klient i nettverket, og litt over 1 Mbit/s per klient når det er 16 av dem. Den totale throughput holdt seg som ved den første testen på rundt 20 Mbit/s. For Meru har vi tilsvarende verdier for gjennomsnittlig throughput ved en klient på 17,9 Mbit/s, og for 16 samtidige klienter på litt over 1 Mbit/s per klient. Gjennomsnittlig total throughput var i det siste tilfellet på 19,5 Mbit/s. Resultatet viser ingen vesentlig forskjell

mellom de to produktene for throughput med 16 klienter. Med kun en klient assosiert er resultatene omtrent som i tabell 5.9.

Det ble også utført en test på Airespace med fire samtidige klienter. Denne ga et resultat med større forskjeller mellom de ulike klientene. Grafen som plotter resultatene fra denne testen er gjengitt i figur 5.9. Her oppnås en gjennomsnittlig total throughput på 20,3 Mbit/s, men de enkelte klientene får kun en gjennomsnittlig throughput på mellom 3 og 8 Mbit/s. Klientene tiknyttet det samme aksesspunktet opplever derfor relativt stor forskjell i throughput. Det er ikke konfigurert noe form for prioritering av trafikk eller klienter i softwaren til dette systemet. Forskjellen i throughput hos de ulike klientene er derfor ikke mulig å forutse.



Figur 5.9: Throughput for Airespace med 4 klienter

Alle throughputtestene som er gjennomførte på Airespace, ga en total throughput som tilsvarte forventningen for throughput ved de ulike standardene. Gjennomsnittlig throughput ble ikke vesentlig redusert ved samkjøring av flere klienter. Ytelsen og forskjellene med Airespace er også som forventer med bruk av tradisjonelle autonome aksesspunkt.

Throughputtestene som ble gjort med utstyr fra Meru, ga et resultat som hele tiden var lavere enn forventet. I sammenligningen med Airespace viser resultatet en lavere overføringskapasitet ved samtlige throughputtester. Tilbakemeldinger fra leverandøren av Meru-utstyret foreslår alternative testkonfigurasjoner som kanskje kan bidra til å øke gjennomsnittlig throughput for Meru. Det har ikke vært mulig å teste etter disse anbefalingene i denne oppgaven. Testresultatet kan derfor være annerledes med de nye konfigurasjonene. I sammenligningstestingen ble det imidlertid benyttet de samme konfigurasjonene for testing av de ulike produktene.

Appendiks D viser øvrige testresultater for throughput. Mange av testresultatene er også tilgjengelig i det elektroniske vedlegget.

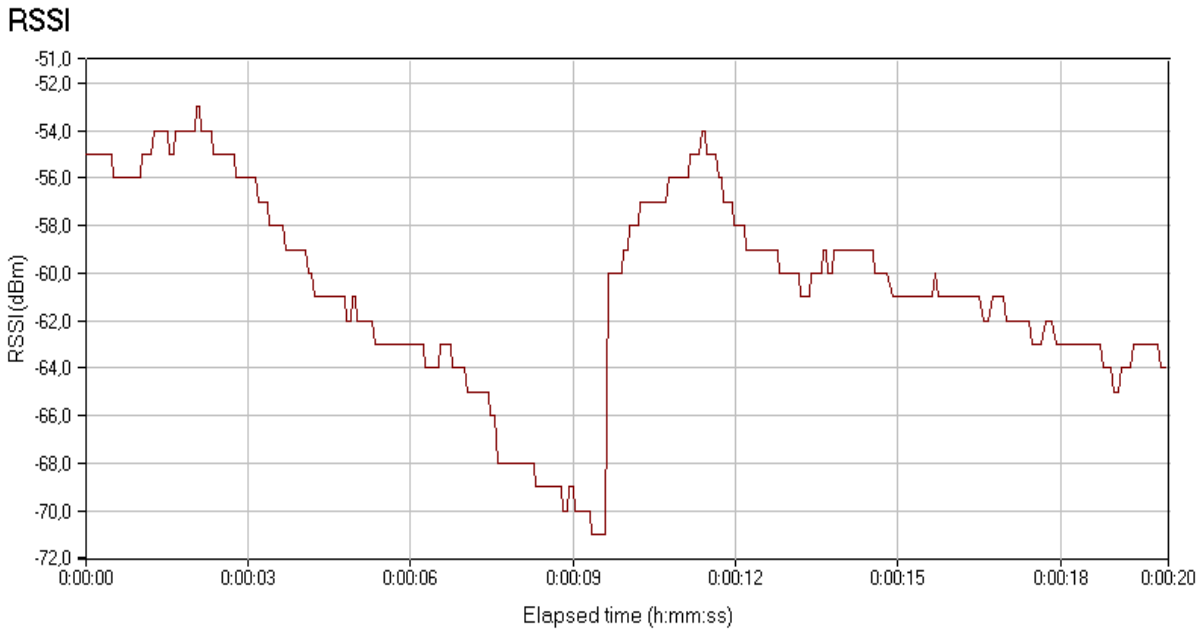
5.3 Roaming

Roaming er tiden det tar å koble fra et aksesspunkt, søke etter det nye aksesspunktet, koble til nytt aksesspunkt og eventuelt reautentisere klienten. Roaming foregår ved at klienter beveger seg fra en BSS til en annen. Aksesspunktet i den nye BSS-en overtar da kommunikasjonen med klienten. På forhånd har aksesspunkt som ligger i nærheten av den BSS-en som klienten befinner seg i, mottatt autentiseringsinformasjon fra kontrolleren. Det vil være en liten periode der klienten ikke er tilkoblet nettverket under roaming. Lengden på denne perioden er avgjørende for om en del tjenester kan benyttes samtidig med at en roamer. Et eksempel på en slike tjenester er VoIP som ikke tåler store forsinkelser før tjenesten ikke lenger er brukernyttig.

De største utfordringene under testingen av roaming var at det er klienten som tar avgjørelsen om hvordan den roamer og når den roamer. Det betyr at det kan være vanskelig å få nøyaktige testresultater for roamingtid. Klienter skal ideelt sett roame før signalet fra den tilknyttede basen er dårligere enn signalet fra den nye basen. Her kan imidlertid signal og støyforhold spille inn, slik at roamingen ikke skjer på samme måte hver gang. Jeg opplevde også at klienten noen ganger mistet forbindelsen totalt, og at den måtte assosieres på nytt før forbindelsen var tilbake. Enkelte av roamingtestene hadde derfor et mye dårligere resultat enn det som kommer fram i det neste kapittelet.

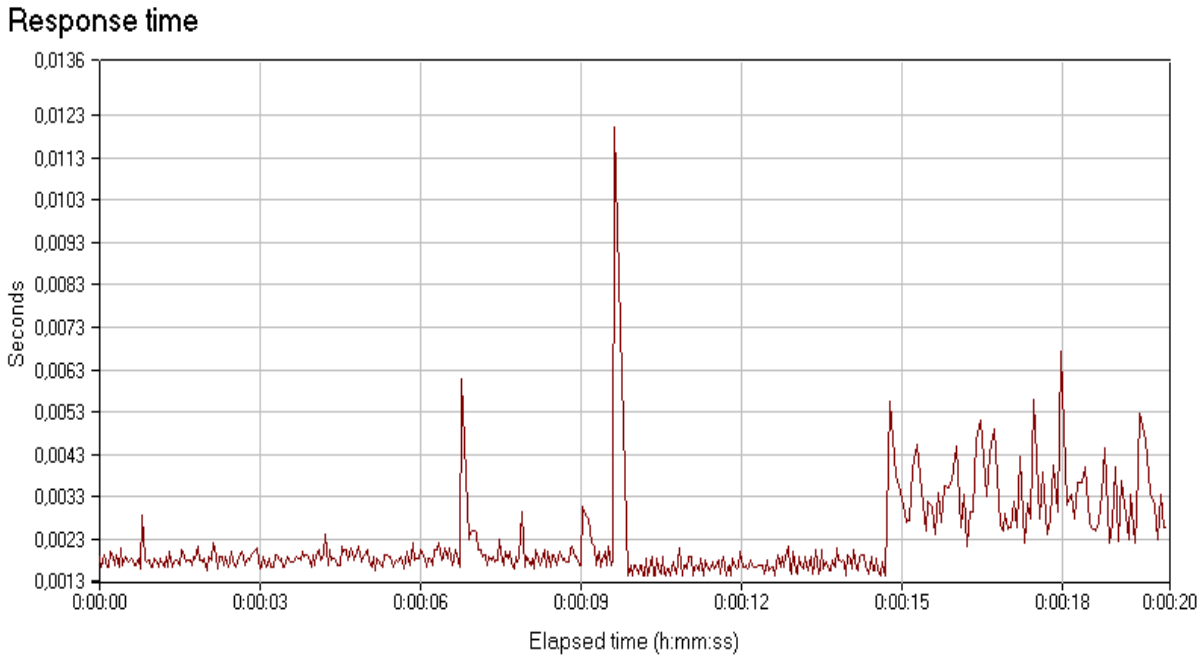
5.3.1 Testresultater for roaming

Roaming ble testet for Airespace med et AP1010-aksesspunkt og med WEP-kryptering. Roamingtiden ble funnet ved å se på responstiden når klienten roamet fra et aksesspunkt til et annet. I tillegg ble Received Signal Strength Indication (RSSI) brukt for å verifisere at roaming hadde forekommet. For å utføre roamingtestene ble IxChariot kjørt med Response-Timer.scr-skriptet som er laget av IxChariot. For å fremprovosere roaming benyttet jeg en mobil klient som ble forflyttet fra dekningsområdet til et aksesspunkt til et annet. Denne fremprovoserte roamingen ble gjort ti ganger for at det skulle være mulig å finne en representativ verdi for roamingtiden.



Figur 5.10: RSSI ved klientroaming

Figur 5.10 viser at RSSI er høy før klienten beveger seg mot det nye aksesspunkt. Den får da gradvis lavere RSSI før den skifter aksesspunkt og igjen får høyere RSSI.



Figur 5.11: Representativt resultat for responstid ved roaming

I det klienten bytter aksesspunkt, ser vi av figur 5.11 at vi får en økt responstid. Denne økte responstiden viser hvor lang tid det tar for klienten å roame. Målingen som er gjengitt i figur 5.11 viser en roamingtid på 13 ms, noe som er representativt for de ti gjennomførte testene.

Roamingtiden ble testet mot roamingtid for de tradisjonelle autonome aksesspunktene til Cisco, Cisco Aironet AP1131AG. Tester med dette systemet viser en tilsvarende roamingtid på mellom 11 og 13 ms.

Responstid blir av IxChariot regnet ut ved å finne tiden det tar for en transaksjons Round Trip Time (RTT) i nettverket. Responstiden er den mest effektive parametren for å beskrive menneske-maskin interaksjonen i denne sammenhengen. IxChariot oppgir responstiden i sekunder per transaksjon og blir regnet ut som:

$$\text{Responstid} = \text{Total\_tid} / \text{Antall\_transaksjoner} \quad (2)$$

Her er Total_tid tiden i sekund alle transaksjonene bruker mellom Endpoint1 og Endpoint2, mens Antall_transaksjoner refererer til antallet transaksjoner gjort av Endpoint1. [22]

Det har blitt hevdet at en av de store fordelene til den nye trådløst nettverkarkitekturen med en sentral kontroller, er ved bruk av RADIUS for autentisering. Kontrolleren vil da være det eneste kontrollpunktet mot RADIUS. Dette vil forenkle kommunikasjonen og gi raskere tilbakemelding til aksesspunktene enn det som er tilfellet dersom flere autonome aksesspunkt skal utføre den samme jobben. Kontrolleren kan ta vare på autentiseringsinformasjon og formidle dette til aksesspunktene, i stedet for at hvert enkelt aksesspunkt skal måtte spørre RADIUS og administrere autentisering selv. For å teste denne påstanden, satte jeg opp Airespace med IEEE 802.1X som autentisering og med TKIP-kryptering. Resultatet av testene var litt overraskende og uventet. De viste en responstid på rundt 150 ms. Tilsvarende tester med det autonome systemet til Aironet ga, som tidligere, en responstid på mellom 11 og 13 ms. En av grunnene til det overraskende resultatet kan være at Airespace har problemer med ”Fast Reconnect” der aksesspunkt overfører krypteringsnøkler og portåpninger seg i mellom for å slippe reautentisering mot RADIUS-serveren når en klient roamer. Den høye responstiden kan tyde på at klienten må autentisere seg på nytt ved roaming.

Resultatene fra roamingtestingen viser at det ikke er noen store forskjeller på roamingtid ved bruk av Airespace eller Aironet, når en ikke bruker IEEE 802.1X og RADIUS. Dersom roamingen skjer uten at man må assosiere seg på nytt, vil begge arkitekturene ha en roamingtid på mellom 11 og 13 ms. I tilfeller der klienten mister forbindelsen og må assosieres på nytt, vil også roamingtiden være omtrent lik for begge systemene.

5.4 Voice over Wireless IP

Voice over Wireless IP (VoWIP) har av mange blitt omtalt som den avgjørende tjenesten for utbredelsen til city-wide trådløse nettverk. Etter hvert som nye klientenheter, som for eksempel mobiltelefoner, blir levert med godkjenning fra Wi-Fi, vil denne tjenesten bli mer tilgjengelig. VoIP er en sanntidstjeneste som er avhengig av lite jitter og kort RTT. VoIP sendes over nettverket på samme måte som all annen datatrafikk. Samtalen blir digitalisert og

sendes som IP-pakker mellom samtalepartene. Oppsetting av en VoIP-samtale foregår ved at en bruker en analog til digital konverter som digitaliserer samtalen i bits. Deretter blir bitsene komprimert for å tilpasse dem overføringen på datanettverket. For å utføre dette finnes det flere forskjellige komprimeringsprotokoller. Talepakkene blir etter komprimering innsatt i datapakker ved bruk av en Real-Time Transport protocol (RTP) som sendes over UDP over IP, som vist i figur 5.12.

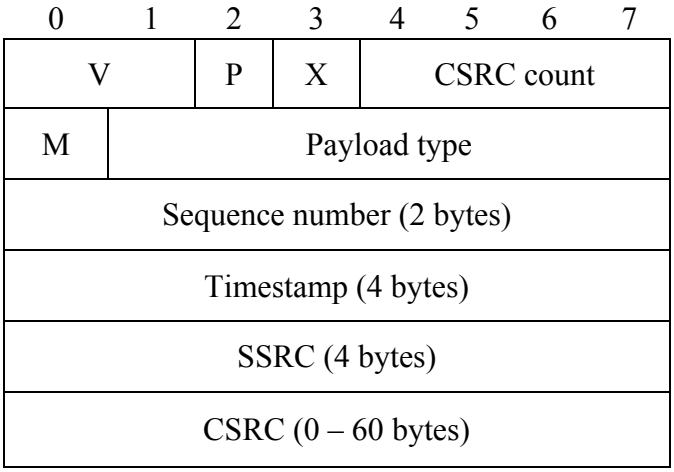
IP (20 bytes)	UDP (8 bytes)	RTP (12 Bytes)	VoIP datapakke

Figur 5.12: VoIP-protokollstakk

For å få kontakt med mottakeren blir det benyttet en signaleringsprotokoll. Her er ITU-T-H323 en vanlig protokoll. Hos mottakeren må pakkene taes fra hverandre, og data må leses og konverteres tilbake til analoge signaler, før de sendes til telefonhøytaleren eller til lydkortet i klienten. Alt dette må skje i sanntid for at denne tjenesten skal kunne være nyttig for brukerne.

Etter at den analoge til digitale konverteringen har funnet sted, blir de digitale dataene tilpasset en standard som gjør signalene egnet for sending over et datanettverk. Her er kodekser som ITU-T G.711 og ITU-T G.726 vanlige. De ulike kodeksene komprimerer de digitale signalene i ulik grad som beskrevet i tabell 5.11 i kapittel 5.4.2.

RTP er protokollen som blir brukt for å innkapsle rådataen. Den blir igjen innkapslet i en UDP-pakke og sendt over IP. UDP støtter ikke muligheten for å sjekke hvilken rekkefølge pakkene ankommer mottakeren, eller hvor lang tid pakkene bruker for å nå frem. Dette er viktige egenskaper for å kunne tilby god samtalekvalitet. RTP-protokollen erstatter disse manglende egenskapene ved å fortelle mottakeren hvilket nummer i rekkefølgen pakken er, og dermed gi mottakeren muligheten til å droppe pakker som bruker for lang tid gjennom nettverket. VoIP er ikke avhengig av å motta alle pakkene i en pakkestrøm. Det er viktigere at pakkeforsinkelsen ikke blir for stor.



Figur 5.13: RTP-headerformat

RTP-protokollen er vist i figur 5.13. De forskjellige feltene representerer:

V	Versjon: RTP-versjonen som er benyttet
P	Padding: Et bit som settes dersom pakken inneholder en eller flere oktetter på enden av pakken som ikke er en del av nyttedataen. Dette skjer når antall bit i RTP-pakken ikke er et multiplum av 8.
X	Extension: Når dette bitet er satt, blir headeren etterfulgt av en header-forlengelse med et definert format.
CSRC cont	Gir antall Contributing Source Identifier (CSRC) som etterfølger headeren.
M	Marker: Dette bitet brukes for å markere viktige hendelser, for eksempel rammegrenser.
PT	Payload type: Identifiserer formatet til RTP-dataen og forteller hvilke applikasjoner den skal bruke.
Sequence nr	Øker sekvensnummeret med en for hver RTP-pakke som blir sendt. Dette kan brukes for å detektere pakketap og organisere rekkefølgen på pakker.
Timestamp:	Forteller når den første oktetten i RTP-pakken ble samplet. Det kan hjelpe til med å synkronisere datapakker. Dette brukes også til jitterkalkulasjoner og for å kunne droppe pakker som bruker for lang tid til destinasjonen.
SSRC	Synchronization Source Identifier (SSRC) brukes for å finne synkroniseringskilden.
CSRC	Lister kilder for nyttedataen i den aktuelle pakken. [24]

Det er flere grunner til at UDP blir valgt som transportprotokoll i stedet for TCP når RTP-pakker skal overføres. For sanntidsapplikasjoner er TCP lite egnet fordi den retransporterer tapte datapakker. Det vil ta en RTT før mottaker og sender har oppdaget den tapte pakken og fått den sendt på nytt. Ved å vente så lenge på en tapt pakke, vil det oppstå en merkbar forsinkelse i samtalen. UDP har ikke støtte for slik retransport av tapte datapakker. I tillegg støtter ikke TCP multikast, og den opererer med et oppholdsvindu som starter når en oppdager et pakketap. UDP blir derfor brukt som transportprotokoll for sanntidspakker fremfor TCP. For kvaliteten på VoIP-samtaler er det mye viktigere med liten forsinkelse enn det et pakketap i begrenset skala er. Pakketap som forekommer i form av tilfeldige enkeltpakker, vil ikke være merkbart i en samtale.

For å unngå dårlig samtalekvalitet i trådløse nettverk med mange samtidige samtaler eller med mye annen datatrafikk, er det ønskelig med prioritering av IP-pakker som inneholder digitalisert tale. Dette kan gjøres over Ethernet ved å tilby forskjellige typer tjenestekvalitet. I trådløse datanettverk er det ikke like lett å garantere prioritet til enkeltpakker. Kapittel 3.7 omhandler IEEE 802.11e som er en standard som gjøre det mulig å tilby tjenestekvalitet også over et trådløst nettverk. Ved siden av prioriteringsmekanismer er det flere faktorer som

spiller inn for samtalekvaliteten til en VoWIP-samtale. Signalkvalitet, SNR og antall samtidige klienter som kommuniserer med aksesspunktet, kan være avgjørende for om samtalen kan gjennomføres med tilfredsstillende kvalitet i trådløst nettverk. Den mest brukte standarden for å måle samtalekvalitet er Mean Opinion Score (MOS). [24]

5.4.1 Mean Opinion Score

Mean Opinion Score er et markedsledende sett av kvalitetsnormer som er standardisert av ITU for å måle talekvalitet ved IP-telefoni. MOS-verdiene går fra 5,0 som er beste kvalitet, til dårligste samtalekvalitet med MOS-verdi 1,0. Denne måleverdien er utviklet for å tallfeste den tidligere subjektive vurderingen av samtalekvalitet over en telefonlinje. MOS-verdier kan også benyttes i trådløse datanettverk for å måle samtalekvaliteten ved VoWIP.

For å kalkulere MOS-verdien har ITU lager en anbefaling (ITU-T Rec. G.107) som introduserer E-modellen. E-modellen regner ut en enkel tallstørrelse som kalles Transmission Rating Factor (R-faktoren) ut i fra pakkeforsinkelser og signalforringelser på grunn av utstyr. Når en har kalkulert en R-faktor, kan denne konverteres til en MOS-verdi. [21]

E-modellen genererer en antagelse om forventet talekvalitet, slik den blir oppfattet hos en vanlig telefonbruker, i en komplett ende-til-ende samtale. Modellen tar med i beregningen mange typiske signalforringelser som enveisforsinkelser, enheter med lav bitratekoding, pakketap, støy og ekko. R-faktoren som E-modellen gir som output, blir kalkulert på grunnlag av resultatet fra en rekke subjektive tester som har vært gjort med ulike samtaleparametre. [21]

E-modellen er basert på en matematisk algoritme bygget opp av ulike transmisjonsparametre som har betydning for opplevd samtalekvalitet. Modellen tar også hensyn til kombinasjonen av disse parametrene dersom de forekommer samtidig. Sammenhengen mellom de ulike transmisjonsparametrene og R-faktoren kan uttrykkes med ligningen [14]:

$$R = SNR - Is - Id - Ie,eff + F \quad (3)$$

- SNR SNR er her en benevning for mottatt talenivå i forhold til nettverksstøy og akustisk støy
- Is Is uttrykker alle forringelser av talesignalet som blir generert samtidig med talesignalet. Dette kan for eksempel være kvantiseringsstøy eller andre mekanismer som utfører funksjoner på signalet.
- Id Id er en sum av alle forringelser som er forårsaket av ende-til-ende forsinkelsen og ekko.
- Ie,eff Ie,eff står for Effective equipment impairment factor og representerer forringelser som er forårsaket av kodekser for VoIP.

F F er benevnelsen for fordelsfaktoren. I motsetning til Is, Id og Ie,eff blir denne lagt til SNR. Det betyr at denne faktoren benevner villigheten til å akseptere en dårligere samtalekvalitet i bytte mot for eksempel lett tilgjengelig teknologi og mobilitet. [15]

R-faktoren har verdifelt $0 \leq R < 100$, der høyere verdier gir høyere samtalekvalitet. Tabell 5.10 viser en oversikt over hvordan forskjellig R-faktor oppleves [14].

R-faktor	Samtalekvalitet	Brukertilfredshet
$90 \leq R < 100$	Best	Veldig tilfredsstillende
$80 \leq R < 90$	Høy	Tilfredsstillende
$70 \leq R < 80$	Medium	Noen brukere misfornøyde
$60 \leq R < 70$	Lav	Mange brukere misfornøyde
$50 \leq R < 60$	Dårlig	Nesten alle brukere misfornøyde

Tabell 5.10: R-faktor og samtalekvalitet
Tabellen er hentet fra [14]

Forbindelser med R-faktor under 50 er for dårlig til at tjenesten er nyttig for brukerne. Den utregnede R-faktoren kan brukes for å finne en egnet MOS-verdi. Forholdet mellom R-faktor og MOS-verdi er vist i figur 5.14.

Figur 5.14: Forholdet mellom R-faktor og MOS-verdi
Figuren er hentet fra [16]

Når en samtale blir digitalisert for å sendes gjennom et datanettverk, blir det en naturlig forringelse av det opprinnelige signalet. Av den grunn er den maksimale teoretiske verdien på R-faktoren 93,2. Dette tilsvarer en MOS-verdi på 4,41 [16].

5.4.2 VoIP-kodekser

Enveisforsinkelse, jitter og pakketap er faktorer som forringer samtalekvaliteten. I tillegg er kvaliteten avhengig av hvilken VoIP-kodeks som blir benyttet. En kodeks er software eller hardware som benyttes for å konvertere et analogt signal til et digitalt og tilbake igjen. De forskjellige kodeksene som blir brukt til dette har ulike egenskaper og påvirkninger på signalet de konverterer. Tabell 5.11 viser parametre for de fem mest brukte kodeksene for VoIP.

Kodeks	Bitrate (Kbps)	Rammetid (ms)	Kodeksforringelse i R-faktoren
G.711	64.0	10	0
G.729	8.0	10	11
G.723.1-MPMLQ	6.3	30	15
G.723.1-ACELP	5.3	30	19
G.726	32.0	10	7

Tabell 5.11: VoIP-kodekser
Tabellen er hentet fra [16]

Tabellen viser at G.711-kodeksen gir den beste samtalekvaliteten. Denne komprimerer ikke signalet, og bruker derfor større båndbredde enn det som er tilfelle med de andre kodeksene. Antallet samtidige samtaler med tilfredsstillende kvalitet er minst for de kodeksene som bruker størst båndbredde. Det er derfor en avveining mellom antall mulige samtidige VoWIP-samtaler og samtalekvalitet. Tabell 5.11 viser også hvor stor påvirkning valg av kodeks har for størrelsen på R-faktoren. Kodeksforringelsen subtraheres direkte inn i ligningen for utregning av R-faktoren. Dersom en for eksempel benytter en G.723.1-MPMLQ kodeks, kan en trekke 15 poeng fra den maksimale teoretiske R-faktorverdien på 93,2.

5.4.3 Enveisforsinkelse

Enveisforsinkelse er tiden datapakker bruker på å krysse nettverket. Denne forsinkelsen er merkbar for samtalepartene dersom den overstiger 150 ms [16]. Dersom den skulle bli noe særlig høyere enn det, vil forsinkelsen være forstyrrende og samtalekvaliteten karakteriseres som dårlig. Enveisforsinkelsen er forårsaket av fire faktorer: Avstandsforsinkelse, transportforsinkelse, digitaliseringsforsinkelse og jitterbufferforsinkelse [16]. Avstandsforsinkelse er tiden det tar for en pakke å forflytte seg fra en ende til den andre i et nettverk. Denne forsinkelsen er større jo lenger fysisk avstand det er mellom sender og mottaker. Transportforsinkelse er tiden pakkene bruker på å passere nettverksenheter. Det er større forsinkelser i nettverk som for eksempel inneholder mange rutere eller brannmurer. Digitaliseringsforsinkelse betegner tiden kodeksen bruker på å digitalisere den analoge samtalen og på å gjenskape det analoge signalet. Jitterbufferforsinkelse er forsinkelsen som blir til ved at mottaker buffrer pakker for å demme opp for variasjonen i ankomsttid for pakkene. Jitter oppstår fordi pakkene bruker forskjellig tid fra avsender til mottaker gjennom

nettverket. Avsender sender pakker i bestemte tidsintervaller. Pakkene kan ta ulik vei gjennom nettverket, eller møte ulike hindringer. Jitterfilteret er plassert hos mottaker for å utligne denne jitteren. Fordi bufferet holder på pakkene en viss tid, får vi jitterbufferforsinkelse. Enveisforsinkelse utgjør Id i formel (3).

5.4.4 Pakketap

Pakketap får vi når pakker av ulik grunn ikke kommer fram til mottakeren. Når pakketap oppstår, får vi en tom tidsluke i samtalen. Dette oppholdet er ikke veldig ødeleggende for samtalekvaliteten dersom pakketapet ikke er stort og pakketapene forekommer tilfeldig. Det er pakketap av flere etterfølgende pakker som kan være ødeleggende for opplevd samtalekvalitet. For menneskeøret er ikke pakketap av mindre enn 5 etterfølgende pakker merkbart [16].

MOS-verdien brukes for å tallfeste de overnevnte parametrene ved VoIP. En MOS-verdi på over 4,0 er ønskelig for at tjenesten skal tilfredsstille krav til god samtalekvalitet. MOS-verdier kan gi svar på om et trådløst nettverk kan brukes for overføring av IP-telefoni. En vil også kunne bruke MOS-verdien til å se hvordan samtalekvaliteten endrer seg når flere samtaler blir satt opp samtidig og når det kommer annen samtidig trafikk i nettverket.

5.4.5 Testresultater for samtalekvalitet

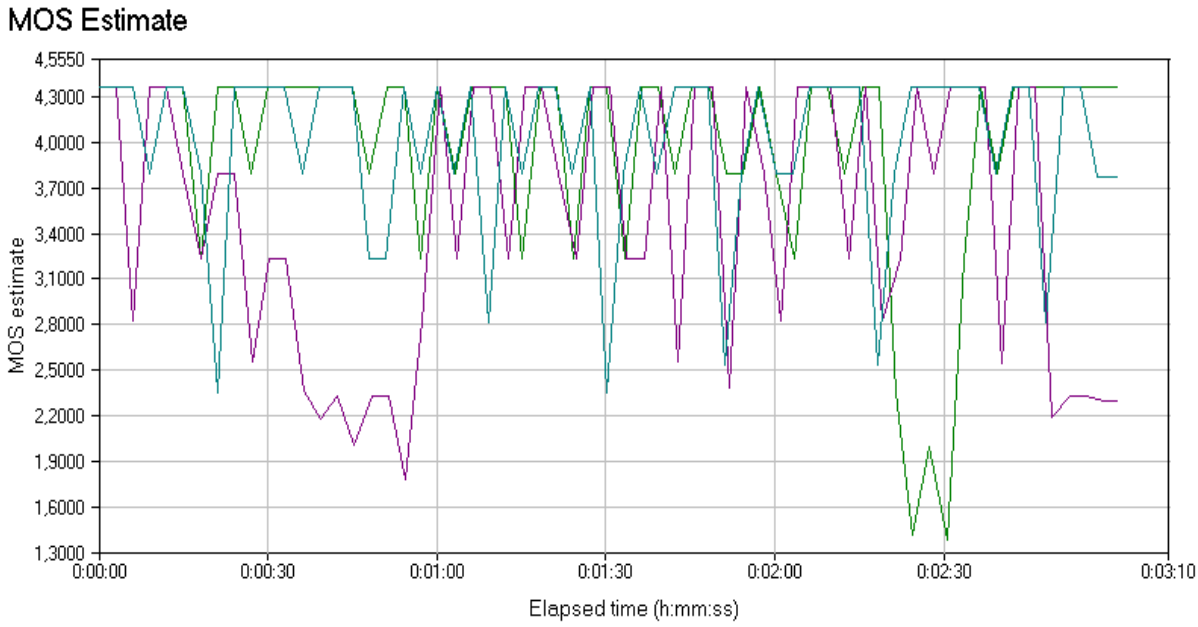
For å undersøke samtalekvalitet i de testede trådløse nettverkene, brukte jeg IxChariot oppsatt for å simulere samtaler mellom trådløse klienter. De ulike testene for VoWIP ble utført med en enkel samtale, flere samtidige samtaler og samtaler som foregikk samtidig med annen datatrafikk. MOS-verdiene jeg fikk som resultat, viser hvor godt nettverksproduktene taklet VoWIP. I tillegg kunne jeg finne ut om der var innebygde mekanismer i utstyret som gjorde at det taklet bedre skalering i form av datatrafikk samtidig som VoWIP-samtaler foregikk.

IxChariot regner ut MOS-verdien ved å benytte en modifisert versjon av E-modell-ligningen. Denne versjonen bruker forsinkelse, jitter, pakketap og valg av kodeks for å regne seg fram til MOS-verdien for en simulert samtale [22].

Under testingen av VoWIP-egenskapene til Airespace og Meru, valgte jeg først å simulere en G.711a-samtale mellom Endpoint1 og Endpoint2. Deretter ble antall samtidige samtaler skalert opp. De siste VoWIP-testene ble gjort ved å legge på datatrafikk i nettverket samtidig med samtalene. Testene ble utført med opp til fire fysiske trådløse klienter for både IEEE 802.11a, IEEE 802.11g og i miks modus mellom b- og g-standarden. Hver fysiske klient ble konfigurert til å kunne simulere trafikk fra opp til fire virtuelle klienter.

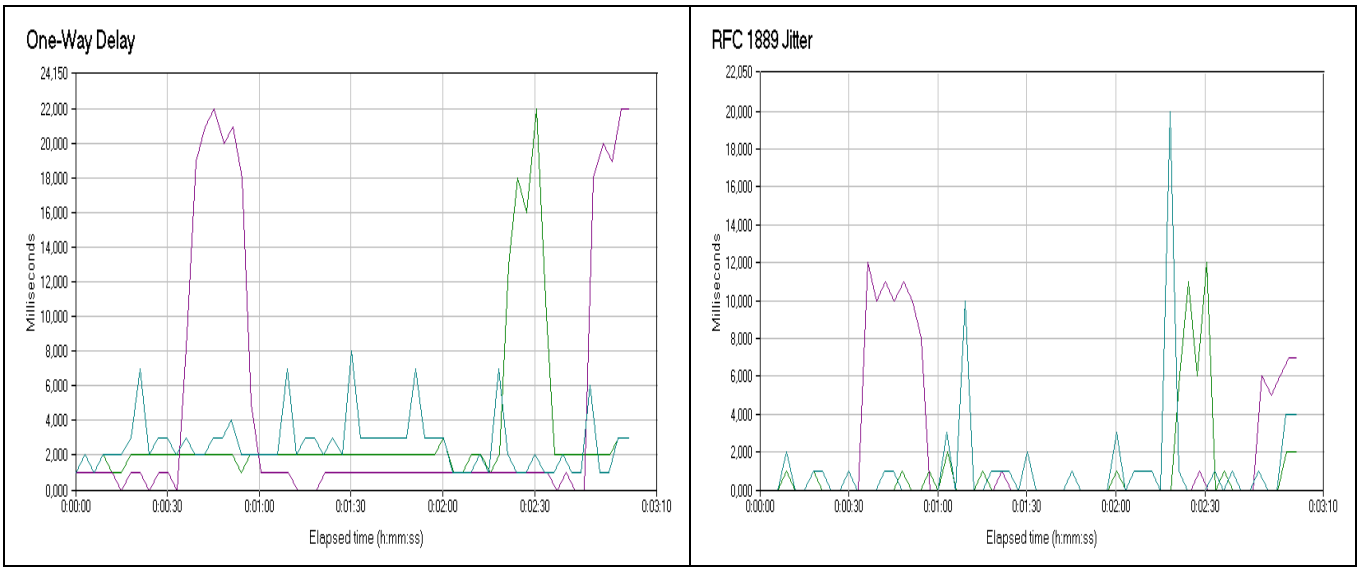
Både Meru og Airespace ga tilfredsstillende resultat og omtrent den samme MOS-verdien for testing av en enkel VoWIP-samtale. En slik samtale har en gjennomsnittlig throughput på

rundt 64 Kbps og bør derfor kunne gjennomføres med god MOS-verdi for det trådløse nettverksutstyret.



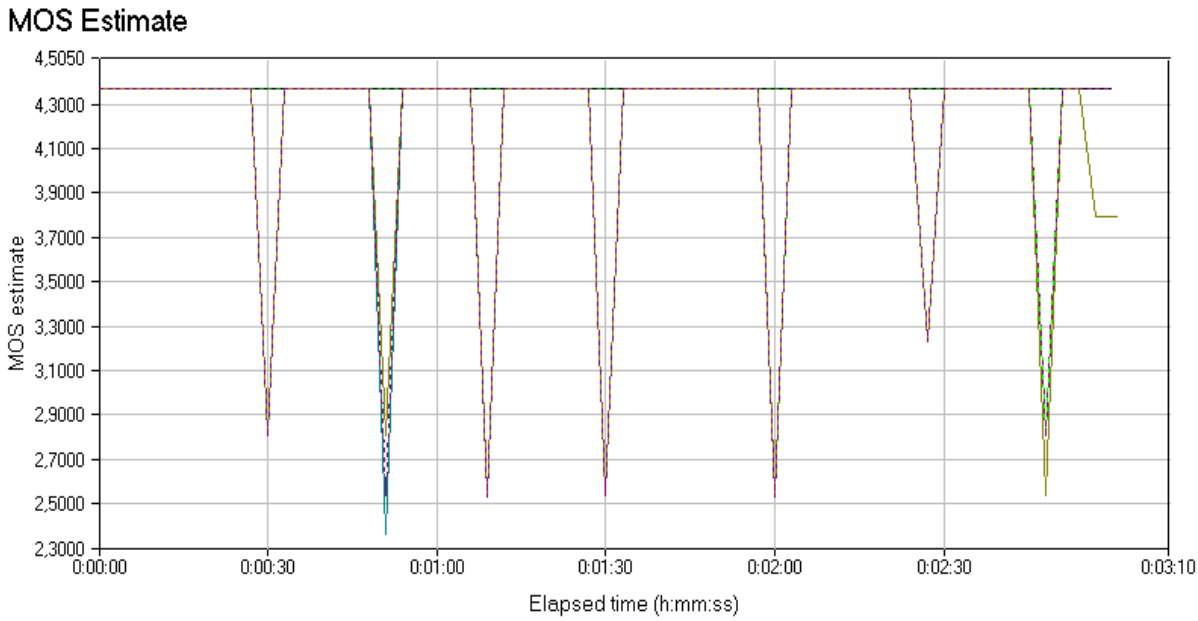
Figur 5.15: MOS-verdier for tre VoWIP-samtaler og en samtidig datapakkestrøm med nettverksutstyr fra Airespace

Figur 5.15 viser en oversikt over MOS-verdier for Airespace ved tre simulerte samtale der det samtidig er en klient som sender datatrafikk. Samtaler som har en MOS-verdi på 3,5 og oppover blir regnet som samtaler med god samtalekvalitet. Testen som er gjengitt i figur 5.15 har en total gjennomsnittlig MOS-verdi på 3,83. I denne testen ser vi likevel at alle de tre samtalene har perioder der MOS-verdien er lavere enn dette. Minimum MOS-verdi er nede på 1,38. Dersom disse lavpunktene for samtalekvalitet vedvarer over en lengre tidsperiode, vil samtalene trolig bli avsluttet i praksis. Sammenhengen mellom MOS-verdi, jitter og forsinkelse kommer frem av testresultatet dersom man samtidig ser på grafene for jitter- og enveisforsinkelsen i figur 5.16. De viser høye verdier for de tidspunktene der MOS-verdien har en dropp for tilsvarende samtale. Dette er i samsvar med teorien bak kalkuleringen av MOS-verdi gitt av formel (3) i kapittel 5.4.1.



Figur 5.16: Enveisforsinkelse og jitter i testeksempelet

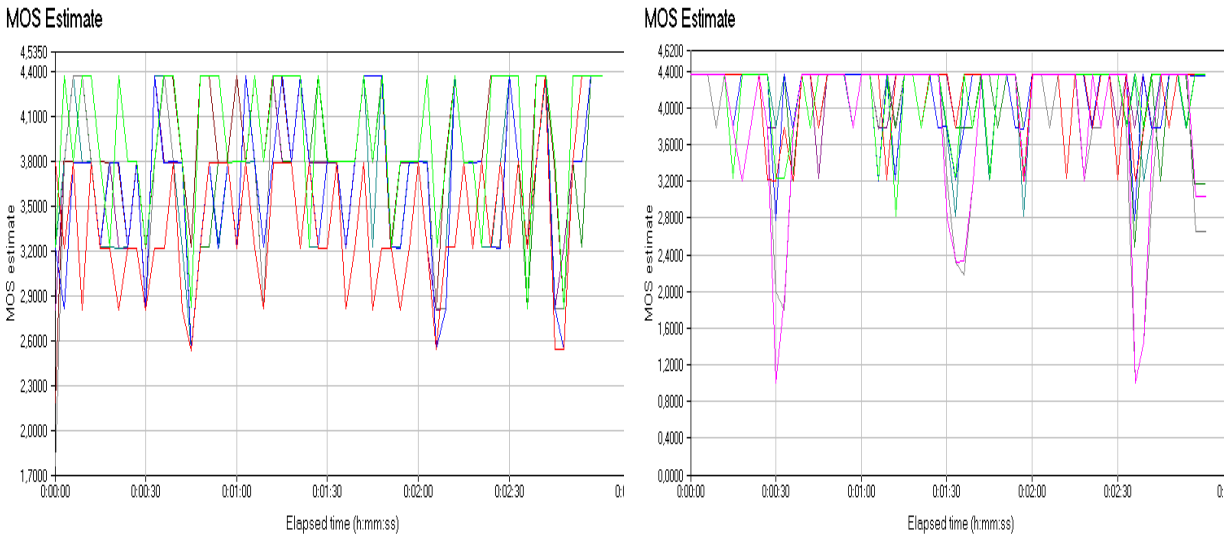
Figur 5.17 viser MOS-verdien for seksten samtidige samtaler over tre minutter. Denne testen er gjort med nettverksutstyr fra Airespace, uten samtidig datatrafikk. Figuren viser at utstyret takler skaleringen i antall samtidige samtaler godt. Her oppnås en gjennomsnittlig MOS-verdi på 4,32, med minimum MOS-verdi på 2,36. Sammenlignet med graf 5.15 viser dette at det er datatrafikk i det trådløse nettverket som er ødeleggende for samtalekvalitet til VoWIP-samtaler, og at en skalering av antall VoWIP gir tilfredsstillende resultat for minst 16 samtidige samtaler.



Figur 5.17: MOS-verdi for 16 samtidige samtaler med IEEE 802.11a for Airespace

I dagens trådløse nettverk støtter de fleste VoWIP-klienter IEEE 802.11b eller IEEE 802.11g. De fleste av disse produkter har imidlertid ikke støtte for IEEE 802.11a. Det er derfor mest

aktuelt, etter dagens forhold, å finne ut hvordan produktene takler samtaler på 2,4 GHz frekvensbåndet. En av testene som ble utført for å undersøke dette, var å simulere fire samtaler som benyttet IEEE 802.11b og fire samtaler som benyttet IEEE 802.11g over det samme aksesspunktet. Figur 5.18 viser resultatet fra denne testen for Airespace til venstre i figuren og Meru til høgre i figuren. Denne testen ga en gjennomsnittlig MOS-verdi på 3,69 for Airespace og 4,08 for Meru.



Figur 5.18: MOS-verdier for fire klienter med IEEE 802.11g og fire klienter med IEEE 802.11b for Airespace til venstre og Meru til høgre.

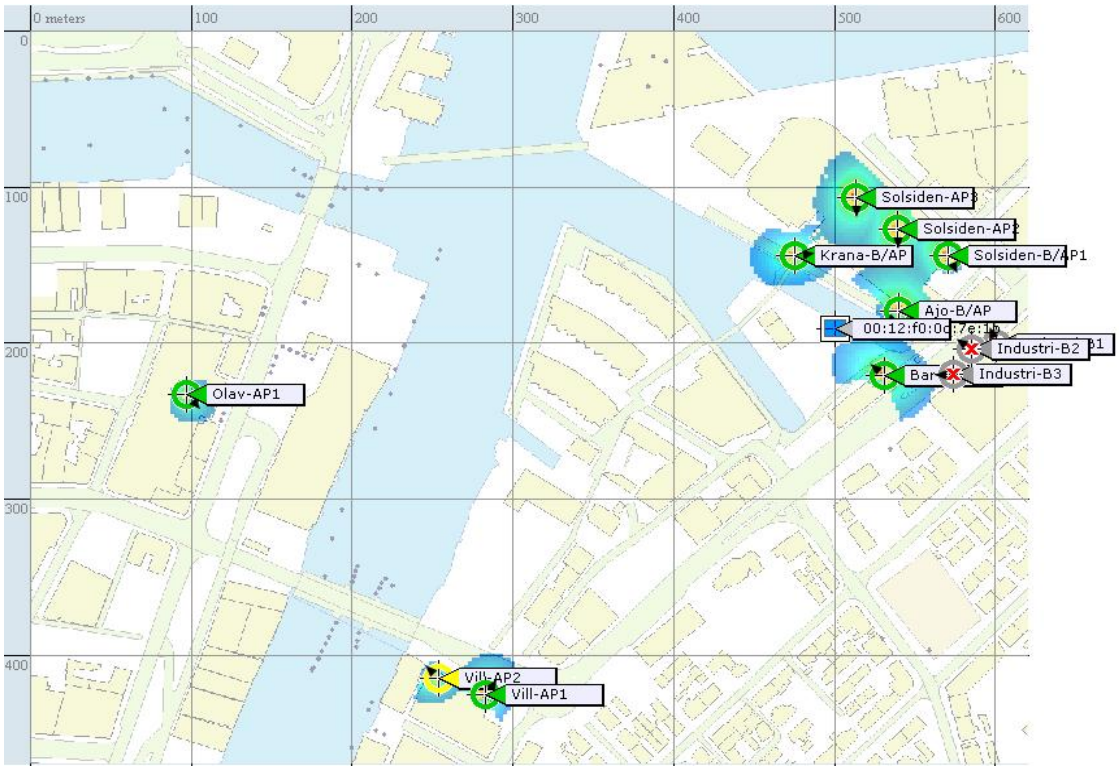
Sammenligning av de to grafene i figur 5.18 kan tyde på at Meru takler bedre en skalering av antall VoWIP-samtaler på 2,4 GHz båndet enn det Airespace gjør. MOS-verdien holder seg mer stabil over testperioden med utstyr fra Meru. Dette kan igjen bety at Meru har en form for innebygd tjenestefunksjonalitet som gir bedre forhold for denne skaleringen.

5.5 Posisjonering

Posisjonering i city-wide trådløse nettverk er en funksjonalitet som kan åpne for mange nye lokasjons- og personbaserte tjenester. For eksempel vil restauranter kunne sende menyen sin til forbipasserende klienter, butikker kan aktivt presentere sine tilbudsvarer, eller turister kan få informasjon om nærliggende severdigheter. Alle slike tjenester er avhengige av at posisjoneringsnøyaktigheten i systemet er tilfredsstillende. Hva som er tilfredsstillende er i dette tilfellet avhengig av tjenestene som skal tilbys. For en restaurant er det ikke nøyaktig nok dersom besøkende på nabokafeen 50 meter unna mottar deres menytilbud, mens det for turister kan være tilfredsstillende nøyaktighet at de får informasjon om Solsiden når de kommer over gangbroen fra sentrum. Hvor nøyaktig systemet klarer å posisjonere klienter er avgjørende for hvilke posisjonsbaserte tjenester som kan utvikles i city-wide trådløse nettverk. Uansett tjeneste, vil det være en fordel med størst mulig posisjoneringsnøyaktighet.

Posisjoneringstestingen i denne oppgaven er utført i piloten til Trådløse Trondheim. Testingen er utført for å undersøke nøyaktigheten til posisjoneringsteknologien i det oppsatte utstyret.

I Trådløse nettverk som det Trådløse Trondheim har satt opp i sin pilot, er det støtte for å kunne angi posisjonen til klienter som befinner seg innenfor dekningsområdet. Med Airespace kan en få oppgitt posisjoner til ulike klienter grafisk ved hjelp av Cisco Airespace Wireless Control System (WCS). Et bilde av denne WCS-en er vist i figur 5.19. Her er de forskjellige aksesspunktene vist som rundinger og en klient er posisjonert som en blå firkant. Kartutsnittet viser området på Solsiden i Trondheim der piloten er satt opp.



Figur 5.19: Cisco WCS-kart med posisjonert klient

For å teste posisjoneringsegenskapene til utstyret, ble WSC-en og kartprogrammet ArcMap tatt i bruk. ArcMap er nærmere beskrevet i appendiks C. Ved hjelp av disse verktøyene kunne posisjoneringsnøyaktigheten til systemet evalueres. Posisjoneringsverktøyet plasserer klienter i kartutsnittet. Hvordan denne teknologien utfører posisjoneringen har det ikke vært mulig å sette seg skikkelig inn i, da produsenten foreløpig ikke ønsker å frigi denne kildekoden. De opplyser imidlertid at systemet bruker RSSI fra to eller flere aksesspunkt for å finne den mest sannsynlige klientlokasjonen, og plasserer den blå firkanten ut i fra dette. Ved hjelp av ArcMap og klientplottingen til WCS-en kan en finne ut hvor mye posisjoneringen avviker fra reell posisjon. For å finne normalavviket for posisjoneringsnøyaktigheten valgte jeg å utføre 10 forskjellige posisjoneringstester. I tillegg utførte jeg to tester helt i utkanten av dekningsområdet. Ved å bruke et program som NetStumbler, var det mulig å se hvilke aksesspunkt klienten ser ved de aktuelle posisjoneringstestene. Denne informasjonen kan si

om det er en sammenheng mellom antall aksesspunkt en klient ser og nøyaktigheten til posisjoneringen.

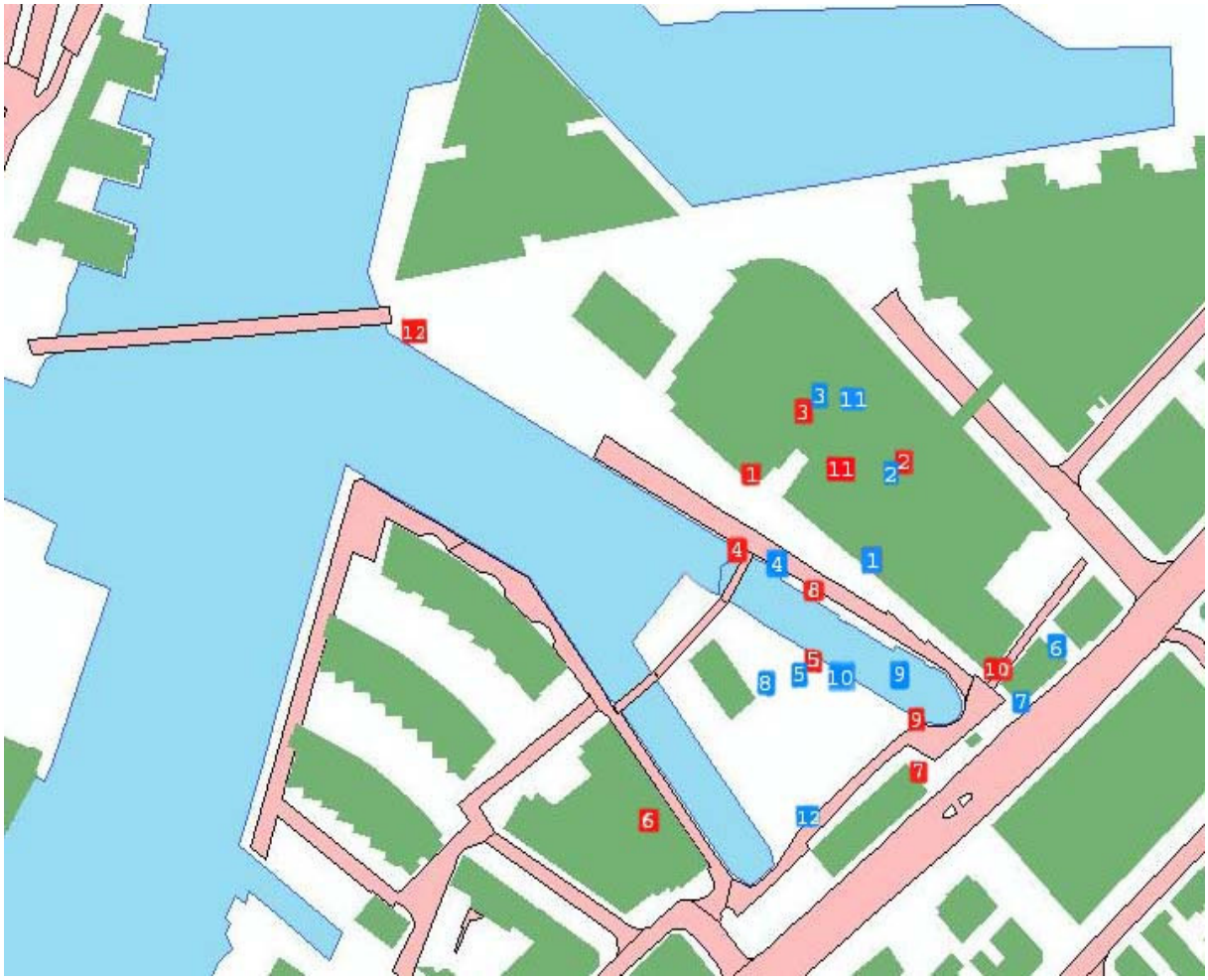
For hver enkel test er jeg, med andre ord, interessert i å registrere Airespace sin plassering av klienten, avvik fra reell posisjon i meter, og hvilke BSSID klienten ser. Ved å registrere denne informasjonen for 10 ulike posisjoner innenfor dekningsområdet, vil jeg kunne si noe om posisjoneringsnøyaktigheten til systemet som er satt opp i piloten på Solsiden.

I tillegg til å forflytte klienten rundt i dekningsområdet til aksesspunktene, har jeg også utført en test der klienten beholder samme posisjon under hele testen. WCS-en ble da satt til å oppdatere posisjoneringsinformasjonen med et intervall på ett minutt. Denne testen ble utført på ulike lokasjoner innenfor dekningsområdet. Målet med testen var å se om et eventuelt posisjoneringsavvik var konstant, eller om det var stor variasjon i hvor systemet plasserte en klient som i realiteten befant seg på samme fysiske lokasjon.

5.5.1 Posisjoneringsresultater

Figur 5.20 viser resultatet av den første posisjoneringstesten. I figuren er de reelle plasseringene til klienten merket med røde firkanter, mens WSC-en sin posisjonering av klienten er merket med blå firkanter. Sammenhørende testresultat er merket med like tall.

Test 6 og 12 er gjort helt i ytterkant av dekningsområdet og oppnår veldig unøyaktige posisjoneringsresultat. Disse testene er gjort i grenseområdet for hvor aksesspunktene gir dekning. Jeg har derfor valg å se bort fra resultatene fra de to testene. I neste utbyggingsfase av Trådløse Trondheim vil det komme opp flere aksesspunkt i området, noe som vil gjør posisjoneringen mer nøyaktig også i disse ytterkantene.

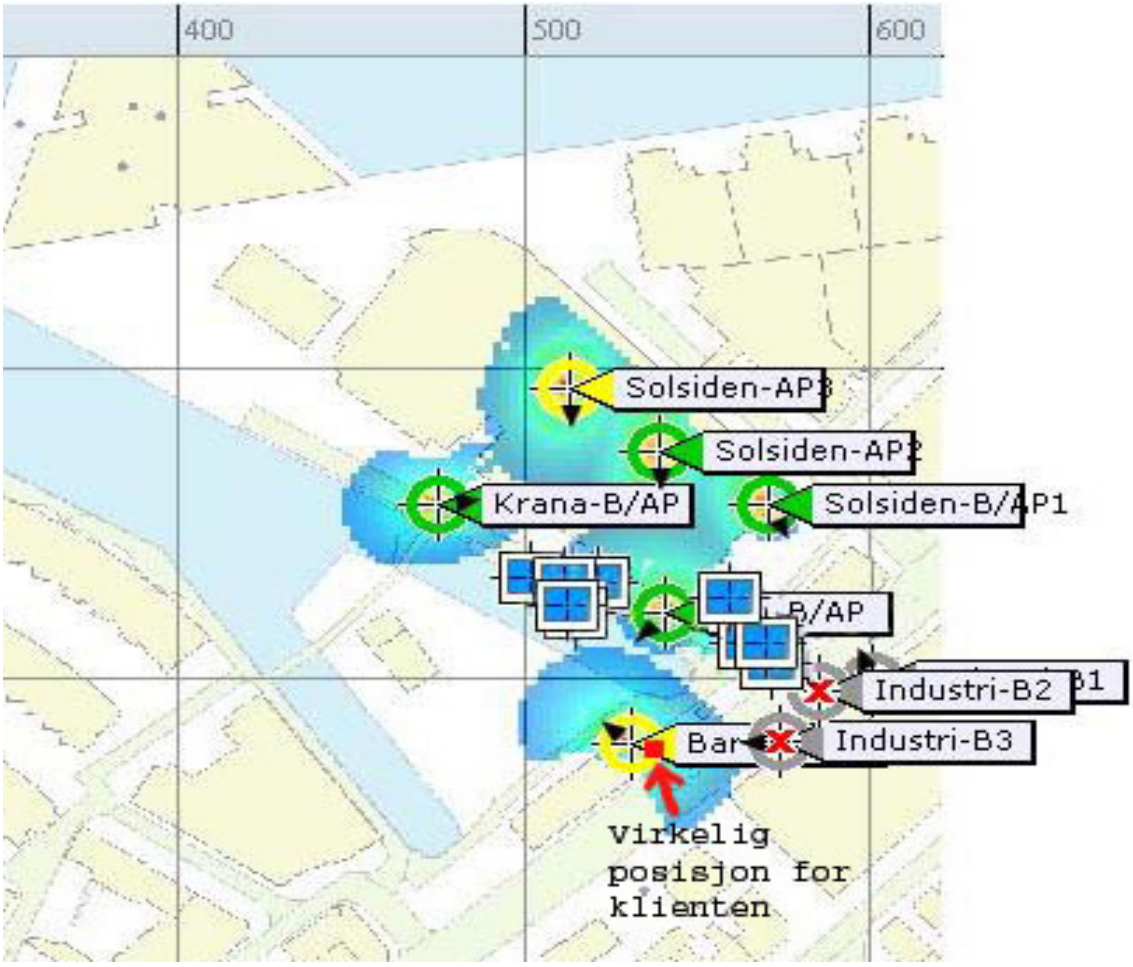


Figur 5.20: Klientplassering og tilhørende posisjonering gjort av WCS-en

Når jeg ser bort fra de ekstreme testene, vil jeg likevel få et gjennomsnittlig utendørs avvik på 29,30 meter. Innendørs på kjøpesenteret er det gjennomsnittlige avviket på 13 meter. Det største målte avviket er på 51 meter, mens systemet i enkelte tilfeller traff den reelle posisjoneringen til klienten innenfor den grafiske posisjoneringsrammen. Denne grafiske posisjoneringsrammen er ganske grov. Figur 5.19 viser at den oppgir posisjoner ved hjelp av et kvadrat på omtrent 5x5 meter i reell målestokk. Et krav til posisjoneringsresultatet burde derfor være at klienten befinner seg i området som er avgrenset av dette kvadratet. Cisco hevder at Airespace kan ha en nøyaktighet på +/- 10 meter. I denne testen skjedde dette kun 3 ganger, der to av gangene var innendørs. Posisjoneringstestene som ble utført viser at teknologien fungerer bedre innendørs enn utendørs. Dette forklares av Airespaceleverandører med at posisjoneringsteknologien er optimalisert med aksesspunktenes interne antenner. Dette kan vi se igjen i resultatene fra posisjoneringstestingen. I piloten har de aksesspunktene som er satt opp innendørs interne antenner, mens de aksesspunktene som er plassert utendørs har tilkoblet eksterne antenner. Dette kan være noe av forklaringen på avviket til posisjoneringsresultatene i forhold til produsentens oppgitte posisjoneringsnøyaktighet.

Appendiks C viser hvilke aksesspunkt klienten ser på de forskjellige lokasjonene og posisjoneringsavviket i meter. Jeg fant ingen sammenheng mellom antall synlige aksesspunkt og størrelsen på avviket for oppgitt posisjon fra WCS-en. Det er trolig at systemet beregner posisjonen til en klient ut fra opplysninger fra flere aksesspunkt, men resultatet viser, som sagt, ingen sammenheng mellom nøyaktighet og antall aksesspunkt klienten ser.

Den andre testmetoden for posisjonering ble gjort ved å beholde klienten på den samme posisjonen gjennom hele testen og la WCS-en oppdatere posisjonen til klienten hvert minutt. Figur 5.19 viser den reelle plasseringen av klienten som en rød firkant. De blå firkantene viser WCS-ens posisjoneringer. Disse posisjoneringene er gjort med ett minutts intervaller. Testen er kjørt over 20 minutter og inneholder derfor 20 posisjoneringer av klienten. Noen av resultatene er imidlertid overlappende slik at det ikke går frem av figuren at det er utført 20 posisjoneringer.



Figur 5.21: Posisjonering av stasjonær klient

Resultatet viser at systemet byttet på å plassere klienten i et av to områder med små avvik. Det største avviket fra reell posisjon er 63 meter, mens den nærmeste oppgitte posisjonen er 41 meter unna reell posisjon. Gjennomsnittlig avvik for denne testen er 48,05 meter. Lignende

tester ble utført på forskjellige steder utendørs i dekningsområdet. De viste alle omtrent det samme resultatet som i figur 5.21.

Innendørs på kjøpesenteret viste posisjoneringstestene et litt mer korrekt resultat. Her er aksesspunktene satt opp uten eksterne antenner. På to av stedene som er avmerket innendørs i figur 5.20 ble det gjort tester der klienten ble holdt på den samme fysiske plassen i ti minutter, mens WCS-en oppdaterte posisjonen med intervall på ett minutt. I disse testene viste det seg at systemet klarte å posisjonere klienten innenfor den grafiske firkanten i 80 % av tilfellene. Samtidig er det tilfeller der WCS-en oppgir en posisjon som avviker ca. 43 meter fra reell posisjon, også innendørs.

Airespace har innebygd verktøy for å kunne posisjonere klienter mer nøyaktig. Den opprinnelige teknologien som blir benyttet posisjonerer klienter etter forhåndsbestemte regler. Systemet støtter imidlertid en mer forutsigbar metode for posisjonering. Dersom administrator av systemet ønsker å finkalibrere systemet, er dette mulig. Det gjøres ved å forflytte en klient som har kontakt med WCS-en rundt i dekningsområdet. Her måles nøyaktig posisjon og signalstyrke og lagres i WCS-ens database. Resultatet av kalibreringen brukes senere til en mer nøyaktig posisjonering av klienter. Hvordan posisjoneringen fungerer etter denne kalibreringen har det ikke vært mulig å teste i denne oppgaven.

I det elektroniske vedlegget er resultatet av posisjoneringstesten vist i figur 5.21 tilgjengelig som en HTML-presentasjon. Denne gjengir, på en bedre måte, hvordan den stasjonære klienten ”hopper” rundt i kartet fra oppdatering til oppdatering.

5.6 Administrative verktøy

Et stort trådløst nettverk med mange aksesspunkt og flere kontrollere, trenger gode verktøy for å kunne administreres. Gode administrative verktøy vil forenkle vedlikeholdsarbeidet og den daglige driften av systemet. Verktøy er også nyttig for å kunne oppdage mangler og trusler for det trådløse nettverket.

Hva som er gode administrative verktøyer, er til en viss grad en subjektiv vurdering. Ved hjelp av den oppsatte piloten har det vært mulig å få erfaringer med hvilke administrative verktøy som er nødvendig for å drifte systemet. Piloten er styrt gjennom Cisco Airespace Wireless Control System (WCS) software. Her kan man blant annet få en geografisk og topologisk oversikt over dekningsområdet, man kan sette og oppdatere sikkerhetsløsninger for alle aksesspunktene, konfigurere systemparametre, overvåke systemet i sanntid, og utføre feilsøking og brukeradministrasjon [29]. I tradisjonelle trådløse nettverk med flere aksesspunkt er man avhengig av å gjøre oppdateringer på hver enkelt basestasjon eller benytte en tredjeparts anordning for å utføre dette. Med kontrollere som styrer aksesspunktene kan denne jobben utføres på kontrolleren som igjen oppdaterer aksesspunktene. WCS-en kan

oppdatere hele systemet slik at man unngår konfigurasjonsfeil og forenkler den administrative jobben.

Den store fordelen med Cisco Airespace WCS er den geografiske fremstillingen av systemet. På en enkel måte kan en laste opp kart over dekningsområdet og legge inn eventuelle hindringer for radiosignalene i dette kartet. En kan da se dekningsområdet for radiosignalene for hvert av aksesspunktene tatt i betraktning de registrerte signalhindringene. I tillegg plasserer WCS-en klientene i forhold til RSSI som beskrevet i kapittelet om posisjoneringsegenskapene til systemet. Denne funksjonaliteten kan også brukes for å finne hull i dekningsområdet der klienter ikke kan motta signaler fra det trådløse nettverket [29]. Systemet har en egen innebygd funksjon som kalles Radio Resource Management (RRM) som identifiserer dekningshullene og rapporterer dette til WCS-en. All informasjon om posisjoner til klienter og aksesspunkt lagres, slik at administrator kan hente ut historiske posisjoneringsdata. [29]

Et problem i tradisjonelle trådløse nettverk er hackere som benytter klienter som simulerer et aksesspunkt. Slike aksesspunkt kan avbryte WLAN-operasjoner ved å kapre lovlig assosierte klienter og lure nettverkssensitive opplysninger, som brukernavn og passord, ut av dem. Hackeren kan da sende en serie med CTS-pakker som gir seg ut for å være pakker som aksesspunktene sender for å informere om kommende nettverkstrafikk fra en klient. I slike tilfeller er dette trafikk fra hackerens klient. Det resulterer i at hackeren er den eneste som får aksess til å overføre datapakker, mens de legitime klientene ikke får aksess til å sende data.

WCS-en i piloten har innebygd støtte for å forhindre hackerangrep med uvedkommende aksesspunkt. Sikkerhetssystemet til kontrolleren bruker den innebygde RRM for å kontinuerlig overvåke alle nærliggende aksesspunkt og automatisk identifisere om det finnes fremmede aksesspunkt innenfor dekningsområdet til systemet. WCS-en varsler i så fall om, slik at systemet kan overvåke aksesspunktene, eller slik at administrator kan utføre videre sikkerhetstiltak ved hjelp av nærliggende legitime aksesspunkt. I det siste tilfellet kan aksesspunkt som befinner seg i nærheten av det fremmede aksesspunktet varsle klienter når de assosierer seg med det ukjente aksesspunktet. [29]

WCS-en har et nettverkssammendrag med oversikt over blant annet dekningsområdet, kontrollerne og aksesspunktene i systemet, de nyeste fremmede aksesspunktene, de fem mest aktive aksesspunktene og eventuelle nye dekningshull. Den mest brukte oversikten i WSC-en er likevel kartoversikten som er vist i figur 5.19. Her er det mulig å overvåke klienter og aksesspunkt i sanntid. En kan til en hver tid se alle klienter i dekningsområdet til aksesspunktene, både de assosierte og de som ikke er assosierte. Kartoversikten gir også en fremstilling av aksesspunktene og statusen for hver enkelt av dem. Ved å holde pekeren over et aksesspunkt, vil en få opp nødvendig konfigureringsinformasjon og adresser.

5.6.1 Erfaringer fra piloten

Nødvendigheten av de forskjellige mulighetene og konfigurasjonene som WCS-en gir, avhenger av størrelsen på systemet og hvordan nettverket skal brukes. Erfaringer som er gjort i piloten til Trådløse Trondheim avdekker administrative behov for systemer av denne typen.

Den geografiske oversikten over klienter og aksesspunkt har vært nyttig for å kunne få et bilde av systemet og vise status for de forskjellige nettverksenhetene. WCS-en gir i den geografiske oversikten beskjed dersom et aksesspunkt er nede og hvilket aksesspunkt dette er. Erfaring fra piloten avdekker imidlertid at dette ikke alltid fungerer optimalt. Enkelte ganger viser WCS-en at et aksesspunkt er nede uten at det i realiteten er det. Ved pinging er det likevel mulig å få kontakt, og det er også mulig å koble seg opp mot aksesspunktet.

En annen nyttig funksjon er muligheten for å kunne detektere og få tilbakemeldinger på interferensproblemer, og samtidig få kanal og signaloversikt som kan endres etter tilbakemeldingene fra systemet.

WCS-en kan stilles inn til å gi alarmer på mange forskjellige typer problemer. Interferensproblemer, fremmede aksesspunkt, sikkerhetsproblemer, og aksesspunkt eller kontrollere som går ned, er de mest vanlige problemene. WCS-en kan konfigureres til å gi alarmer om dette via e-post eller sms i tillegg til varsling i WCS-en. En drifter av systemet kan derfor motta alarmen selv om han ikke er pålogget kontrolleren eller WCS-en. En kan selv velge hva som skal være kritiske alarmer og hva det ikke er behov for å varsle om.

Statistikkoversikten i WCS-en har også vist seg å være et nyttig verktøy. Generelt er all statistikk som WCS-en presenterer nyttig for å gi et bilde av bruksmønsteret i systemet. En kan, ut i fra statistikken, konfigurere systemet på en ideell måte etter bruksmønsteret. WCS-en samler inn og tar vare på data om alle aksesspunktene og klientene som har vært assosiert. Dataen viser hvilke aksesspunkt som har størst trafikk og hvor det kan være behov for flere aksesspunkt for lastavveksling. Statistikken viser også hvor mye trafikk hver enkelt klient har hatt. Dette kan brukes for å finne klienter som ødelegger for andre ved å hele tidene å generere trafikk til aksesspunktet. Et slikt problem kan ofte oppstå med virusinfiserte klienter. Med IEEE 802.1X og RADIUS-autentisering kan WCSen vise brukernavn til hver enkelt klient i systemet, slik at brukere av eventuelle virusinfiserte klienter kan varsles.

For Trådløse Trondheim er det ønskelig å kunne gi forskjellige brukergrupper ulike rettigheter selv om de er tilknyttet den samme SSID-en. Systemet må da støtte bruk av forskjellige VLAN som blir fordelt gjennom rettigheter gitt av RADIUS. En annen mulighet er å gi rettigheter ved å la forskjellige brukergrupper koble til ulike SSID. RADIUS-styrt VLAN-tildeling er imidlertid å foretrekke. Spesielt i nettverk med mange ulike brukergrupper..

Under driftingen av piloten har det også vist seg at det har vært nyttig med konfigurasjons og data backup. Ved versjonsoppdateringer har det vært nødvendig å laste inn alle innstillingene

på nytt. Dette kan også være aktuelt i andre sammenhenger. En form for backup av systemet er viktig for å unngå mye arbeid dersom konfigurasjonen av en eller annen grunn skulle resettes. Det kan også være nyttig med backup av de forskjellige loggene og statistikkene som systemet til en hver tid genererer og lagrer.

Administrative verktøy er software som blir solgt som tilbehør til det trådløse nettverksutstyret. Det er likevel en viktig del av et velfungerende system. Software som Cisco Airespace WCS vil kontinuerlig bli oppdaterte og tilført ny funksjonalitet etter hvert som produsenten får tilbakemeldinger fra brukerne. De fleste softwarefeil som har blitt oppdaget under testingen av piloten vil mest sannsynlig bli rettet i kommende versjoner.

6 Hvilke parametre trengs for å beskrive et city-wide WLAN?

Siden de første datamaskinene ble koblet sammen i enkle trådløse nettverk der data ble sendt mellom dem ved hjelp av radiobølger, har WLAN-teknologien hatt en kraftig utvikling. Fra enkeltmaskiner koblet sammen i små trådløse nettverk, til trådløse nettverk med autonome aksesspunkt som styrer kommunikasjonen, og til den nyeste arkitekturen med aksesspunkt som samarbeider ved hjelp av tilknyttede kontrollere. Standardiseringsorganisasjoner som IEEE har satt ned arbeidsgrupper og publisert internasjonale standarder for at nettverksutstyr skal være kompatible på tvers av utstyrsprodusenter. Det har ført til at den globale teknologiske utviklingen har gått i den samme retningen og gitt kompatibelt utstyr på tvers av produsenter. Stadig flere teknologiske nyvinninger gir muligheter for nye tjenester til trådløse klienter som igjen skaper nye brukerkrav til nettverksutstyret. Utstyrskrav har gjort det nødvendig med testing og evaluering for å kunne finne utstyr som tilfredsstiller de nye behovene som brukere og tjenester har fått. Nødvendigheten av god testing er større jo flere brukere og jo flere tjenester som finnes i det trådløse nettverket.

IEEE har satt ned arbeidsgruppen 802.11T for å utvikle testmetoder og målspesifikasjoner for IEEE 802.11-nettverk. Arbeidsgruppen skal utvikle et testspesifikasjonsdokument med tittel, ”Recommended Practice for the Evaluation of 802.11 Wireless Performance” [30]. Målet er at en felles testmetode for trådløse nettverk skal bidra til at utstyrsprodusenter skal lage produkter med best mulige egenskaper, og ikke bare lage utstyr som tilfredsstiller kravspesifikasjonene i standardene. I tillegg skal en felles test- og evalueringsmetode fra standardiseringskomiteen kunne hjelpe brukere til å sammenligne produkter på et objektivt grunnlag. Arbeidsgruppen IEEE 802.11T har jevnlige møter og holder telefonkonferanser hver uke, men de har enda ikke kommet med noen endelige anbefalinger.

Testkriterier for trådløse datanettverk er mer komplekse enn det som er tilfellet for trådbundne nettverk. I tillegg til kompleks teknologi og komplekst utstyr, må en i trådløse systemer ta hensyn til signalhindringer, interferens og andre påvirkninger på radiosignalet. Den store utfordringen ved testing av trådløse nettverk er å kunne holde testmiljøet stabilt og likt under all testing, uavhengig av tid og sted. Et ideelt testmiljø for WLAN-utstyr er beskyttet mot påvirkninger fra andre radiokilder og signalhindringer. Dette er vanskelig å oppnå i praksis, spesielt under testing av roaming- og mobilitetsegenskaper der klienten må forflyttes over et geografisk område. IEEE 802.11T jobber med flere mulige løsninger som kan skape en standardanbefaling for testing som tar hensyn til problemene med å gjenskape et likt testmiljø hver gang tester blir utført. Den mest aktuelle av disse løsningene er å benytte kablede miljøer som kan programmeres til en fast demping av radiosignal for å simulere forskjellig avstand mellom enheter i et trådløst nettverk [30].

Det har ikke tidligere vært noen felles standarder eller beskrivelseskriterier for testing av trådløst nettverksutstyr. Likevel har det vært gjort tester og evalueringer på dette feltet, uten at disse har fulgt noen felles mal eller retningslinjer. Testresultatene har derfor vært vanskelige å sammenligne og dra helhetlige slutninger ut i fra.

I city-wide trådløse nettverk med kontrollere er det ikke nødvendigvis de samme egenskapene som er viktige som i mindre trådløse systemer. Forskjellige nettverkstyper gir ulike krav til forskjellige nettverksparametre. IEEE 802.11T vil likevel kunne brukes som en felles retningslinje for hvordan alt nettverksutstyr skal testes.

City-wide trådløse nettverk stiller strengere krav til blant annet skalering og administrative verktøy enn det mindre hjemmenettverk eller hotspots gjør. I tillegg kommer nye funksjonaliteter som sømløs roaming og posisjonering med den nye arkitekturen. Ut i fra evaluering av nettverksutstyr i Trådløse Trondheim-piloten og i laboratorium hos Uninett, mener jeg at følgende parametre er nødvendige for å beskrive egenskapene til nettverksutstyr for city-wide trådløse nettverk:

- Roamingtid
- Throughput
- Posisjoneringsnøyaktighet
- VoIP-egenskaper
- Skaleringsegenskaper
- Administrative verktøy
- Sikkerhet
- Tekniske spesifikasjoner

6.1 Roamingtid

I fremtidige utbygginger av Trådløse Trondheim skal det tilbys trådløs dekning i store deler av sentrale Trondheim. Brukerne kan da være oppkoblet mot nettverket mens de forflytter seg rundt i byen. Denne forflytningen medfører at klienten beveger seg gjennom dekningsområdet til flere aksesspunkt. Tiden roamingen tar bestemmer hvilke tjenester som kan tilbys de mobile brukerne. En mest mulig sømløs roaming er ønskelig, slik at brukerne ikke merker at klienten skifter aksesspunkttilknytning.

Trådløse systemer med sentrale kontrollere skal forenkle roamingprosessen og dermed medføre kortere roamingtid. Sammenligningstester som ble utførte mellom Airespace og det autonome Cisco Aironet, kunne ikke bevise at det var noe fordel til Airespace når det gjaldt roamingtid. Tvert i mot, avdekket testene et mulig problem med fast reconnect ved bruk av IEEE 802.1X og RADIUS. Dette førte til at klienten måtte autentiseres på nytt, med et brudd i forbindelsen på rundt 150 ms. Testingen viste en normal roamintid på mellom 11 og 13 ms for

både aksesspunkt med kontroller og for det autonome alternativet fra Cisco. For sanntidstjenester som for eksempel VoIP, vil pakketap som følge av lang roamingtid være ødeleggende for tjenesten. Dersom pakketapet av etterfølgende pakker overstiger 5 pakker, vil menneskeøret kunne merke tapet [16]. Ende-til-ende forsinkelse vil etter formel (3) i kapittel 5.4.1 redusere MOS-verdien for samtalen. Det er derfor en direkte sammenheng mellom roamingtid og MOS-verdi for en VoWIP-samtale. Med tanke på forsinkelser og pakketap, bør ikke roamingtiden overstige det som kreves av sanntidsapplikasjoner som skal brukes i nettverket.

6.2 Throughput

De teoretiske utregningene av maksimal overføringskapasitet for nyttedata i kapittel 5.2, gir et øvre nivå for forventet throughput i et trådløst system. Under ideelle forhold, bør nettversutstyr kunne yte tilfredsstillende i forhold til det teoretisk maksimale nivået. Som vist i figur 5.5 og tabell 5.8 vil det teoretisk maksimale nivået for overføringskapasitet reduseres noe på grunn av CAPWAP-innkapslingen mellom aksesspunkt og kontroller. Denne innkapslingen og den periodiske skanningen av radiospekteret som kan sees i figur 5.4, vil utgjøre den eneste teoretiske forskjellen i throughput for systemer med kontroller og systemer med autonome aksesspunkt. Forskjellen er imidlertid så liten at den ikke vil ha noe praktisk betydning.

Når flere klienter er tilkoblet det samme aksesspunktet, deler de på overføringskapasiteten. For å unngå interferensproblemer er det bare en klient som kan sende over det trådløse mediet om gangen. Hvilken klient som sender er bestemt av mellomrammeavstander og CSMA/CA som beskrevet i kapittel 3.1.2. Throughputtestingen som ble utført i laboratorium ble gjort med opp til 16 samtidige klienter på et aksesspunkt. Resultatet viste at det ikke ble noe vesentlig tap i total gjennomsnittlig throughput når antall klienter økte. Variasjonen i throughput for de ulike klientene var imidlertid relativt stor. Uten noen form for tjenestekvalitet og prioriteringer av pakker, er det ikke mulig å forutse hvilken klient som opplever best throughput. I slike tilfeller er det ønskelig med mest mulig lik overføringskapasitet for de assosierte klientene for å kunne tilby forutsigbare tjenester, tatt i betraktning antall assosierte klienter.

6.3 Posisjoneringsnøyaktighet

Posisjonering av klienter er en plattformtjeneste det er mulig å tilby i en arkitektur med flere aksesspunkt. Aksesspunktene kan da benytte forhåndsdefinerte verdier for signalstyrke for å posisjonere klienter. Nøyaktigheten på denne posisjoneringen bestemmer hvilke tjenester som kan tilbys brukerne.

Airespace oppgir en posisjoneringsnøyaktighet på +/- 10 meter med interne antenner. For å oppnå denne nøyaktigheten, må det imidlertid legges ned en god del administrativt arbeid. På

forhånd må drifter av systemet registrere posisjoner i forhold til signalstyrke som beskrevet i kapittel 5.5.1. Dette må igjen lagres i Location Appliance databasen, slik at dataene kan brukes til mer nøyaktig posisjonering. I store systemer, som Trådløse Trondheim, vil en slik kalibrering være et ressurskrevende arbeid. For å oppnå oppgitt nøyaktighet, må posisjoneringsteknologien i tillegg oppgraderes til å støtte bruk av eksterne antenner. Testresultatene viser at de oppgitte posisjoneringsresultatene stemmer i 80% av tilfellene for innendørs aksesspunktene som ikke bruker eksterne antenner.

En posisjoneringsnøyaktighet som ligger innenfor de oppgitte verdiene til Airespace, vil kunne åpne for mange nye tjenester og muligheter i Trådløse Trondheim. Slik som teknologien fungerer i dag, vil dette imidlertid være svært ressurskrevende å få til denne nøyaktigheten, dersom det i det hele tatt er mulig med eksterne antenner.

6.4 VoIP egenskaper

Voice over Wireless IP blir av mange regnet som den avgjørende tjenesten for utbredelsen av offentlige trådløse nettverk. Et ferdig utbygd Trådløse Trondheim som dekker store deler av Trondheim sentrum, vil ved hjelp av sanntidsapplikasjoner for tale kunne tilby gratis telefonsamtaler over det trådløse nettverket. Brukere med Wi-Fi-mobiltelefoner vil da ha mulighet for å benytte det trådløse nettverket til telefoni i stedet for GSM (Global System for Mobile Communication). Dette forutsetter at det trådløse nettverket kan tilby forhold som gir tilfredsstillende talekvalitet. Den vanligste måten å benevne samtalekvalitet er ved bruk av MOS-verdier. For at kvaliteten på en samtale skal oppleves som god, må den ha en MOS-verdi over 3.5, men det er mulig at brukerne aksepterer lavere MOS-verdier enn dette i bytte mot at samtalene kan gjennomføres kostnadsfritt.

For city-wide trådløse nettverk er det viktig at MOS-verdien ikke synker betraktelig ved flere samtidige samtaler og i tilfeller der det er klienter som samtidig sender datatrafikk. Dersom VoWIP blir så populær som det mange tror, kan det være nettopp støtte for god samtalekvalitet som er avgjørende for valg av nettversutstyr. Utstyr som har innebygd IEEE 802.11e eller andre prioriteringsmekanismer, kan brukes for å prioritere trafikk fra sanntidsapplikasjoner. IEEE 802.11e prioriterer trafikk som beskrevet i kapittel 3.7. Dette vil gi datapakker fra sanntidsapplikasjoner prioritet fremfor andre datapakker. Testingen av samtalekvalitet viste at det var nettopp samtidig datatrafikk som var ødeleggende for MOS-verdien. En prioriteringsmekanisme for pakker som er avhengig av liten forsinkelse, vil kunne rette på dette. I trådløse nettverk med mange brukere er det nødvendig med støtte for IEEE 802.11e eller andre løsninger for tjenestekvalitet, for at VoIP skal kunne benyttes effektivt.

6.5 Skaleringsegenskaper

Skaleringsegenskapene til et trådløst nettverk er blant annet gitt ved total throughput og prioriteringsmekanismer når antall klienter øker. I city-wide trådløse nettverk er det spesielt

viktig med gode skaleringsegenskaper, da antall assosierte klienter kan bli stort i populære områder. Fordi klienter deler på å sende over transmisjonskanalen, vil den totale overføringskapasiteten maksimalt være som de utregnede verdiene for throughput i kapittel 5.2. Det er viktig at et økt antall klienter ikke fører til en stor nedgang i total throughput.

Prioriteringsmekanismer som IEEE 802.11e gjør at tjenester som er avhengige av en viss tjenestekvalitet kan benyttes, selv om det er flere samtidige klienter som deler på aksesslinjen. Dette kan for eksempel gi mulighet for flere samtidige brukere uten at det ødelegger for VoWIP-samtaler.

6.6 Administrative verktøy

Ulike produsenter tilbyr forskjellige administrative verktøy til deres trådløse nettverksutstyr. Hvilke administrative krav som stilles til systemet er delvis avhengig av tjenester i det trådløse nettverket, antall brukere og brukergrupper. Evaluering av administrative verktøy er til en viss grad en subjektiv vurdering, men det finnes likevel enkelte verktøy som er nødvendige for å betjene city-wide trådløse nettverk. Piloten til Trådløse Trondheim her vært nyttig for å evaluere og teste de administrative mulighetene som dette systemet gir. De administrative vertøyene i piloten gir mange ulike muligheter til å forenkle konfigurering og drifting av nettverket. Det er imidlertid noen verktøy som har vist seg å være mer nødvendige enn andre.

Den geografiske framstillingen av dekningsområdet er nyttig for å kunne overvåke nettverket og se hvilke klienter som er assosierte og statusen til de forskjellige nettverkselementene. Kartoversikten gir også et bilde av dekningsområdet for de forskjellige aksesspunktene når hindringer som vegger, vinduer og eventuelt andre signalhinder er registrert. I tillegg til den topologiske oversikten, har det vært nyttig med alarmer dersom det oppstår kritiske situasjoner i nettverket. Alarmene kan leses av i WCS-en eller mottas av administrator på e-post eller SMS. Et eksempel på en slik alarm kan være dersom det oppstår interferensproblemer. Dette blir oppdaget av aksesspunktene ved at de ved faste intervall skanner hele radiospekteret og rapporterer resultatet tilbake til kontrolleren. Figur 5.4 viser korte periodiske fall i throughput for et aksesspunkt. Fallene skyldes, mest trolig, denne skanningen av radiospekteret, og den fører til en liten reduksjon i total throughput. En bedre oversikt over interferensproblemer og verktøy for å løse disse problemene vil imidlertid kompensere kraftig for den lave reduksjonen i total throughput.

Det administrative verktøyet må også kunne betjene alt av konfigurasjon. Med sentrale kontrollere er det mulig å forandre innstillinger til alle aksesspunktene ved kun å endre konfigurasjonen gjennom administrasjonsverktøyet. Ved utskiftninger og eventuelle datatap er det viktig med muligheten til å ta backup av disse konfigurasjonsinnstillinger og data som er lagret i systemet. Det vil være svært arbeidsbesparende og redusere nedetiden for det trådløse nettverket, dersom uhellet skulle være ute.

Brukerstatistikk og statistikk knyttet til andre nettverkselementer har også vist seg å være et godt administrativt verktøy. Denne statistikken gir tilbakemeldinger om hvordan nettverket blir brukt og hvor det eventuelt er behov for flere aksesspunkt og mer kapasitet.

I Trådløse Trondheim skal det gis forskjellige rettigheter til forskjellige brukergrupper. Brukerne i de ulike gruppene skal imidlertid assosiere seg mot samme SSID. Systemet krever derfor støtte for RADIUS-styrt VLAN-tildeling. Denne muligheten er ønskelig i city-wide trådløse nettverk med brukergrupper som skal ha ulike brukerrettigheter.

6.7 Sikkerhet

Sikkerhet er viktig i city-wide trådløse nettverk. Et minimumskrav er at nettverksutstyret har støtte for sikker kryptering av data som sendes i nettverket og autentisering av brukere. Systemet bør derfor støtte IEEE 802.1X samtidig med IEEE 802.11i med TKIP- og AES-CCMP-kryptering. I tillegg bør der være muligheter for detektering av uvedkommende aksesspunkt og klienter. Airespace hevder at de for eksempel kan gjenkjenne trafikk fra kjente hackerprogrammer, som blant annet NetStumbler, og varsle om dette. Appendiks E viser blant annet hvilke sikkerhetsinnstillinger Airespace støtter.

6.8 Tekniske spesifikasjoner

Hva som er nødvendig av teknisk støtte i det trådløse nettverket er avhengig av brukergrupper og størrelsen på nettverket. For Airespace har det, i denne oppgaven, blitt utarbeidet en oversikt over tekniske spesifikasjoner. Denne er gjengitt i appendiks E. En tilsvarende spesifikasjon bør lages for hvert enkelt produkt for å kunne sammenligne de tekniske mulighetene for de forskjellige nettverkproduktene. Støtte for mange tekniske spesifikasjoner vil gi større valgfrihet under oppsett og konfigurasjon av systemet, men konfigurasjonskompleksiteten til utstyret øker med antall støttede tekniske spesifikasjoner.

7 Konklusjon

Der er to viktige aspekter ved testing av trådløst nettverksutstyr. Det første går på testmiljøet og det andre går på hvilke parametre som skal testes. Arbeidsgruppen IEEE 802.11T jobber med en internasjonal standard for testmiljø ved testing av trådløse nettverk. Denne arbeidsgruppen vil etter hvert komme med en anbefaling om hvordan testing skal utføres for alltid å få et likt testmiljø. Med denne anbefalingen vil det være mulig å gjenskape det samme testmiljøet uavhengig av tid og sted. En slik anbefaling vil gjøre det mulig å sammenligne testresultater fra alle tester som er utført innenfor anbefalingens rammer.

Det andre hovedaspektet ved testing av trådløse systemer er hvilke parametre som må testes for å kunne beskrive de ulike løsningene. Dette kan være forskjellig for hvert enkelt WLAN og bestemmes blant annet av arkitektur, tjenester i nettverket, antall brukere, brukergrupper og bruksmønster. I city-wide trådløse nettverk vil det derfor være andre parametre som er avgjørende for nettverket enn det er for tradisjonelle trådløse nettverk med et enkelt autonomt aksesspunkt.

For å kunne utføre tester på trådløst nettverksutstyr, er det viktig å ha gode testverktøy. I denne oppgaven har det, ved testing av de fleste parametrene, vært benyttet IxChariot fra Ixia. For å kunne konfigurere og benytte seg av testverktøy som dette, er det avgjørende å ha god innsikt i den grunnleggende teorien bak trådløs nettverkskommunikasjon. I tillegg må tester som skal brukes for produktsammenligning utføres med de samme innstillinger og konfigurasjoner.

Når testmiljøet, testverktøyet og konfigurasjoner er likt for alle testene, kan testede parametre vise forskjeller på nettverksutstyr. For city-wide trådløse nettverk er det de målbare verdiene for throughput, roamingtid, prioriteringsegenskaper i forbindelse med blant annet samtalekvalitet, og posisjoneringsnøyaktighet som kan beskrive systemet. Disse parametrene må en igjen se i sammenheng med skalering mot forventet antall brukere og ressurskrevende tjenester. I tillegg er det nødvendig med en vurdering av de ikke-målbare parametrene administrative verktøy, tilgjengelige sikkerhetsinnstillinger og tekniske spesifikasjoner.

Testing av de målbare parametrene gir sammenlignbare resultater, mens vurderingen av de ikke-målbare delene av et trådløst system til en viss grad er subjektive. Det er likevel noen administrative verktøy, sikkerhetsinnstillinger og tekniske spesifikasjoner som er viktige i city-wide trådløse nettverk. En egenskapsliste for utstyret, som appendiks E er et eksempel på, gir god oversikt over ikke-målbare egenskaper. Ved testing bør det utarbeides en tilsvarende egenskapsmatrise for hvert enkelt produkt som skal testes. Den vil vise tekniske spesifikasjoner for utstyrets ikke-målbare egenskaper. En slik liste gir svar på om utstyret støtter de ikke-målbare kravene for systemet og kan brukes for sammenligning av produkter.

Evaluering av piloten til Trådløse Trondheim har vist at minstekrav til administrative verktøy er mulighet for brukerstatistikker, SSH og HTTP pålogging mot administrasjonssoftware, alarmer ved systemfeil eller interferensproblemer, backup mekanismer og systemloggføring. I tillegg er geografisk fremstilling av klient- og aksesspunktposisjoner et verktøy som er mye brukt og nyttig i det administrative arbeidet. Når det gjelder sikkerhet er det nødvendig at systemet støtter IEEE 802.1X-autentisering og IEEE 802.11i, og innehar muligheter for TKIP- og AES-CCMP-kryptering. I tillegg er det ønskelig med RADIUS-styrt VLAN-tildeling, dersom systemet har brukergrupper med ulike rettigheter som en vil autentisere på samme SSID. Utstyr som skal brukes i city-wide trådløse nettverk må også ha godkjent støtte for radioteknologiene IEEE 802.l1a, IEEE 802.11h, IEEE 802.11b og IEEE 802.11g. For at tjenester som VoWIP og andre sanntidsapplikasjoner skal kunne benyttes effektivt, bør systemet støtter IEEE 802.11e for prioriterting av denne typen trafikk.

Testingen av nettverksutstyr fra de to produsentene som ble gjort i forbindelse med denne oppgaven, viste til dels store forskjeller for målbare parametre som beskriver produktene. På grunnlag av de utførte testene er det mulig å se hvilket produkt som egnet seg best for bruk i et city-wide trådløst nettverk. Resultatet viser at Airespace totalt sett kommer bedre ut for de målbare parametrene i forhold til utstyret fra Meru. I tillegg støtter Airespace alle de nødvendige krav og ønsker til ikke-målbare egenskaper.

Referanser

Referanser merket med * er vedlagt elektronisk. De elektroniske vedleggene består av internettkilder og andre dokumenter som har vært tilgjengelig elektronisk.

[1]* Pablo Brenner; *A Technical Tutorial on the IEEE 802.11 Protocol*, BreezeCOM artikkel, 1997.

[2]* *IEEE Std. 802.11-1999*

[3] http://www.wifi-forum.com

[4] Matthew Gast; *802.11 Wireless Networks: The Definitive Guide*, O'Reilly 2005, ISBN: 0-596-10052-3, 2005

[5] T.Tan, B.Bing; *World Wide Wi-Fi: Technological Trends and Business Strategies*, 2003, ISBN: 0-471-46356-6

[6] http://wlan.nat.sdu.dk

[7] http://www.npt.no

[8]* *IEEE Std 802.11a-1999*

[9]* *IEEE Std. 802.11b-1999*

[10]* Cisco System Inc.; *Capacity, Coverage, and Deployment Considerations for IEEE 802.11g*, White Paper 2003

[11]* Calhound, Montemurro, Stanley; *CAPWAP Protocol Specification*, draft-ietf-capwap-protocol-specification-00, 2006. http://www1.tools.ietf.org/wg/capwap/

[12]* Post- og teletilsynet: *Informasjon om regelverk for trådløse nettverk (WLAN)*, 2005

[13] Tor A. Ramstad; *Representing Information by Signals*, Fourth edition, 2003

[14]* International Telecommunication Union; *E-Model Tutorial,* http://www.itu.int/ITU-T/studygroups/com12/emodelv1/introduction.htm

[15] ITU-T Rec. G.109, *Definition of categories of speech transmission quality*

[16]* Ixiacom; *Assessing VoIP Call Quality Using the E-model*, White Paper, 1998.

[17] http://www.cisco.com

[18]* Thomas Jelle; *Trådløse Trondheim 1:2006*

[19]* Matthew Gast; *When Is 54 Not Equal to 54? A Look at 802.11a, b and g Throughput*, O'Reilly, august 2003

[20]* *IEEE Std. 802.11g-2003*

[21]* K.Medepalli, P.Gopalakrishnan, D.Famolari, T.Kodama; *Voice Capacity of IEEE 802.11b, 802.11a and 802.11g Wireless LANs*, http://www.winlab.rutgers.edu/~praveen/Resume_files/gcom-vc.pdf

[22] IxChariot, www.ixchariot.com

[23]* J.Geier; *802.11 WEP: Concepts and Vulnerability*, 2002 http://www.wi-fiplanet.com/tutorials/article.php/1368661

[24] T.Moseng; Forelesningsnotater i faget TTM4140 Videoteknologi, høsten 2003

[25] Kompendium i faget SIE5035 Nettintelligens og Mobilitet, Våren 2003, Institutt for Telematikk NTNU

[26]* *IEEE Std 802.11i™-2004*

[27]* P.Judge;*Wi-Fi vendors get SLAPP-happy*, Techworld 05. april 2005, http://www.techworld.com/mobility/news/index.cfm?newsid=3425, 06.06.2006.

[28]* J.Leira; *Trondløst – Frekvensbruken i Trondheim*, http://www.uninett.no/tradlos/trondlost/frekvens.html

[29]* Cisco System Inc.; *Cisco Wireless Control System Configuration Guide*, Software Release 3.2. November 2005

[30]* F.Mlinarsky, Azimuth Systems*; Wi-Fi Metrics*. Publisert i Test & Measurements World, 10.01.2004.

[31] http://www.ieee.org

[32] Trådløse Trondheim; *Samtale med Thomas Jelle,* 28.06.06

[33]* Proxim Corporation White Paper, *A detailed Examination of the Enviromental and Protocol Parameters That Affect 802.11g Network Performance*, 2003.

Appendiks

Appendiks A

Oversikt over frekvensplan og hoppsekvenser ved bruk av FHSS. [28]

FHSS-frekvensplan							
Kanal-ID	Frekvens (MHz)	Kanal-ID	Frekvens (MHz)	Kanal-ID	Frekvens (MHz)	Kanal-ID	Frekvens (MHz)
2	2402	22	2422	42	2442	62	2462
3	2403	23	2423	43	2443	63	2463
4	2404	24	2424	44	2444	64	2464
5	2405	25	2425	45	2445	65	2465
6	2406	26	2426	46	2446	66	2466
7	2407	27	2427	47	2447	67	2467
8	2408	28	2428	48	2448	68	2468
9	2409	29	2429	49	2449	69	2469
10	2410	30	2430	50	2450	70	2470
11	2411	31	2431	51	2451	71	2471
12	2412	32	2432	52	2452	72	2472
13	2413	33	2433	53	2453	73	2473
14	2414	34	2434	54	2454	74	2474
15	2415	35	2435	55	2455	75	2475
16	2416	36	2436	56	2456	76	2476
17	2417	37	2437	57	2457	77	2477
18	2418	38	2438	58	2458	78	2478
19	2419	39	2439	59	2459	79	2479
20	2420	40	2440	60	2460	80	2480
21	2421	41	2441	61	2461		

Hoppesekvenser	
Sett 1	0, 3, 6 ,9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75
Sett 2	1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 61, 64, 67, 70, 73, 76
Sett 3	2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, 62, 65, 68, 72, 74, 77

Appendiks B

Oversikt over frekvensplan ved bruk av DSSS. [28]

DSSS-frekvensplan	
Kanal-ID	Frekvens (MHz)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

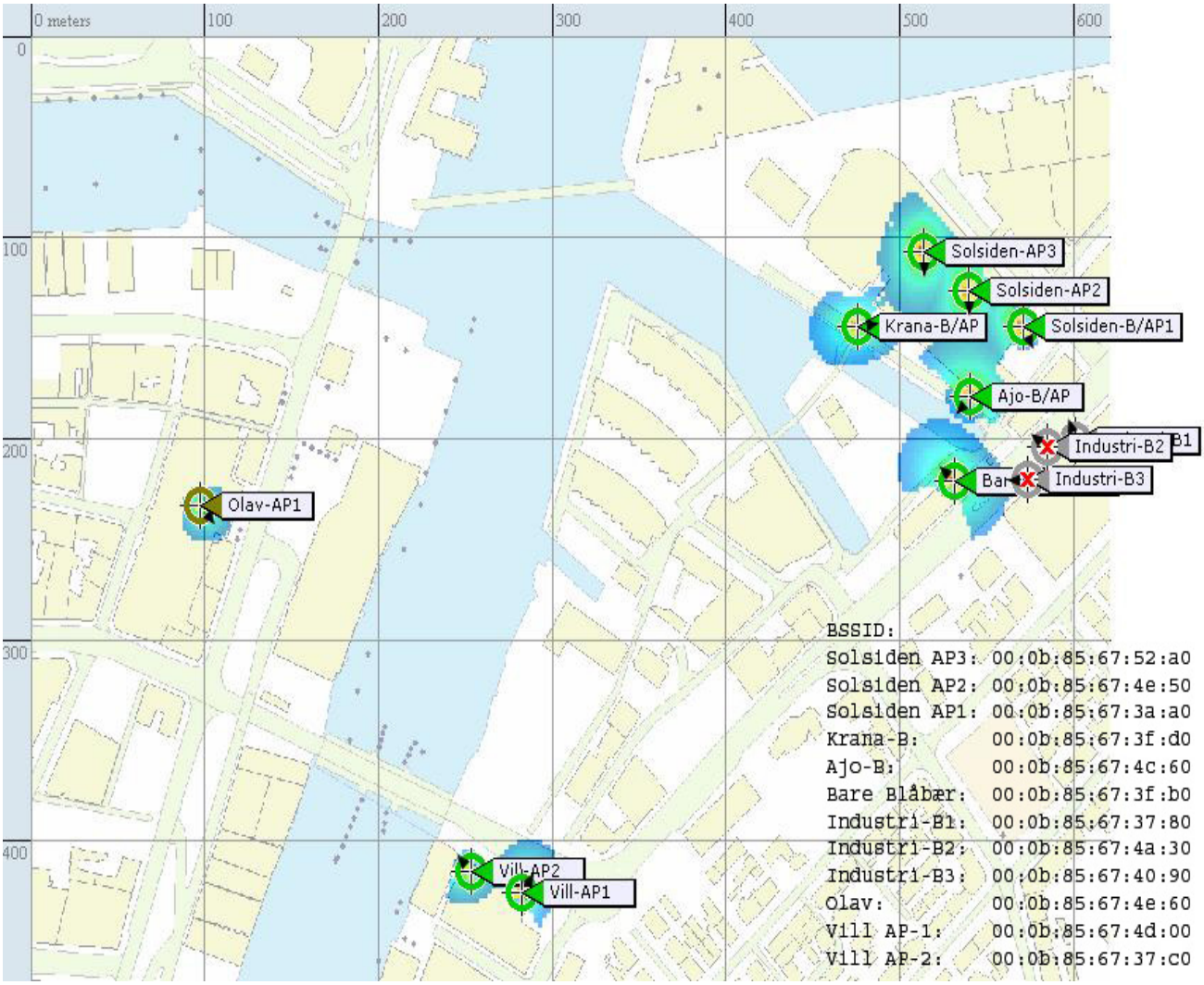
Appendiks C

Testdata fra posisjoneringstestingen i piloten på Solsiden:

Test nummer	BSSID	Reell plassering	WCS-posisjonering	Avvik (meter)	Kommentar
1	00:0B:85:67:3F:BF* 00:0B:85:67:3F:DF 00:0B:85:67:4C:6F 00:0B:85:67:52:AF	570416,79 7034810,75	570447,02 7034787,58	38	Ute ved inngang kran
2	00:0B:85:67:3A:AF 00:0B:85:67:4E:5F* 00:0B:85:67:52:AF	570471,98 7034819,67	570471,98 7034815,51	4	Telebutikken (Innendørs)
3	00:0B:85:67:4E:5F 00:0B:85:67:52:AF*	570436,91 7034835,71	570439,89 7034839,28	4	Inngang Ultra (Innendørs)
4	00:0B:85:67:3F:BF 00:0B:85:67:3F:DF 00:0B:85:67:4C:6F 00:0B:85:67:52:AF*	570415,52 7034786,39	570430,38 7034776,29	18	Kran
5	00:0B:85:67:3F:BF 00:0B:85:67:3F:DF 00:0B:85:67:4C:6F* 00:0B:85:67:52:AF	570434,54 7034753,11	570437,51 7034752,51	3	Kulturhus mot kjøpesenter
6	00:0B:85:67:3F:BF 00:0B:85:67:3F:DF 00:0B:85:67:4C:6F*	570534,37 7034758,46	570524,86 7034756,68	158	Tak i Dokkveien 1
7	00:0B:85:67:3F:BF 00:0B:85:67:4C:6F*	570463,66 7034757,87	570513,57 7034736,47	43	I hjørnet utenfor Bare Blåbær
8	00:0B:85:67:3F:BF* 00:0B:85:67:3F:DF 00:0B:85:67:4C:6F 00:0B:85:67:52:AF	570438,10 7034773,91	570422,06 7034745,39	33	Primo vannkant
9	00:0B:85:67:3F:BF 00:0B:85:67:3F:DF 00:0B:85:67:4C:6F*	570476,13 7034732,31	570466,63 7034748,36	19	Dokk ved Bare Blåbær
10	00:0B:85:67:3F:BF* 00:0B:85:67:4C:6F	570495,75 7034752,52	570444,64 7034747,76	51	Choco Bocco
11	00:0B:85:67:3A:AF 00:0B:85:67:4E:5F 00:0B:85:67:52:AF*	570454,74 7034817,29	570442,26 7034846,41	31	Rosenborg Bageri (Innendørs)
12	00:0B:85:67:3F:BF* 00:0B:85:67:4C:6F	570435,73 7034683,59	570435,13 7034704,38	215	Ved gangbrua

* Tilkoblet BSSID under testtidspunktet

ArcMap oppgir koordinater etter UTM-koordinatsystemet. Trondheim ligger under UTM32. Dette er en nordgående linje som passerer like utenfor Trondheim. På Solsiden er nord-sør koordinater gitt rundt ca. 570 000 meter. UTM har lagt til 500 000 meter i forhold til sitt nullpunkt for å unngå å få negative koordinater. Dette betyr at Solsiden befinner seg ca. 70 000 meter øst for UTM32.



Appendiks D

Resultater fra utstyrstestingen med IxChariot:

Testene er utført med opp til fire fysiske trådløse klienter. Hver av disse er konfigurert med opp til fire virtuelle Endpoint2. Til sammen kan derfor hver test utføres med 16 virtuelle trådløse klienter.

Testresultater Meru

IEEE 802.11a med send/motta-buffer på 1420 byte		
Antall klienter	Antall virtuelle klienter	Gjennomsnittlig total throughput (TCP)
1	1	17,9 Mbit/s
4	4	19,8 Mbit/s
4	16	19,5 Mbit/s

VoIP med IEEE 802.11a						
Antall klienter	Antall virtuelle klienter	VoIP-klienter	Data-klienter (TCP)	Gjennomsnittlig MOS-verdi	Minimums MOS-verdi	Gjennomsnittlig throughput
4	8	3	1	4	2	17,4 Mbit/s
4	8	6	2	3,9	2	18,6 Mbit/s

IEEE 802.11g		
Antall klienter	Antall b-klienter assosiert	Gjennomsnittlig throughput
1	0	6,2 Mbit/s

IEEE 802.11 b/g		
Antall klienter	Antall b-klienter assosiert	Gjennomsnittlig throughput
1	2	5,5 Mbit/s

IEEE 802.11 b/g			
Antall klienter	Antall b-klienter	Antall g-klienter	Gjennomsnittlig throughput
4	2	2	2,1 Mbit/s

VoIP miks modus						
Antall klienter	VoIP b-klienter	VoIP g-klienter	IEEE 802.11g data	Gjennomsnittlig MOS-verdi	Minimum MOS-verdi	Throughput
4	2	2	0	4,2	2,2	
4	4	4	0	4,1	1	
4	8	8	0	2	1	
4	2	1	1	2,9	1	3,3 Mbit/s

Testresultater Airespace

IEEE 802.11a med send/motta-buffer på 1420 byte		
Antall klienter	Antall virtuelle klienter	Gjennomsnittlig total throughput (TCP)
1	1	22,8 Mbit/s
2	2	22,4 Mbit/s
3	3	21,1 Mbit/s
4	4	20,3 Mbit/s
4	8	19,8 Mbit/s
4	12	20,1 Mbit/s
4	16	20,0 Mbit/s

VoIP med IEEE 802.11a						
Antall klienter	Antall virtuelle klienter	VoIP-klienter	Data-klienter (TCP)	Gjennomsnittlig MOS-verdi	Minimums MOS-verdi	Gjennomsnittlig throughput
1	1	1	0	4,33		
4	4	4	0	4,21		
4	8	8	0	4,26	2,33	
4	16	16	0	4,32	2,54	
4	32	32	0	4,23	1	
4	8	3	1	3,83	1,38	15,0 Mbit/s
4	8	6	2	3,83	1,09	20,4 Mbit/s

IEEE 802.11g		
Antall klienter	Antall b-klienter assosiert	Gjennomsnittlig throughput
1	0	14,1 Mbit/s

IEEE 802.11 b/g		
Antall klienter	Antall b-klienter assosiert	Gjennomsnittlig throughput
1	2	9,2 Mbit/s

IEEE 802.11 b/g			
Antall klienter	Antall b-klienter	Antall g-klienter	Gjennomsnittlig throughput
4	2	2	6,3 Mbit/s
4	4	4	6,9 Mbit/s
4	8	8	6,7 Mbit/s

VoIP miks modus						
Antall klienter	VoIP b-klienter	VoIP g-klienter	IEEE 802.11g-data	Gjennomsnittlig MOS-verdi	Minimum MOS-verdi	Throughput
4	2	2	0	4,0	2,8	
4	4	4	0	3,7	1,8	
4	2	1	1	3,0	2,3	7,7 Mbit/s

IEEE 802.11g-only					
Antall klienter	Antall virtuelle klienter	Gjennomsnittlig throughput	VoIP-klienter	Gjennomsnittlig MOS-verdi	Minimums MOS-verdi
4	4	17,4 Mbit/s	0		
4	16	17,3 Mbit/s	0		
1	1	18,8 Mbit/s	0		
4	1	15,0 Mbit/s	3	2,1	1

Appendiks E

Tekniske spesifikasjoner for Airespace med Lightweight AP og kontroller som benytter LWAPP-protokollen i kommunikasjonen mellom dem. Listen er laget ut i fra leverandørenes tekniske spesifikasjonspapirer.

Radio	
802.11a	Ja
802.11h	Ja
802.11b	Ja
802.11g	Ja
Automatisk valg av kanaler	Ja
Manuellet valg av kanaler	Ja
Automatisk valg av effekt	Ja
Manuelt valg av effekt	Ja
Konfigurasjonsmuligheter	
Antall samtidige SSID	16
Antall samtidige BSSID	16
Tjenestekvalitet	IEEE 802.11e
IEEE 802.1Q (VLAN)	Ja
Forskjellig krypteringsprofiler for de ulike SSID	Ja
Det samme VLAN på forskjellig SSID	Ja
RADIUS styrt VLAN-tildeling	Ja
AP-bridging	Kun med AP1030
Fysiske attributter	
Eksterne antenner	RC-TNC for AP1020 og AP1030 (bg/a)
Power Over Ethernet (PoE)	IEEE 802.3af
Administrasjonsmuligheter	
SSH	Mot kontroller
http	Mot kontroller og WCS
HTTPS	Mot kontroller og WCS
Telenet	Mot kontroller
SNMP	Mot kontroller
TFTP	Ja
Alarmmuligheter	Ja, med ulik varsling
Backup	Ja
Systemlogg	Ja
Sikkerhet	
Skjult SSID	Ja
MAC-adressefilter	Ja
WEP 40/104	Ja
IEEE 802.1X-autentisering	Ja
TKIP	Ja
AES-CCMP	Ja
IEEE 802.11i	Ja
WPA	Ja
WPA2	Ja

Andre sikkerhetsmuligheter	Crainte, Fortress Web-portal, VPN Klientekskludering
Detektering av uvedkommende elementer	Fremmede aksesspunkt og fremmede klienter i form av blant annet stumbling