

ÖREBRO UNIVERSITET  
Institutionen för Ekonomi, Statistik och ADB/Informatik  
Temarapport  
Handledare: Jenny Lagsten  
2001-11-09

# WLAN - säkerhet

Översikt av begreppet WLAN samt beskrivning av säkerhetsaspekter vid användning och implementering av WLAN-nät



Lydia Eliasson, 761128

## Sammanfattning

Vad är ett Wireless Local Area Network (WLAN)? Hur fungerar det och vad finns det för säkerhetsaspekter som är specifika för användning av WLAN? Denna rapport syftar till att ge svar på dessa frågor. Underlaget till rapporten är hämtad från facklitteratur samt artiklar och andra skrifter.

För att kunna förstå säkerhetsrisker förknippade med WLAN behövs en viss förståelse. Därför ger denna rapport en beskrivning av begreppet WLAN ur ett tekniskt perspektiv.

I beskrivningen av begreppet WLAN ges en kort historisk tillbakablick följt av en beskrivning av de olika topologier som WLAN kan förekomma i. Därefter kommer en genomgång av IEEE:s standard 802.11 och dess innehåll. Vidare beskrivs olika tekniker för informationsöverföring i denna typ av nätverk. Det redogörs även för några problem som kan uppstå vid implementering av WLAN.

När WLAN som fenomen har förklarats enligt ovan går rapporten in på säkerhetsaspekterna vid användning av WLAN. I denna del av rapporten kartläggs vilka säkerhetsrisker som är specifika vid användning av WLAN. Här kretsar mycket runt det faktum att det är svårt att skydda sig mot intrång eller avlyssning då signalerna sänds i luften över stora områden. Slutligen ges en beskrivning av de säkerhetsåtgärder som finns idag, implementerade i 802.11 eller på annat sätt. Rapporten redogör även för vissa diskussioner kring styrkor och svagheter hos olika säkerhetsåtgärder.

## Innehållsförteckning

<b>1</b>	<b>Inledning</b>	<b>3</b>
1.1	Bakgrund	3
1.2	Problemdiskussion	3
1.3	Problemformulering	4
1.4	Syfte	4
1.5	Intressenter/Målgrupp	4
1.6	Kunskapsmål	5
1.7	Avgränsning	5
<b>2</b>	<b>Metod</b>	<b>5</b>
2.1	Perspektiv	5
2.1.1	Koppling till befintlig kunskap	6
2.1.2	Centrala begrepp	6
2.1.2.1	Begreppsgraf	7
2.1.2.2	Ordlista	8
2.1.2.3	Definitioner	8
2.1.3	Alternativa perspektiv	9
2.2	Datainsamling	9
2.2.1	Vald metod och alternativa metoder	9
2.2.2	Sekundärdata	10
2.3	Analys av data/Genomförande	10
2.4	Källkritik	11
2.5	Validitet	11
2.6	Reliabilitet	11
<b>3</b>	<b>Teori</b>	<b>12</b>
3.1	Vad innebär begreppet WLAN?	12
3.1.1	Olika topologier	12
3.1.2	IEEE:s standard 802.11	14
3.1.3	Informationsöverföring i WLAN	15
3.1.3.1	Kort beskrivning av OSI-modellen	15
3.1.3.2	Informationsöverföring, fysiska skiktet	16
3.1.4	Implementeringsproblem	17
3.2	Vilka säkerhetsaspekter är specifika vid användning av WLAN?	18
3.2.1	Vilka säkerhetsrisker föreligger?	18
3.2.2	Vad finns det för lösningar i dagsläget?	18
<b>4</b>	<b>Analys/Diskussion</b>	<b>22</b>

### Källförteckning

# 1 Inledning

## 1.1 Bakgrund

Det talas mycket om trådlös kommunikation i dagens IT-samhälle. Utvecklingen går fort och begreppen är många. Allteftersom fler företag använder WLAN i sin verksamhet upptäcks även brister i tekniken. Precis som med de flesta tekniska revolutioner så dämpas nyhetens behag av en rädsla för de faror som de nya möjligheterna för med sig.

Det är lätt att känna sig förvirrad av företags marknadsföring av den trådlösa framtiden å ena sidan och larmrapporter om näst intill obefintlig säkerhet å andra sidan.

Jag vill i detta arbete ge en beskrivning av vad WLAN är och hur det fungerar. Jag går sedan vidare och tittar närmare på de säkerhetsrisker som diskuteras av sakkunniga på området samt vad det idag finns för åtgärder mot dessa. Är det verkligen så osäkert som de största kritikerna hävdar eller finns det lösningar som alltför få använder sig av?

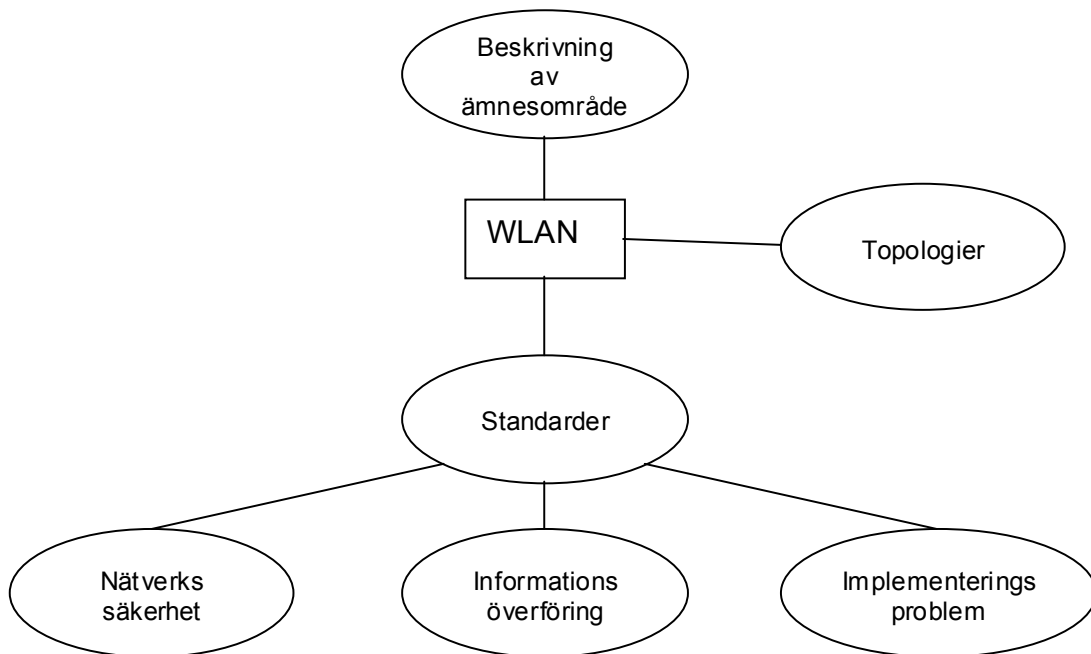
Detta arbete skrivs i samarbete med Possio. Possio utvecklar och tillverkar produkter för trådlösa digitala nät<sup>1</sup>. Säkerhet i trådlösa nätverk är därför ett viktigt inslag i deras verksamhet.

## 1.2 Problemdiskussion

Jag är främst intresserad av säkerheten i trådlösa lokala nätverk (WLAN). För att kunna få insikt i de säkerhetsproblem som kan finnas är det viktigt att känna till vad WLAN är och då främst ur tekniskt avseende. Det är viktigt att veta hur något fungerar för att se var dess brister ligger. I min översikt av området WLAN vill jag därför få med en kort beskrivning av ämnesområdet vilket i stort sett innebär lite historik. Jag vill även beskriva hur WLAN kan vara uppbyggda, det vill säga vilka olika topologier de förekommer i samt hur själva informationsöverföringen går till. Eftersom mycket styrs av de standarder som följs så kommer jag ta upp detta i ett separat avsnitt, men det är något som hela tiden återkommer eftersom det berör i stort sett alla delar av fenomenet WLAN. När jag beskrivit den tekniska utformningen så har jag grunden för att se och förstå problem i samband med WLAN. Innan jag går in på säkerhet vill jag dock även beskriva andra saker som kan störa funktionaliteten i WLAN, implementeringsproblem som störningar med mera, dessa är förstås i första hand saker som bör beaktas vid implementering av trådlösa lokala nätverk ur ren funktionalitetssynpunkt men jag tror även att kännedom om dessa svagheter kan öka säkerheten. Kanske kan dessa svagheter utnyttjas av en sabotör? När dessa områden är kartlagda kommer jag slutligen att gå in på det jag är mest intresserad av, nätverkssäkerheten i WLAN. Vad finns det egentligen för risker? Att bara säga att något är osäkert säger egentligen inte så mycket. Finns det lösningar på dessa säkerhetsrisker och täpper lösningarna till säkerhetshålen eller gör de det bara en aning svårare för hackers och sabotörer. Mycket händer väldigt fort inom säkerhetsområdet, något som anses säkert idag kan förkastas imorgon. Min ambition är dock att beskriva vilka kända risker och lösningar som finns idag samt även redogöra för eventuell kritik mot de säkerhetslösningar som finns.

---

<sup>1</sup> Possios hemsida



Figur 1. Översikt över rapportens disposition.

### **1.3 Problemformulering**

Vad innebär begreppet WLAN?

- Hur kan ämnesområdet beskrivas?
- Vad finns det för olika topologier?
- Vilka standarder finns för WLAN?
- Hur fungerar informationsöverföringen?
- Vilka problem kan finnas vid implementering av WLAN?

Vilka säkerhetsaspekter är specifika vid användning av WLAN?

- Vilka risker föreligger?
- Vad finns det för lösningar i dagsläget?

### **1.4 Syfte**

Syftet med detta temaarbete är att beskriva WLAN ur ett tekniskt perspektiv. Vidare redogöra för kända säkerhetsrisker som är specifika för WLAN samt åtgärder mot dessa.

### **1.5 Intressenter/Målgrupp**

Rapporten riktar sig främst till personer som har en viss teknisk förståelse, såsom mina studiekamrater på det systemvetenskapliga programmet vid Örebro Universitet, och som dessutom är intresserade av WLAN och säkerheten i dessa nätverk.

Rapporten är skriven som en förberedande kunskapsinsamling inför den c-uppsats som jag och Anna Stenquist ska skriva i samarbete med Possio. Possio är ett företag som bl.a. utvecklar produkter för WLAN.

Resultatet av detta arbete kan även vara intressant och användbart för andra Informatikstudenter, nu och kommande terminer. Andra företag i branschen är också tänkbara intressenter.

I rapporten förekommer det mycket förkortningar och tekniska termer. Många förkortningar och termer är säkert nya för dig som läsare. För att underlätta läsningen av rapporten finns en ordlista i avsnitt 2.1.2.2. Jag rekommenderar att läsaren ögnar igenom denna innan läsningen påbörjar och sedan återkommer till ordlistan vid behov under läsningens gång.

## ***1.6 Kunskapsmål***

Denna rapport ska ge en bild av vad ett WLAN är genom att beskriva hur det kan vara uppbyggt, vilka standarder som styr på området samt hur informationsöverföringen går till i dessa nätverk. I rapporten ska det även redogöras för problem som kan uppstå vid implementering av WLAN.

Rapporten ska även behandla säkerhetsaspekter som är specifika vid användning av WLAN genom att redogöra för de säkerhetsrisker samt lösningar som är kända i dagsläget.

## ***1.7 Avgränsning***

Jag är intresserad av att beskriva vad begreppet WLAN innebär ur ett tekniskt perspektiv i syfte att utifrån detta kunna förstå och redogöra för säkerhetsrisker och åtgärder. Beskrivningen av WLAN kommer inte att gå in på djupet vad gäller tekniska detaljer hos hårdvara och dylikt eftersom jag inte anser att detta behövs för att få den förståelse som krävs för kunna sätta sig in i säkerhetsaspekterna.

Vad gäller kända säkerhetsrisker och lösningar vill jag göra en kartläggning och inte fördjupa mig alltför mycket i specifika risker eller lösningar. Jag kommer till exempel inte redogöra för hur krypteringsalgoritmer är utformade rent matematiskt vilket kan vara intressant för den som vill förbättra en algoritm. Jag kommer istället att berätta översiktligt om hur lösningarna fungerar och vad de är tänkta att lösa eftersom jag anser att detta ger den övergripande bild som jag vill ge.

Jag har valt att inte diskutera vad som är relevanta säkerhetskrav för olika användarkategorier. Olika användare (t.ex. privatpersoner och företagsanvändare) måste rimligen ha olika stora behov av att skydda data som skickas. I dagens debatt känner jag personligen att även de som har lägre säkerhetskrav blir avskräckta av larmrapporter om att säkerheten inte är fullkomlig.

# **2 Metod**

## ***2.1 Perspektiv***

Jag har en ganska positiv och optimistisk syn på dator teknik. Det är sällan som jag inte ser teknisk utveckling som något positivt och jag tycker att det är intressant att arbeta med bristerna i existerande lösningar för att hela tiden närma sig den perfekta lösningen.

Möjligtvis kan detta leda till bristande kritik i arbetet. Det är t.ex. inte särskilt troligt att jag i min slutsats fördömer WLAN och rekommenderar en tillbakagång till fysiska nätverk, men syftet med arbetet är inte heller att ta ställning utan endast att beskriva. Min utgångspunkt är att WLAN är bra men att det finns brister. Dessa brister och eventuella lösningar som redan är funna vill jag kartlägga.

Jag har visserligen intresserat mig för datorer relativt länge och har utbildning inom området, men just nätverk är jag ingen expert på och jag kommer att närma mig området WLAN som en kunnig nybörjare. Detta i kombination med att min målgrupp är personer med liknande förkunskaper innebär att jag när jag förklarar fenomen kommer att utgå från att läsaren har vissa grundläggande datatekniska kunskaper, till exempel bör läsaren känna till vad ett LAN är för att få ut så mycket som möjligt av rapporten.

Eftersom jag genomför detta arbete i samarbete med företaget Possio är det ganska naturligt att mitt perspektiv till viss del styrs av Possios intressen. Possio utvecklar produkter för trådlösa digitala nät och är därför intresserade av att ta del av den kunskap som andra har om säkerhet i denna typ av nätverk. Dessutom ligger det i deras intresse att jag ökar min kunskap om säkerhet i WLAN eftersom detta kommer att påverka den c-opsats som jag och planerar att skriva i samarbete med Possio.

### **2.1.1 Koppling till befintlig kunskap**

Trådlösa lokala nätverk är en relativt ny företeelse mycket av tekniken bygger dock på fysiska lokala nätverk som har funnits en längre tid. Det finns därför litteratur som på ett bra sätt beskriver grunderna i ett trådlöst lokalt nätverk. När man däremot närmar sig frågor som rör standard och säkerhet för lokala nätverk så är detta frågor som först dykt upp under de senaste åren. Detta gör naturligtvis att mycket kan ha förändrats på bara ett år. Att skriva en bok och få den publicerad tar längre tid än att skriva en rapport och publicera den elektroniskt vilket leder till att det är i elektroniska skrifter som den mest aktuella informationen finns angående utvecklingsarbete med standard samt säkerhetsfrågor. Eftersom detta ämne är mycket aktuellt är det dock flera företag och Universitet som redan hunnit ge ut rapporter och liknande i ämnet, dessa har jag självfallet utnyttjat i mitt arbete.

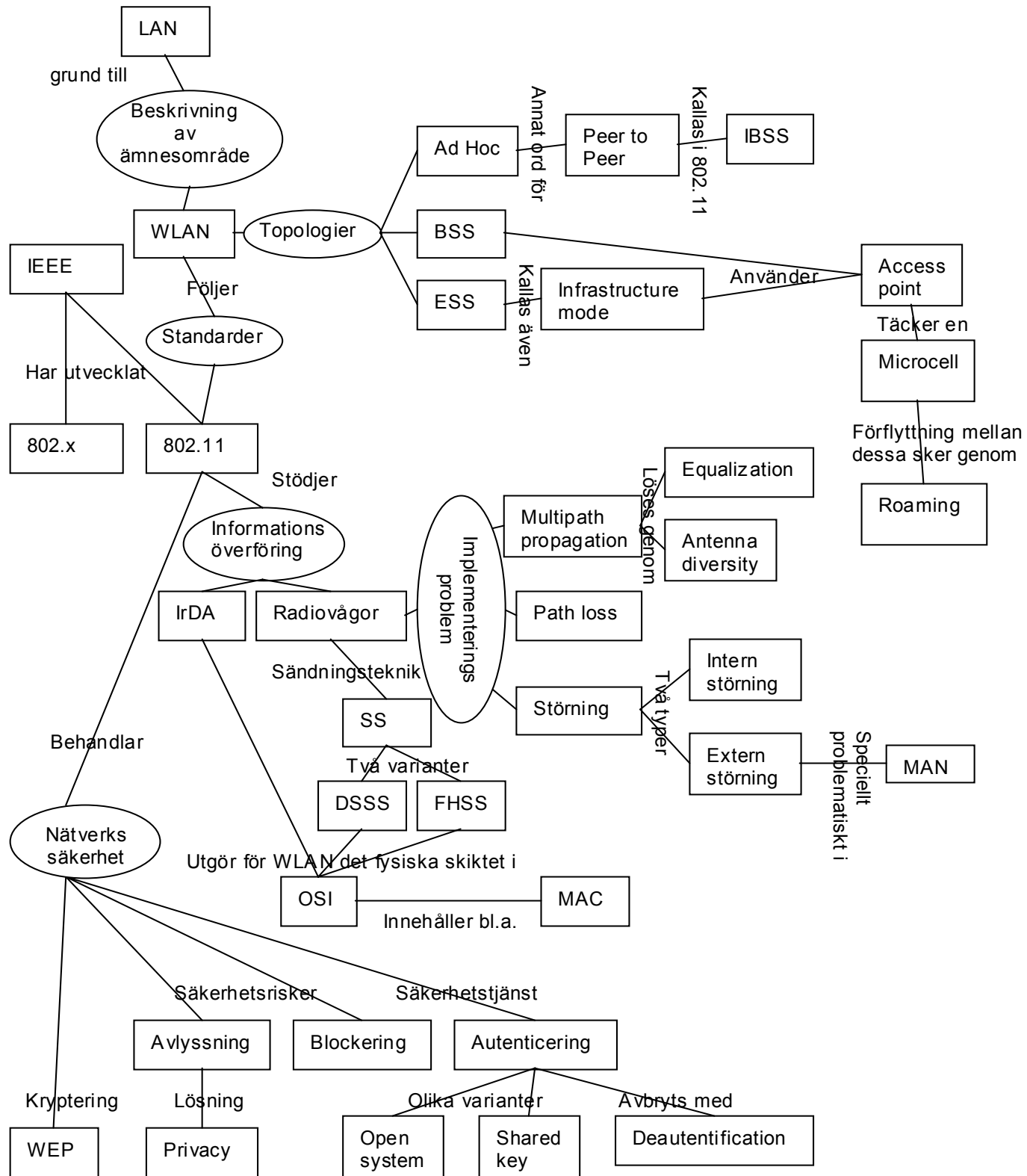
### **2.1.2 Centrala begrepp**

Det förekommer många tekniska begrepp och förkortningar i denna rapport. För att underlätta för läsaren att få en helhetsbild över hur dessa begrepp hänger ihop har jag gjort en begreppsgraf. I begreppsgrafens finns centrala begrepp och deras samband.

För att underlätta läsningen har jag även gjort en ordlista där en del termer förklaras. Denna kan med fördel användas vid behov under tiden rapporten läses.

Jag har även ett avsnitt kallat definitioner där jag redogör för min egen definition och användning av begrepp som är centrala i rapporten. Detta för att minska risken för mångtydighet vilket kan skapa förvirring.

### 2.1.2.1 Begreppsgraf



Figur 2. Översikt över begrepp och begreppssamband.

### 2.1.2.2 Ordlista

**Access point (AP)** – En enhet som transporterar data mellan ett trådlöst nätverk och ett fysiskt nätverk, eller mellan två trådlösa nätverk<sup>2</sup>.

**Bandbredd/frekvensband** – Ett spann av frekvenser, t ex 2,400 GHz till 2,485 GHz, kallas ett frekvensband.

**IEEE** – the Institute of Electrical and Electronics Engineers

**IrDA** – Infrarött ljus. En typ av elektromagnetiska vågor som kan användas för informationsöverföring i trådlösa nätverk.

**LAN** – Local Area Network. Ett lokalt nätverk av datorer och kringutrustning som skrivare mm.

**MAC** – Medium Access control. En del av länkskiktet i OSI-modellen.

**MAC-adress** - 48 bits adress som identifierar ett NIC.

**Microcell** – Det område som täcks av en sändare i ett trådlöst lokalt nätverk.

**Mbs** –Mätenhet för dataöverföringshastighet, betyder Mega bits per second. Förkortas även Mbps eller Mb/s.

**MHz** – Mega Hertz. Mätenhet för frekvens hos radiovågor.

**NIC** – Network Interface Card, dvs ett nätverkskort.

**NOS** - network operating system (t.ex. winNT)

**OSI-modellen** – Open System Interconnection. Generell modell för datakommunikation.

**Roaming** – Förflyttning av en trådlös enhet mellan olika microcells.<sup>3</sup>

**Station (STA)** – Enhet med nätverkskort avsett för trådlösa nätverk<sup>4</sup>.

**VPN** – Virtual Privacy Network

**WEP** - Wired Equivalent Privacy. WEP är en symmetrisk krypteringsalgoritm där samma algoritm och nyckel används för både kryptering och dekryptering av data<sup>5</sup>.

**WLAN** - fungerar som ett LAN (se ovan) med undantaget att enheterna i nätverket kommunicerar via elektromagnetiska vågor istället för via strömförande kablage.

**Wi-Fi** – En certifiering som företaget WECA<sup>6</sup> ger produkter för WLAN som följer standarden 802.11 och därför är kompatibla med övriga Wi-Fi produkter.

### 2.1.2.3 Definitioner

WLAN är en förkortning som betyder Wireless Local Area Network. WLAN är alltså ett trådlöst lokalt nätverk. Jag kommer att använda begreppen WLAN, trådlöst lokalt nätverk och trådlöst LAN för att omnämna samma fenomen.

Benämningen fysiskt nätverk använder jag för att beteckna traditionella nätverk där datorer är sammankopplade med kablar.

När jag talar om säkerhetsrisker i min rapport så menar jag risk för intrång, störning eller avlyssning i nätverket.

Med nätverkssäkerhet menar jag säkerheten i ett nätverk med avseende på säkerhetsrisker (enligt ovan).

---

<sup>2</sup> WLANA

<sup>3</sup> Ibid

<sup>4</sup> The linux-wlan Company

<sup>5</sup> Cisco systems

<sup>6</sup> <http://www.wi-fi.com/>

Det förekommer ett antal engelska ord i rapporten. Dessa ord har jag valt att inte översätta då jag anser att en översättning med bibehållen innebörd var svår att finna. Ofta är det också de engelska termerna som används i svenskspråkiga texter på området. Rapporten vänder sig till personer i branschen vilket jag tycker gör att det är acceptabelt med fackuttryck av detta slag.

### **2.1.3 Alternativa perspektiv**

Både WLAN och säkerhet är stora områden och personer med andra bakomliggande intressen skulle kunna utveckla andra delar av ämnet än vad jag har gjort och även tagit med aspekter som jag ignorerat. Min utgångspunkt har varit att förklara det som är nödvändigt för att kunna se närmare på säkerhetsaspekter och förstå dessa. Vilka aspekter jag lagt tonvikt på präglas även av vilken kunskap Possio är intresserad av, samt mina förkunskaper. Det går till exempel att tänka sig ett liknande arbete med långa avsnitt programkod eller matematiska beräkningar. Med detta i åtanke tror jag att en annan rapport med samma titel skulle kunna se mycket annorlunda ut i många olika avseenden. Till exempel mer inriktat på hur lösningarna fungerar tekniskt eller matematiskt, det går också att tänka sig en värderande inställning som rangordnade säkerhetslösningar.

Jag hade även kunnat utforma detta arbete som en jämförande studie av WLAN och LAN, men jag anser att ett sådant arbete skulle bli onödigt stort då det egentligen bara är WLAN som jag är intresserad av även om WLAN har många likheter med fysiska LAN och kunskaper om det ena säkert ger bättre förståelse för det andra.

## **2.2 Datainsamling**

### **2.2.1 Vald metod och alternativa metoder**

Vid arbetet med denna rapport var det ganska självklart att jag skulle använda en kvalitativ metod och inte en kvantitativ eftersom jag inte är ute efter statistiska samband eller orsaksförklaringar.

Jag ville på fem veckor på bästa sätt få en bild av vad WLAN är och vad det finns för säkerhetsaspekter vid användning av WLAN. Denna kunskap finns ute hos företag som tillverkar eller använder WLAN, hos forskare, journalister och andra intresserade. Vilket är då bästa sättet att samla och få en överblick över denna kunskap? Jag skulle ha kunnat intervjua personer från ovanstående grupper men jag är ju egentligen inte intresserad av personliga åsikter utan mer fakta. Jag valde därför att göra en litteraturstudie. På detta sätt får jag på ett enkelt sätt tillgång till välstrukturerad och förhoppningsvis genomtänkt och granskad information. Jag kan välja olika typer av källor för att få basfakta eller senaste forskningsresultaten och genom att jag känner min källa vet jag även hur den kan användas. En enda persons laborationsresultat bör till exempel inte användas som ensam grund för hela arbetet men kan bidra med tänkvärda inslag beroende på vem personen är och laborationens art.

## 2.2.2 Sekundärdata

Underlaget till denna rapport är sekundärdata i form av litteratur och skrifter av olika slag. Jag har sökt böcker på universitetsbiblioteket för att få en stabil grund att utgå ifrån eftersom utvecklingen går snabbt inom detta område så har jag även sökt i universitetsbibliotekets databaser efter skrifter samt på Internet. Vid mina sökningar har jag använt nyckelord som wireless LAN och säkerhet (eller security). Efterhand som jag har stött på begrepp har jag även använt dessa i mina sökningar, t.ex. 802.11. Vissa Internetkällor har jag även hittat genom tips från min handledare på Possio samt genom referenser i litteratur och skrifter.

## 2.3 *Analys av data/Genomförande*

Jag har gjort en kvalitativ bearbetning av det material som jag samlat. Detta innebär att jag har bearbetat materialet i syfte att försöka förstå och analysera en helhet<sup>7</sup>.

Eftersom jag hade mycket begränsade förkunskaper om trådlösa LAN före detta arbete så var mitt första mål att bättra på mina kunskaper angående detta. När jag började läsa om WLAN mötte jag genast en rad nya termer och begrepp. Till att börja med skrev jag ned de nya orden och försökte lära mig innebörden av de som förekom återkommande i litteraturen. För att få struktur och bättre översikt valde jag att kartlägga sambandet mellan och kategorisera begreppen genom att göra en begreppsgraf. De kategorier som uppstod bildar ramverket för detta arbete.

Samtidigt som jag nedtecknade centrala begrepp så uppmärksammade och markerade jag även var det fanns förklaringar av begreppen samt annan text som berörde begreppen. Nästa steg i bearbetningen av materialet var att i det insamlade materialet identifiera de delar som jag ansåg intressanta att ha med i rapporten. När det gäller den första delen av rapporten som handlar om vad WLAN är så bedömde jag sådant som återkom i olika källor mer intressant och tog med det i rapporten. När jag kom in på säkerhetsaspekterna så gällde samma metod till viss del men här tyckte jag även att det var intressant med olika synvinklar även om de inte delades av flera. Det underlag som jag på detta vis vaskat fram bearbetade jag sedan och infogade på lämplig plats i ramverket. Jag gjorde med andra ord en kategorisering av materialet utifrån min begreppsgraf. Denna process var självklart iterativ. Under arbetets gång hittade jag nya begrepp jag ville förstå och på så vis nya källor med ännu mer information. Jag förstod även mer om sambanden mellan olika begrepp med tiden och allt detta ledde förstås till att begreppsgrafan ändrades samtidigt som rapporten växte fram.

Utifrån det material jag läst har jag dragit slutsatsen att de allra flesta WLAN utnyttjar radiovågor för informationsöverföring samt att de följer standarden 802.11 eller någon av dess tillägg. Jag har därför valt att i huvudsak skriva om sådana nätverk i den här rapporten.

---

<sup>7</sup> Patel Runa, Davidson Bo, 1994, Forskningsmetodikens grunder

## **2.4 Källkritik**

Internet är en osäker källa. Många av de dokument jag har hämtat på Internet kommer dock från större webbforum och är skrivna av företag eller universitet. Att hämta material från Internet till denna rapport var nödvändigt eftersom utvecklingen går snabbt och information snabbt blir inaktuell. Jag har använt några böcker för att verifiera och beskriva grunderna hos fenomenet WLAN. När jag valt böcker har jag genomgående sökt de nyaste. I vissa fall anser jag att information kan vara relevant i ett par år gammal litteratur, när man läser sådan är det dock extra viktigt att verifiera med de senaste rönen eftersom förändringar i standard eller liknande kan ha skett.

## **2.5 Validitet**

Syftet med denna rapport är att beskriva vad WLAN är och vilka kända säkerhetsaspekter som är specifika vid användning av WLAN-nät. Jag anser att jag genom att studera litteratur och andra skrifter på ämnet får en bra bild av detta. En invändning skulle kunna vara att jag på detta sätt endast kartlägger dokumenterade säkerhetsaspekter och inte alla kända, vilket skulle kunna uppnås genom intervjuer. Men man kan även ha som krav att för att något ska betraktas som känt så måste det vara externaliserat. Om inte annat blir arbetet orimligt resurskrävande annars. Idéer som endast existerar i någons huvud tenderar även att vara mindre genomarbetade och därför inte lika intressanta för denna rapport.

Jag anser att jag genom den metod jag har valt verkligen har fått det resultat jag sökte, en beskrivning av begreppet WLAN som stöds av många källor samt en överblick av säkerhetsrisker och lösningar som är kända (dokumenterade).

## **2.6 Reliabilitet**

Det är svårare att bedöma reliabilitet i ett kvalitativt arbete av det här slaget än i exempelvis en statistisk undersökning. Samma frågor till ett stort urval människor inom givna ramar ger ganska säkert liknande resultat. I detta arbete är det till viss del svårare att beskriva metoden men framför allt är det svårt att beskriva mitt perspektiv. Mitt perspektiv styr till stor del hur denna rapport kommer att se ut. För att någon annan skulle kunna göra om arbetet med samma slutresultat krävs att metoden följs samt att denna person gör mitt perspektiv till sitt. Eftersom perspektiv är ett så komplext begrepp som består av egna erfarenheter, tankar och värderingar är det svårt att för det första dokumentera sitt perspektiv. För det andra så är det om möjligt ännu svårare för en läsare att anta mitt perspektiv eftersom läsaren automatiskt tolkar min dokumentation utifrån sitt eget perspektiv.

Jag har strävat efter att så tydligt som möjligt beskriva mitt tillvägagångssätt och mitt perspektiv. I beskrivning av perspektiv har jag beskrivit de aspekter som jag tror är av större betydelse för rapportens utformning. I och med att rapporten är skriven för personer med liknande utbildning som mig tror jag att reliabiliteten blir något högre eftersom de till viss del har liknande erfarenheter.

## 3 Teori

Beskrivning av ämnesområde, 3.1

Topologier, 3.1.1

Standarder, 3.1.2

Informationsöverföring, 3.1.3

OSI-modellen, 3.1.3.1

Fysiska skiktet hos WLAN, 3.1.3.2

Implementeringsproblem, 3.1.4

Nätverkssäkerhet, 3.2

Säkerhetsrisker, 3.2.1

Lösningar, 3.2.2

### 3.1 Vad innebär begreppet WLAN?

WLAN är ett trådlöst lokalt nätverk. Ett WLAN liknar i mycket ett fysiskt LAN med den stora skillnaden att informationsöverföringen i ett WLAN sker genom elektromagnetiska vågor, alltså i luften, istället för genom kablar som är fallet i ett fysiskt LAN. WLAN utvecklades under 1980-talet. Lösningar med WLAN utvecklades från början som ett stöd i vertikala marknader såsom sjukvård, utbildning och detaljhandel<sup>8</sup>. Det var specifika lösningar för specifika problem där det krävdes att användare och stationer kunde vara mobila. Exempelvis handlade det om mobila terminaler med patientinformation på sjukhus samt inventerings- och prissättningsterminaler på varuhus. Senare kom WLAN att användas som ett komplement till fysiska nätverk.<sup>9</sup> 1997 kom standarden 802.11, den första standarden för WLAN<sup>10</sup>.

#### 3.1.1 Olika topologier

WLAN kan förekomma i två typer av topologier. Dessa kallas Ad Hoc och Infrastructure mode.<sup>11</sup>

##### Ad Hoc

Ad Hoc eller peer to peer innebär att det trådlösa lokala nätverket är fristående<sup>12</sup>. I dessa WLAN kan alla datorer kommunicera med varandra via trådlösa datalänksprotokoll<sup>13</sup>. Maximalt avstånd mellan mottagare och sändare i ett WLAN är vanligen 50-100m<sup>14</sup>. För att kunna använda ett fristående WLAN över längre avstånd kan man använda en repeater som fördubblar det maximala avståndet mellan trådlösa stationer<sup>15</sup>.

---

<sup>8</sup> Cisco Systems

<sup>9</sup> The linux-wlan Company

<sup>10</sup> Wireless LANs, Geier Jim

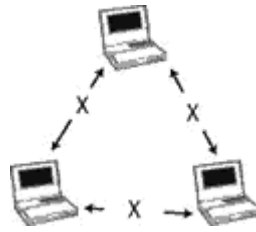
<sup>11</sup> Your 802.11 Wireless Network has No Clothes, Arbaugh W A m.fl.

<sup>12</sup> WLANA

<sup>13</sup> Datakommunikation, Jensen S m.fl.

<sup>14</sup> Ibid

<sup>15</sup> WLANA



Figur 3. Fristående WLAN, IBSS. Källa: WLANA

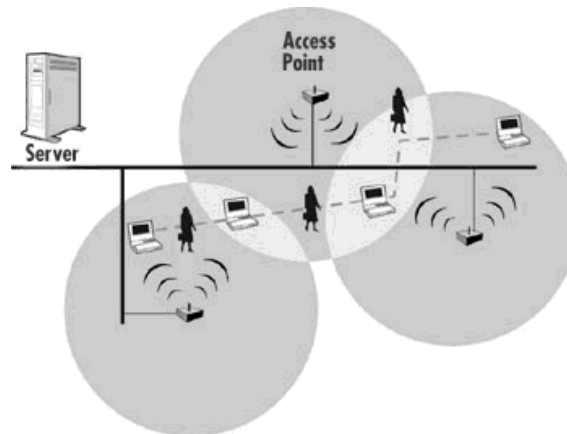
IEEE:s standard 802.11 definierar ett Ad Hoc LAN som Independent Basic Server Set (IBSS) och infrastructure mode som Basic Server Set (BSS).<sup>16</sup>

### Infrastructure mode

I ett BSS kommunicerar varje station med en access point som förmedlar datan till den mottagaren som kan vara en annan trådlös station eller en station i ett fysiskt nätverk. En access point kan sägas fungera som en ethernet-brygga.<sup>17</sup>

Ett fysiskt LAN som kopplats ihop med flera BSS via access points kallas Extended Service Set (ESS).<sup>18</sup>

Det område som en access point täcker kallas en microcell. När en trådlös station kommer utanför en microcell använder den sig av roaming som innebär att den söker upp den access point som täcker det aktuella området.<sup>19</sup>



Figur 4. Förflyttning mellan microcells i ett ESS. Källa: WLANA

<sup>16</sup> Your 802.11 Wireless Network has No Clothes, Arbaugh W A m.fl.

<sup>17</sup> Ibid

<sup>18</sup> Datakommunikation , Jensen S m.fl.

<sup>19</sup> WLANA

### 3.1.2 IEEE:s standard 802.11

När en ny teknik utvecklas finns det vanligtvis inga standarder vilket gör att olika tillverkare använder olika sätt att implementera tekniken. Detta försvårar för konsumenten eftersom produkter från olika tillverkare inte alltid är kompatibla. Brist på allmänt accepterad standard ger även lägre säkerhet eftersom det är svårt för kunden att veta vilka säkerhetstjänster som finns i systemet och vilka tillägg som måste göras därutöver.

#### IEEE

The Institute of Electrical and Electronic Engineers (IEEE). IEEE har utvecklat standarder för fysiska lokala nätverk, dessa ligger alla i nummerserien 802.x. 1997 presenterade IEEE även en standard för trådlösa lokala nätverk, 802.11.<sup>20</sup>

#### 802.11

Standarden 802.11 är den första standarden för WLAN. 802.11 standardiserar signaler och protokoll i trådlösa nätverk. Standarden definierar tre olika fysiska implementeringar, en Media Access Control funktion samt en Management funktion. De tre fysiska implementeringarna är Direct Sequence Spread Spectrum (DSSS) och Frequency Hopping Spread Spectrum (FHSS) på frekvensbandet 2,4 GHz samt infrarött ljus (IrDA).<sup>21</sup> Dessa implementeringar beskrivs i avsnitt 3.1.3.2.

802.11 definierar topologierna BSS, IBSS och ESS. Standarden säger även att en access point kan göra en behörighetskontroll på en terminal när denna ansluts samt att informationen kan krypteras.<sup>22</sup>

1999 gjorde IEEE två tillägg till 802.11 som heter 802.11a och 802.11b.

#### 802.11b

802.11b innebar en ökning av datahastigheten från maximalt 2 Mbs enligt 802.11 till upp till 11 Mbs. 802.11b kan endast implementeras om DSSS används<sup>23</sup>. De flesta WLAN idag följer standarden 802.11b.<sup>24</sup>

#### 802.11a

802.11a innebär möjlighet att sända upp till 54 Mbs. WLAN som följer 802.11a kan ha datahastigheterna 6, 9, 12, 18, 24, 36, 48 och 54 Mbs. Alla produkter som följer 802.11a ska ha dataöverföring på 6, 12 och 24 Mbs.<sup>25</sup> Frekvensbandet som används i 802.11a ligger mellan 5 och 6 GHz. I dagsläget är 802.11a inte speciellt vanlig men kommer troligtvis ersätta 802.11b i framtiden.<sup>26</sup>

---

<sup>20</sup> WLANA

<sup>21</sup> Ibid

<sup>22</sup> Datakommunikation, Jensen S m.fl.

<sup>23</sup> PCTechGuide, Wireless networks

<sup>24</sup> Wireless LANs, Geier Jim

<sup>25</sup> Wireless LANs, Geier Jim

<sup>26</sup> Kristoffer Mårild, Possio

### Stationer och access points

I 802.11 definieras trådlösa stationer (STA) och access points (AP). En station är oftast en PC med ett nätverkskort (NIC) avsett för trådlösa nätverk men det kan även vara handdatorer och liknande med nätverkskort. Varje NIC identifieras av en 48 bits adress som kallas MAC-adress<sup>27</sup>. En access point är en enhet som både kan sända och ta emot signaler och kopplar ihop trådlösa nätverk med varandra eller med fysiska nätverk.<sup>28</sup>

### 802.11i

IEEE håller för närvarande på att utveckla tillägg till krypteringsalgoritmen WEP (Wired Equivalent Privacy), 802.11i, som skall implementeras i en framtida version av 802.11. Förbättringar som kan förväntas i tillägget är en ny algoritm för privacy samt föreskrifter för förbättrad autentisering. När 802.11i har godkänts som standard kommer implementering av denna vara ett krav för Wi-Fi certifiering.<sup>29</sup>

## 3.1.3 Informationsöverföring i WLAN

### 3.1.3.1 Kort beskrivning av OSI-modellen

OSI står för Open Systems Interconnection.<sup>30</sup> OSI-modellen togs fram av standardorganisationen ISO på 1980 talet. Modellen är ett ramverk som beskriver olika nivåer vid datakommunikation. Modellen är generell för alla typer av nätverk. Skiktens utformning varierar sedan för olika typer av nätverk.

7	Applikationsskikt	Applikationer som använder nätverket
6	Presentationsskikt	Standardiserar data som används av applikationerna
5	Sessionsskikt	Handhar sessioner mellan applikationer
4	Transportskikt	Tillhandahåller felsökning och korrigerering
3	Nätverksskikt	Administrerar nätverksförbindelser. Adressering, vägval m.m.
2	Länkskikt	Har hand om dataöverföring över nätverket.
1	Fysiskt skikt	Definierar den fysiska överföringslänken

Figur 5. OSI-modellen. Källa: PCTechGuide, OSI Model

Det är det fysiska skiktet och länkskiktet som har med nätverkskortet att göra. Länkskiktet är indelat i två nivåer, Media Access Control (MAC) samt Logical Link Control (LLC). I MAC hanteras de olika accessmetoderna för lokala nätverk.<sup>31</sup>

<sup>27</sup> Datakommunikation, Jensen S m.fl.

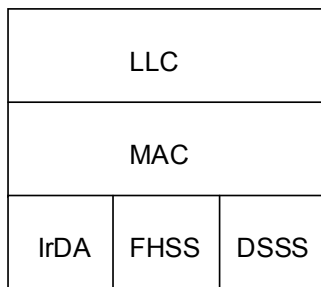
<sup>28</sup> The linux-wlan Company

<sup>29</sup> WEP Security Statement, Wireless Ethernet Compability Alliance

<sup>30</sup> PCTechGuide, OSI Model

<sup>31</sup> Internet & TCP/IP, Ottosson B

För WLAN kan tre fysiska skikt användas: IrDA, FHSS och DSSS.<sup>32</sup>



Figur 6. Fysiska skiktet och länkskiktet hos WLAN.<sup>33</sup>

### 3.1.3.2 Informationsöverföring, fysiska skiktet

I det fysiska skiktet i ett WLAN används elektromagnetiska vågor för dataöverföring. Dessa elektromagnetiska vågor kan antingen vara av typen infrarött ljus (IrDA) eller radiovågor<sup>34</sup>. IrDA har den nackdelen att avståndet mellan sändare och mottagare inte får vara större än 10-20 meter samt att inget får stå i vägen för signalen<sup>35</sup>. Radiovågor är det sätt som är vanligast och det är därför huvudsakligen detta som kommer att behandlas i detta temaarbete. Med radiovågor är maximalt avstånd mellan sändare och mottagare vanligen 50-100 meter<sup>36</sup>.

#### Spread Spectrum

Spread Spectrum (SS) är den teknik som används för informationsöverföring i de flesta WLAN. SS-tekniken innebär att informationen som ska sändas delas upp över den tillgängliga bandbredden istället för att använda hela bandbredden som en kanal. Syftet med denna teknik är att signalen ska vara svår att avlyssna, förändra eller störa eftersom den liknar brus på grund av att signalen är så utspridd över frekvensbandet. Tekniken togs fram av militären på 1940-talet för att tillgodose behovet av säker kommunikation.<sup>37</sup>

#### DSSS

Det finns två varianter av Spread Spectrum. Den ena varianten är Direct Sequence Spread Spectrum (DSSS). Denna teknik går ut på att alla data som sänds är kodad genom att tillsynas slumpmässiga bitar blandas med datan. Dessa kodade bitar sänds sedan över hela det tillgängliga frekvensbandet.<sup>38</sup> Hur datan är kodad är endast känt för den sändande och den mottagande stationen. Eftersom de ”onödiga” bitarna i själva verket är redundant data, alltså kopior av bitar som ingår i datan, så innebär detta att det är lättare att reparera ett skadat meddelande utan att behöva sända det igen. DSSS används i nätverk som följer standarden 802.11b.<sup>39</sup>

<sup>32</sup> Se avsnitt 3.1.3.2, Informationsöverföring, fysiska skiktet

<sup>33</sup> Wireless LANs, Geier Jim, s 82, egen avritning och översättning

<sup>34</sup> WLANA

<sup>35</sup> Datakommunikation, Ewert Magnus

<sup>36</sup> Datakommunikation, Jensen S m.fl

<sup>37</sup> Datakommunikation, Ewert Magnus t

<sup>38</sup> Ibid

<sup>39</sup> PCTechGuide, Wireless networks

## **FHSS**

Den andra varianten av SS heter Frequency Hopping Spread Spectrum (FHSS). Som namnet antyder så innebär denna teknik att både sändare och mottagare hoppar mellan olika frekvenser. Det är endast den sändande och den mottagande stationen som känner till det till synes slumpmässiga mönstret i hoppningen mellan frekvenser. I både Europa och USA har IEEE i standarden 802.11 specificerat 79 kanaler och 78 olika hoppmönster.<sup>40</sup>

### **3.1.4 Implementeringsproblem<sup>41</sup>**

Det finns vissa problem som kan uppstå vid implementering av WLAN som är unika för trådlösa nätverk.

#### **Path loss**

Då en WLAN-lösning designas måste beaktas att signalen avtar i styrka med avseende på avståndet. Beroende på avståndet mellan sändare och mottagare måste känsligheten på mottagare och styrka hos sändare anpassas. På 30 meter minskar signalen ca 20 dB (i vanlig inomhusmiljö). Detta fenomen kallas path loss.

#### **Multipath propagation**

Ett annat problem som kallas Multipath propagation är att signalen studsar på väggar och möbler vilket gör att den blir oläslig när den tas emot. Effekterna av detta kan dock dämpas med hjälp av olika åtgärder som equalization och antenna diversity.

#### **Interferens**

Eftersom signalerna i ett WLAN rör sig i luften kan signalerna störas av annan utrustning (intern interferens) likväl som signalerna från WLAN:et kan störa annan utrustning (extern interferens).

Annan utrustning såsom mikrovågsugnar, hissmotorer, larmsystem och trådlösa telefoner kan störa kommunikationen i ett WLAN. Detta resulterar i att data som sänds i WLAN:et blockeras och fördröjs eller kommer fram felaktig. Samma sak gäller omvänt då signaler från ett WLAN stör t.ex. navigeringssystemet på ett flygplan. De flesta WLAN som använder Spread Spectrum interfererar inte eftersom de har så låg effekt (>1 Watt), undantaget är om de är väldigt nära känslig utrustning. WLAN med Spread Spectrum tekniken är inte heller lika känsligt för interferens eftersom signalen är utspridd över ett stort frekvensband. Utrustningen måste alltså vara väldigt nära och använda samma band för att extern eller intern interferens skall uppstå.

#### **Strömförbrukning**

För bärbara datorer kan batteritiden sänkas dramatiskt om de kopplas upp mot ett WLAN. Tillverkare av access points och radiokort använder olika tekniker för strömhushållning i sina produkter. Två av dessa är Doze Mode och Sleep Mode. Doze mode innebär att apparaten kopplar upp och tar emot eventuella meddelanden med jämna mellanrum men annars är fränkopplad. Sleep Mode innebär att apparaten kopplar på radiofunktionen när information ska sändas men annars är fränkopplad, i detta läge kan apparaten alltså aldrig ta emot information.

---

<sup>40</sup> PCTechGuide, Wireless networks

<sup>41</sup> Wireless LANs, Geier Jim

## 3.2 Vilka säkerhetsaspekter är specifika vid användning av WLAN?

### 3.2.1 Vilka säkerhetsrisker föreligger?

WLAN är ett sätt att överföra data mellan två punkter och innehåller funktioner som synkronisering och felkontroll som återfinns på de lägre nivåerna i OSI-modellen.<sup>42</sup>

#### Avlyssning

Största säkerhetsrisken är det faktum att signalerna från ett WLAN täcker ett stort område vilket gör det möjligt för en utomstående person att lyssna av datatrafiken t.ex. utanför ett företags fysiska väggar. Detta förutsätter dock att inkräktaren känner till det SSID (alltså nätverksnamn, se avsnitt 3.2.2) som behövs för att komma in i nätverket.<sup>43</sup>

Teoretiskt sett finns samma risk med fysiska LAN då en inkräktare kan lyssna av de elektromagnetiska vågor som skapas av ström i kablarna. I detta fall måste dock inkräktaren vara mycket närmare än i fallet med WLAN.<sup>44</sup>

#### Denial of service

Ett annat hot är att någon saboterar genom att blockera nätverket. I de flesta fall delar flera sändare på samma medium (luftrum) och om en station sänder så måste alla andra vänta. Sabotören kan då använda en produkt av samma fabrikat som används i ett nätverk och göra så att denna sänder data oavbrutet. Detta leder till att alla andra stationer i området blockeras och nätverket blir obrukbart.<sup>45</sup> När en access point blockeras på detta vis kallas det för en denial-of-service attack<sup>46</sup>.

#### Stöld av hårdvara

Det är vanligt att en krypteringsnyckel (WEP-nyckel) statistiskt placeras på hårddisken eller liknande hos en trådlös station. Detta innebär att den som har stationen har både stationens MAC-adress och krypteringsnyckeln vilket ger tillgång till det trådlösa lokala nätverket vilket inte är bra i det fall att hårdvaran blir stulen.<sup>47</sup>

### 3.2.2 Vad finns det för lösningar i dagsläget?

#### Access control och privacy

I sammanhanget säkerhet i WLAN är begreppen access control och privacy centrala. Access control försäkrar att endast auktoriserade användare har tillgång till känslig data. Privacy syftar till att överförd data endast kan tas emot och förstås av dem den är avsedd för.<sup>48</sup>

I standarden 802.11 ingår komponenter för access control och privacy. Dessa måste dock implementeras på alla stationer i ett WLAN vilket kan vara komplicerat i stora nätverk. Komponenterna är service set identifiers (SSIDs) samt wired equivalent privacy (WEP).<sup>49</sup>

---

<sup>42</sup> Wireless LANs, Geier Jim

<sup>43</sup> Wireless LANs, Geier Jim

<sup>44</sup> Ibid

<sup>45</sup> Ibid

<sup>46</sup> Wireless Network Security, Wavelink

<sup>47</sup> Cisco Systems

<sup>48</sup> Cisco Systems

<sup>49</sup> Ibid

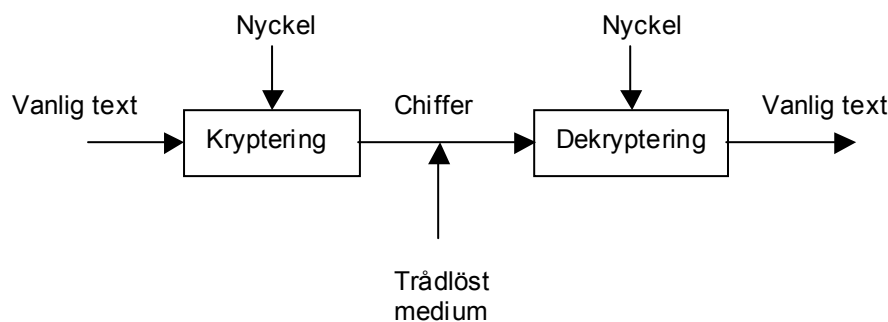
**SSID**

Ett SSID är ett nätverksnamn för alla stationer i ett BSS<sup>50</sup>. De flesta produkter för WLAN kräver att man har ett SSID och att man lägger in denna kod i alla stationer. En station i ett WLAN behandlar ingen data om inte dess kod stämmer överens med nätverkets.<sup>51</sup>

**WEP**

WEP är ett frivilligt tillval i 802.11, det är dock ett krav för Wi-Fi<sup>52</sup> certifiering. WEP är en symmetrisk krypteringsalgoritm där samma algoritm och nyckel används för både kryptering och dekryptering av data. Syftet med WEP är att uppnå access control genom att användare som saknar korrekt WEP nyckel nekas tillträde till nätverket. WEP syftar även till privacy genom att skydda data som överförs genom kryptering så att ingen användare som saknar korrekt WEP nyckel kan dekryptera datan.<sup>53</sup>

WEP togs fram för att ge det extra skydd i WLAN som ges i fysiska LAN i form av fysiska väggar och liknande. I sina standarder för fysiska LAN har IEEE inte någon krypteringsfunktion.<sup>54</sup>



Figur 6. Kryptering med WEP<sup>55</sup>

Eftersom signalerna från ett WLAN kan fångas upp inom ett stort område som kan sträcka sig över fysiska gränser som väggar mm så är det omöjligt att rikta en signal i ett WLAN till endast en användare.<sup>56</sup>

I ett trådlöst nätverk kan alltså alla stationer och annan apparatur höra datatrafiken inom nätverket. Privacy-tjänsten i 802.11 höjer nivån för privacy så att den motsvarar den för fysiska nätverk där trafiken skyddas från avlyssning via fysiska barriärer. Privacy-tjänsten baseras på WEP som minskar risken för tjuvlyssning.<sup>57</sup>

<sup>50</sup> Cisco Systems

<sup>51</sup> Wireless LANs, Geier Jim

<sup>52</sup> Se ordlista

<sup>53</sup> Cisco Systems

<sup>54</sup> WEP Security Statement, Wireless Ethernet Compability Alliance

<sup>55</sup> Wireless LANs, Geier Jim, s 84 (egen avritning och översättning)

<sup>56</sup> Cisco Systems

<sup>57</sup> Wireless LANs, Geier Jim

WEP stödjer enligt standarden kryptering per paket men inte autentisering per paket. En hacker kan ta reda på MAC-adressen hos STA och AP, tidpunkter för association med mera genom att titta på data- och kontroll kanalerna i 802.11. En hacker kan använda sådan information för att göra analyser som kan ge information om användare eller utrustning. För att förebygga detta bör WEP-nycklarna bytas ofta, till exempel kan nyckeln bytas ut efter varje session.<sup>58</sup>

### Autentisering

Eftersom WLAN fysiskt sett är mer oskyddade än fysiska LAN vad gäller obehörig åtkomst så innefattar 802.11 autentiseringstjänster som kontrollerar åtkomst så att WLAN ska vara lika säkra som fysiska. 802.11 definierar två sådana tjänster.<sup>59</sup>

Open system authentication är default enligt 802.11. Autentiseringen sker i två steg. Stationen som vill bli autentiserad skickar en förfrågan som bland annat innehåller den frågande stationens identitet. Mottagande station returnerar sedan ett avslag eller accepterar.<sup>60</sup>

Den andra tjänsten för autentisering heter shared key authentication. Denna metod förutsätter att varje station har mottagit en hemlig nyckel på annan väg än via WLAN:et. Nyckeln är gemensam för alla stationer i WLAN:et. Gemensam nyckel kräver implementering av WEP.<sup>61</sup>

Rekommenderat är att använda både WEP och authenticationstjänster för bästa säkerhet<sup>62</sup>.

När en station inte längre vill kommunicera med en annan meddelar stationen detta genom en deauthentication-tjänst. Detta meddelande kan inte accepteras eller avslås, det är endast en upplysning om att förbindelsen kommer att upphöra.<sup>63</sup>

### ACL

En säkerhetsåtgärd för access points är en Access Control List (ACL) vilket är en lista över alla stationer som är auktoriserade att använda nätverket. Listan innehåller stationernas MAC-adresser. En station som inte finns med på listan kan inte kommunicera med denna access point.<sup>64</sup> Denna funktion är dock inte definierad i 802.11<sup>65</sup>.

Ett problem är att MAC-adresser aldrig kodas, inte ens om WEP används, och det går att ändra MAC-adress på ett NIC med hjälp av särskild mjukvara. Detta gör att en inkräktare kan ta reda på en MAC-adress i ett nätverk som skyddas av ACL och sedan lura AP:n att släppa in inkräktaren.<sup>66</sup>

---

<sup>58</sup> Cisco Systems

<sup>59</sup> Wireless LANs, Geier Jim

<sup>60</sup> Ibid

<sup>61</sup> Ibid

<sup>62</sup> Ibid

<sup>63</sup> Ibid

<sup>64</sup> Wireless Network Security, Wavelink

<sup>65</sup> Your 802.11 Wireless Network has No Clothes, Arbaugh W A m.fl.

<sup>66</sup> Ibid

## VPN

I fysiska nätverk används oftast ingen säkerhetsåtgärd i det fysiska skiktet eller länkskiktet. Data i dessa nätverk skyddas istället genom åtgärder i nätverksskiktet eller i högre skikt. Ett exempel är VPN (Virtual Private Networking) som används för uppkoppling mot ett företags nätverk på distans (till exempel över Internet). VPN är till för att säkert kunna överföra data över ett osäkert medium.<sup>67</sup>

## Hur ska WLAN skyddas?

Det absolut största hotet mot trådlösa LAN är underlåtenhet att vidta de säkerhetsåtgärder som finns tillgängliga. WEP bör användas som ett första försök att avskräcka inkräktare. Ytterligare säkerhetsåtgärder bör anpassas efter situation (hemanvändning, försvarsdepartementet och så vidare).<sup>68</sup>

Wireless Ethernet Compability Alliance (WECA) rekommenderar Mindre organisationer och privatpersoner att använda WEP, ändra förinställd nyckel och därefter byta nyckel regelbundet, lösenordsskydda hårddiskar och mappar, ändra förinställt SSID, använda sessionsspecifika WEP-nycklar om produkten stödjer det, använda MAC-adress filter om produkten stödjer det samt använda VPN.<sup>69</sup>

För större organisationer där data behöver skyddas ytterligare rekommenderar WECA att man vidtar ytterligare säkerhetsåtgärder. Exempel på sådana åtgärder är end-to-end kryptering, lösenordsskydd, autentisering av användare, VPN och brandväggar.<sup>70</sup>

---

<sup>67</sup> Trudeau Pierre, Building Secure Wireless Local Area Networks

<sup>68</sup> WEP Security Statement, Wireless Ethernet Compability Alliance

<sup>69</sup> Ibid

<sup>70</sup> Ibid

## 4 Analys/Diskussion

Enligt det jag läst så går mycket arbete åt att förbättra säkerhetsfunktionerna i standarden 802.11 (eller någon utveckling av den) och det verkar också som om de allra flesta använder sig av denna standard. Det som är bra med att arbeta med standarden på detta vis är att en förbättring i standarden ger en förbättring för alla som använder produkter som följer denna. Om två WLAN som följer 802.11 kopplas ihop vet man alltså att detta nya ESS följer standarden och är så säkert som standarden medger. Förutsatt att säkerhetsfunktionerna används.

I arbetet med säkerhet i WLAN kretsar mycket kring det faktum att radiovågor är lättare att lyssna av än kablar i fysiska LAN. De säkerhetsåtgärder som finns strävar därför efter att få ett WLAN att fungera som om det vore ett fysiskt LAN på det sättet att det ska vara lika svårt att avlyssna.

Det finns dock olika ståndpunkter. Antingen koncentrerar man sig på det fysiska skiktet och länkskiktet som jag beskrivit ovan eller implementerar man säkerhetsåtgärder på de högre skikten. Eftersom det är lättare att ta sig in i trådlösa nätverk kanske det inte räcker med att göra det svårare att ta sig in och tjuvlyssna (genom WEP) utan man bör även höja säkerheten inne i nätet (till exempel med VPN). Med VPN åtgärdas säkerhetsrisker som även finns i fysiska LAN. Vad jag förstår så handlar de två ståndpunkterna om ifall det är viktigast att inte släppa in vem som helst i nätverket eller om man kan sänka kraven på den säkerheten men höja säkerheten inuti nätverket. Med säkerheten inuti nätverket menar jag säkerhet vid dataöverföring från en station till en annan.

Det är viktigt att användare är medvetna om de risker som finns så att de kan skydda sig så mycket som behövs beroende på verksamheten. Vissa kanske klarar sig med den säkerhet som finns idag, andra kanske bör vänta tills nya lösningar utvecklats. Jag tror dock att kunskap som vanligt är mycket viktigt för att veta vad det finns för risker, hur stora de är, hur det påverkar mig och vad det finns för lösningar i dagsläget. Om de säkerhetsåtgärder som finns inte används så är de inte till mycket hjälp.

## Källförteckning

### *Publicerade källor*

Ewert Magnus, Datakommunikation – Nu och I framtiden, Studentlitteratur, Lund, 1999

Geier Jim, Wireless LANs – Implementing High Performance IEEE 802.11 Networks, SAMS, Indiana, USA, 2002

Jensen Stig, Gjelstrup Arne och Berti Valentino, Datakommunikation, Liber, Stockholm, 2000

Ottosson Benny, Internet & TCP/IP, Kompendium, Högskolan i Örebro, 1995

Patel Runa, Davidson Bo, Forskningsmetodikens grunder – Att planera, genomföra och rapportera en undersökning, Studentlitteratur, 1994

Simon Singh, "Kodboken", 1999, Norstedts förlag, Stockholm  
ISBN 91-7643-697-7

### *Oppublicerade källor*

#### **Internet**

Arbaugh William A, Shankar Narendar, Wan Y.C. Justin, Your 802.11 Wireless Network has No Clothes, Department of Computer Science, University of Maryland, 2001-03-30  
<http://www.cs.umd.edu/~waa/wireless.pdf>, 011020

Borisov Nikita, Goldberg Ian och Wagner David, Security of the WEP algorithm  
<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>, 011020

Cisco Systems, 2001-04-11  
[http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w\\_ov.htm](http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm), 011010

Karve Anita, 802.11 and Spread Spectrum, 1997-12-01, NetworkMagazine.com  
<http://www.networkmagazine.com/article/NMG20000726S0001/2>, 011016

PCTechGuide, OSI Model  
<http://www.pctechguide.com/29network.htm#OSI#Model>, 011016

PCTechGuide, Wireless networks  
[http://www.pctechguide.com/29net2.htm#Wireless\\_networks](http://www.pctechguide.com/29net2.htm#Wireless_networks), 011016

Possios hemsida  
<http://www.possio.com/spread.asp?dynfile=company&cat=1&loop=1&dh=1>, 011106

The linux-wlan Company

<http://www.linux-wlan.com/writings/std-wlan-whitepaper.html>, 011016

Trudeau Pierre, Building Secure Wireless Local Area Networks – A White Paper By Colubris Networks Inc., 2001

[http://www.wlana.com/pdf/security\\_colubris.pdf](http://www.wlana.com/pdf/security_colubris.pdf), 011010

Wavelink, Wireless Network Security – White Paper

[http://www.wlana.com/pdf/security\\_wavelink.pdf](http://www.wlana.com/pdf/security_wavelink.pdf), 011010

Wireless Ethernet Compability Alliance, WEP Security Statement, 010907

[http://www.wlana.com/pdf/security\\_weca.pdf](http://www.wlana.com/pdf/security_weca.pdf), 011010

WLANA, The Wireless LAN Association

[http://www.wlana.com/learning\\_center.html](http://www.wlana.com/learning_center.html), 011010

### **e-post**

Mårild Kristoffer, Possio, 011024