



Skolens trådløse netværk

Anbefalinger vedrørende etablering og drift af trådløse netværk

Skolens trådløse netværk
Anbefalinger vedrørende etablering og drift af trådløse netværk

Forfattere:

Specialkonsulent Michael Glud Andersen,
sikkerhedschef Tommy Ravn Jensen,
specialkonsulent Jan Pagh,
salgschef Jens R. Rasmussen

© UNI•C

Indhold

1	Resumé.....	6
2	Indledning	7
	2.1 Baggrund.....	7
	2.2 Målgruppe og indhold	7
	2.3 Hvad med fremtiden?	8
3	Valg af arkitektur og teknologi.....	11
	3.1 Arkitektur.....	11
	3.2 Teknologi.....	14
4	Adgang til det trådløse netværk	18
	4.1 Sikker login.....	18
	4.2 Segmentering.....	21
5	Administration af brugere.....	23
	5.1 Brugertyper.....	23
	5.2 Rettighedsstyring.....	23
	5.3 RADIUS-server og brugerdatabase	25
	5.4 Gæster på skolens trådløse net	26
6	Private enheder på skolens trådløse net	28
	6.1 Typer af enheder	28
	6.2 Generelle sikkerhedsovervejelser og tiltag	29
	6.3 Adgang til lokale ressourcer	31
7	Installation og opsætning	33
	7.1 Netforbindelse til AP'er	33
	7.2 Strøm til AP'er.....	35
	7.3 PoE og grøn it.....	36
8	Økonomi og rådgivning.....	37
	8.1 Supplement eller alternativ	37
	8.2 De kendte og de skjulte udgifter	37
	8.3 Hvordan køber man et trådløst netværk.....	37
	8.4 Hvor meget skal man købe	38

8.5	Minimér udgifterne	38
9	Kravspecifikation og indhentning af tilbud	40
9.1	Hvad skal kravspecifikationen indeholde	40
9.2	Hvor skal det trådløse netværk anvendes	41
9.3	Hvem skal have adgang til det trådløse netværk	41
9.4	Hvordan skal det trådløse netværk anvendes	41
9.5	Samspil med det fastkoblede net	41
9.6	Driftskrav	42
9.7	Uddannelse	42
9.8	Udvidelser	42
9.9	Service og support	43
9.10	Økonomi	43
9.11	Levetid	43
9.12	Udfærdigelse af kravspecifikation	43
10	Valg af tilbud	45
10.1	Tilbud vs. kravspecifikation	45
10.2	Hvem træffer afgørelsen	45
10.3	Hvad koster det	46
10.4	Ting man skal være specielt opmærksom på	46
10.5	Køb	47
11	Drift og overvågning	49
11.1	Ændringer i konfiguration	49
11.2	Fejl på net eller udstyr	50
11.3	Overbelastning af netværket	51
12	Håndtering af sikkerhedsbrud	56
12.1	Hvad er et sikkerhedsbrud?	56
12.2	Hvordan konstateres et sikkerhedsbrud?	56
12.3	Håndtering af en hændelse	57
12.4	Anvendelsespolitik	59
13	Lovgivning og myndighedskrav	61
13.1	De juridiske aspekter	61
13.2	Skolens behov for logning – et myndighedskrav?	61
13.3	Persondataloven	62
13.4	Et minimum af sikkerhed: culpa (objektivt ansvar)	63

14	Bilag 1 – Ordliste	65
	14.1 Ordliste med tekniske udtryk og forkortelser	65
15	Bilag 2: Eksempel på kravspecifikation	72
	15.1 Kravspecifikation for Den Grønne Skole	72
16	Bilag 3: Eksempel på anvendelsespolitik	75
	16.1 Accepteret brug af netværket	75
	16.2 Brugernavne og adgangskoder	75
	16.3 Tilgængelighed og opetid	75
	16.4 Ansvar for medbragte pc'er.....	75
	16.5 Krav til udstyr, der tilsluttes netværket.....	76
	16.6 Logning.....	76
	16.7 Anmeldelse og efterforskning af misbrug	76
	16.8 Sanktioner.....	76
	16.9 Erklæring.....	77
17	Bilag 4 – De mest almindelige driftsproblemer	78
	17.1 Problemer med at logge på net beskyttet med captive portal (hotspot)	78
	17.2 Problemer med at logge på net med WPA2-Enterprise PEAP-MSCHAPv2.....	78
	17.3 Nettet er ustabil – jeg mister ofte forbindelsen.....	79
	17.4 Der er forbindelse, men nettet er meget langsomt	80

1 Resumé

Det er UNI•Cs mission at fremme og optimere it-anvendelse i den samlede uddannelses-sektor. Derfor ønsker vi med dette materiale at rådgive og hjælpe uddannelsesinstituti-oner med nogle af de overvejelser, der indgår i etablering og drift af et trådløst netværk, så processen hen mod en velfungerende infrastruktur fremmes.

UNI•C anbefaler derfor, at skolerne

- i forbindelse med etablering og udbygning af trådløst netværk anvender en controllerbaseret arkitektur med AP'er, der understøtter 802.11n på både 2,4 og 5 GHz og anvender PoE-switcher med gigabit mellem krydsfelterne.
- opdeler brugerne i to-tre typer, som alle logger på med individuelt login. Pålog-ningmetoden for gæster kan være captive portal, mens elever og lærere med deres egne bærbare enheder bør bruge WPA2-Enterprise med PEAP-MSCHAPv2. Alle brugere skal, inden de tildeles adgangsprivilegier, informeres om og god-kende skolens anvendelsespolitik for nettet.
- segmenterer deres net svarende til brugertyperne, at AP'erne konfigureres til et tilsvarende antal SSID'er, og at der anvendes en RADIUS-server til autentifikation af brugerne.
- ved køb sammen med en uafhængig konsulent udarbejder en egentlig kravspeci-fikation dækkende både køb og efterfølgende drift. Investeringen bør afskrives inden for fem år.
- benytter et overvågningssystem som støtte i den daglige drift. Systemet skal bl.a. kunne alarmere ved almindeligt forekommende driftsforstyrrelser og be-nyttes i fejlsøgningsituationer, hvor nettet er belastet.
- udformer en anvendelsespolitik, som brugerne skal acceptere, og som håndhæ-ves konsekvent. Driften skal bl.a. sørge for at der logges i nødvendigt omfang (og at dette anmeldes til Datatilsynet) – som minimum med tildeling af IP-adresse, tidsrum og bruger-id for brugerne. Hvis der er tvivl om skolens status som kom-merciel eller ikke kommerciel virksomhed, rettes forespørgsel til It- og Telesty-relsen.

2 Indledning

2.1 Baggrund

Det er UNI•Cs mission at fremme og optimere it-anvendelse i den samlede uddannelsessektor. Derfor ønsker vi med dette materiale at rådgive og hjælpe uddannelsesinstitutioner med nogle af de overvejelser, der indgår i etablering og drift af et trådløst netværk, så processen hen mod en velfungerende infrastruktur fremmes.

Vi oplever i disse år et paradigmeskift, hvor uddannelsessektorens brugere i stigende grad møder op på uddannelsesinstitutionen med privat, mobilt udstyr og samtidig forventer et tilgængeligt og driftssikkert trådløst netværk.

Samtidig bliver mere og mere undervisningsmateriale udbudt via internetet, og dermed er undervisningen i stigende grad afhængig af både internetforbindelsen og trådløst netværk.

På efterskoler og ungdomsuddannelser er det en udbredt praksis, at eleverne møder op med egne bærbare pc'er, der anvendes i og uden for undervisningen – til tider til udveksling af "tunge" undervisningsdata i form af video og lignende. Denne trend er ikke helt så gennemgående på grundskoleniveau her i 2010.

Smartphones og andre mobile enheder er derimod på vej overalt – også i uddannelsessektoren – og med dem forventer man også adgang til et hurtigt trådløst netværk.

Disse trends stiller skolen over for to store udfordringer:

- et lettilgængeligt, hurtigt og driftssikkert trådløst netværk med internetadgang
- eleverne møder med deres eget private udstyr, hvor skolen kun i begrænset omfang har indflydelse på, hvad udstyret anvendes til, og hvad der er installeret af software på udstyret.

Dertil kommer, at man som uddannelsesinstitution står over for helt særlige udfordringer omkring udnyttelsen af det trådløse netværk. Der er behov for mange samtidige brugere, der er tale om høje krav til båndbredde, og ofte skal det hele afvikles i et koncentreret geografisk område (fx et klasselokale). Dette sammenholdt med, at et trådløst netværk udgør et "delt medium", stiller ekstra store krav til udstyret.

2.2 Målgruppe og indhold

Materialet er primært henvendt til skolens it-ansvarlige og netværksadministrator, men kan dog anvendes af alle, der kommer i berøring med institutionens trådløse netværk.

Vi forsøger i materialet at belyse aspekter af alle faser i et forløb om etablering og drift af et trådløst netværk på en uddannelsesinstitution.

Materialet indeholder en del gentagelser af hensyn til læsere, der kun har interesse i enkelte kapitler. Da materialet indeholder en del fagtermer, er disse for størstedelens vedkommende forklaret i ordlisten (bilag 1).

Priser er pr. december 2010 og angivet eksklusiv moms.

I slutningen af hvert kapitel opsummeres UNI•Cs anbefalinger.

2.3 Hvad med fremtiden?

I dette materiale fokuserer vi på udfordringer og teknologi, som det ser ud her i 2010. Trådløse netværk er inde i en rivende udvikling, og hvad vi anbefaler som et godt valg nu, var knap nok kendt teknologi for fem år siden. Hvis udviklingen fortsætter, vil fremtiden byde på endnu flere og mere moderne muligheder, som skal inddrages i institutionens overvejelser – ligesom de trådløse netværk i stigende grad bliver suppleret af mobilt bredbånd. Derfor er det vigtigt at understrege behovet for i en konkret situation at tage bestik af de aktuelle, teknologiske muligheder.

2.3.1 Trådløse netværk og mobilt bredbånd (3G og 4G)

I materialet er der fokus på skolens trådløse netværk. Betegnelsen "trådløse netværk" dækker mere præcist over trådløse lokalnetværk opbygget ved hjælp af AP'er, der understøtter en eller flere 802.11-standarder, også kaldet Wi-Fi.

Der findes adskillige andre trådløse teknologier som fx Bluetooth, WinMax og 3G/4G, hvor sidstnævnte er teknologien bag mobilt bredbånd, der sælges af landets teleselskaber. De sidste par år er udrulningen af 3G gået stærkt, og teleselskaberne har meget store forventninger til mobilt bredbånd fremover. Konkurrencen er hård, og priserne hastigt på vej ned. Derfor oplever mange skoler nu, at elever og lærere kommer med laptops og smartphones, der har internetforbindelse via mobilt bredbånd.

Når skolen begynder at opleve, at brugerne både medbringer eget udstyr og egen internetforbindelse, opstår der naturligt en overvejelse om, hvorvidt mobilt bredbånd snart vil blive så almindeligt, at det kan udgøre et reelt alternativ til skolens trådløse netværk. Hvis det er tilfældet, kan en stor investering måske undlades.

Men er mobilt bredbånd på vej til at blive et reelt alternativ til det trådløse netværk? Svaret er nej – i hvert fald ikke foreløbig. Og den primære årsag er manglende båndbredde. Godt nok kan man i dag købe 3G-forbindelser med teoretiske hastigheder på op til omkring 20 Mbit/s, og de første selskaber har her i efteråret 2010 lanceret LTE/4G med teoretiske hastigheder op i nærheden af 100 Mbit/s. Men det er helt afgørende at bemærke, at hastighederne er den samlede kapacitet for en telemast. Dvs. at ikke bare skolens brugere deles om hastigheden, det gør alle andre brugere i samme område også. Så der vil være rigtig mange brugere, der skal deles om en samlet kapacitet, der ligger væsentligt under kapaciteten for et enkelt moderne AP. Dertil kommer, at de høje hastigheder på 3G/4G kun er opnåelige, hvis man er så heldig, at være tæt på en mast, og i praksis vil de ligge væsentligt lavere. Endelig er upload-hastighederne betydeligt lavere end download-hastighederne.

Mobilt bredbånd har til gengæld den store fordel, at det er mobilt, dvs. at der kan forventes god dækning i de fleste større byområder og som regel også en forbindelse i landområder, der blot er betydeligt langsommere.

Man skal derudover være opmærksom på, at mobilt bredbånd giver en direkte internetforbindelse uden om skolens lokalnet. Der er som udgangspunkt ikke adgang til skolens lokale ressourcer som fil, print mv. via mobilt bredbånd.

Så foreløbig vil mobilt bredbånd ikke være et reelt alternativ til et trådløst netværk på skolen. Hvis et mindre antal brugere har mobilt bredbånd, kan det køre udmærket, men den samlede kapacitet er langt fra tilstrækkelig til at håndtere alle skolens brugere.

UNI•C, december 2010

3 Valg af arkitektur og teknologi

Når skolen står over for at skulle indkøbe et nyt trådløst netværk, er der en række tekniske spørgsmål, man bør forholde sig til. I første omgang bør man beslutte sig for en arkitektur og for en teknologi.

3.1 Arkitektur

Arkitekturen handler om det trådløse nets komponenter og deres indbyrdes sammenhænge. Der findes grundlæggende set to forskellige arkitekturer – eller modeller – for opbygning af et net, som man kan vælge imellem: den autonome og den controllerbase-rede.

3.1.1 Autonom arkitektur

Den autonome arkitektur er den klassiske 1.-generations-model for opbygning af et trådløst net. Det autonome netværk består af en række uafhængige access-punkter (AP'er), der fungerer hver for sig og afvikler trafik uafhængigt af de øvrige AP'er. Der er ingen automatisk koordinering eller optimering AP'erne imellem, og al konfiguration, justering, fejlsøgning osv. foregår ved logge ind i hvert enkelt AP. Det betyder, at det kan være en både stor og kompleks opgave at fejlsøge på og vedligeholde et autonomt trådløst netværk med mere end nogle ganske få AP'er.

Autonome AP'er findes i to forskellige typer til hver sin målgruppe. Første type består af de helt billige AP'er, der udelukkende er beregnet til hjemmebrug, eller helt små netværk med et enkelt eller ganske få AP'er. Her vil der ikke være mere end maks. 2-3 maskiner tilsluttet samme AP. Denne type AP'er forhandles i bl.a. supermarkeder og varehuse helt ned til et par hundrede kroner stykket. Mange skoler er startet ud med at opbygge et netværk med disse AP'er, men har også erfaret, at der ofte opstår problemer, efterhånden som der kommer flere klienter (maskiner) på det trådløse net. Hastigheden falder, og der opleves ustabilitet. AP'erne er som nævnt primært beregnet til hjemmebrug, og det frarådes, at man som skole begynder at etablere et trådløst netværk med disse AP'er.

Den anden type består af betydeligt dyrere AP'er i professionel kvalitet. Disse AP'er er karakteriseret ved generelt at have flere funktioner, og frem for alt er de bedre i stand til at håndtere flere samtidige klienter på samme AP. De forhandles af professionelle it-leverandører, og prismæssigt ligger de omkring 1.500 – 5.000 kr. pr. stk. ekskl. moms.

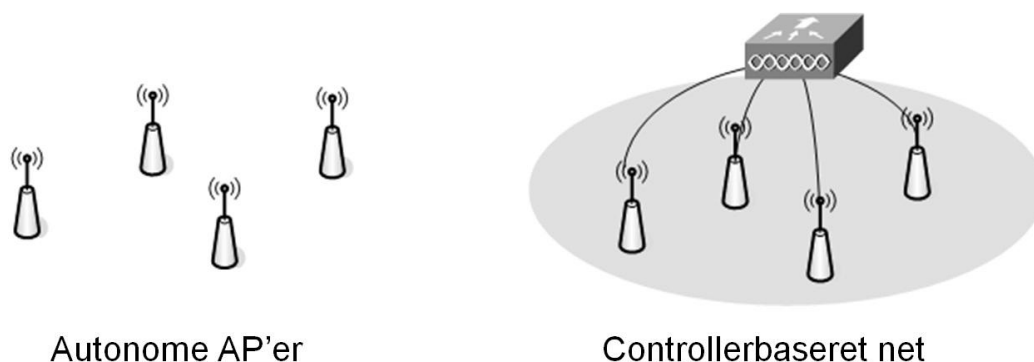
Fælles for alle trådløse netværk baseret på autonome AP'er er en række indbyggede mangler og u hensigtsmæssigheder, som det er afgørende at være opmærksom på.

For det første er der – som tidligere nævnt – ingen indbyrdes koordinering imellem AP'erne. Hvert AP konfigureres med en fast kanal og en fast sendestyrke. Der er ingen

automatisk optimering i forhold til at minimere interferens og overlap på nettet, og det kan resultere i nedsat ydelse og stabilitet.

For det andet er det autonome net tidskrævende at have med at gøre. I etableringsfasen skal hvert AP konfigureres for sig, og det samme er tilfældet, når der efterfølgende er behov for ændringer eller opdateringer. Der skal logges ud i hvert eneste AP for at foretage ændringen. Med mange AP'er kan det blive en rigtig stor opgave at vedligeholde nettet. Dertil kommer, at det autonome net stiller krav om VLAN i skolens kablede netværk. Det vil således være nødvendigt med VLAN i alle underkrydsfelter, såfremt man blot ønsker mere end et enkelt SSID.

For det tredje er der ikke noget centralt overblik på et autonomt trådløst net. Alle relevante oplysninger ligger ude i de enkelte AP'er, og med mange AP'er kan det derfor være svært at finde den relevante information. Det besværliggør den almindelige daglige drift, og ikke mindst fejlsøgning kan være meget besværligt på et autonomt net.



Figur 1. Controlleren er en central styreenhed, der løser uhen-sigtsmæssigheder og mangler ved den autonome løsning.

3.1.2 Controllerbaseret arkitektur

I den nyere controllerbaserede arkitektur er der en lang række forbedringer i forhold til den autonome arkitektur. Alle de ovenfor nævnte mangler og uhen-sigtsmæssigheder er løst, og desuden er der typisk tilføjet en række nye funktioner afhængig af det konkrete valg af produkt.

Helt centralt i den controllerbaserede arkitektur er den centrale styreenhed – controlleren – som illustreret på figuren. Al konfiguration, vedligehold, styring og overvågning er samlet i controlleren. Så i et netværk med 25 AP'er går man fra 25 enheder til 1 enhed, når det handler om konfiguration, vedligehold osv. Det er en kæmpegevinst, der betyder, at der kan spares mange timer i både etableringsfasen og den daglige drift.

Dertil kommer, at controlleren kan koordinere og optimere AP'erne i forhold til hinanden. Når information om, hvordan AP'erne indbyrdes kan "se" hinanden, er samlet i controlleren, er det muligt for controlleren at lægge en optimal kanalplan og justere sendestyrken på hvert AP, så overlap minimeres. Det betyder bedre hastighed og øget stabilitet på nettet. De fleste controllerbaserede systemer kan endda foretage justering af kanal og sendestyrke løbende, så der helt automatisk kan korrigeres for en evt. midlertidig støjkilde på skolens område.

I praksis er AP'erne helt underlagt controllerens kontrol. Når et AP tilsluttes det kablede net, etablerer det så vidt muligt automatisk forbindelse til controlleren, nyeste AP-firmware downloades og installeres automatisk, hvorefter AP'et modtager sin konfiguration inkl. kanalvalg og sendestyrke. Fra AP'et tilsluttes, til det er i drift, går der ofte kun nogle minutter. Når det er i drift, sendes normalt både kontrol-trafik og data-trafik (til/fra klienter) via en særlig punkt-til-punkt forbindelse mellem AP og controller, sådan som det er illustreret på figuren. Det har bl.a. den fordel, at information om den enkelte pakkes VLAN-tilhørsforhold sendes op til controlleren via denne forbindelse og først sendes ud på det korrekte VLAN af controlleren, hvorfor der ikke er behov for nye VLAN i underkrydsfelterne, selvom man ønsker flere SSID'er.

Foruden de ovenfor nævnte forbedringer, indeholder controlleren normalt en række relevante ekstra funktioner. Eksempler på disse funktioner er:

- *Captive portal*-funktion (hotspot), der giver mulighed for at lade brugerne logge ind via en simpel webseite
- *Load balancing*, der kan medvirke til en pæn fordeling af klienterne over flere AP'er og på den måde sikre, at ikke alle klienter i et område vælger samme AP
- *Band steering/band select*, der medvirker til, at klienter, der både har en 2,4 og en 5 GHz radio, så vidt muligt vælger at tilslutte sig på 5 GHz-båndet, hvor der ofte vil være bedst performance
- *Firewall*, der kan lægge firewall-regler på brugere tilsluttet det trådløse net
- *Tidsstyrkede regler*, der fx kan styre, at udvalgte grupper af brugere kun kan anvende nettet i bestemt tidsrum
- *Rogue AP detektering*, der kan detektere fremmede AP'er, som kan udgøre en sikkerhedsrisiko
- *Remote AP*, der er et særligt AP beregnet til en sikker opkobling mod skolens controller fra en medarbejders private net
- *Lokationsbestemmelse*, der handler om at bestemme en omtrentlig lokation af klienter mv.

Endelig skal det nævnes, at der foruden den almindelige "flerkanaals"-arkitektur også findes enkelte producenter, der satser på en 1-kanals arkitektur, hvor alle AP'er kører på samme kanal. Der er både fordele og ulemper ved begge arkitekturer, og man kan slet ikke entydigt fremhæve den ene arkitektur som værende bedre end den anden.

3.1.3 Hvad bør skolen vælge?

Det er vigtigt at være opmærksom på, at der, når det drejer sig om en skole, stilles nogle helt ekstraordinære krav til det trådløse net i forhold til de krav, der typisk stilles til private virksomheder eller offentlige institutioner i øvrigt.

I en undervisningssituation vil der typisk være mange samtidige brugere på det trådløse netværk i samme område. Og ofte ønsker brugerne at anvende forbindelsen samtidig (logger på samtidig, henter information samtidig). Endelig kan der være tale om "tunge" og krævende brugere, der stiller store krav til båndbredde, fx for at kunne streame video.

En situation med mange samtidige brugere i samme område er en stor udfordring på et trådløst netværk¹. Derfor bør skoler satse på en professionel løsning, der er baseret på en controllerbaseret arkitektur. Det er ikke en billig løsning, men det er nødvendigt for at imødekomme de krav, der typisk stilles til det trådløse netværk i skolemæssig sammenhæng.

Valg af leverandør og producent foretages bl.a. ud fra prisniveau og på baggrund af ønsker og behov til funktionalitet. Der henvises til kapitel 9 "Kravspecifikation og indhentning af tilbud".

3.2 Teknologi

De teknologier, der anvendes på et trådløst netværk, er specificeret af IEEE² i en række 802.11-standarder. De primære af disse standarder er listet i tabel 1 nedenfor.

¹ Et trådløst netværk fungerer på et delt medium, hvor der (på samme frekvens) kun er en, der kan sende ad gangen. På den måde kan der nemt opstå "kø" og "kollisioner", når der er mange, der forsøger at sende samtidig.

² www.ieee.org

Trådløs standard	Fra år	Frekvensbånd	Maks. forbindelseshastighed ³⁾	Skønnet maks. effektiv båndbredde ⁴⁾
802.11b	1999	2,4 GHz	11 Mbit/s	~ 5 Mbit/s
802.11a	1999	5 GHz	54 Mbit/s	~ 25 Mbit/s
802.11g	2003	2,4 GHz	54 Mbit/s	~ 25 Mbit/s
802.11n (2,4)	2009	2,4 GHz	144 Mbit/s ⁵⁾	~ 75 Mbit/s
802.11n (5)	2009	5 GHz	300 Mbit/s	~ 150 Mbit/s

Tabel 1. 802.11 standarder

Som det fremgår, er der i 2009 fastlagt en ny standard, der betegnes 802.11n. I tabellen kan det se ud, som om 802.11n er to standarder, men det skyldes, at standarden er specificeret i to frekvensbånd, nemlig både for 2,4 GHz og 5 GHz. Formelt set er der kun tale om én samlet standard, men det er vigtigt at være opmærksom på, om konkret udstyr understøtter 802.11n på både 2,4 og 5 GHz, eller om det evt. kun er beregnet til 2,4 GHz, hvilket ofte er tilfældet for udstyr beregnet til hjemmebrug. Det er baggrunden for opdelingen i tabellen.

3.2.1 Bør vi satse på 802.11n?

Nye AP'er, der understøtter 802.11n på både 2,4 og 5 GHz, er naturligvis dyrere end ældre AP'er, der fx kun understøtter 802.11g på 2,4 GHz, men for merprisen får man et netværk med to væsentlige fordele:

- Væsentligt højere båndbredde. Når man sammenholder båndbredderne i tabel 1, er det tydeligt, at især 802.11n har betydet en væsentlig forøgelse af den effektive båndbredde. Der er omtrent en faktor 5 mellem hver af standarderne 802.11b > 802.11g > 802.11n (5 GHz). Et AP med 802.11n og to radioer (2,4 og 5 GHz) vil næsten 10-doble AP'ets båndbredde i forhold til et billigere AP med kun en radio og 802.11g.

³ Forbindelseshastigheden er hastigheden på det fysiske lag. Det er den samlede mængde bits, der kan overføres pr. sek. inkl. overhead.

⁴ Den maksimale effektive båndbredde angiver, hvilken båndbredde en enkelt bruger kan opnå på et trådløst netværk under helt optimale forhold. Brugeren skal være alene på nettet, tæt på AP'et, og der skal overføres store filer.

⁵ På et lille hjemmenetværk med et enkelt AP kan man også køre op til 300 Mbit/s på 2,4 GHz. På et større net med mange AP'er er det ikke muligt at køre med bundlede kanaler (40 MHz) på 2,4 GHz, da der ikke er et tilstrækkeligt antal ikke-overlappende kanaler. Derfor bliver hastigheden i praksis maks. 144 Mbit/s, som det er angivet.

3 Valg af arkitektur og teknologi

- Bedre stabilitet. 802.11n er udbygget med teknologier, der i væsentlig grad forøger stabiliteten og dermed mærkbart mindsker risikoen for at en klient mister forbindelsen.

For at kunne udnytte fordelene ved 802.11n er det selvfølgelig afgørende, at både netværk og klienter understøtter standarden. Og man kunne være af den opfattelse, at det ville være en årrække inden en så relativ ny standard ville være gængs i det udstyr, der ses på skolerne. I praksis viser det sig dog ikke at være tilfældet, forudsat at tallene i tabel 2 fra tilfældigt udvalgte skoler giver et retvisende billede.

Tabel 2 er baseret på talmateriale fra tre tilfældigt udvalgte skoler. I en periode fra 15. – 28. september 2010 er samtlige brugeres trådløse forbindelser registreret og fordelt over de fem standarder i tabellen.

Den første skole er et gymnasium med et lidt ældre net uden 802.11n. Her er hele 87 % af forbindelserne via den ældre og langsomme 802.11g-standard.

Den anden skole er ligeledes et gymnasium, men denne skole har et nyere net, der understøtter alle standarderne i tabellen. Som det fremgår, er brugernes udstyr i høj grad klar til at udnytte fordelene ved 802.11n: 41 % af forbindelserne er via 802.11n på 2,4 GHz og 19 % via 802.11n på 5 GHz. Samlet er hele 60 % af forbindelserne via 802.11n.

Den tredje skole er en efterskole ligeledes med et nyt net med 802.11n. Paratheden er stort set lige så udbredt på efterskolen som gymnasiet.

Trådløs standard	Maks. forbindelseshastighed i Mbit/s	Gymnasium 1 med a/b/g	Gymnasium 2 med a/b/g/n	Efterskole med a/b/g/n
802.11b	11 Mbit/s	0 %	0 %	0 %
802.11a	54 Mbit/s	13 %	9 %	6 %
802.11g	54 Mbit/s	87 %	31 %	37 %
802.11n (2,4)	144 Mbit/s	-	41 %	40 %
802.11n (5)	300 Mbit/s	-	19 %	17 %

Tabel 2. Statistik indsamlet over to uger i september 2010 fra tre tilfældigt udvalgte skoler. Statistikken viser, at eleverne har udstyr der er parat til at udnytte fordelene ved 802.11n-teknologi.

De to skoler med 802.11n opnår i øvrigt forbedringer for alle brugere. Brugere med nyt udstyr, der kan køre 802.11n vil opleve både hastigheds- og stabilitetsfordele og vil derfor hurtigere få afviklet deres trafik. Det betyder, at der bliver lidt mere tid til at håndtere trafik for brugere med lidt ældre udstyr med 802.11g.

Men skolerne kan reelt opnå endnu mere ved i højere grad at sikre, at brugerne har udstyr, der kan køre 802.11n på 5 GHz. Her er hastigheden højest, og hvis en større del af brugerne kører på 5 GHz, bliver der mere ledig kapacitet til ældre 802.11g-klienter på 2,4 GHz. Derfor er det vigtigt at orientere brugerne korrekt og informere dem om, at de med fordel kan medbringe udstyr, der kører 802.11n på 5 GHz.

Konklusionen er klar. Når der skal indkøbes nyt udstyr, skal det sikres, at AP'erne understøtter 802.11n på både 2,4 og 5 GHz.

UNI•C anbefaler:

- controllerbaseret arkitektur
- AP'er, der understøtter 802.11n på både 2,4 og 5 GHz.

4 Adgang til det trådløse netværk

Formålet med dette kapitel er at gennemgå de væsentligste sikkerhedsmæssige spørgsmål, der skal tages stilling til i forbindelse med etablering af et trådløst net.

4.1 Sikker login

Tidligere var det udbredt, at skolen stillede et mere eller mindre åbent net til rådighed. Alle, der var inden for det trådløse nets dækningsområde, kunne uden videre tilslutte sig, og alle kom på samme SSID⁶ med samme rettigheder.

Det helt grundlæggende problem ved det åbne net er den manglende validering af brugerne. Når der ikke afkræves login, kan alle, der opholder sig på eller i nærheden af skolen, uden videre benytte nettet, og skolen har derfor ingen kontrol med hvem, der anvender det. Endvidere betyder det manglende login, at det ikke er muligt at opsamle log af, hvem der har anvendt nettet, og skolen har dermed ingen mulighed for at henføre evt. misbrug til en navngiven person⁷.

Derfor bør man som hovedregel sikre, at det ikke er muligt at få adgang til nettet uden personligt login. Der findes adskillige loginmetoder med hver deres fordele og ulemper. Det er vigtigt at få valgt en metode, som sikrer, at brugerne oplever, at login sker gnidningsfrit og uden irritationsmomenter. Loginmetoden vælges primært afhængig af, om der er tale om elever og læreres personlige maskiner, eller om der er tale om skolens klassesæt, der benyttes af mange forskellige personer. Endelig kan der være behov for at tage særlige hensyn, hvis grundskolens yngste elever også skal kunne logge på.

Tabellen herunder indeholder en oversigt over de mest gængse sikkerheds løsninger til trådløse net. For hver løsning er angivet loginmetode, om der er kryptering eller ej, og i hvilken sammenhæng løsningen er mest velegnet.

⁶ SSID (Service Set identifier) er navnet på det trådløse net man kobler maskinen til.

⁷ Se i den forbindelse kapitel 11 om "Håndtering af sikkerhedsbrud" og kapitel 12 om "Lovgivning og myndighedskrav".

Sikkerhedsløsning		Login med	Kryptering	Velegnet til
MAC-filtrering		MAC-adresse	-	-
WEP		Delt nøgle	(v)	-
WPA2-PSK (WPA-PSK)		Delt nøgle	v	Klassesæt i skolens domæne
Captive portal / hotspot		Brugernavn + password	(v) kun login, ikke datatrafik	Gæster/ personlige maski- ner/ klassesæt uden for domæne
WPA2- Enterprise (WPA-Ent.)	PEAP- MSCHAPv2	Brugernavn + pass- word/maskinkonto i do- mænet	v	Personlige maski- ner / Klassesæt i skolens domæne
	EAP-TLS	Certifikat	v	Klassesæt i skolens domæne

Tabel 3. Skema, der viser en række karakteristika for de mest udbredte trådløse sikkerhedsløsninger.

Både MAC-filtrering og WEP er forældede løsninger, der ikke bør anvendes. MAC-filtrering er baseret på registrering af maskinernes MAC-adresser. Det er nemt at snyde med MAC-adresser og dermed opnå uautoriseret adgang, fordi der ingen kryptering er, og fordi det rent administrativt kan være en stor opgave at holde styr på mange maskiners MAC-adresser. Med hensyn til WEP er der tale om en løsning baseret på en fælles nøgle, og man opnår derfor ikke nogen individuel validering af brugerne. Derudover har WEP i mange år været anset som usikker, da der findes standardmetoder til at omgå krypteringen med. Hverken MAC-filtrering eller WEP-kryptering kan derfor anbefales.

WPA2-PSK (og den ældre WPA-PSK⁸) er ligesom WEP baseret på en delt nøgle (PSK står for Pre Shared Key) og giver derfor ingen individuel validering af brugerne. Alle brugere, der kender nøglen, vil kunne logge på uden at give sig personligt til kende. Desuden vil det være teknisk muligt at aflytte trafik til/fra andre brugere. Så på et netværk, hvor

⁸ WPA2 er afløseren for WPA. Den eneste grund til at anvende WPA skulle være, at man har noget gammelt udstyr, der ikke kan køre WPA2. I dag kan så godt som alt nyere udstyr (klienter og AP'er) køre WPA2, og derfor bør valget være let. Teknisk set er den primære forskel, at de to standarder er baseret på forskellige krypteringstyper. WPA2 er baseret på AES, hvor WPA er baseret på TKIP. Desuden er WPA2 forbedret på andre områder, så roaming-tiderne (den tid det tager at skifte fra et AP til et andet) er forbedret.

brugere medbringer personlige maskiner, er løsningen uegnet. Hvis skolen har et classesæt af maskiner, der er indmeldt i et domæne, kan WPA2-PSK derimod have en funktion. Hvis det kun er skolens it-ansvarlige, der kender nøglen, og det er den it-ansvarlige, der indtaster nøglen på skolens maskiner, vil det sikre, at ikke andre end skolens egne maskiner kan komme på nettet. Hvis maskinerne er sat op, så brugeren afkræves domænelogin for at logge på, er der via domænet kontrol med hvem, der har været på hvornår.

Captive portal er betegnelsen for en "hotspot"-funktion, hvor brugeren afkræves et login, første gang browseren startes. Nettet er som sådan åbent – alle kan få en IP-adresse – men man afkræves login via browseren, inden man får adgang til internet og evt. interne ressourcer. Det er umiddelbart en simpel og meget lettilgængelig løsning set fra et brugersynspunkt. Løsningen forudsætter ingen installation eller opsætning på maskinerne og er derfor særlig velegnet for gæster, der kun har behov for at logge på nettet enkelte gange. Løsningen kan også anvendes af skolens almindelige brugere – elever og lærere – men man skal være opmærksom på følgende ulemper:

- Brugere vil skulle logge på hver dag – og afhængig af opsætning mange gange i løbet af en dag, hvilket kan være generende
- Trafikken er ikke krypteret. Normalt sikrer captive portal-løsningen overførsel af selve login'et via https, men efterfølgende trafik er ikke krypteret
- Captive portal-funktionen kan ikke logge et ubegrænset antal brugere på samtidig. I forhold til alternative løsninger er det den løsning, der skalerer dårligst. Hvis man fx vil sikre, at flere hundrede elever kan logge på i løbet af et minut, er det vigtigt at afklare med leverandøren, om det er muligt via captive portal-funktionen.

Captive portal er som angivet i tabel 1 særligt velegnet til gæster. Desuden kan løsningen anbefales til at sikre login for elever og lærere, der medbringer egne maskiner, men med ovenstående kommentarer in mente. Endelig kan løsningen også anvendes, hvis skolen har et classesæt af maskiner, der ikke er indmeldt i et domæne. Her er det så vigtigt, at den valgte captive portal-funktion giver brugere mulighed for at logge af det trådløse net, inden maskinen overtages af en anden bruger.

WPA2-Enterprise (og den ældre WPA-Enterprise) er også kendt under betegnelsen WPA2-Radius. I modsætning til WPA2-PSK er sikkerheden her baseret på individuelt login, og der er ingen fælles nøgler. Det gør løsningen særdeles interessant i skolemæssig sammenhæng.

I forbindelse med WPA2-Enterprise er der flere forskellige login-metoder, hvoraf kun de to mest udbredte er medtaget i skemaet: PEAP-MSCHAPv2 og EAP-TLS.

PEAP-MSCHAPv2 er den mest interessante løsning. Her er login baseret på en Windows-konto – enten i form af en brugerkonto bestående af brugernavn + password eller i form af en maskinkonto, der automatisk findes på maskiner, der er indmeldt i skolens Windows-domæne.

Løsningen med brugernavn + password er særdeles velegnet, hvis skolens brugere medbringer private maskiner. Afhængigt af styresystem og platform – Windows, Linux, iPhone osv. – kan det være nødvendigt med opsætning på maskinen, inden man logger på, men det smarte er, at opsætning og login kun skal foretages første gang, der logges på. Oplysningerne gemmes efterfølgende på maskinen, som derfor automatisk kan logge brugeren på. Der opnås en meget sikker forbindelse, hvor al trafik er krypteret med individuelle nøgler.

Med maskinkonto er løsningen velegnet i forbindelse med klassesæt, der er indmeldt i skolens domæne. Maskinen logger sig på under opstart, og maskinen har derfor netværksforbindelse, så brugeren kan logge sig på domænet.

EAP-TLS forudsætter en PKI (Public Key Infrastructure), da valideringen udelukkende er baseret på certifikater. Det forudsættes derfor, at der er bruger- eller maskincertifikat installeret på de maskiner, hvorfra man skal logges på. I praksis betyder det, at løsningen kan være relevant for skoler, der kun har maskiner, der er indmeldt i skolens domæne. Det er de færreste, der har det, og løsningen vil derfor ikke blive omtalt yderligere i dette kapitel.

Som det fremgår af ovenstående diskussion, bør skoler, der satser på, at det er brugernes personlige maskiner, der skal på nettet, basere sig på captive portal og/eller WPA2-Enterprise med PEAP-MSCHAPv2.

I begge tilfælde er der behov for en RADIUS-server med adgang til skolens brugerdatabase. Spørgsmålet omkring brugerdatabase behandles yderligere i kapitel 5 om "Administration af brugere".

4.2 Segmentering

Foruden at sikre adgangen til nettet gennem personligt login, bør skolen segmentere nettet, så ikke alle trådløse brugere har samme rettigheder.

Måske er der interne ressourcer, som kun lærere skal have adgang til. Tilsvarende kan der være ressourcer, som eleverne må tilgå, men som udefrakommende gæster ikke bør have adgang til. Det kan fx være intranet og printere. Derfor bør man segmentere nettet, så der er et SSID til gæster og et andet SSID til lærere og elever. Foruden den netværksmæssige segmentering, giver det mulighed for at anvende forskellige sikkerhedsløsninger til de enkelte SSID'er. På den måde kan gæste-SSID'et anvende captive portal, mens elev/lærer-SSID'et fx anvender WPA2-Enterprise.

Når nettet segmenteres, sikrer man ligeledes, at et sikkerhedsbrud i form af virus, orm og lignende ikke har uhindret adgang til at sprede sig til alle maskiner på skolens net. Man får på den måde inddæmmet skaden og mindsket konsekvenserne, hvis det en dag går galt.

For at vurdere, hvilke SSID'er det er relevant at operere med, bør man først fastlægge, hvilke brugergrupper der har behov for at anvende skolens net. Typisk kan det være gæster, elever, lærere og evt. administration.

4 Adgang til det trådløse netværk

For hver gruppe fastlægges, hvilket VLAN brugerne i gruppen skal have adgang til. Ofte har skolen allerede et net til undervisning, hvor eleverne skal have adgang. Lærerne skal måske på samme VLAN eller på et separat VLAN. Gæster typisk på et nyoprettet VLAN.

Herefter besluttet det, hvordan brugerne skal knyttes til det korrekte VLAN. Der kan peges på to løsningsmuligheder:

- Det mest udbredte er entydigt at mappe hvert VLAN til et SSID, så SSID x peger på VLAN x, SSID y peger på VLAN y osv. Er brugerne placeret på samme RADIUS-server, kan udfordringen her være at sikre, at brugerne kun kan logge på det SSID, der er tiltænkt dem, så elever fx ikke logger på lærer-SSID'et.
- Alternativt kan man – såfremt ens controller understøtter det – lade registreringer i brugerdata-basen om brugerens type returnere til kontrollere via radius og på den måde placere brugeren i det korrekte VLAN. På den måde vil man kunne nøjes med et enkelt SSID og alligevel sikre, at brugerne segmenteres i forskellige VLAN.

Endelig skal der vælges en sikkerheds-løsning for hvert SSID. Det gøres ved at se på, hvilke maskiner der skal på SSID'et – personlige eller klassesæt – og så finde den mest fornuftige løsning for hvert SSID med udgangspunkt i diskussionen om "Sikker login" ovenfor.

Alle oplysningerne kan fx samles i et skema som vist i eksemplet nedenfor. Så er der et godt udgangspunkt for en efterfølgende dialog med en leverandør.

SSID	Skole-hotspot	Skole-net
VLAN	4	5/6
Anvendes af	Gæster og evt. elever	Elever/lærere
Personlige maskiner/ klassesæt	Personlige maskiner	Personlige maskiner
Brugerdatabase	UNI•Radius suppleret med lokal brugerdatabase på kontrollere	Active Directory
Sikkerheds-løsning	Captive portal	WPA2-Enterprise PEAP-MSCHAPv2

UNI•C anbefaler:

- Alle brugere logger på med individuelt login.
- Der benyttes SSID med captive portal til gæsternet.
- Der benyttes SSID med WPA2-Enterprise med PEAP-MSCHAPv2 til elever og læreres personlige maskiner.

5 Administration af brugere

En central anbefaling i kapitel 4 om "Adgang til det trådløse netværk" er, at alle, der skal på skolens trådløse net, bør logge på med personligt login. En forudsætning for at indføre dette er, at der er adgang til en brugerdatabase, hvor alle brugere er oprettet med brugernavn og password. I den forbindelse bør man overveje, hvilke brugertyper man har, hvordan rettighederne skal styres, og hvilken konkret brugerdatabase og RADIUS-server man vil basere sig på.

5.1 Brugertyper

Allerførst bør man identificere, hvilke brugertyper der er behov for at operere med. Hvis man ønsker mulighed for at differentiere en type af brugere i forhold til en anden – typisk sikkerhedsmæssigt i form af, hvilke rettigheder brugerne skal have – er det nødvendigt at behandle disse brugere som en særlig brugertype.

Typisk vil det være relevant at operere med en eller flere af følgende brugertyper:

- lærere
- elever
- gæster.

I særlige situationer kan det være på sin plads at anvende flere brugertyper som fx administration, kursister og klasser, men medmindre der er et reelt behov for det, kan det ikke anbefales, at operere med mere end 2-3 brugertyper, da opsætningen kompliceres, jo flere brugertyper der er.

5.2 Rettighedsstyring

5.2.1 Nettype / VLAN

Med hensyn til tildeling af rettigheder handler det primært om, hvilket netværk en given bruger skal placeres på. Afhængigt af det konkrete valg af trådløst udstyr kan der være flere metoder til at sikre en korrekt placering.

Standardmetoden, som alle professionelle systemer understøtter, er at mappe hvert net/VLAN til et SSID. Denne metode blev omtalt i kapitel 3. Princippet er at lade SSID x pege på VLAN x, SSID y pege på VLAN y osv. På den måde er der en entydig sammenhæng mellem et SSID og et VLAN.

Det kan være en udfordring at sikre, at en bruger kun kan logge på det SSID, som er tiltænkt vedkommende – eksempelvis at sikre, at elever kan logge på elev-SSID'et, men ikke lærer-SSID'et. Afhængigt af udstyr kan det være nødvendigt at have brugerne placeret på to forskellige RADIUS-servere, men normalt er det ikke hensigtsmæssigt.

En alternativ og mere elegant metode (til separate RADIUS-servere) er at lade registreringer i brugerdatabase om brugerens type (elev, lærer eller gæster) returnere til controlleren via RADIUS og benytte denne oplysning til at placere brugeren i det korrek-

te VLAN. Med denne metode bliver mappingen af SSID-til-VLAN en proformaregistrering – i praksis fastsættes den enkelte brugers VLAN-placering via brugertyperegistreringen i brugerdata-basen.

Ovenstående løsning vil typisk også begrænse behovet for SSID'er. Et SSID for hver ønsket sikkerhedsmodel vil være tilstrækkeligt, fx:

- SSID 1 med WPA2-Enterprise PEAP-MSCHAPv2 til skolens interne brugere. RADIUS-serveren sikrer så, at lærere fx placeres i ét VLAN og elever i et andet VLAN
- SSID2 med captive portal til gæster.

Det skal understreges, at det ikke er alt udstyr, der understøtter denne teknologi, og at der i øvrigt kan være forskellige måder at understøtte den på. Det vil derfor være nødvendigt med en teknisk vurdering for at afgøre, hvilket udstyr der kan opfylde skolens konkrete ønsker.

5.2.2 Tidsstyring

Kostskoler kan fx have et ønske om tidsstyrede rettigheder, der giver mulighed for at lukke for det trådløse net i nattetimerne. Mere avancerede regler, der fx begrænser elevernes adgang til udvalgte tjenester i undervisningstiden, kan også være ønskelige.

De tidsstyrede rettigheder kan implementeres flere forskellige steder i skolens net. En mulighed er helt at droppe brugernes trådløse forbindelse i udvalgte tidsrum. Det kan gøres på to forskellige metoder:

- Hvis RADIUS-serveren understøtter tidsskemaer, er det muligt helt at udelukke brugerne fra at logge på nettet i de ønskede tidsrum. Det skal så sikres, at brugere, der allerede er på nettet, får forbindelsen nedlagt relativt hurtigt herefter. Hvis der benyttes WPA2-Enterprise, kan det let sikres ved at sætte "reauthentication time" lavt, fx til fem minutter. Med captive portal er der desværre ikke tilsvarende muligheder.
- Hvis controlleren understøtter et "rolle"-begreb, kan der være mulighed for at definere et regelsæt for udvalgte brugertyper – fx at elever ikke har nogen forbindelse i nattetimerne. Denne metode er mere generel og vil derfor være at foretrække i forhold til den førstnævnte, men det er langt fra alle controllere, der understøtter mulighed for "rolle"-styring.

Hvis der ikke kan findes en tilfredsstillende løsning ved hjælp af ovenstående muligheder, findes andre udmærkede alternativer. Fælles for dem er, at de er baseret på styring af rettigheder via IP-adresser, og de forudsætter derfor, at der er styr på, hvilke IP-adresser de enkelte brugertyper får tildelt.

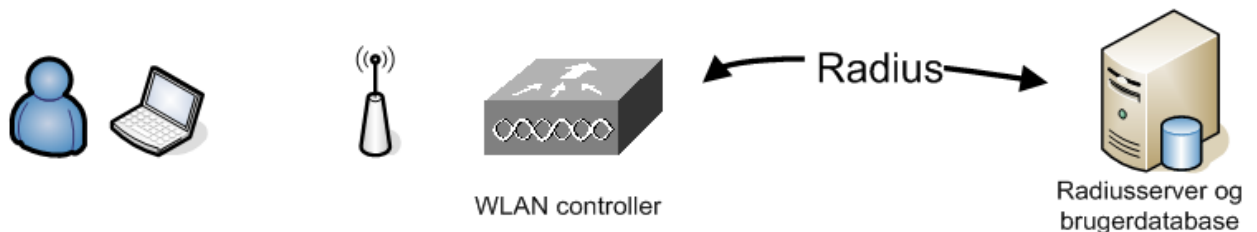
En mulighed er at lade skolens router lukke for netforbindelsen for de IP-adresser, som eleverne er tildelt på de ønskede tidspunkter. Det er enkelt, hvis eleverne er på et separat VLAN og dermed har IP-adresser i et veldefineret subnet. Hvis elever og lærere er i samme VLAN og subnet, kan man lade eleverne få IP-adresser fra en pulje af IP-adresser,

mens lærernes maskiner tildeles faste IP-adresser – også via DHCP – men baseret på mapning af den enkelte maskines MAC-adresse til en fast IP-adresse. Ikke alle routere understøtter tidsstyrede rettigheder (accesslister), men rigtig mange skoler har en Cisco-router, som tilbyder denne mulighed. Ulempen er, at der skal holdes styr på MAC-adresserne, og at det vil være muligt at omgå denne løsning ved at ”spoofe” en lærers MAC-adresse.

Såfremt skolen har en UNI•Gateway eller tilsvarende boks, er det på samme måde muligt at oprette tidsstyrede regler baseret på, hvilke IP-adresser elever og lærere har. Princippet er helt det samme, reglerne implementeres blot i en anden enhed.

5.3 RADIUS-server og brugerdatabase

Når en bruger logger på det trådløse net, sker brugervalideringen ved, at controlleren kommunikerer med en RADIUS-server som illustreret på figur 1.



Figur 2. Validering af brugere på et trådløst net sker via RADIUS.

Der er tekniske forskelle på, om der logges på et SSID beskyttet med captive portal, eller om det er med WPA2-Enterprise, men grundlæggende set skal der være adgang til en RADIUS-server, der igen har adgang til selve brugerdatabase. Ofte vil RADIUS-server og brugerdatabase ligge på samme server, men det behøver ikke at være tilfældet.

I praksis har en skole to muligheder, når den skal vælge RADIUS-server og brugerdatabase: en lokal løsning, som skolen selv driver, eller en central løsning drevet af UNI•C.

5.3.1 Lokal løsning

Mange skoler har i dag en Windows-server med et Active Directory (AD), hvor brugerne er oprettet. Hvis skolen ønsker, at denne brugerdatabase fremover skal danne grundlag for login på skolens trådløse net, skal der blot installeres en RADIUS-server med adgang til brugerdatabase. Microsoft leverer en RADIUS-server med deres servere, der umiddelbart kan installeres uden udgifter til separat licens. Hvis der er tale om en Windows 2003 Server hedder RADIUS-serveren ”Internet Authentication Service” (IAS), mens den i forbindelse med Windows 2008 Server er omdøbt til ”Network Policy Server”.

Selve opgaven med installation, konfiguration og drift af RADIUS-serveren ligger uden for formålet med dette kapitel. De fleste skoler vil have behov for ekstern konsulentassistance i forbindelse med etableringen.

5.3.2 Central løsning

Alternativt kan skolen basere sig på ”UNI•Radius”, der er en central RADIUS-server drevet af UNI•C. Med UNI•Radius logger brugerne på med deres UNI•Login.

Der er fordele og ulemper ved denne løsning. Umiddelbart er den primære fordel, at skolen ikke selv er ansvarlig for drift og opsætning af serveren, sikring af logning mv. Det står UNI•C for. Derudover kan der ligge et strategisk valg i at basere sig på en RADIUS-server ”i skyen”, for efterhånden mindskes behovet for et lokalt AD med alt, hvad det indebærer af administration i forhold til drift af serveren. Mange steder er der ikke længere behov for private mapper til elever og lærere – de gemmer det ”i skyen” eller på private laptops. Og med brugerdatabase og RADIUS-server ”i skyen” er de første skoler rundt omkring begyndt at nedlægge det lokale AD. Der er ikke længere behov for det. Endelig er der med UNI•Radius mulighed for at tillade, at andre brugere med UNI•Login kan få adgang til skolens net. Det kan være en nem måde at håndtere en del af skolens gæster på.

Ulempen ved den centrale løsning er den begrænsede fleksibilitet. Man kan ikke umiddelbart tilføje en funktion, man synes kunne være relevant. Fx kan UNI•Radius kun benyttes til SSID’er med captive portal og/eller WPA2-Enterprise PEAP-MSCHAPv2 sikkerhed. Løsningen er dermed målrettet skoler, hvor brugerne kommer med egne laptops og smartphones.

5.4 Gæster på skolens trådløse net

Ofte er der et ønske om at kunne give gæster adgang til internettet via skolens trådløse net. Det kan fx være leverandører, forældre, vikarer og andre, der ikke skal have adgang til skolens interne net, men blot have internetforbindelse.

Gæster skal typisk kun på nettet nogle enkelte gange, og derfor er det vigtigt, at det er så nemt at gå til som muligt både for skolens brugere og for gæsterne. Samtidig skal det sikres, at der stadig er kontrol med, hvem der har været på nettet.

Det anbefales, at gæster får adgang via et SSID med captive portal-sikkerhed, altså et ”hotspot”, hvor brugeren bliver promptet for brugernavn og password, når browseren startes. Det giver en simpel adgang for gæsten og sikrer samtidig den nødvendige adgangskontrol.

Men hensyn til administration af login (brugernavn + password) til gæster, kan der peges på forskellige løsningsmuligheder.

5.4.1 Lobbyfunktion

Det er muligt at operere med en slags ”lobbyfunktion”. Lobbyfunktionen giver en eller flere medarbejdere – typisk en receptionist eller sekretær – mulighed for at udlevere et login til gæsten, når denne besøger skolen. Løsningen kan laves på flere måder:

- Midlertidig oprettelse af brugeren i controllerens lokale brugerdatabase: Nogle controllere giver mulighed for, at lobbyfunktionen nemt kan oprette et midlertidigt login til de gæster, der besøger skolen. En sekretær eller receptionist har adgang til at oprette et login, der fx virker et eller flere døgn.

- Forud oprettede brugere i controllerens lokale brugerdatabase:
Alternativt kan skolen forud oprette et antal gæstekonti i controllerens lokale brugerdatabase. Disse kan så benyttes en ad gangen, men det kræver lidt mere administration at holde styr på, hvilke konti der har været i brug, og sørge for at få dem deaktiveret eller nedlagt igen.

Fælles for begge løsningsmuligheder er, at skolen bør registrere gæstens navn og adresse og gøre vedkommende bekendt med skolens anvendelsespolitik. Gæsten kan fx udfylde og underskrive en formular, der samtidig indeholder information om, hvilket login vedkommende har haft, og i hvilket tidsrum det har været aktivt.

Ovenstående kan evt. også fungere i kombination med UNI•Radius, så gæster med UNI•Login kan logge ind med deres UNI•Login, og det derved kun er gæster uden UNI•Login, der skal håndteres af lobbyfunktionen.

5.4.2 Sponsor-funktion

Som alternativ kan man overveje at benytte en "sponsor"-løsning, hvor skolens eksisterende brugere giver netadgang til deres gæster. De virker på den måde som "sponsorer" for deres gæster.

Det er det mest optimale, hvis løsningen giver mulighed for, at eksisterende brugere direkte kan oprette gæstekonti. På den måde er der en entydig identifikation af gæster og af hvem, der har været sponsor for hver enkelt gæst.

Alternativt kan man lade eksisterende brugere logge ind på et gæstenet fra gæstens laptop. Man bør aldrig oplyse brugernavn og password til en gæst. Ulempen er, at man ikke på samme måde kan skelne, hvis der er flere gæster, og det kan være nødvendigt at logge ind for gæsten flere gange i løbet af samme dag.

UNI•C anbefaler, at skolen

- opererer med to-tre brugertyper, hvoraf en er gæster
- bruger to SSID'er, hvilket normalt er tilstrækkeligt: et SSID med captive portal-sikkerhed og en SSID med WPA2-Enterprise
- nøje overvejer, om det optimale er en lokal eller en central RADIUS-server
- indtænker en løsning til gæster fra start.

6 Private enheder på skolens trådløse net

De senere år har man set en udvikling, hvor elever og lærere i stigende omfang er begyndt at medbringe private enheder i skolesammenhæng. Der er et generelt ønske om, at disse enheder skal kunne inddrages og benyttes af den enkelte i en undervisningsmæssig sammenhæng og derfor skal kunne komme på internettet via skolens trådløse netværk⁹.

Mange forventer, at udviklingen vil accelerere yderligere de kommende år. Der vil for det første komme flere og flere trådløse enheder – foruden laptops vil man se smartphones og håndholdte computere som iPads og tilsvarende – og man vil samtidig se en udvikling, hvor det i endnu højere grad bliver elever og studerende selv, der medbringer udstyret.

Der vil selvfølgelig være forskelle mellem skoleformerne, men classesættene ser ud til at være på retur, og den situation, vi i dag ser på fx gymnasier og efterskoler, hvor så godt som alle elever medbringer privat udstyr, må forventes at brede sig til de øvrige skoleformer.

6.1 Typer af enheder

I dag er det primært laptops, der medbringes og skal på skolens WLAN, men fremover må det forventes, at også smartphones og ikke mindst håndholdte computere som iPads og tilsvarende vil finde indpas. Og den udvikling har betydning for opsætningen af det trådløse net, både hvad angår valg af loginmetode og sikring af nødvendig dækning.

6.1.1 Valg af loginmetode

Laptops er karakteriseret ved at have et fysisk tastatur, hvorimod man på smartphones og håndholdte computere normalt må nøjes med "taster" på en trykfølsom skærm. Det betyder, at skrivehastigheden er betydeligt lavere på disse enheder, og derfor bør man vælge en loginmetode til det trådløse net, der ikke afkræver brugeren et login (bruger navn + password) ret ofte.

En captive portal-funktion (hotspot) kan betyde, at brugeren skal logge ind mange gange i løbet af en dag, og den er derfor ikke velegnet, fordi det vil genere brugeren unødigt. Med WPA2-Enterprise PEAP-MSCHAPv2 skal brugeren kun indtaste login-oplysninger første gang, der logges på, hvorefter login'et gemmes på enheden, og der efterfølgende kan logges ind automatisk uden indtastning fra brugerens side. Denne metode er derfor

⁹ Det fremgår af "Arbejdsprogram for Undervisningsministeriets koncern 2010" at "Elever og lærere skal kunne studere, arbejde og kommunikere uafhængigt af tid og sted. Det indebærer, at "håndholdte" teknologier som den bærbare pc, mp3-afspilleren, digitalkameraet og mobiltelefonen skal inddrages som en naturlig del af undervisningen". Det er givet, at i hvert fald nogle af de omtalte enheder – herunder laptops og mobiltelefon – ofte er private enheder, der skal på skolens trådløse net.

langt mere velegnet. Der henvises i den forbindelse til kapitel 4 om "Adgang til det trådløse netværk", hvor de forskellige loginmetoder er behandlet i detaljer.

6.1.2 Øgede krav til dækning

Foruden det rent praktiske problem med login stiller de nye meget mobile enheder typisk også større krav til dækningen. En laptop benyttes siddende, og derfor er det normalt ikke noget problem, hvis der er ringe dækning i gangarealer, mellem bygninger og i områder af skolen, hvor det ikke er oplagt at sidde og arbejde med en laptop. Smartphones og håndholdte computere er derimod ikke bundet til at blive benyttet siddende. De kan benyttes stående, og mens man bevæger sig rundt på skolen. Derfor vil en stigende anvendelse af disse enheder øge kravet til dækningen i hele skolens område.

6.2 Generelle sikkerhedsovervejelser og tiltag

Inden de private enheder får adgang til skolens trådløse net, er der en række sikkerhedsrelaterede ting, der bør være på plads.

6.2.1 Ikke i skolens domæne

For det første skal enhederne ikke meldes ind i skolens domæne. Brugere skal blot autentificeres på det trådløse net og have internetforbindelse og evt. adgang til udvalgte lokale ressourcer som print og fil.

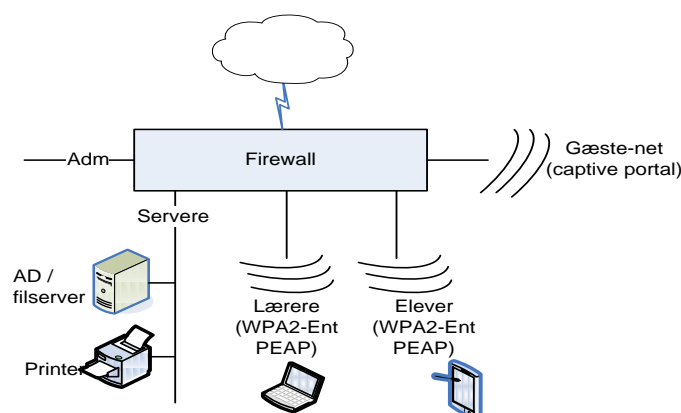
6.2.2 Personligt login og WPA2-Enterprise

Som anbefalet i kapitel 4 om "Adgang til det trådløse netværk" bør alle brugere afkræves personligt login, inden de får adgang til skolens WLAN. Når det drejer sig om private enheder, bør skolen vælge WPA2-Enterprise PEAP-MSCHAPv2 som omtalt ovenfor.

6.2.3 Segmentering

Enhederne – det være sig laptops, smartphones eller andet – må nødvendigvis betragtes som usikre. Skolen har ingen kontrol med maskinerne, de benyttes ofte fra forskellige mere eller mindre usikre net (privat, i byen, offentlige net), og der er ingen kontrol med, om enhederne er opdaterede – hverken i forhold til sikkerhedsrettelser, antivirusprogram eller tilsvarende. Skolen er derfor nødt til at opfatte dem som usikre og bør sikre skolens net og øvrige ressourcer mod en inficeret privat enhed.

Private enheder bør derfor ikke tilsluttes samme net/VLAN som skolens interne ressourcer. Figur 1 illustrerer, hvordan det fx kan designes. Skolens administrative net er et helt separat net. Undervisningsmæssige servere, herunder AD, fil og print er tilsluttet et selvstændigt net, mens alle private trådløse enheder er opdelt på 2-3 net – et til elever, et til lærere og evt. et til gæster. Denne segmentering er med til at inddæmme konsekvenserne af en inficeret maskine. En elevmaskine, der fx er inficeret med en orm, vil på den måde ikke have uhindret adgang til at inficere skolens servere og klienter på andre net.



Figur 3. Eksempel på opdeling i net.

På sigt kan man se en situation, hvor skolen ikke længere driver AD, filserver og tilsvarende lokalt. Disse tjenester er erstattet af tilsvarende i skyen. I den situation vil behovet for segmentering blive minimeret og evt. helt forsvinde.

6.2.4 Central firewall

Som illustreret på figur 3 bør skolen selvfølgelig sikre, at også private trådløse enheder er beskyttet af skolens centrale firewall. Firewallen skal sikre, at enhederne ikke er frit tilgængelige i forhold til ormeangreb og lignende fra internettet.

Det er derudover også meget relevant at se på andre former for filtrering og prioritering af trafik for at sikre en stabil og sikker afvikling af trafik på skolens trådløse net. Spørgsmålet behandles i detaljer i kapitel 11 "Drift og overvågning".

6.2.5 Sikring af den private enhed

Selvom det er svært at kontrollere, bør der også stilles krav til brugerne omkring sikring af enheden, herunder at enheden løbende bliver opdateret, når der er sikkerhedsrettelser tilgængelige, og desuden at der anvendes opdateret antivirus-software og evt. personlig firewall. Kravene kan passende indgå som led i skolens anvendelsespolitik.

6.2.6 Anvendelsespolitik som brugerne er bekendt med

Det vigtigste tiltag er ikke af teknisk art. Det er således afgørende, at skolen udformer en anvendelsespolitik, som brugerne informeres om og accepterer. Anvendelsespolitikken fastlægger bl.a., hvordan brugerne må benytte nettet, hvordan man gebærder sig på nettet, og hvad man især skal holde sig fra. I den forbindelse henvises til kapitel 12 om "Håndtering af sikkerhedsbrud", hvor der også findes et konkret eksempel på en anvendelsespolitik, man kan lade sig inspirere af.

6.3 Adgang til lokale ressourcer

6.3.1 Adgang til fildrev

Anvendelsen af de lokale filservere har i flere år været for nedadgående. Ulempen er nemlig, at dokumenter på skolens filserver ofte kun er tilgængelige, når brugerne er på skolens net, og måske endda kun, når de benytter skolens maskiner. Brugere efterspørger mobilitet. Dokumenterne skal være tilgængelige fra en vilkårlig maskine, uanset om man er på skolen, hjemme eller et helt tredje sted.

Hidtil har mange løst problemet ved at opbevare dokumenterne på USB-nøgler, der er nemme at have med rundt. De kan samtidig udgøre en backup-funktion. De senere år er der imidlertid sket flere ting, der har muliggjort, at dokumenterne fremover kan placeres "i skyen". For det første er der stort set internetforbindelse, uanset hvor man opholder sig, og for det andet er båndbredderne samtidig øget. På den måde kan man få adgang til dokumenter og filer, næsten uanset hvor man er, og hvilken enhed der er tilgængelig.

I en periode har det været udbredt at maile dokumenter til sig selv og på den måde bruge internettet til transmission og mailservere til opbevaring af filer. Den løsning er imidlertid ikke praktisk, og man ser nu adskillige tilbud om noget, der ligner "fildrev i skyen". Eksempler herpå er tjenester som Dropbox, SugarSync, Microsoft SkyDrive og til dels Google Docs.

Når dokumenter sendes over internettet og opbevares i skyen, er der flere sikkerhedsmæssige overvejelser, der bør gøres: For det første, om dokumenterne indeholder følsomme eller fortrolige persondata og dermed er omfattet af krav fra Datatilsynet til bl.a. kryptering og passende sikkerhedsforanstaltninger omkring autentifikation. For det andet bør man for sin egen skyld sikre sig, at adgangen til data er sikret med et fornuftigt/sikkert password, og at de evt. kan overføres krypteret.

Hvis skolen ønsker at dele filer via en lokal filserver, bør brugerne mappe det/de nødvendige drev direkte. Brugerens laptop skal ikke meldes ind i skolens domæne, og mapping via login-scripts er derfor ikke en mulighed.

6.3.2 Adgang til print

Brugere kan få adgang til print på flere måder.

Traditionelt er printerne delt på nettet via skolens Windows-server. Brugere printer til en printkø på serveren, der efterfølgende sender jobbet til printer. Den løsning giver mulighed for rettighedsstyring (hvem må printe hvor), kvotestyring (hvor mange sider må der printes og evt. mod betaling) og udlevering af den relevante printerdriver til klienten.

Nogle skoler har på det seneste valgt at nedlægge de lokale servere. Man har vurderet, at fordelene ikke stod mål med de ressourcer, der blev brugt på drift og vedligehold. I stedet har man stillet et mindre antal netværksprintere til rådighed for brugerne. Brugere printer så direkte til den enkelte printer. Ulempen er her, at der ikke er mulighed for rettigheds- og kvotestyring.

Fremover må det forventes, at også print afleveres "i skyen". Eksempelvis har firmaet HP lanceret "HP ePrint", hvor man fx kan få et dokument printet ved at maile det til printe-

6 Private enheder på skolens trådløse net

rens e-mail-adresse. Google barsler med "Google Cloud Print", og man må forvente, at andre leverandører også kommer med tilsvarende løsninger.

UNI•C anbefaler, at skolen

- bruger login-metoden WPA2-Enterprise PEAP-MSCHAPv2 til private enheder
- får foretaget segmentering, hvis skolen har lokale undervisningsservere
- informerer brugerne om skolens anvendelsespolitik og får dem til at acceptere politikken, der også indbefatter, at den private enhed løbende opdateres og i videst muligt omfang beskyttes med opdateret antivirus.

7 Installation og opsætning

Der er en række forskellige arbejdsopgaver i forbindelse med opsætningen af et trådløst net. En del af opgaverne handler om konfiguration. Det trådløse udstyr – typisk controlleren – skal konfigureres, en RADIUS-server skal installeres og konfigureres, og hvis skolen samtidig får nye switche, skal disse også konfigureres. Konfigurationsopgaverne bør normalt udføres af en ekstern konsulent, der er specialist på området. Der er mange parametre at skrue på, og hvis man selv kaster sig ud i det, er der en forøget risiko for, at man efterfølgende står med et ikke-optimalt konfigureret net samt en række andre problemer.

En anden opgave, leverandøren bør medvirke til, er at udpege de steder, hvor AP'erne skal sættes op, for at sikre den bedste og mest stabile dækning. I den forbindelse kan det være fint at få udført et egentligt site survey, hvor leverandøren med måleudstyr sikrer dækningen, men efterhånden er der – særligt i et skolemiljø med mange brugere og krav om høj båndbredde – behov for, at AP'erne sidder tæt. Derfor er selve dækningen sjældent et problem, hvorfor man kan overveje at spare udgifterne til en dedikeret site survey og i stedet blot få leverandøren til at udpege, hvor AP'erne bør placeres (fx midt på loftet uden større metalgenstande i umiddelbar nærhed). Som tommelfingerregel bør der sættes omkring et AP op i hvert klasselokale, hvis man vil være sikker på, at der er båndbredde nok. I store fælleslokaler skal der naturligvis sættes flere op.

Når leverandøren har udpeget den optimale placering af AP'erne, er der også nogle mere praktisk orienterede opgaver. AP'erne skal fysisk monteres, og der skal kables til de pågældende steder. Disse opgaver kan skolen med fordel overveje selv at stå for. Fx via skolens pedel eller ved hjælp af skolens elektriker, der begge må forventes at have et godt kendskab til skolens bygninger og mulige føringsveje.

7.1 Netforbindelse til AP'er

Et trådløst net vil aldrig blive hurtigere eller bedre end det kablede net, det er baseret på. Derfor bør man som led i etablering af det trådløse net gennemgå og vurdere, om det kablede net, herunder også de eksisterende switche, er af tilstrækkelig god kvalitet både kapacitets- og stabilitetsmæssigt. Alternativt risikerer man at stå med et trådløst net, der i sig selv er i orden, men som man ikke får det fulde udbytte af, fordi det bagvedliggende net er for ringe.

Det anbefales, at hele det kablede netværk gennemgås som led i etablering af det trådløse netværk. Det er kun de færreste, der i forvejen har et præcist overblik over det eksisterende switchudstyr, ledige switchporte, og hvordan switchene er forbundet indbyrdes. Man bør så starte med at danne sig et overblik: hvilke krydsfelter er der, hvilke switche består de af, og hvordan er de forbundne. Man kan skitsere krydsfelter, switche og indbyrdes forbindelser på en topologitegning. Det vil i sig selv være et godt udgangspunkt den dag, der kommer en potentiel leverandør på besøg. Leverandøren kan hurtig-

gere skabe sig et overblik og vurdere, i hvilket omfang det eksisterende net kan genbruges, bør suppleres eller helt udskiftes.

Hvis man føler sig klædt på til at indsamle yderligere information om nettet, vil følgende oplysninger være relevante og hjælpe leverandøren yderligere på vej:

- producentnavn og modelnr. på switche
- antal FE- og GE-porte pr. switch
- antal ledige FE- og GE-porte i hver switch
- uplink-hastighed pr. switch
- kabling til access-porte – hvilken kategori?
- kabling til uplink-porte – kobber eller fiber? Hvilken kategori/standard?
- antal porte med PoE (Power over Ethernet).

Ovenstående oplysninger kan med fordel samles i en tabel for at lette overblikket.

7.1.1 Switche

Der vil ofte være behov for at tilføje og/eller udskifte switche i forbindelse med etableringen, men hvilke kriterier bør lægges til grund for en udskiftning?

Hvis der er tale om billige og ældre switche, som er uden gigabit-uplink og af tvivlsom kvalitet, bør de under alle omstændigheder udskiftes.

Derudover er der antallet af porte. Når der er et overblik over, hvor mange AP'er der skal kables til de enkelte krydsfelter, kan man vurdere, om der er et tilstrækkeligt antal ledige porte. Hvis det ikke er tilfældet, kan man enten supplere med en ekstra switch eller udskifte til en nyere model med flere porte. Ofte vil en udskiftning være at foretrække for at simplificere nettet og få udfaset ældre udstyr.

Porthastigheden er yderligere en parameter. Hovedparten af alle eksisterende switche er med 100 Mbit-porte, og man skal være opmærksom på, at 100 Mbit/s i enkelte situationer kan være en flaskehals for trafik til/fra AP'et. Et moderne 802.11n-AP med to radioer (2,4 GHz og 5 GHz) kan i peak sende eller modtage med over 200 Mbit/s. Derfor kan det – afhængig af skolens ønsker og behov – være relevant med Gbit-porte til AP'erne. Men det er også vigtigt at gøre sig klart, at hvis hovedparten af skolens trafik sendes over en internetforbindelse på fx 50 eller 100 Mbit/s, er det irrelevant, da selve internetforbindelsen i sig selv vil udgøre en samlet flaskehals for alle AP'er.

Uplink-porte, der benyttes til at forbinde switchene indbyrdes, bør under alle omstændigheder være Gbit-porte. Ellers er der risiko for, at intern trafik på skolens net – fx mellem to elevmaskiner – vil belaste uplink uhensigtsmæssigt og på den måde genere trafikafviklingen.

Sidst, men ikke mindst er der spørgsmålet om PoE-porte, der giver mulighed for at strømføde AP'erne via netkablet. Som det fremgår nedenfor, er der så væsentlige fordele ved PoE, at det alene kan give anledning til at investere i nye switche.

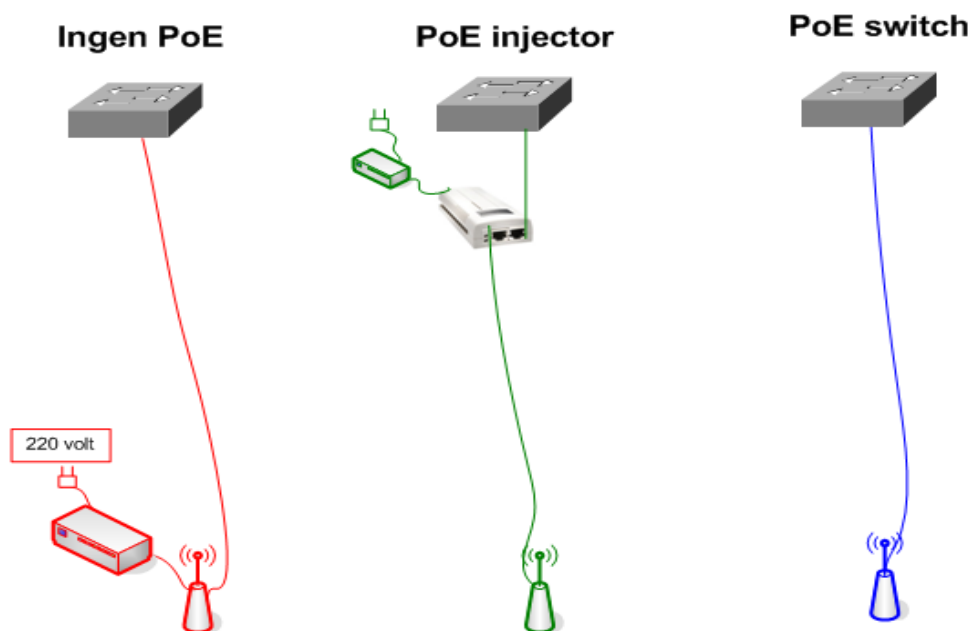
7.1.2 Kabling

I det omfang, der skal kables til AP'erne, bør der minimum anvendes cat6 (kategori 6) PDS-kabel. Denne kabeltype er velegnet til gigabit-transmission og må derfor forventes at være fremtidssikret et godt stykke tid.

7.2 Strøm til AP'er

Foruden netforbindelse skal hvert AP have strøm. Det kan ske via separat 220 volt strømforsyning ved hvert AP, alternativt via PoE, der som nævnt ovenfor strømføder AP'et via netkablet.

PoE kan i praksis leveres på to måder – enten i form af én PoE injector pr. AP eller via PoE-switcher, der kan strømføde mange AP'er samtidigt. De tre muligheder er illustreret på figuren.



7.2.1 Strømforsyning/uden PoE

Der er flere årsager til, at man ikke bør satse på modellen med separat strømforsyning til hvert AP. Den model forudsætter 220 volt i nærheden af hvert AP, og det vil der stort set aldrig være i forvejen. AP'erne vil nemlig normalt skulle placeres midt på et loft eller højt på en væg, og det bliver forholdsmæssigt dyrt, hvis en elektriker skal etablere 220 volt stik alle disse steder. Endelig kan man komme ud for, at et AP eller to efter en indkø-ringsperiode skal flyttes lidt for at optimere dækningen. Så derfor bør man satse på en PoE-løsning i stedet.

7.2.2 PoE-injector

En PoE-injector kan strømføde et enkelt AP, og hver PoE-injector strømfødes igen via en strømforsyning som illustreret på figuren. Både strømforsyning og injector placeres i krydsfeltet, og det er oplagt, at det kan blive til mange ledninger og stik, hvis adskillige AP'er skal strømfødes fra samme krydsfelt. Derfor er injector-løsningen mest velegnet i krydsfelter, hvor der kun skal tilsluttes 1-2 AP'er og ikke allerede er en PoE-switch.

7.2.3 PoE-switch

Switche med PoE er den optimale løsning. Switchporten leverer både netforbindelse og strøm til AP'et og man undgår strømforsyning og PoE-injector til hvert AP. Man bør derfor altid vælge switche med PoE, hvis der alligevel skal købes nye switche, og PoE-funktionen bør i sig selv være tilstrækkeligt til, at der investeres i nye switche især til krydsfelter, hvor der skal tilsluttes mere end to-tre AP'er.

Man skal være opmærksom på, at der findes flere PoE-standarder. Den mest udbredte er 802.3af, der kan levere op til 15,4 watt pr. port.

I et krævende skolemiljø kan det ikke anbefales at investere i de helt billige switche. De er primært velegnet til små kontorer og hjemmebrug.

7.3 PoE og grøn it

Nogle nye PoE-switche giver mulighed for at tænde og slukke for PoE-portene, og dermed for de tilsluttede AP'er, på udvalgte tidspunkter. Derfor er der mulighed for at spare på strømregningen og få en lidt grønnere profil, hvis man fx accepterer, at det trådløse net kun er tændt i undervisningstiden. Et par konkrete beregninger kan anskueliggøre besparelsesmulighederne:

- Hvis WLAN'et er slukket alle dage fra kl. 16.00 - 08.00, opnår man en besparelse på 67 %.
- Hvis WLAN'et desuden er slukket helt i weekender, opnår man en samlet besparelse på 76 %.
- Hvis WLAN'et derudover også slukkes i 12 ferieuger, kan man opnå en samlet besparelse på 82 %.

Hvis et AP fx trækker 15 watt, koster det ca. 263 kr. om året i drift ved en kilowatttime pris på 2 kr. Afhængig af hvor meget AP'et holdes slukket, vil det være muligt at opnå en besparelse på omkring 200 kr./AP/år. På en skole med 25-50 AP'er løber det dermed samlet op i 5.000-10.000 kr. årligt.

UNI•C anbefaler, at

- AP'er strømfødes via PoE (Power over Ethernet)
- ældre og billige switche udskiftes med nye switche med PoE og evt. gigabit
- der benyttes gigabit på uplink mellem krydsfelter.

8 Økonomi og rådgivning

Etablering af trådløse netværk er hverken let eller billig. Der er mange tekniske parametre at tage hensyn til – og der er flere følgeudgifter, som man måske ikke tænker på i første omgang. Af flere årsager bør man kunne afskrive investeringen inden for en kort årrække og erkende, at der ikke i forbindelse med etableringen bliver tale om en drifts- eller anlægsbesparelse på det eksisterende kablede net. Hvis man ikke har en decideret it-afdeling med den nødvendige kompetence, er den bedste fremgangsmåde derfor et parløb med en uvildig rådgivningskonsulent.

8.1 Supplement eller alternativ

Et trådløst net vil fremover være det primære net, som brugerne tilsluttes. Det er dog ikke en erstatning for det gamle kablede net, da der i en overskuelig årrække fortsat vil være et kablet net, der forbinder servere, AP'er, routere, printere mv. på skolerne. Trådløse net er derfor en merudgift, som let kan løbe op i en kvart million kroner eller mere i etablering, hvis man på en almindelig skole skal have et net, der fra bunden er etableret som state-of-the-art. Der er langt billigere trådløse netværk, fx dem man kender fra sin egen trådløse hjemmeopkobling. Men på skolerne er der tale om mange samtidige brugere, store arealer, der skal dækkes, krav om en sikker og stabil drift, og ikke mindst krav om, at fejl og misbrug let skal kunne spores – hvilket alt sammen kræver en professionel installation.

8.2 De kendte og de skjulte udgifter

Som beskrevet tidligere vil en gennemsnitsskole typisk have brug for ca. 25 AP'er styret af en controller. Der er forskellige fabrikater at vælge imellem og dermed også lidt forskel på priserne, men typisk vil udstyrsprisen for controller og AP'er være 125-150.000 kr. ved \$-kurs 5,6.

Dertil kommer installation og konfiguration. Som nævnt i 7 "Installation og opsætning", kan placering af AP'erne kræve et site survey, som næppe fås under 30.000 kr. Hertil kommer selve installationen, konfigurationen og evt. følgeudgifter. Ofte vil der være udgifter i forbindelse med opgradering af det eksisterende kablede net (nye switche, nye kabler o.l.), udgifter til kabelfremføring (kabelbakker, murgennemføringer o.l.) og udgifter til elforsyning (stikkontakter, PoE-injectors o.l.). Alene etablering af en 220 V's stikkontakt fås sjældent under 2-3.000 kr.

8.3 Hvordan køber man et trådløst netværk

Delene til et trådløst net kan købes mange steder og er endvidere med i SKI-aftalerne for visse kombinationers vedkommende. SKI-aftalerne er derfor et godt udgangspunkt, men det er ikke sikkert, at de dækker lige præcist de behov, skolen har.

Dette betyder, at det oftest er en rigtig god idé at indhente tilbud fra flere forskellige leverandører på baggrund af de krav, man har (se om udfærdigelse af en sådan kravspecifikation i kapitel 9).

8.4 Hvor meget skal man købe

Af økonomiske grunde kan man overveje at lade etablering af et trådløst net ske i etaper, fx kun med dækning af de mest besøgte steder på skolen i etape 1 og så senere supplere med de øvrige steder. Der er dog forhold, der taler mod en sådan etapestrategi.

De samlede udgifter for alle etaperne vil givetvis overstige engangsomkostningen, når man skal have elektrikere, murere, malere, it-teknikere mv. til at lave arbejdet af to gange i stedet for samlet. Man risikerer også, at der ved etape to er sket et teknologisk spring, så nye teknologier, nye standarder eller nye enheder nu er at foretrække.

Den investering, man foretager, skal derfor kunne afskrives på kort tid. Og med 'kort tid' menes mindre end fem år. I købssituationen bør man derfor som udgangspunkt vælge den nyeste teknologi frem for en udbredt, men ældre teknologi. Dette gælder også opgraderinger. Oftest er skift til en ny teknologi samlet set mere optimalt end at opgradere et netværk baseret på en ældre teknologi.

Investeringen skal dække ens nuværende behov og ikke tage højde for eventuelle ændringer om 5-10 år. Fx dækker de ovenfor angivne priser en controller, der kan styre op til 25 AP'er. Controlleren kan opgraderes fx til 50 AP'er for en merpris på 25 %. Modsat vil man kunne få en controller, der ikke kan licensopgraderes til ca. halv pris. Forventer man derfor ikke en udbygning på skolen, der kræver flere AP'er inden for fem år, kan man med fordel anskaffe den billige controller uden opgraderingsmulighed – i modsat fald bør den dyrere controller med opgraderingsmulighed vælges.

8.5 Minimér udgifterne

Samlet set anbefales brug af en uvildig konsulent i forbindelse med anskaffelse eller ændring af trådløse net. Udgiften til 5-6 konsulenttimer er marginale i forhold til de samlede omkostninger og mest vigtigt: En sparring med en konsulent vil sikre, at man stiller de rigtige krav, og ikke mindst, at man vælger det mest optimale blandt de indhentede tilbud.

Konsulenten kan med fordel bruges til projektstyring, herunder nogle af følgende opgaver:

- gennemgang og beskrivelse af skolens nuværende kablede net
- afdækning og beskrivelse af skolens behov nu og de næste fem år
- afklaring af, om noget af arbejdet med fordel kan laves af lokale håndværkere, fx el-installation, trækning af kabler, opsætning af AP'er, kabelbakker, efterfølgende maling o.l.
- udformning af en kravspecifikation

- indhentning af tilbud
- sammenligning og prioritering af indkomne tilbud
- hjælp ved afleveringsforretning med leverandøren.

Hvis man vil købe det hele selv, kan det anbefales, at man som minimum får oplyst en række referenceskoler fra de foretrukne leverandører, og at man kontakter disse skoler for at høre om deres erfaringer med anskaffelsen og den efterfølgende drift.

UNI•C anbefaler at

- der bruges en uafhængig konsulent
- afskrivningen højst er på fem år
- man kun ser på dækning af de behov, man har og forventer inden for afskrivningsperioden
- skolen opstiller de samlede omkostninger inkl. omkostninger, der vedrører de dele, som pedel, it-ansvarlig og lokale håndværkere skal stå for.

9 Kravspecifikation og indhentning af tilbud

Som angivet i sidste kapitel om økonomi og rådgivning er det væsentligt at udfærdige en egentlig kravspecifikation og indhente to-tre tilbud. I det følgende gennemgås, hvad der bør medtages i sådan en kravspecifikation, for at man kan indhente så retvisende tilbud som muligt.

Det er dog en god idé allerede i kravspecifikationsfasen at alliere sig med en uvildig ekstern konsulent, som med sin professionelle viden kan støtte med afdækning af begrænsninger og opstilling af muligheder ved den trådløse teknologi set i relation til skolens behov og dets kablede netværk. Kunsten er jo hverken at stille for få eller stille unødvendige krav.

9.1 Hvad skal kravspecifikationen indeholde

Når der skal laves en kravspecifikation, er det helt afgørende at gøre sig klart, hvilken funktionalitet og drift skolen ønsker, og kun i mindre omfang at stille krav til modeller, teknologier, standarder osv. Sidstnævnte krav kan nemlig let udelukke tilbud fra leverandører, der rent faktisk kan dække skolens behov.

Som angivet i kapitel 8 om økonomi og rådgivning er der en del følgeudgifter i forbindelse med etablering af et trådløst netværk på skolen. Ud over AP'er og controllere vil der kunne være behov for

- dokumentation af det eksisterende kablede netværk
- site survey
- nye switche
- kabelfremføringer og murgennemføringer
- opsætning af AP'er
- installation og konfiguration
- el-forsyning
- murer- og malerarbejde.

Hertil kommer udgifter til den efterfølgende drift, fx

- driftsovervågningsystem
- serviceaftale.

Nok er det væsentligt, at skolen danner sig et overblik over de totale udgifter, men en del af arbejdet kan måske med fordel udføres af pedel, en it-ansvarlig og lokale håndværkere eller udliciteres og skal derfor ikke medtages i kravspecifikationen, men nævnes som dele, skolen selv sørger for, og som leverandøren derfor kan forudsætte. Eksempelvis skal kravspecifikationen indeholde en beskrivelse af det kablede netværk, hvilket skolens it-ansvarlige sikkert med fordel kan beskrive frem for at lade leverandøren inspicere netværket.

9.2 Hvor skal det trådløse netværk anvendes

Kravspecifikationen skal angive, hvor på skolens matrikel der skal være forbindelse til det trådløse net. Én ting er at specificere lokalerne, men man bør også tænke på, om nogle af gangarealerne, gymnastiksal, depotrum, kantine og udendørsarealerne skal være dækket. Hvis en handelsskole fx har borde og bænke udendørs, hvor de studerende opholder sig i mellemtimer og frokostpauser, ønsker man sikkert også at have dækning her.

Udbredelsen af radiobølger på skolerne er først og fremmest påvirket af vægkonstruktioner og etageadskillelser og i mindre omfang også af temperatur og luftfugtighed. For at en leverandør kan beregne antal og placering af AP'er, er det derfor væsentlig at skolen vedlægger en målfast plantegning af skolen med angivelse af, hvor der ønskes dækning, og en angivelse af, hvor mange samtidige brugere der skal have trådløs adgang i de enkelte områder. Tænk her på, om det forventes, at der i visse lokaler undertiden skal kunne benyttes trådløst netværk med flere samtidige brugere end normalt, fx ved skriftlig eksamen i gymnastiksalen.

9.3 Hvem skal have adgang til det trådløse netværk

Skal alle og enhver, der besøger skolen, kunne få en trådløs forbindelse, eller skal adgangen begrænses til en kendt skare af mennesker, som fx skolens ansatte og elever og gæster fra naboskolen? Eller sagt på en anden måde: Hvilke krav skal der stilles til validering af de brugere, der forsøger at få en trådløs adgang (jf. kapitel 4, "Adgang til det trådløse netværk..")? Da skolen – som omtalt i kapitel 13 – kan blive gjort ansvarlig for misbrug foretaget fra skolens net, skal der nok ikke vælges fri adgang for alle og enhver.

Kravspecifikationen bør derfor indeholde en beskrivelse af, hvordan adgangen skal være for de potentielle brugere. Gæster fra naboskolen skal måske have en hotspot-adgang, mens ansatte og elever skal have en WPA2-Enterprise-adgang, som beskrevet i kapitel 4.

9.4 Hvordan skal det trådløse netværk anvendes

Kravspecifikationen bør angive, hvad skolens brugere skal bruge det trådløse netværk til. Skal det kun benyttes til internetadgang, eller skal det også være muligt at give adgang til ressourcer på skolens kablede netværk, som fx print og fil.

Det bør også angives, hvilke typer applikationer brugerne skal kunne afvikle, da nogle af disse kan stille krav til antal og placering af AP'er. Er der eksempelvis (i visse områder/lokaler) behov for særligt båndbreddekrævende applikationer som streaming af video eller behov for meget mobile applikationer, som fx mobiltelefoni (Voice over IP).

9.5 Samspil med det fastkoblede net

Der skal vedlægges en opdateret tegning over det eksisterende net, så leverandørerne kan se, hvor der er tilslutningsmuligheder for AP'er, hvor der er switche, om disse har ledige porte, og om disse tillader PoE osv. Dette er ikke en triviell opgave – og slet ikke for mindre skoler uden en decideret it-afdeling. Erfaringer fra tidligere leverancer er, at leverandørerne ofte enten ikke kan fæste lid til de oplysninger om det kablede net, som

skolen har givet, eller også slet ingen oplysninger har fået, hvilket medfører at leverandøren tilbyder nye (og måske unødvendige) switche og nye kabelfremføringer overalt.

Hvis eksisterende kabelbakker, murgennemføringer osv. skal bruges ved etablering af det trådløse netværk, skal dette også fremgå af kravspecifikationen. Man kan fx i denne anførelse, at leverandøren er velkommen til at besigtige forholdene på skolen, hvis han ikke finder oplysningerne i kravspecifikationen fyldestgørende.

9.6 Driftskrav

Som det gennemgås i kapitel 13 om lovgivning og myndighedskrav, er det væsentligt, at skolen sørger for, at der bliver foretaget logning, så det kan verificeres, hvem der har brugt netværket på et givet tidspunkt i forbindelse med misbrug af nettet og eventuelle politianmeldelser. Men også i dagligdagen er det ønskeligt at kunne følge nettets driftstilstand, som det gennemgås i kapitel 11 om drift og overvågning.

Derfor skal kravspecifikationen indeholde de driftsstyringskrav og de muligheder for fejlfinding/afdækning af misbrug, som skolen har. Som minimum skal der kræves en opgørelse af, hvilke muligheder leverandøren tilbyder.

Eksempler på krav kan være, at det fra centralt hold skal være muligt at

- spore en brugers adfærd historisk et år tilbage
- se og kunne ændre den nuværende dækning overalt på skolen fra centralt hold
- se og kunne sætte grænser for de enkelte brugeres brug af netværket
- se og kunne få alarmer ved AP'er, der ikke virker eller ikke virker til den indstillede performance, herunder fremmede AP, der uberettiget er blevet tilsluttet netværket
- se og kunne få alarmer, når et driftsparameter nærmer sig en foruddefineret grænse, fx antallet af tilsluttede brugere til AP nr. 11.

Alternativt kan skolen udlicitere overvågningsopgaven til et centralt driftscenter. I et sådant tilfælde er det undtagelsesvis nødvendigt på forhånd at undersøge, hvilke systemer det foretrukne centrale driftscenter kan understøtte, og medtage disse i kravspecifikationen, fx Cisco, Meru, Aruba, HP eller Trapeze.

9.7 Uddannelse

Hvis skolen beslutter selv at stå for den daglige drift af det trådløse netværk, kan det være fornuftigt at indhente tilbud på et "administratorkursus", så man kan få det optimale ud af løsningen. Alternativt kan man som nævnt ovenfor abonnere på en central driftsovervågning, så skolens slipper for dette. Ét eksempel på en sådan udliciteringsmulighed er at abonnere på UNI•Wireless Management Pro fra UNI•C.

9.8 Udvidelser

Hvis der inden for investeringshorisonten (maks. fem år) forudses en stigning i antallet af brugere og/eller lokaler, der skal være dækket af det trådløse netværk, skal det angives, at netværket skal kunne opgraderes til dette maksimum. Eksempelvis kan nogle control-

lere licensopgraderes, mens andre ikke kan. Og dagsprisen for en sådan opgradering skal angives, så man får et fingerpeg om prisen for en fremtidig udvidelse.

9.9 Service og support

Controlleren er knudepunktet i det trådløse netværket, og derfor bør denne altid være opgraderet både funktions- og sikkerhedsmæssigt. Derfor er det en god idé at sikre, at software- og firmware-opgraderinger er inkluderet i prisen – i hvert fald de første par år.

Der bør også være krav om en serviceaftale, så man hurtigt, dvs. inden for få timer, kan få en fejlramt controller udskiftet eller repareret uden ekstra udgifter, hvis uheldet skulle være ude. Har man ikke en sådan aftale, kan man risikere at være uden trådløst net i længere tid.

Ud over fejlsituationer er den daglige drift væsentlig, men svær at beskrive objektivt for leverandøren, som måske ikke kender dagligdagen på skolen. Derfor er det en god ide at bede om et antal referenceskoler, som allerede har købt pågældende trådløse net, og så kontakte disse med henblik på deres driftserfaringer.

9.10 Økonomi

Man bør også forlange, at tilbuddet klart angiver, under hvilke forudsætninger det er angivet, så skolen ikke efterfølgende præsenteres for ekstraregninger. Hvis leverandøren fx skal stå for kabelfremføring, må der ikke komme ekstraregninger med henvisning til, at "der ikke fandtes kabelbakker", eller at "det var nødvendigt at foretage syv murgennemføringer".

Tilbud vil oftest være ekskl. moms og udregnet på baggrund af den aktuelle \$-kurs. Hvis man derfor regner med en længere betænkningstid end fire uger, bør dette angives, sådan at leverandøren evt. kan binde tilbuddet op på \$-kursen.

Hvis man ønsker en trinvis betaling over flere rater (jf. kapitel 8), skal dette medtages som option.

9.11 Levetid

Det er væsentligt, at leverandøren stiller garanti for, i hvor lang tid han vil kunne skaffe eller reparere enheder af hensyn til både udbygninger og evt. fejl. Dette bør normalt være lig investeringshorisonten og medtages som et krav.

9.12 Udfærdigelse af kravspecifikation

Når de økonomiske, funktionelle og driftsmæssige rammer er afklaret, tilrådes det at lave en egentlig kravspecifikation med henblik på at kunne indhente to-tre tilbud. Jo mere præcis kravspecifikationen er, desto nemmere bliver det at sammenligne de indkomne tilbud. Det kan eventuelt være en god idé at dele kravspecifikationen op i ønsker, optioner og deciderede krav.

Kravet om dokumentation og argumentation er generelt og ufravigeligt. Man skal kræve beskrivelser af, hvordan en leverandør vil opfylde de krav, man har stillet. Og her dur en afkrydsningsliste ikke. Leverandøren må forklare, hvordan han eksempelvis opfylder

kravet om 45 samtidige brugere i lokale C2. (Fx: På baggrund af et site survey opsættes AP'er således, at signalstyrken pr. bruger er mindst xx, opkoblingstiden maks. yy og båndbredden mindst zz). Det tilbud, man vælger, kan med fordel bruges i den endelige salgsaftale sammen med kravspecifikationen, så der ikke sidenhen er tvivl om, hvad man har bedt om, og hvad man er blevet lovet.

Eksempel på en simpel kravspecifikation er vedlagt som bilag 2.

UNI•C anbefaler, at

- skolen får hjælp fra en uvildig konsulent til udfærdigelse af en egentlig kravspecifikation (og efterfølgende hjælp til tilbudsvurdering)
- kravspecifikationen lægger hovedvægten på funktions- og driftskrav og i mindre omfang nævner specifikke teknikker og standarder
- kravspecifikationen indeholder en god beskrivelse af det eksisterende kablede net og en målfast plantegning af skolens arealer
- kravene dækker både køb og drift – herunder mulighed for serviceaftale og udbygning
- leverandøren skal beskrive, hvordan han vil opfylde de stillede krav
- skolen opstiller de samlede omkostninger ved etableringen inkl. de omkostninger, der er forbundet med, at skolens ansatte og lokale håndværkere udfører en del af installationen
- skolen medtager krav til et driftsovervågningssystem, hvad enten dette betjenes lokalt eller udliciteres til et centralt driftscenter.

10 Valg af tilbud

At vælge det bedste tilbud til skolen er på en gang en banal og en kompliceret opgave. Det kan næppe forventes, at alle potentielle leverandører svarer fuldstændigt og præcist på det, skolen har bedt om. Der vil derfor som oftest være tale om en vurdering af det tilbudte. Denne proces er beskrevet i dette kapitel, med hovedvægt på de forhold, der som oftest er de mest vigtige at få afklaret i forbindelse med tilbudsvurderingen. Endelig anbefales det at lade både kravspecifikation og tilbud indgå i en kontakt med den foretrukne leverandør.

10.1 Tilbud vs. kravspecifikation

Første trin ved vurdering af de indkomne tilbud er naturligvis at sammenholde tilbudene med kravspecifikationen. Dette arbejde lettes, hvis kravspecifikationen, som anbefalet i kapitel 9, er systematisk opbygget med klare krav, ønsker og optionsmuligheder. Alligevel kan det være et større arbejde at afklare dette, specielt i de tilfælde hvor leverandøren tilbyder noget andet end det krævede.

Kravspecifikationen siger tydeligt, at leverandøren ikke alene skal kunne tilbyde det krævede, han skal også argumentere for, hvordan det tilbudte vil opfylde de stillede krav. Er der stillet krav om, at standarden 802.11n med to radioer skal anvendes, er det let at konstatere, om dette er tilbudt eller ej. Sværere er det, hvis kravspecifikationen fx kræver en serviceaftale med fire timers tilkaldevagt ved fejl. Hvordan vil leverandøren opfylde dette? Har han lokale kontorer, samarbejde med lokale firmaer, eller betjener han sig af taxaudbringning af reserveudstyr?

Hvis leverandøren tilbyder en rimelig bod, såfremt han ikke kan opfylde det krævede, giver dette en vis formodning om, at leverandøren mener, han normalt vil kunne leve op til de stillede krav. Er der ingen garanti eller bod, har man kun hans ord for det.

10.2 Hvem træffer afgørelsen

Det er naturligvis skolens ledelse, der skal vælge mellem de indkomne tilbud. Men ligesom med udfærdigelse af en kravspecifikation er det ved vurdering af indkomne tilbud en god idé at sparre med en ekstern og uafhængig konsulent. Udgiften hertil vil være marginal og effekten stor. Konsulentens opgave vil først og fremmest være

- at afklare, om det tilbudte opfylder de stillede krav (jf. ovenfor)
- at udtrække og vurdere eventuelle faciliteter i det tilbudte, der ikke er stillet krav om
- at præsentere dette for skolen til en endelig afklaring af, hvilket tilbud skolen er bedst tjent med.

10.3 Hvad koster det

Skolen bør under alle omstændigheder opstille et totalt budget for hele installationen og den kommende drift. Hvis skolen vil bruge lokale håndværkere til dele af installationen, skal dette huskes. Måske kan der blive tale om overarbejde for visse ansatte i installationsfasen, og måske vil driften kræve, at denne indgår i nogens arbejdstid fremover.

Hvis nogle af disse ting er medtaget som optioner i det tilbudte, skal det vurderes, om disse optioner med fordel kan vælges, frem for at man selv laver dette arbejde.

10.4 Ting man skal være specielt opmærksom på

Det vil være forskelligt fra skole til skole, hvad man lægger mest vægt på og derfor er særlig opmærksom på ved tilbudsvurderingen. Selvfølgelig kan man matematisk tillægge alle krav og ønsker en vægt og så udregne tilbuddenes samlede score, men det kan næppe stå alene. Der er psykologiske faktorer og menneskelige faktorer, som givetvis spiller en rolle ved den endelige beslutning.

Nedenfor er nævnt en række ikke-udtømmende forhold, som en konsulent givetvis vil hæfte sig specielt ved. Men det skal tages med det store forbehold, at ikke alle skoler vil lægge samme vægt på de nævnte ting.

10.4.1 Controller

Der er ganske stor forskel på, hvor avancerede de enkelte controllere er, og dermed på, hvilke funktioner der afvikles i controlleren, og hvilke der afvikles på andre enheder som routere, switche, firewalls og enheder til styring af trafikken. Valget af controller har derfor indflydelse på, hvor let styring og overvågning vil være i hverdagen for skolen.

10.4.2 AP

De facto-standard er i dag 802.11n med to radioer, hvorfor der næppe vil blive set med milde øjne på tilbud, som kun tilbyder de ældre 802.11b/g-standarder.

Af praktiske og økonomiske årsager skal AP'erne strømforsynes over ethernetet (PoE), så man undgår etablering af en 220 V's stikkontakter ved hvert AP. (Etablering af én stikkontakt betyder nemt en ekstraudgift på 2.500 kr.).

10.4.3 Kapacitet, båndbredde, dækning, signalstyrke og roaming

Kapacitet, båndbredde, dækning, signalstyrke og roaming er alle parametre for, hvor god en forbindelse brugere oplever. Er tilbuddet realistisk? Kan man opnå den forventede dækning og kapacitet med det antal AP'er, der er foreslået? Som tommelfingerregel skal der være et AP i almindelige klasselokaler ved brug af almindelige applikationer og to eller flere i områder med særlig båndbreddekrævende applikationer eller med særlig mange brugere.

10.4.4 Site survey

Hvis leverandøren foreslår et-to AP'er pr. klasselokale, er der næppe problemer med dækningen her. Men hvis ét AP er forudsat at skulle dække flere lokaler (måske oven i købet på hver sin etage), eller hvis der skal sikres dækning på gangarealer, depotrum og udendørsarealer, kan leverandøren foretage et site survey med henblik på, hvor de en-

kelte AP'er bedst placeres. Dette kan i princippet foretages på tre måder, som er meget forskellige med hensyn til, hvor præcist det trådløse nets dækning er overalt på skolen:

- En teoretisk gennemgang baseret på den sendestyrke og rækkevidde et givet AP har. Denne type af survey bliver ofte kombineret med visuel inspektion, så der delvis kan tages højde for tykkelsen af mure osv.
- En lidt mere præcis måde at lave site survey på er at kombinere ovenstående med at sætte enkelte AP'er op på nogle udvalgte steder for at se, om teorien holder.
- Den sidste og mest præcise metode er radiomæssigt at måle hele lokaliteten igennem.

Den sidste form for site survey er normalt meget omkostningsfuld, men samtidig den bedste metode til at få et velfungerende trådløst netværk. Konsulenten vil se på, om valg af metode står rimeligt mål med usikkerheden.

10.4.5 Eventuel opgradering/udbygning af det eksisterende kablede net

Hvis der er mangel på ledige switchporte i de enkelte krydsfelter, skal der også placeres flere switche. I denne situation vil det være fornuftigt at anskaffe PoE-switchene. Hvis switchene ikke er PoE-switcher, kan man sætte PoE-injectorer i de switchporte, der skal benyttes til det trådløse netværk. Har leverandøren tilbudt det, eller omfatter hans tilbud helt nye PoE-switcher?

10.4.6 Konfiguration af controller m.m.

Er det klart angivet, om leverandøren står for konfigurationen, og i givet fald hvad konfigurationen omfatter. Ønskes der blot en grundkonfiguration af controlleren, eller skal der konfigureres forskellige SSID'er? Det kan også være aktuelt at klarlægge, hvordan brugerauthentifikation via en RADIUS-server er foreslået. Er der ekstraudgifter, der ikke er medtaget?

10.4.7 Daglig drift

Hvis skolen ikke udliciterer den daglige drift, men selv skal stå for denne, vil konsulenten nøje vurdere, hvilke faciliteter det tilbudte drifts- og overvågningssystem har, og herunder hvad det må forventes at koste rent tidsmæssigt for skolen at drive.

10.5 Køb

Når skolen har bestemt sig for valg af leverandør, foreslås det at lave en egentlig kontrakt for handelen, hvori der indgår både skolens kravspecifikation og leverandørens tilbud.

UNI•C anbefaler

- at skolen anvender en ekstern og uafhængig konsulent til at vurdere de indkomne tilbud
- at både kravspecifikation og tilbud indgår som bilag i den endelige købsaftale.

11 Drift og overvågning

Selv et velopsat og korrekt konfigureret trådløst netværk kræver, at der afsættes ressourcer til løbende drift. Nogle gange skal konfigurationen ændres som følge af nye ønsker og behov. Andre gange skal der fejlsøges og fejlrettes på grund af fejl på net eller udstyr. Desuden vil man i perioder kunne løbe ind i, at nettet overbelastes i visse områder. Det er alt sammen situationer, hvor det er nødvendigt, at der findes personer med viden om skolens net, og hvor systemer til overvågning og alarmering kan være en stor hjælp.

Nedenfor gennemgås de typiske driftsopgaver, og hvordan de kan gribes an. Der skelnes mellem konfigurationsændringer som følge af nye ønsker og behov, fejl på nettet og problemer som følge af overbelastning.

Bilag 4 er en FAQ-liste over løsningsforslag til en række udbredte driftsproblemer på det trådløse net.

11.1 Ændringer i konfiguration

Ændringer i konfigurationen som følge af nye ønsker eller behov bør kun være nødvendige maks. en-to gange om året. Det kan fx handle om at ændre et SSID, tilføje et nyt SSID, tilføje AP'er eller ændre i sikkerhedsopsætning.

I ældre autonome netværk er sådanne konfigurationsændringer typisk en manuel proces, hvor administrator er nødt til at logge ud og foretage ændringerne i hvert eneste AP. Det er en meget omstændelig og tidskrævende proces, og risikoen for fejl er stor.

I moderne controllerbaserede netværk foretager man som udgangspunkt konfigurationsændringer i controlleren. De fleste skoler kan nøjes med en enkelt controller, og derfor skal en ændring kun foretages ét sted og slår så igennem med det samme. Det er meget mere effektivt, og der er sikkerhed for, at konfigurationen i alle AP'er er ens.

En del producenter tilbyder managementsystemer ved siden af controlleren. Der er tale om software, der afvikles på en separat server. Et managementsystem kan foruden konfigurationsændringer normalt også tilbyde overvågning og alarmeringsfunktioner. I forhold til konfigurationsændringer er managementsystemet smart, hvis man har mange controllere, der skal konfigureres ens, men det er normalt aldrig tilfældet på skoler, hvor de fleste har en-to controllere. Derfor er managementsystemet ikke nødvendigt i forhold til konfigurationsopgaverne. Tværtimod vil det ofte være bedre at konfigurere direkte i controlleren, da man så undgår de problemer, der kan opstå, hvis managementsystem og controllersoftware ikke kører samme version.

Konfigurationsændringer er som nævnt ikke noget, der foretages ret ofte. Derfor kan det være svært for skolens it-ansvarlige at huske, hvordan det foregår fra gang til gang, og de fleste skoler vil derfor være bedst hjulpet ved at betale en ekstern konsulent for at foretage de nødvendige ændringer. Udgangspunktet er, at sådanne ændringer afregnes

på timebasis, men nogle firmaer tilbyder også at håndtere sådanne ændringer på abonnementsform til fast pris.

11.2 Fejl på net eller udstyr

Fejl på net eller udstyr bør ikke forekomme ret ofte, men helt undgåes kan de ikke. Eksempler på sådanne fejl er:

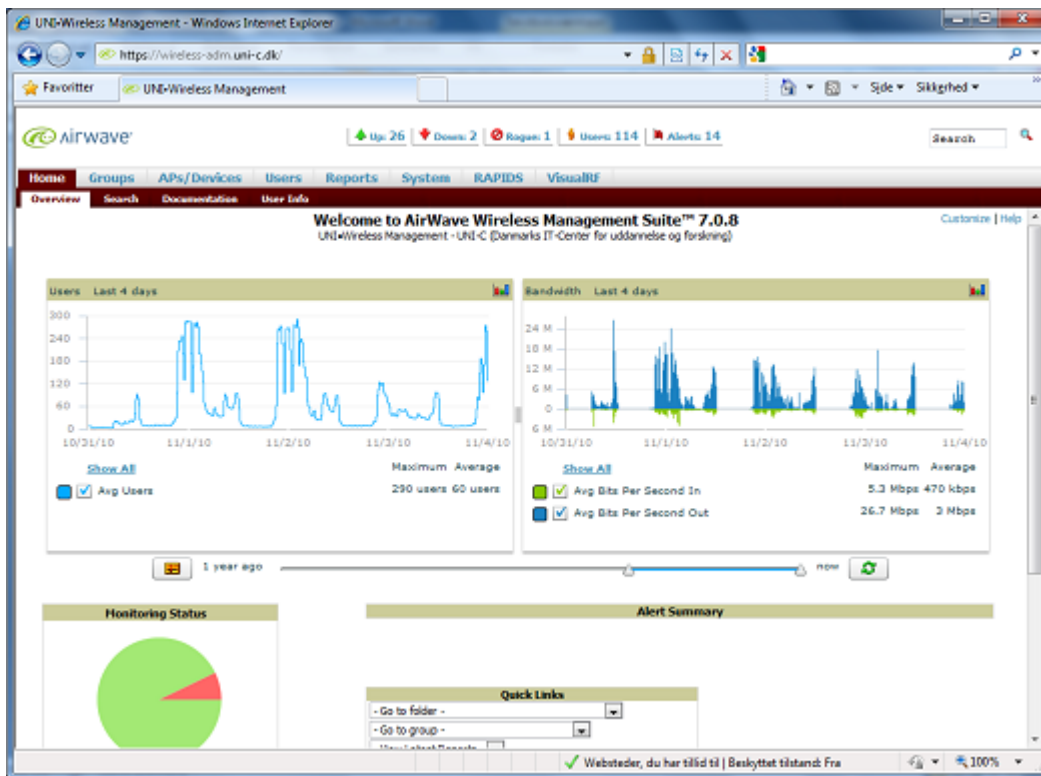
- AP, der går ned
- AP, der er ustabil og genstarter ofte
- Controller er nede, ustabil eller i øvrigt fejlbehæftet
- RADIUS-serveren svarer ikke
- Fejl på skolens LAN, fx defekt switch.

Et problem med et enkelt AP har normalt ikke afgørende indflydelse på trafikafviklingen. Nabo-AP'er vil ofte sikre en svag dækning, og brugerne vil derfor opleve, at forbindelsen måske nok er meget langsom, men at der stadig er forbindelse. Og brugerne finder hurtigt ud af, at forbindelsen er bedre andre steder på skolen og søger derfor derhen. Hvis skolen ikke har et overvågningssystem, kan der derfor gå lang tid inden fejlen opdages og rettes.

Andre fejl har større konsekvenser for trafikafviklingen og vil derfor normalt blive opdaget noget hurtigere, også uden et overvågningssystem. Det gælder fx hvis en switch med mange AP'er går ned, hvis controlleren går ned, eller hvis RADIUS-serveren ikke svarer.

Til gengæld kan et eller flere AP'ers ustabilitet være meget svært at fange uden et overvågningssystem. Der er eksempler på AP'er, der pga. en software-fejl genstarter to-tre gange om dagen, og hvor de tilsluttede brugere hver gang oplever, at de kortvarigt mister forbindelsen. I løbet af nogle minutter er AP'et oppe igen, og så bliver der oftest ikke gjort mere ved det. Men det er stadig et unødigt irritationsmoment i den daglige undervisning.

Generelt vil en skole kunne have stor glæde af et overvågningssystem, der kan alarmere øjeblikkeligt, når der er fejl på nettet. Det kan medvirke til, at fejlene bliver identificeret og løst hurtigere til glæde for alle parter. Et eksempel på et sådant system er UNI•Wireless Management, der er illustreret på figur 4.



Figur 4. UNI•Wireless Management er et eksempel på et overvågnings- og alarmeringsystem, der kan medvirke til at sikre et velfungerende trådløst netværk.

11.3 Overbelastning af netværket

De fleste skoler vil fra tid til anden opleve, at det trådløse net er så belastet, at det udgør et problem. Svartiderne vil være generende langsomme, og brugerne oplever måske, at forbindelsen virker ustabil.

Der kan være mange årsager til en så uheldig stor belastning af nettet.

Én mulig årsag er selvfølgelig, at den generelle stigning i brugen af det trådløse netværk – både i forhold til antal enheder og den belastning, den enkelte enhed lægger på nettet – kan betyde, at nettet i perioder vil være belastet af helt legitim trafik fra et stort antal brugere.

En anden sandsynlig årsag er, at en enkelt eller ganske få enheder belaster det trådløse net ekstremt meget. På skoler er der typisk to scenarier, der kan være årsag til den type af belastning:

- En inficeret maskine, der – oftest uden brugerens viden – medvirker til distribution af ulovligt materiale i stor stil. Det typiske er, at maskinen bruges til masseudsendelse af spam-mails eller agerer servercentral for udveksling af spil, film mv.

- En bruger, der bevidst udveksler ulovlige filer som fx spil, film og musik med andre. I praksis betyder det, at der downloades/uploads mange store filer, typisk via Bittorrent.

Er der tale om distribution af ulovligt materiale, er der tale om et sikkerhedsbrud, som bør håndteres som beskrevet i kapitel 12, "Håndtering af sikkerhedsbrud".

Uanset årsagen vil belastningen imidlertid være generende og kan hurtigt være et problem i forhold til afviklingen af den almindelige undervisning. Derfor bør belastningsproblematikken under alle omstændigheder håndteres af skolen.

Nedenfor følger først en gennemgang af en række proaktive tiltag, skolen kan tage med henblik på at forebygge de belastningsmæssige problemer. Dernæst forklares det, hvordan et overvågningssystem kan være et godt værktøj den dag, hvor problemerne alligevel opstår.

11.3.1 Forebyggelse af belastningsmæssige problemer

De proaktive tiltag har to formål. For det første at sikre, at skolens trådløse net udnyttes bedst muligt. For det andet i videst mulig omfang at forhindre, at brugernes maskiner belaster nettet via distribution af ulovligt materiale eller på anden måde belaster nettet u hensigtsmæssigt.

Hvad sikring af den optimale udnyttelse af nettet angår, bør skolen overveje følgende:

- **Moderne klienter**
At brugerne så vidt muligt anvender enheder, der kan tilslutte sig nettet via de nyeste standarder. Hvis skolens trådløse net understøtter 802.11n, er det vigtigt, at så mange af klienterne som muligt udnytter de høje hastigheder, som 802.11n tilbyder. Som udgangspunkt bør en klient derfor understøtte 802.11n på både 2,4 og 5 GHz.
- **Forhindre lave associeringshastigheder**
At det trådløse net er konfigureret, så det ikke tillader associeringshastigheder lavere end nødvendigt. Normalt er dækningen så god, at de laveste hastigheder på i hvert fald 1 Mbit/s og 2 Mbit/s ikke bør tillades. Og ofte kan også 5,5 Mbit/s udelades.
- **Load balancing**
At anvende load balancing, hvis det trådløse net understøtter funktionen. Formålet er at undgå, at hovedparten af klienterne vælger at forbinde sig til et og samme AP, hvis der er flere tilgængelige AP'er i området. Det er særlig vigtigt i fællesområder, hvor der i perioder er rigtig mange samtidige brugere. Load balancing kan enten ske på AP-niveau eller på frekvens-niveau.
- **Band steering/select**
Generelt er hastighed og stabilitet betydeligt bedre på 5 GHz end på 2,4 GHz. Imidlertid er der blandt mange klienter en tendens til at vælge 2,4 GHz, selvom de faktisk kan anvende begge frekvensbånd. Band steering/select medvirker til

at få flere af disse klienter til at køre i 5 GHz-båndet. Det forbedrer hastighed og stabilitet for samtlige klienter, både for dem der kommer op på 5 GHz, og for dem der er tilbage på 2,4 GHz.

- Trafikprioritering
Selv den hurtigste internetforbindelse kan belastes. I de situationer kan man – via trafikprioritering – sikre, at undervisningsrelevant trafik prioriteres højere end andre typer af trafik. På den måde sikrer skolen sig, at den vigtigste trafik så vidt muligt afvikles først. Et eksempel på en trafikprioriteringsboks er UNI•Gateway.

I forhold til det andet formål – at forhindre, at brugernes maskiner belaster nettet via distribution af ulovligt materiale – enten som følge af, at en maskine er inficeret, eller som følge af en bevidst handling – er der ligeledes en række proaktive tiltag, skolen kan tage:

- Udforme en anvendelsespolitik
Anvendelsespolitikken informerer bl.a. brugerne om, hvad nettet må bruges til, og hvad det ikke må bruges til. Politikken bør ligeledes stille krav om opdatering til de enheder, brugerne anvender. Brugere bør aktivt tilkendegive, at de accepterer politikken. Der henvises til et eksempel på en anvendelsespolitik i kapitel 12, "Håndtering af sikkerhedsbrud".
- Kræve at brugernes maskiner er opdaterede
Som nævnt bør det fremgå af anvendelsespolitikken, at alle enheder på skolens netværk skal være opdaterede i forhold til både sikkerhedsrettelser og antivirus.
- Personligt login og log af anvendelsen
Det bør kun være muligt at få adgang til skolens net via anvendelse af personligt login baseret på brugernavn + password. I forhold til bevidst misbrug kan det have en god præventiv effekt, at brugerne ved, at de ikke er anonyme på nettet. Ligeledes bør brugerne oplyses om den logning, skolen foretager. Det kan være med til at forstærke den præventive effekt.
- Tekniske foranstaltninger i øvrigt
Skolen kan derudover overveje at supplere med en eller flere af følgende former for filtrering, der har til formål at forhindre, at det omtalte misbrug sker – uanset om det er bevidst eller ubevidst:
 - Filtrere SMTP-trafik
Hvis en maskine bliver inficeret, sker der ofte det, at den medvirker til distribution af spam. For at forhindre maskinen i at udsende spam – selvom den er blevet inficeret – kan skolen vælge at spærre for SMTP fra skolens net. Det sker i praksis ved at lukke for TCP-port 25 i udgående retning fra skolens net mod internettet.

- Udgående filtrering i øvrigt
Mere generelt kan skolen vælge at filtrere udp- og TCP-trafik, der ikke eksplicit er tilladt. Normalt er alt tilladt fra skolens net mod internet. Ved kun at tillade trafik mod porte på de mest almindelige tjenester vil en del uønsket trafik kunne forhindres.
- Filtrering via DNS
Navneopløsning via DNS er en forudsætning for langt hovedparten af de tjenester – både webbaserede og andre – der afvikles via internettet. Derfor er det også muligt at filtrere brugernes adgang til tjenester ved at filtrere i, hvad der kan opløses via DNS. Der findes DNS-tjenester, der har specialiseret sig i at klassificere domæner på nettet, hvorved det vil være ret let for en skole at lægge sin egen politik på området. Et eksempel på en sådan tjeneste er OpenDNS.
- Filtrering af webtrafik
I dag er det helt almindeligt at filtrere mailtrafik baseret på indhold. Det primære formål er at frafiltrere spam og mails, der i øvrigt kan udgøre en sikkerhedsrisiko. Langt mindre udbredt er det at filtrere webtrafik, men teknisk er det muligt. Der findes både appliance-bokse til lokal drift og skybaserede tjenester, der tilbyder at filtrere al webtrafik for skolen.

11.3.2 Årsagen til belastningen – overvågningssystemet giver svaret

Et overvågningssystem har ikke mindst sin berettigelse i forhold kapacitetsstyring og håndtering af belastningsmæssige problemer. Uden et overvågningssystem, der løbende opsamler data over trafikafviklingen, er det så godt som umuligt at vurdere, hvordan belastningen på skolens trådløse net udvikler sig. Måske oplever nogen, at det i perioder kører langsomt, men hvordan udvikler det sig over tid? Er belastningen knyttet til enkelte tidspunkter, enkelte AP'er eller måske blot enkelte brugere, der belaster nettet uhenigtsmæssigt?

Disse spørgsmål kan overvågningssystemet bl.a. give svar på og dermed medvirke til, at man kan tage de rigtige beslutninger i forhold til at nedbringe belastningen. I skolesammenhæng er det ofte et lille antal brugere, der er ansvarlige for en stor del af belastningen, og overvågningssystemet kan øjeblikkeligt give svar på, hvem det evt. er, så der kan tages aktion på problemet.

Desuden tilbyder flere af systemerne at holde øje med belastningen og alarmere – fx i form af en e-mail – når en foruddefineret grænseværdi overskrides. På den måde kan man handle proaktivt og ofte nå at gribe ind, inden belastningen bliver et problem.

Eksempler på sådanne grænseværdier, der kan give anledning til en alarm er:

- mere end 30 brugere på et AP i mere end 45 minutter
- trafikken til/fra et AP har været højere end 40 Mbit/s i 30 minutter

- en enkelt bruger har belastet nettet med mere end 10 Mbit/s i 60 minutter.

Bemærk, at der i controlleren er fokus på opsætning og konfiguration af nettet. Controlleren opsamler ikke historik i nævneværdigt omfang og giver derfor kun et øjebliksbillede. Ovenstående eksempler vil derfor ikke kunne fanges af controlleren, hvorfor det er nødvendigt med et overvågningssystem, hvis man vil kunne gribe ind og sikre et velfungerende trådløst netværk.

UNI•C anbefaler:

- Skolen får en ekstern konsulent til at stå for opsætning og konfiguration af det trådløse net.
- Skolen benytter et overvågningssystem som støtte i den daglige drift. Systemet skal bl.a. kunne alarmere ved almindeligt forekommende driftsforstyrrelser og benyttes i fejlsøgningsituationer, hvor nettet er belastet.
- Skolen forebygger belastningsmæssige problemer som beskrevet i kapitlet.

12 Håndtering af sikkerhedsbrud

Flere og flere brugere på skolerne medbringer egne enheder – såvel bærbare pc'er som andre håndholdte enheder – der tilsluttes skolens trådløse netværk og derigennem opnår forbindelse til internettet. Skolen har kun begrænset mulighed for at kontrollere og sætte rammer for, hvordan eleverne anvender internetadgangen, som skolen stiller til rådighed. Imidlertid skal skolen stadig optræde ansvarligt ved at tage hånd om de sikkerhedsbrud, der forekommer fra skolens netværk og dermed i mange tilfælde fra en pc medbragt af en bruger – hvad enten der er tale om elever, lærere, kursister eller for den sags skyld it-kriminelle, der har skabt sig uautoriseret adgang til nettet.

12.1 Hvad er et sikkerhedsbrud?

I klassisk forstand taler man om brud på sikkerheden, hvis der er sket uønsket kompromittering af fortrolighed, tilgængelighed eller integritet af data og systemer.

For en skole med brugere på et trådløst netværk vil vi dog fokusere på de situationer, hvor det trådløse netværk er anvendt på en måde, der strider mod god skik (evt. præciseret i skolens etiske regler eller anvendelsespolitik). Ofte er der tale om en situation, hvor det reelle sikkerhedsbrud er foregået et andet sted, mens kilden til sikkerhedsbruddet vil være at finde på skolens netværk.

Eksempler på sådanne brud på god skik kan være: Fildeling, hacking fra skolens netværk, spredning af virus/malware og spam m.m. – alt sammen med tilknytning til skolens netværk.

Der findes også eksempler på "lokale" brud på sikkerheden: Hacking af andre pc'er på netværket og sniffing og efterfølgende misbrug af oplysninger på et ukrypteret trådløst netværk. En aktuell (november 2010) "trend" inspireret af Firefox-plug-in'en *Firesheep* er opsnapping af *session-cookies* og overtagelse af andre brugeres identitet på Facebook og andre sociale tjenester, der udveksler data med brugeren ukrypteret.

12.2 Hvordan konstateres et sikkerhedsbrud?

Der er normalt to tilgange, som bør kombineres:

For det første er der proaktiv overvågning. Det er en netværksbaseret overvågning af forbrugsmønstre, gennemgang af logdata m.v. Når der konstateres et usædvanligt mønster, der kunne tyde på et misbrug, tages aktion på sagen – ofte alene ud fra mistanken, hvilket kræver en større indsats og et større ansvar. Eksempler på fænomener, der kan tages aktion på, er: Pludselig stigning i internetforbrug for en bruger eller usædvanlig trafik – fx belastning på et tidspunkt, hvor der ikke bør forekomme trafik på nettet. Overvågningen kræver et overvågningssystem (se også kapitel 11 om driftsovervågning). I dag har flere skoler defineret "baselines" for elevernes normale forbrug, mens der så proaktivt tages aktion på overskridelser i forhold til denne norm.

For det andet er der den reaktive overvågning, der populært sagt dækker følgende: Vi afventer og tager affære, når der er en konkret sag – fx en henvendelse fra politiet eller internetleverandøren.

Som minimum skal skolen altid tage aktion på konkrete henvendelser. Omfanget af proaktive tiltag er meget afhængig af skolens teknologiske muligheder og ressourcer. Ved gentagelser af samme type sikkerhedsbrud bør skolen dog under alle omstændigheder overveje præventive initiativer og proaktive tiltag.

12.3 Håndtering af en hændelse

Håndteringen af et sikkerhedsbrud består typisk af følgende trin:

1. "Stands ulykken". (Hvis misbruget stadig pågår, skal skolen sørge for, at det bringes til ophør hurtigst muligt.)
2. Analyse, efterforskning og bevissikring
3. Vurdering
4. Handling – evt. anmeldelse til myndigheder.

12.3.1 Stands ulykken

I det øjeblik skolens medarbejdere bliver gjort opmærksom på et misbrug, er de forpligtede til at gøre en indsats for at bringe misbruget til ophør.

Det optimale vil selvfølgelig være, hvis kilden kan lokaliseres straks og med det samme kontaktes og instrueres i at bringe misbruget til ophør.

Af alternative muligheder, skolen har for at bringe misbruget til ophør, er der tidsbegrænset firewallfiltrering eller øjeblikkelig udelukkelse af specifikke brugere eller pc'er fra netværket. I et controllerbaseret trådløst netværk er det relativt let at "smide en bruger på porten".

12.3.2 Analyse, efterforskning og bevissikring

Misbrug konstateres ofte først ved en henvendelse fra internetudbyderen (efter at en klage er sendt til udbyderens abuse-funktion), fra politiet eller ved konstatering af problemer i driftsovervågningen.

Henvendelser fra politiet eller internetudbyderen indeholder information, der ofte er begrænset til: Vi har konstateret misbrug i form af yy fra IP-adresse zz og port pp på tidspunkt tt. IP-adressen er i sagens natur den registrerede IP-adresse, som klageren har oplevet angrebet komme fra.

For at kunne henføre oplysningerne til en specifik pc – og i bedste fald en specifik bruger – kræves de nødvendige logdata. Behovet for disse logdata er i praksis meget afhængig af skolens aktuelle netværksopsætning og dokumentation. Anvendte teknologier som adressekonvertering (NAT) og dynamisk tildeling af IP-adresser (DHCP) letter netværksadministrationen, men komplicerer samtidig billedet af sammenhængene mellem en netværks-session og en bruger. Og for at kunne samle op på et misbrug er vi nødt til at indhente de nødvendige oplysninger fra vores logfiler. Intet er umuligt – og teknologien understøtter opsamling af de nødvendige oplysninger.

For at henføre et konkret misbrug til en specifik bruger, forudsættes dog først og fremmest, at netværket er sat op til at forlange et (identitetsbærende) bruger-id, før der

gives adgang til det trådløse netværk og internet. Det er derfor en væsentlig forudsætning.

Dernæst bør der indsamles:

- Accounting log (IP-adresse, bruger-id og tidspunkt for start og slut på brugersessionen). Denne log knytter brugeren til en IP-adresse i et givet tidsrum.
- Evt. adressekonvertering (IP-adresser, porte og tidspunkt) for alle sessioner, hvis skolen anvender NAT/PAT. Tildeling sker ofte dynamisk pr. session, hvilket i sig selv er en sikkerhedsfeature, fordi det samtidig beskytter interne systemer mod tilgang fra internettet. Dette knytter registreret IP-adresse og port til lokal IP-adresse og port.
- Evt. DHCP tildelingslog (MAC-adresser og tildelte IP-adresser og tidspunkt)
- Evt. sessionsoplysninger (afsender- og modtager-IP-adresser og porte, tidsstempel – evt. suppleret med yderligere oplysninger som mængden af data, der er overført). Dette registrerer oplysninger for alle netværks-sessioner med henblik på dybere efterforskning.
- Bemærk, at logs kræver korrekt tidsstempel for at kunne matches. Derfor bør der anvendes NTP på de servere, der opsamler logoplysninger, så alle enheder er synkroniserede.

Oplysningerne bør gemmes i et år og derefter slettes.

Afhængig af skolens konkrete løsning kan nogle af oplysningerne hentes hos en leverandør. For at være på den sikre side bør skolen dog på forhånd tage kontakt til leverandøren for at afdække, hvilke oplysninger leverandøren kan stille med, og hvilke oplysninger skolen selv må stå for at indsamle.

Hvis sagen er alvorlig nok til, at skolen vurderer, at misbruget skal politianmeldes, skal beviser på misbruget sikres, så det er hævet over enhver tvivl, at der er tale om valide beviser. Yderligere oplysninger kan evt. søges hos politiet eller DK-CERT.

12.3.3 Vurdering

Inden skolen tager aktion på en hændelse, bør sagen vurderes ud fra forskellige kriterier:

- Hvor alvorlig er misbruget? I visse sager er klagerne meget aggressive, selvom sagen er relativt harmløs.
- Er der tale om gentagelsestilfælde for den samme bruger?
- Vidste brugeren noget om det? Ofte kan der være tale om en pc, der er blevet inficeret med ondsindet kode, som udfører misbruget uden ejerens vidende.
- Hvor konsekvent behandles misbrug generelt i henhold til anvendelsespolitikken?
- Skal brugeren hjælpes eller straffes?

12.3.4 Handling

Det er op til skolen at vurdere, hvor alvorlig en reaktion, et misbrug i den konkrete situation bør foranledige. Men en reaktion bør der komme.

Afhængig af alvoren foretages anmeldelse til politi og myndigheder. Bemærk, at en politianmeldelse stiller krav til kvaliteten af beviser.

Fremadrettet kan skolen overveje at indføre mere intensiv overvågning. Skolen skal dog passe på ikke at overskride grænserne for privatlivets fred.

12.3.5 Sanktionsmuligheder

Skoler anvender lidt forskellige sanktionsmuligheder. Fælles for alle er dog, at de bør være nedfældet i anvendelsespolitikken.

Eksempler på almindelige sanktioner er en (evt. midlertidig) bortvisning og inddragelse af adgangen til det trådløse netværk. Andre ikke helt så graverende sanktionsmuligheder er skærpet kontrol eller begrænsninger i adgangen til netværket.

Det centrale må dog være, at sanktionsmulighederne passer til skolens kultur og er formuleret i en anvendelsespolitik, som alle skolens brugere er gjort bekendt med.

12.4 Anvendelsespolitik

Det har været nævnt flere gange i kapitlet her: Skolen bør have en anvendelsespolitik eller sikkerhedspolitik, der udstikker rammerne for "accepteret brug af skolens trådløse netværk" og sanktionsmuligheder i tilfælde af brud på politikken.

Anvendelsespolitikken skal samtidig fastslå, hvad skolen evt. har indført af initiativer til overvågning af netværkets drift og sikkerhed.

Praksis viser, at skolen har svært ved at straffe misbrug, der ikke har hjemmel i en anvendelsespolitik, som brugerne er gjort bekendt med. Samtidig siger det næsten sig selv, at ikke alle brugere har samme standarder for, hvad der er god skik og moral. Også derfor er det vigtigt, at skolen med en anvendelsespolitik slår fast, hvad det er for rammer, der gælder – og at det ikke er op til den enkelte bruger selv at definere, hvor grænsen går for accepteret brug.

Anvendelsespolitikken skal håndhæves konsekvent og tilpasses, hvis der sker ændringer i skolens praksis for overvågning eller principper for, hvad der er accepteret praksis.

I bilag 3 findes et eksempel på en anvendelsespolitik for brugen af skolens trådløse netværk.

UNI•C anbefaler

- at der udformes en anvendelsespolitik, som brugerne skal acceptere, og som håndhæves konsekvent
- at adgangen til netværket begrænses til registrerede brugere, hvilket også gælder kursister og gæster
- at adgangen til netværket logges i nødvendigt omfang – som minimum med tildeling af IP-adresse, tidsrum og bruger-id.

13 Lovgivning og myndighedskrav

Et stigende antal skoler indfører – ofte som en central del af skolens infrastruktur – trådløst netværk, der stilles til rådighed for alle skolens brugere, dvs. lærere, gæster, administratorer og ikke mindst elever, der medbringer egne bærbare pc'er og håndholdte enheder. Det stiller skolen over for visse lovgivningsmæssige krav og begrænsninger i forhold til drift, overvågning og logning på det trådløse netværk. Om skolen er forpligtet til selv at opfylde kravene i logningsbekendtgørelsen, afhænger af, om skolen udbyder sine ydelser på "kommercielt grundlag".

13.1 De juridiske aspekter

Skolen skal i den daglige drift forholde sig til en lang række af love og myndighedskrav – herunder forhold omkring ophavsret, dataindsigt, privatlivets fred og mange andre forhold.

Når vi begrænser os til at tale drift og sikkerhed på et trådløst netværk, er der imidlertid tre særligt relevante aspekter af lovgivning og myndighedskrav, vi vil søge afklaret i det følgende:

- Logningsbekendtgørelsen – skal skolen logge?
- Persondataloven – hvor meget kan skolen tillade sig at kigge brugerne over skulderen og registrere om deres adfærd på nettet?
- Det juridiske begreb "culpa" – når skolen har handlet uagtsomt og burde vide bedre.

For lovgivningskrav i øvrigt henvises til *Skolejura ABC*: http://www.uni-c.dk/generelt/materiale/abc_bog.pdf

13.2 Skolens behov for logning – et myndighedskrav?

De væsentligste årsager for skolen til at iværksætte logning af adgang til det trådløse netværk og internetanvendelsen er driftsovervågning og efterforskning af misbrug. Her til kommer en vurdering af, om skolen skal efterleve det eneste reelle myndighedskrav, der i dag findes om logning: Logningsbekendtgørelsen i terrorlovgivningen.

13.2.1 Logningsbekendtgørelsen

Logningsbekendtgørelsen

(<https://www.retsinformation.dk/Forms/R0710.aspx?id=2445>) stiller krav om logning for udbydere, der stiller net eller tjenester til rådighed for slutbrugere.

"Udbydere" er i henhold til vejledning i Logningsbekendtgørelsen:

"Alle selskaber, der på kommercielt grundlag betjener mere end én slutbruger eller mere end én anden udbyder af elektroniske kommunikationsnet eller -tjenester med henblik på formidling af dele af disses trafik.

Det er uden betydning, om udbyderen har egen infrastruktur, om der er tale om offentligt tilgængelige tjenester eller lukkede net, hvilket omfang udbudet har, samt hvilken form for tjenester der udbydes.”

Her er det vigtigt at slå fast, at begrebet ”slutbrugere” ikke skal tolkes som ”brugere af det trådløse netværk”, hvad man måske ville forvente. ”Slutbruger” er i telelovgivningens forstand blot en, der ikke er udbyder – og det vil være gældende for mange uddannelsesinstitutioner.

Det centrale forhold er således, om skolen udbyder det trådløse netværk (evt. som en del af en ydelse, der leveres) på kommercielt grundlag. Det trådløse netværk behøver ikke i sig selv være en selvstændig og betalt ydelse, men kan også være en gratis ydelse i en større pakke, der udbydes på kommercielle vilkår. Derfor er fx hoteller og cafeer omfattet, selvom de stiller et trådløst netværk gratis og dermed på overfladen ikke kommercielt til rådighed for kunderne.

Når vi taler uddannelsesinstitutioner, vil nogen være omfattet og andre ikke. Det hænger sammen med, at uddannelsesinstitutioner i dag har en del af deres forretning ved kurser, udlejning af faciliteter, kostelever m.v., hvori også et trådløst netværk indgår. Det vil derfor altid være en konkret vurdering, om institutionen er udbyder. Her er It- og Telestyrelsen den rette myndighed at rette henvendelse til for at få det afklaret.

Som generel tommelfingerregel er uddannelsesinstitutioner, der fortrinsvist afholder undervisning på ikke-kommercielle vilkår, ikke omfattet af Logningsbekendtgørelsen. I sådanne tilfælde er det institutionens internetudbyder, der skal forestå logningen. Bemærk i den forbindelse, at internetudbyderen ikke som sådan kan stille de opsamlede logdata til rådighed for skolen i forbindelse med efterforskning af misbrug. I det omfang skolen har behov for logning, vil det derfor under alle omstændigheder være nødvendigt med selvstændige logningsinitiativer.

Logningsbekendtgørelsen stiller krav om registrering af en række konkrete netværksoplysninger, der her er sammenskrevet til en kort form (for præcis information henvises til §5 i Logningsbekendtgørelsen):

- IP-adresse, protokol og port for afsender og modtager (sessionsoplysninger)
- tidspunktet for kommunikationens start og afslutning
- den tildelte brugeridentitet
- lokale netværks præcise geografiske eller fysiske placering samt identiteten på det benyttede kommunikationsudstyr (specifikt for trådløse netværk).

Oplysningerne skal opbevares i et år og herefter slettes.

Har du brug for yderligere information, så kontakt It- og Telestyrelsen.

13.3 Persondataloven

Må skolen logge brugernes adgang til det trådløse netværk og internet uden at komme på kant med Persondataloven?

Det korte svar er: Ja. I henhold til loven kræver det, at skolen derved forfølger en berettiget interesse, og at omfanget af databehandling (registrering, gennemgang m.m.) står mål med denne interesse. Varetagelse af drift og sikkerhed – herunder behovet for efterforskning af misbrug anses i den forbindelse for at være en berettiget interesse. Men skolen bør dog undlade at registrere oplysninger om brugernes internettrafik ud over, hvad den berettigede interesse dækker. Som et fingerpeg anviser netop Logningsbekendtgørelsen et hensigtsmæssigt detailniveau for logdata, som ligger inden for, hvad der må anses for acceptabelt (se tidligere afsnit om Logningsbekendtgørelsen).

For at logge persondata kræves endvidere, at brugerne har givet deres samtykke til logningen. Den problemstilling kan klares på flere måder, men det optimale vil være, at skolen udarbejder en anvendelsespolitik for det trådløse netværk, hvoraf det fremgår, hvad der logges, og hvad data anvendes til. Politikken skal brugerne acceptere forud for adgangen til det trådløse netværk. Om skolen skal udarbejde en selvstændig anvendelsespolitik for det trådløse netværk, eller om dette skal indgå i en samlet anvendelsespolitik for alle skolens it-systemer, er op til skolen. Flere skoler kan med fordel arbejde sammen om en fælles formulering af politikken.

Logningen og brug af logdata til overvågning og efterforskning kan udgøre behandling af fortrolige persondata og skal i så fald anmeldes til Datatilsynet. Ligeledes kan Datatilsynet være behjælpelig med anvisninger på, hvad der er god og dårlig databehandlingsskik i forhold til registrering af internetbrug.

Logdata bør slettes, når de ikke længere anvendes.

Læs mere om Persondataloven på

<http://www.datatilsynet.dk/lovgivning/persondataloven/>

13.4 Et minimum af sikkerhed: culpa (objektivt ansvar)

I jura arbejdes med begreber som "bonus pater" og "culpøs adfærd". Omsat til dansk handler det om, hvornår man er i god tro, og hvornår man "burde vide bedre". En skole, der ikke lever op til et vist minimum af "sund fornuft", kan blive påført et erstatningsansvar.

På et område som trådløse netværk udvides opfattelsen af, hvad der er "sund fornuft" over tid, efterhånden som teknologien stiller bedre muligheder til rådighed for sikkerheden og sikkerhedsproblemer, og løsninger omtales i medierne og bliver lettere at sætte op og anvende. I sidste ende vil det dog være op til en domstol at afgøre et evt. søgsmål, men ud fra en teknologisk vurdering kan det i dag næppe anses for "god skik", hvis en skole har stillet et ukontrolleret, åbent trådløst netværk til rådighed for fri, anonym adgang.

UNI•C anbefaler:

- Adgang til netværket begrænses til registrerede brugere.
- Der udformes en anvendelsespolitik, som brugerne skal acceptere.
- Logning anmeldes til Datatilsynet.
- Hvis skolen udbyder trådløst netværk som en del af en kommerciel virksomhed, undersøges logningskrav hos It- og Telestyrelsen.

14 Bilag 1 – Ordliste

Nedenstående ord er brugt med den angivne betydning i denne rapport om skolers trådløse netværk. Ord, der i beskrivelserne er markeret med *kursiv*, indgår selv i ordlisten.

14.1 Ordliste med tekniske udtryk og forkortelser

802.11., se *IEEE 802.11-standard*.

abuse, alle ISP'er (Internet Service Provideres) har en abuse-funktion, som sørger for, at brugerne af ISP'ens netværk overholder spillereglerne. Internettet er jo i bund og grund et fællesskab. I ethvert fællesskab er der regler, som skal overholdes – ellers fungerer fællesskabet ikke. Hvis ISP'en, og dermed ISP'ens kunder, skal deltage i fællesskabet, er det derfor nødvendigt have en abuse-funktion. ISP'ens abuse-funktion har til opgave at håndhæve spillereglerne over for ISP'ens kunder og om nødvendigt anvende de sanktionsmuligheder, der er beføjet den, for at bringe misbruget til standsning.

AD, Active Directory, er en teknologi udviklet af Microsoft og som bruger ændrede versioner af eksisterende protokoller og tjenester, der indeholder en række netværkstjenester.

AES (Advanced Encryption Standard), også kendt som Rijndael, er en blokkrypteringsalgoritme som blev gjort til national amerikansk standard (FIPS) af det amerikanske standardiseringsinstitut NIST i november 2001.

accessport, accesslink port, accessporte på en *switch* anvendes til tilslutning af enheder som maskiner og *AP*'er. Normalt er der kun konfigureret et enkelt *VLAN* på en *accessport*. *Uplink*-porte anvendes i modsætning til accessporte til tilslutning af andre *switch*e. *Uplink*-porte er normalt konfigureret som trunk-porte.

accesspunkt, access Point (AP), en trådløs basisstation, *WLAN* basisstation, er betegnelsen for en enhed, der forbinder *WLAN*-kompatible klienter til et kablet *LAN*.

AP, se *Accesspunkt*.

applikation, et program, der tjener et brugerformål, modsat systemprogrammer, fx

- tekstbehandlingsprogrammer
- webbrowsere
- elektronisk post (e-mail)
- regneark
- regnskabsprogrammer
- tegneprogrammer
- multimedia, fx til afspilning af musik og visning af videoer
- bankernes kontoføringssystemer
- kontopakker, som Microsoft Office, StarOffice, OpenOffice.org m.fl.

autonomt WLAN, et *WLAN*, hvor *AP*'erne ikke er styret af en *controller*, dvs. et netværk, hvor konfiguration foretages direkte i de enkelte *AP*'er, og hvor der ikke centralt foretages overvågning af *AP*'erne.

band select, se *Band steering*.

band steering/band select, funktion, der medvirker til at *klienter*, der både har en 2,4 og en 5 GHz *radio*, så vidt muligt vælger at tilslutte sig på 5 GHz-båndet, hvor der ofte vil være bedst performance.

Bonus Pater Familias, se *Culpa*.

captive portal (hotspot), en funktion, der giver mulighed for at lade brugerne logge ind på det trådløse net via en simpel webside.

Cat6 (kategori 6), betegnelse for *PDS* netværkskabel med 4 snoede ledningspar.

Cisco, navn på netværksudstyrsfirma placeret i San Francisco.

controller, WLAN-controller, en netværksenhed, der bruges til at styre de *AP*'er, der er i netværket. Styringen omfatter konfiguration, vedligehold og overvågning af *AP*'erne.

culpa, culpøs, culpa er et juridisk udtryk (der stammer fra latin) for skyld, brøde, uagtsomhed, forseelse og synd. Det er en grundlæggende retsgrundsætning, som – selvom den ikke er nedskrevet i dansk lov– udgør dansk rets almindelige erstatningsgrundlag. En person, der volder skade, siges at have handlet culpøst eller have overtrådt culpapreglen, hvis vedkommende har handlet forsætligt eller uagtsomt. Ved vurderingen af, om der er handlet culpøst, ser man på, om den skadegørende handling afveg fra et på handlingens tidspunkt anerkendt adfærdsmønster.

Før i tiden brugte man en fiktiv gennemsnitsperson, en såkaldt Bonus Pater Familias, og sammenlignede den skadegørende handling med, hvilken reaktion denne ufejlbarlige person ville have udøvet. Men i erkendelse af, at ingen mennesker er ufejlbarlige, er denne vurderingsmetode på kraftigt tilbagetog.

DHCP (Dynamic Host Configuration Protocol), en DHCP-server på et *LAN* giver dataterminaludstyr med en DHCP/BOOTP-klient alle de netværksoplysninger, der skal til, for at de kan fungere korrekt.

DNS, DNS-server (Domain Name System, Domain Name Server, Domain Name Service), En *DNS-server* eller *navneserver* er en server placeret på et *IP*-baseret datanet, der tager sig af oversættelsen af de navne, man normalt arbejder med på internet til *IP*-adresser.

domæne, skolens domæne, Windowsdomæne, en gruppe af servere, der er baseret på et og samme directory over brugere, maskiner m.v.

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security), *login*metode for *WPA2-Enterprise*.

ethernet, den mest udbredte standard til locale netværk(LANs).

FE (Fast Ethernet), et *LAN* med transmissionshastigheden 100 Mb/s.

fil, se *print og fil*.

firewall, netværksenhed, der adgangssorterer på trafiktype, nettype, brugertype m.v.

firmware, er ligesom software et edb-program. Der er ikke en klar skelnen mellem software og firmware. Mens software betegner højniveau-programmer, der kan skiftes uafhængig af hardware, er firmware lavniveau-programmer, der ofte er hardware-specifikke. Firmware er derfor bundet til hardwaren.

GB (Gigabit), et GB-LAN har transmissionshastigheden 1 Gb/s.

GHz: 10^9 Hz, som er enheden for frekvenser.

hotspot, se captive portal.

IEEE802.11-standard, en standard for *WLAN* udarbejdet af Institute of Electrical and Electronics Engineers. IEEE er en non-profit brancheorganisation, som har til formål at fremme teknologisk innovation inden for elektricitet. Foreningen har mere end 395.000 medlemmer i mere end 160 lande, 45 % uden for USA.

Internet Authentication Service (IAS), Microsoft *RADIUS-server* for Windows 2003 Server.

IP, IP-adresse (Internet Protokol), et unikt nummer som netværksenheder (fx computere) bruger til at kommunikere med hinanden over internetprotokollen (IP).

klient, en mobil, trådløs computer, der kan kobles på *WLAN*'et. I dag er det primært laptops, der medbringes og skal på skolen *WLAN*, men fremover må det forventes, at også smartphones og ikke mindst håndholdte computere som iPad og tilsvarende vil finde indpas.

krydsfelt, netværkspunkt, hvor flere fysiske ledninger/netværk sammenkobles.

LAN (Local Area Network), det netværk, der er opbygget, fx på en skole.

load balancing, udjævning af trafikmængden på de tilsluttede enheder.

lobbyfunktion, en adgangsstyring for gæster, hvor en eller flere medarbejdere – typisk en receptionist eller sekretær – har mulighed for at udlevere et *login* til gæster, når denne besøger skolen. Se også *sponsorfunktion*.

login, bruges både om processen med at få adgang til et netværk og om selve adgangskoderne.

MAC-adresse (Media Access Control), en unik adresse for fysisk udstyr på et netværk.

navneserver, se *DNS-server*.

NAT (Network Address Translation), proces, der ændrer netværksadressen i IP-pakkeheaderen, mens den transmitteres igennem en router, med det formål at oversætte et IP-adresseområde til et andet.

Relevant, hvis man på et netværk bruger *IP-adresser* fra de lokale *IP-adresseområder*. Disse adresser kan ikke routes over internet, hvorfor de skal konverteres til officielle eller globale *IP-adresser*, når de forlader skolens *LAN*.

netværksdrev, skolens filserver tilgås fra klienter på nettet via netværksdrev.

Network Policy Server, Microsoft *RADIUS-server* for Windows 2008 Server.

objektivt ansvar, den juridiske definition af et udvidet ansvarsgrundlag der er hjemlet (fastsat ved lov eller domstolspraksis) og som ikke kræver *culpa* hos skadevolder. Altså er skadevolder erstatningsansvarlig, også uden at have handlet uforsigtigt eller uagtsomt.

pakke, både datatrafik og kontroltrafik opdeles og sendes digital i pakker. Hver pakke har en identitet, således at afsender og modtager kan synkronisere trafikstrømmen; hvilket også medfører at flere klienter kan udveksle pakker (næsten) samtidigt.

PDS-kabel (Protective Distribution System), et netværkskabel inklusiv termineringer, der bruges til ukrypteret transmission af klassificerede oplysninger.

PEAP-MSCHAPv2 (Protected Extensible Authentication Protocol. MSCHAPv2, er Microsofts version af Challenge-Handshake Authentication Protocol). *Login*-metode for *WPA2-Enterprise*.

PKI (Public Key Infrastructure), et sæt af hardware, software, mennesker, politikker og procedurer, som er nødvendige for at udstede, administrere, distribuere, bruge, opbevare og tilbagekalde digitale certifikater.

PoE (Power over Ethernet), teknologi, der giver mulighed for, at strøm og datatrafik ligger i ét og samme *ethernetkabel*.

PoE-injector, netværksenhed, som placeres ved en *switch*port (hvor der i forvejen er 220 V-strømforsyning), og som kan strømføde et enkelt *AP*.

PoE-switch, *switch*, hvor alle portene har *PoE*.

print og fil, mulighed for at brugerne kan udskrive samt lagre og hente dokumenter (filer).

radio, bruges som betegnelse for den bærebølge, der benyttes ved trådløs transmission. Et *WLAN* med to radioer er typisk med 2,4 GHz og 5 GHz.

RADIUS, RADIUS-server (Remote Authentication Dial-In User Service), er en server der indeholder brugeroplysninger. Decentrale enheder kommunikerer med den centrale *RADIUS-server* for at godkende brugere og give dem adgang til det ønskede system eller tjeneste.

remote AP, et særligt *AP*, der er beregnet til opkobling mod skolens *controller* fx fra en medarbejders private net.

roaming, skift fra ét *AP* til et andet. Specielt vigtigt ved brug af mobile enheder, sådan at *WLAN*-forbindelsen ikke tabes, når man bevæger sig rundt på skolen.

Rogue AP, fremmed/utilsigtet *AP*, dvs. *AP*, som ikke bør være tilsluttet *WLAN*'et.

router, Netværksenhed, der fordeler trafik mellem flere fysiske og/eller logiske net. Routeren indeholder *accesslister* (der angiver, hvilke brugere og systemprocesser der kan få adgang til ressourcer på netværket bag routeren) og politikker for fordelingen.

server, en computer, som deler sine resurser såsom periferiudstyr og *filer* med andre computere, kaldet *klienter*, på et LAN.

site survey, en radiomæssig gennemmåling af hele det område, hvor der skal være tilslutning til det trådløse net med henblik på den mest optimale placering af *AP*'er.

SKI-aftalerne, en række indkøbsaftaler som finansministeriet – efter udbud – har indgået med en række leverandører, som kan benyttes af offentlige og halvoffentlige institutioner. Læs mere her: <http://www.ski.dk/aftaler/Sider/default.aspx>

skyen, topologisk tegnes internet ofte som en sky. Når noget ligger 'i skyen', menes der, at det ligger uden for skolens *VLAN*.

SMTP, Simple Mail Transfer Protocol er en protokol, man bruger til at sende e-mail med over internettet.

sniffer, sniffing: En "packet analyzer" (også kendt som "network analyzer", "protocol analyzer" eller "sniffer" eller for særlige typer af netværk en "ethernet sniffer" eller "trådløssniffer") er et computerprogram eller et stykke computerhardware, der kan opfange trafikken over et digitalt netværk eller en del af et netværk. Sniffere vil detektere hver pakke og afkode og analysere indholdet.

sponsor-funktion, en adgangsstyring for gæster, hvor skolens eksisterende brugere kan give netadgang til deres gæster. Medarbejderne virker på den måde som "sponsorer" for deres gæster. Se også *lobbyfunktion*.

spoofing, spoofe: Den grundlæggende protokol for at sende data over internetnetværket og mange andre computernetværk er Internet Protokollen (*IP*). "Headeren" af hver *IP*-pakke indeholder bl.a. afsender- og modtageradresse for pakken. Afsenderadressen er normalt den adresse, hvor pakken er sendt fra. Ved at ændre "headeren" så den indeholder en anden adresse, kan en hacker få det til at se ud, som om pakken er sendt fra en anden maskine. Maskinen, som modtager de falske pakker, vil sende en melding tilbage til de forfalskede afsenderadresser, hvilket betyder at denne teknik hovedsagligt bliver brugt, når hackeren ikke bekymrer sig om tilbakemeldingerne, eller når hackeren har mulighed for at gætte sig til tilbakemeldingerne på forhånd. I visse tilfælde er det muligt for hackeren at se eller omdirigere tilbakemeldingerne til hans egen maskine. Den mest brugte metode er, når hackeren laver en forfalskning af en adresse på det samme *LAN* eller *WAN*. Derfra har hackeren en uautoriseret adgang over computerne.

SSID (Service Set Identifier), navnet på det logiske *WLAN*, man kobler *klienten* til.

stream, streaming media, er media, der bliver konsumeret (læst, hørt, set) i takt med, at det bliver leveret. Det modsatte princip er, at man kopierer mediet, hvorefter man kan bruge det. Streaming er selve det, at media bliver distribueret over et datanet. Ordet "stream" kan oversættes til dansk som en strøm, og det bliver også anvendt som et verbum, hvor det betyder dette at levere medier i "strømmende form".

switch, en netværksenhed, der fordeler trafikken mellem flere fysiske og/eller logiske net.

switchport, en netværkstilslutning i en *switch*, som kan forbindes til andre tilsluttede netværk.

TCP, TCP/IP (Transmission Control Protocol), en af kerneprotokollerne på internettet. Gennem TCP kan programmer på forskellige værtsmaskiner på nettet oprette forbindelser mellem hinanden, gennem hvilke der kan udveksles datapakker. Protokollen giver, modsat *UDP*, programmelle på værtsmaskinerne et par vitale garantier for disse datapakkers afsendelse og modtagelse.

TKIP (Temporal Key Integrity Protocol), er en sikkerhedsprotokol i IEEE 802.11 wireless networkingstandard. TKIP blev udviklet, som en erstatning for WEP.

UDP (User Datagram Protocol), en protokol til overførsel af data. UDP er en del af Internet-protokolstakken, som oftest benævnes *TCP/IP*. I protokolstakken anvendes enten *TCP* eller *UDP*. *UDP* giver ingen garanti for, at data kommer frem (eller rettere: afsenderen får ikke besked, hvis data ikke kommer frem).

UNI•Gateway, en netværksboks med et kontrolsystem, der prioriterer trafik til og fra skolen. Sælges af UNI•C.

UNI•Login, fælles gratis adgangskode for en lang række tjenester i uddannelsesverdenen. UNI•Login drives af UNI•C, mens adgangskoder administreres af lokale brugeradministratorer på skolerne.

UNI•Radius, en central *RADIUS-server* drevet af UNI•C. Med UNI•Radius logger brugere på med deres *UNI•Login*.

UNI•Wireless Management, et overvågningsystem for *controllerbaserede WLAN*. Drives af UNI•C.

UNI•Wireless Management Pro, som *UNI•Wireless Management*, men hvor overvågningen foretages centralt af UNI•C på skolens vegne.

uplink hastighed, er hastigheden på en uplink port.

uplink port, en *switch* har normalt 1-4 uplink porte, der anvendes til tilslutning af andre *switch*e. Uplink porte er normalt konfigureret som trunk porte. Se også *access-port*.

VLAN (Virtual Local Area Network), et logisk lokalnetværk, dvs. et separat netværk, der ikke nødvendigvis er fysisk adskilt fra andre netværk.

Voice over IP (VoIP), en teknologi, så man kan føre telefonsamtaler over internettet.

WEP (Wired Equivalent Privacy), en nu forældet sikkerhedsalgoritme for IEEE 802.11 *WLAN*.

WLAN (Wireless Local Area Network), et trådløst lokalnetværk, dvs. et netværk hvor klienter trådløst kan koble sig på netværket.

WLAN-controller, se *Controller*.

WPA-Enterprise og **WPA2-Enterprise**, (Wi-Fi Protected Access) er et certificeringsprogram udviklet af Wi-Fi Alliance (brancheorganisation), som skal indikere overholdelse af sikkerhedsprotokollen, som er lavet af Wi-Fi Alliance. Sikkerhedsprotokollen er med til at sikre trådløse computernetværk og blev udarbejdet som reaktion på flere alvorlige svagheder, som forskere havde fundet i det tidligere system WEP.

15 Bilag 2: Eksempel på kravspecifikation

Dette bilag indeholder et eksempel på en kravspecifikation for en fiktiv større kommuneskole, der ikke har en egentlig it-afdeling, men har en lærer med specielt interesse og kendskab til it generelt og til skolens brug af it. Endvidere bruges skolens pedel til almindelig mindre håndværkeropgaver bortset fra el-arbejde, som udføres af den lokale installatør.

15.1 Kravspecifikation for Den Grønne Skole

Der ønskes tilbud på et WLAN, der kan opfylde flest mulige af nedenstående punkter. For alle punkter ønskes en besvarelse på, om og i givet fald hvorledes punktet vil kunne opfyldes.

Punkterne er opdelt i:

K står for **krav**

Ø står for **ønsker**, som vil veje med i vurdering af, hvilket system der vælges.

O står for **optioner**, som skolen kan købe som tillæg/erstatning.

Tilbud (som skal være gyldig indtil d. 15. om tre måneder) bedes senest fredag d. 12. i næste måned sendt til:

Den Grønne Skole
Skolevej 3
1234 Storby
Tlf.: 12345678
E-mail: kontoret@DengronneSkole.dk

Uddybning af nedenstående punkter, herunder inspicering af skolen og dets netværk, kan ske ved henvendelse til:

Skoleleder Jens Rasmussen
It-ansvarlig Jan Pagh
Kontorassistent Benedicte Hansen
Konsulent Michael Andersen, UNI•C, telefon 35 87 88 89

K1 Det trådløse net skal kunne anvendes med kraftig signalstyrke og kapacitet på de med grønt markerede områder på vedlagte plantegning, hvor der også er anført antallet af samtidige brugere i de forskellige områder. I de med gult markerede områder skal der være god forbindelse. I gymnastiksalen (markeret med rødt) skal der være ekstra sikkerhed for, at 80 samtidige elever kan betjene sig af nettet med kraftig kapacitet og uden

ventetid (maks. 5 sekunders på-lognings-tid), da der her afholdes eksamener. I alt har skolen 600 elever og 53 ansatte. Der er aftenskole med 15-25 kursister i hvert af lokalerne 13-17 alle hverdage fra 19-21 undtagen fredag og lørdag.

Ø1 På områder uden farvemarkering må der gerne være en rimelig signalstyrke og kapacitet for 50 samtidige brugere.

K2 Der skal være adgang for følgende brugertyper: Ansatte (A) og elever (E) på skolen med en WPA2-Enterprise-sikkerhedsløsning samt gæster (G) fra Den Gule Skole med en hotspot sikkerhedsløsning. Hvis anden sikkerhedsløsning tilbydes, skal denne og førnævnte standarder sammenholdes.

K3 Alle brugertyper skal ved pålogging anvende deres UNI•Login, og de skal valideres op imod UNI•Radius.

K4 Skolen har tre VLAN, nemlig A-VLAN'et beregnet for de ansatte (lærere og administrativt personale), P-VLAN'et beregnet for elever samt for gæster et O-VLAN, som alene giver adgang til internet. Der vil skulle laves en 1-1 mapning mellem 3 SSID'er og de 3 VLANs. Alle brugere skal kunne tilslutte alle AP'er.

K5 I lokale mærket Musik og arealet mærket Aula vil der skulle kunne streames video af 2-3 samtidige brugere.

Ø2 På alle gangarealer, udendørsarealer og i kantinen må der gerne være mulighed for brug af VoIP.

K6 Det eksisterende faste net skal benyttes i så høj grad som muligt. På vedlagte topologitegning er anført eksisterende switche (model) og krydsfelter. Switche markeret som x-PoE angiver, at det er en PoE-switch. Antallet af ledige porte er ligeledes vist.

Ø3 AP'er bør strømfødes over nettet. Hvis dette ikke kan opfyldes 100 %, angives de AP'er, som skal have egen strømforsyning etableret, hvilket skolen i givet fald vil sørge for efter anvisning fra leverandør.

O1 Skolen påtager sig selv kabelfremføring efter anvisning fra leverandør, men som option ses gerne en pris, hvis dette indgår i tilbuddet. Skolens eksisterende fremføringsveje (primært lofter med aftagelige loftplader) kan beses ved henvendelse til skolen.

K7 Systemet skal indeholde mulighed for logning af, hvem der bruger nettet hvornår og til hvad. Skolen påtænker selv at anskaffe et separat overvågningssystem (UNI•Wireless Management), hvorfor leverandøren skal angive evt. begrænsninger for dette.

O2 Skolen ønsker at to personer uddannes i konfiguration og drift af systemet. Omfang og pris for et sådan kursus bedes anført separat som option.

O3 Inden for de næste fem år påtænkes opførelse af en ny fløj C (vist stiplede og ikke farvemarkeret) på plantegningen. Tilbuddet skal indeholde en dagspris for udbygning, så fløj C med ca. 150 elever i 10 lokaler også kan tilsluttes systemet.

K8 Tilbuddet skal omfatte løbende fejl- og sikkerhedsopgraderinger i fem år.

O4 Der ønskes en option for indgåelse af en tre-årig servicekontrakt med fejlafhjælpning inden for seks timer mandag-fredag kl. 7:00-16:00.

K9 Der ønskes mindst fem referencekunder – og helst skoler – som har fået samme eller et lignende WLAN installeret.

K10 Hvis etablering forudsætter udgifter, som leverandøren ikke har tænkt sig at afholde, og som ikke i denne specifikation er nævnt som ting, skolen tager sig af, skal dette oplyses, fx indkøb af 4 PoE-injectors til brug for switch X17 og tilhørende strømforsyning.

O5 Det valgte tilbud ønskes betalt kontant. Men der ses gerne en option for opdeling i tre årlige rater.

K11 Leverandøren skal angive, i hvor mange år han forventer at kunne vedligeholde, opgradere og udbygge systemet – ud fra egne og eventuelle underleverandørers nuværende planer. Som minimum forventes systemet at have en levetid på fem år – og det kræves, at evt. 'End-of-life' kommunikerer til skolen med mindst 36 måneders varsel.

Ø4 Systemet må gerne baseres på én central controller af mærket xx el.lign., som styrer alle AP'er.

Ø5 Skolen har et mindre ikke-professionelt trådløst netværk på kontorgangen. Dette er af mærket yy. Hvis dele af dette kan anvendes, ses det gerne.

Ø6 Det er et stærkt ønske, at systemet er baseret på AP'er med 802.11n-standarden på både 2,4 og 5 GHz. Hvis dette ikke er tilfældet, bør leverandøren redegøre for forskelle mellem det tilbudte og førstnævnte standard.

Ø7 AP'er må gerne have indvendige antenner.

K12 Leverandøren skal angive, hvordan han udregner antal og placering af AP'er. Vil der fx blive gennemført et komplet site survey, en stikprøvekontrol eller foregår beregningen anderledes?

16 Bilag 3: Eksempel på anvendelsespolitik

Skolen forventer, at alle brugere optræder ansvarsbevidst og påtager sig et medansvar for skolens it-ressourcer.

16.1 Accepteret brug af netværket

Skolens trådløse netværk er fortrinsvist stillet til rådighed for undervisningsrelevante formål.

Derudover må netværket anvendes til andre formål, der ikke strider mod skolens etiske regelsæt eller dansk lovgivning. Skolens etiske regelsæt kan læses på skolens hjemmeside.

Misbrug omfatter, men er ikke begrænset til:

- udveksling eller kopiering af ophavsretligt beskyttet materiale uden forudgående accept
- hacking
- forsøg på at skaffe sig adgang til eller misbruge andre brugeres bruger-id, password eller øvrige private oplysninger.

16.2 Brugernavne og adgangskoder

Alle skolens brugere skal anvende UNI•Login ved login til det trådløse netværk.

UNI•Login, der består af et brugernavn og et password, er strengt personligt og må ikke deles eller lånes ud. Har du mistanke om, at dit UNI•Login har været misbrugt, så skift straks password og anmeld mistanken til skolens it-administration.

16.3 Tilgængelighed og oppetid

Under normale forhold kan skolens trådløse netværk tilgås fra alle skolens lokaler og udendørs områder.

Skolen bestræber sig på at sikre en optimal drift af det trådløse netværk til gavn for alle brugere.

Skolen kan dog ikke garantere 100 % oppetid, ligesom der ved udfald eller tekniske fejl kan opstå lokale "huller" i netværkets dækning.

Såfremt der opleves driftsproblemer, anmeldes dette straks til skolens it-administration.

16.4 Ansvar for medbragte pc'er

Ansvar for medbragt udstyr påhviler ejeren. Dette gælder såvel det fysiske udstyr som lagrede data og programmer m.m.

Skolen kan ikke påtage sig noget ansvar for data og programmer på pc'er og andet udstyr medbragt af brugerne. Dette gælder også, selvom evt. problemer kan være forårsaget af tilslutningen til skolens trådløse netværk.

Skolens forsikringer dækker ikke tyveri eller hærværk mod medbragt, privat udstyr.

16.5 Krav til udstyr, der tilsluttes netværket

Udstyr, der tilsluttes skolens trådløse netværk, skal opfylde følgende krav:

For bærbare pc'er:

- Antivirus skal være installeret.
- Automatisk opdatering er aktiveret for antivirus og øvrige programmer, hvor det er muligt (som minimum for Microsoft og Adobe).

16.6 Logning

Skolen registrerer følgende oplysninger om al tilgang til det trådløse netværk med henblik på driftsovervågning og opklaring af driftsproblemer og misbrug:

- ved logon: Bruger-id, tidspunkt for logon og logoff samt tildelt IP-adresse
- båndbreddeforbrug – download og upload for alle brugere
- alle fejlslagte forsøg på logon: Tidspunkt og bruger-id
- NAT- og sessionsoplysninger (tidspunkt, IP-adresser og porte).

Oplysningerne opbevares i et år og slettes herefter.

Kun skolens it-administrator og skolens it-leverandør har adgang til disse logningsoplysninger. Oplysningerne anvendes alene til brug for driftsovervågning og opklaring af problemer og misbrug.

16.7 Anmeldelse og efterforskning af misbrug

Skolens brugere forpligter sig til at rette ekstra opmærksomhed på og anmelde alle forsøg på misbrug til skolens it-administration.

Ved anmeldelse af misbrug (fra brugere eller udefra) påtager skolen sig at medvirke til efterforskning af anmeldelsen og efterfølgende vurdering af evt. misbrug og sanktioner.

16.8 Sanktioner

Der er følgende sanktionsmuligheder:

- mundtlig påtale og advarsel
- skriftlig advarsel (evt. underretning af elevens forældre, hvis eleven er under 18 år)
- inddragelse af adgang til det trådløse netværk (evt. permanent)
- bortvisning.

Politiangivelse vil kunne komme på tale i forbindelse med alle ovennævnte sanktioner.

16.9 Erklæring

Alle skolens brugere udfylder og underskriver en erklæring om at have læst og accepteret denne politik. I erklæringen gives endvidere samtykke til, at skolen kan foretage den i politikken anførte behandling af persondata uden yderligere accept fra brugerne.

17 Bilag 4 – De mest almindelige driftsproblemer

17.1 Problemer med at logge på net beskyttet med captive portal (hotspot)

1. Jeg får ikke login-siden frem?
 - Tjek, om du har fået den rigtige IP-adresse, default gateway og DNS.
2. Jeg har fået en IP-adresse, der starter med 169 (169.x.x.x)?
 - Maskinen har ikke fået en IP-adresse via DHCP og har derfor automatisk tildelt sig selv den pågældende IP-adresse. Det er ikke muligt at få netforbindelse med denne IP-adresse. Det skal sikres, at DHCP-serveren kører korrekt.
3. Jeg har fået en korrekt IP-adresse, men får ikke login-siden frem?
 - Tjek, om der er god dækning der, hvor du opholder dig. Hvis du er ene om problemet, forsøges med en anden browser og/eller en genstart af maskinen. Hvis andre har tilsvarende problemer, er der formentlig et generelt problem med controlleren eller den enhed, der står for captive portal-funktionen. Tjek controllerens log.
4. Jeg får login-siden frem, men bliver afvist hver gang?
 - Hvis andre godt kan logge ind, er det RADIUS-serveren, der afviser dig. Tjek, at brugernavn og password er korrekt. Tjek efterfølgende, at du har rettighed til at logge på. Hvis ingen kan logge på, er der problemer med kommunikation mellem controller og RADIUS-server. Undersøg, om RADIUS-serveren er nede, og genstart den i givet fald.
5. Min maskine kan slet ikke se nettet?
 - Tjek, om det trådløse netkort er aktiveret. Hvis det er tilfældet, og der ikke er andre i samme område, der har problemer, genstartes maskinen. Hvis det ikke løser problemet, tjekkes, om driveren til det trådløse netkort er opdateret til nyeste version. Undersøg producent og model for netkortet, og gå på producentens hjemmeside og download nyeste version. Installér driveren, genstart maskinen, og forsøg igen.

17.2 Problemer med at logge på net med WPA2-Enterprise PEAP-MSCHAPv2

6. Min maskine kan se nettet, men jeg bliver ikke promptet for login, når jeg forsøger at tilslutte?
 - Tjek, om maskinen er sat korrekt op til WPA2-Enterprise PEAP-MSCHAPv2. Der findes bl.a. et antal vejledninger her: <http://support.emu.dk/UNI•radius> Hvis opsætningen er korrekt, skal du sikre dig, at driveren til netkortet er opdateret til nyeste version. Undersøg producent og model for netkortet, og gå på producentens hjemmeside og download nyeste version. Installér driveren, genstart maskinen og forsøg igen.

7. Jeg bliver promptet for login, men kommer ikke på?
 - Her er det afgørende at skelne mellem, om du faktisk bliver autentificeret eller ej. Hvis du kun bliver promptet en enkelt gang, tyder det på, at dit login er korrekt. Det bør dog verificeres via controllerens eller RADIUS-serveren log. Hvis login er o.k., kan det skyldes, at du ikke har fået en korrekt IP-adresse. Tjek at du har fået en korrekt IP-konfiguration via DHCP med både IP-adresse, default gateway og DNS-servere.
8. Jeg ser ud til at komme korrekt på nettet, men får ikke trafik igennem?
 - Hvis andre er på samme net uden problemer: Genstart maskinen og prøv igen. Hvis det ikke løser problemet tjekkes, om driveren til det trådløse netkort er opdateret til nyeste version. Undersøg producent og model for netkortet og gå på producentens hjemmeside og download nyeste version. Installér driveren, genstart maskinen og forsøg igen.
 - Hvis ingen brugere får trafik igennem, er det et generelt problem – måske med internetforbindelsen. Tjek evt., om der er forbindelse fra en maskine på det kablede net. Eller må der trinvis fejlsøgning til vha. ping. Kan controllerens IP-adresse pinges, kan default gateway pinges, DNS-serveren. På den baggrund kan en sandsynlig årsag fastlægges.

17.3 Nettet er ustabil – jeg mister ofte forbindelsen

9. Nettet er ustabil i et bestemt område af skolen. Hvad kan der være galt?
 - Hvis klienten ofte mister og fornyer IP-adressen, kan det skyldes, at signalstyrken er svag (dækningen er dårlig) i det pågældende område. Måske er et AP ustabil (genstarter ofte), gået ned eller har mistet netforbindelsen. Eller også bør der sættes et ekstra AP op for at sikre tilstrækkelig dækning.
 - Hvis signalstyrken i øvrigt er god, og maskinen ikke fornyer IP-adresse, kan det skyldes overbelastning af spektret. Enten fra andre brugere eller eksterne støjkilder. Prøv evt. at flytte kanal – enten ved at gennemtvinge et kanalskift på AP'et eller ved at lade maskinen gå på 5 GHz båndet (hvis det er en mulighed). Tjek også, om der evt. kan være et fremmed AP, der støjer.
10. Det plejer at køre fint, men pludselig er alle begyndt at få problemer?
 - Hvis problemet også ses på det kablede net, er der formentlig tale om en ustabil eller overbelastet internetforbindelse eller firewall/router.
 - Hvis problemet kun ses på det trådløse, kan det skyldes, at belastningen er steget, og at nettet efterhånden er overbelastet. Ses problemet evt. kun på tidspunkter, hvor der generelt er mange aktive trådløse brugere? Undersøg vha. et overvågningsværktøj belastningen generelt, pr. AP og pr. bruger. Ofte er det et mindre antal brugere, der belaster nettet ekstremt meget.
11. Der er flere der har problemer med at nettet er ustabil. Problemet er ikke bundet til bestemt områder eller tidspunkter. Hvad kan der være galt?
 - Formentlig en driverfejl eller inkompatibilitet mellem klient og trådløst net.

Undersøg producent og model for det trådløse netkort, og gå på producentens hjemmeside og download nyeste version. Installér driveren, genstart maskinen, og forsøg igen.

17.4 Der er forbindelse, men nettet er meget langsomt

12. Det virker som om, det kun er i et bestemt område, det kører langsomt?
Det er sandsynligt, at nettet er overbelastet i det omtalte område. Ved hjælp af overvågningssystemet kan årsagen let fastlægges. Det kan være et AP, der er gået ned. Mere sandsynligt er der en bruger eller to, der lægger beslag på en stor del af båndbredden. I så fald kan systemet fastlægge, hvem det er, og brugere kan kontaktes.
13. Nettet er langsomt på bestemt tidspunkt hver dag?
Overvågningssystemet kan være med til at fastlægge årsagen. Hvis hele nettet er langsomt – også det kablede – kan det være internetforbindelse eller firewall, der er belastet. Hvis kun det trådløse er langsomt, er der sandsynligvis tale om belastning pga. mange samtidige brugere. Det bør vurderes, om belastningen er jævnt fordelt over AP'er og bånd (2,4 og 5 GHz). Igen er det overvågningssystemet, der er værktøjet.