

## Unngå trådløst kaos

*Så er vi klare. Vi har testet trådløst Ethernet i ulike sammenhenger og funnet at dette er noe for oss. Sikkerhetsproblematikken lar seg løse, båndbredden synes tilstrekkelig for bruksmønsteret i flere avdelinger, og kostnadsbildet står i forhold til den gevinsten vi regner med å få. Sist, men ikke minst har mer enn et dusin medarbeidere allerede skaffet seg trådløse nettverk hjemme, og bærer seg over IT-avdelingens tilbakeståenhet og sendrektighet.*

### Konsolideringen i gang

Det trådløse LAN-markedet er ungt, uansett synsvinkel, men ikke desto mindre foregår det allerede konsolidering i segmentet. Proxim, en av de eldste aktørene innen trådløs teknologi generelt, overtok nylig Orinoco, som på kort tid har rukket å bli den største i USA på WI-FI produkter (hvilket i praksis vil si 802.11b-produkter). En integrasjon av de to selskaperes produkt-familier og teknologier utgjør en både spennende og slagkraftig kombinasjon, som spenner fra 11 Mbps lokalnett til høyhastighets, sikrede samband med opp til 108 Mbps båndbredde og over avstander på inntil 50 km.

<[www.proxim.com](http://www.proxim.com)>

Her må det handles. Det står ikke bare om teknologi og gevinster, men om ego og ære. IT-avdelingen skal ligge foran, ikke henge etter, den skal vite mer, og ikke minst ha kunnskap om hva som er lurt, hva som ikke er det og hvorfor. Her skorter det spesielt ofte i forbindelse med trådløse lokalnett: Sikkerhetsproblemer har vært unnskyldningen så langt, men holder ikke lenger, og de fleste er klar over nettopp det.

Det finnes ingen vei utenom. Her er det lite annet å gjøre enn å brette opp armene og sette i gang: Kartlegge utfordringene, skaffe oversikt over produkter, leverandører og priser, finne ut hvem som er kompetente på hvilke områder – og så videre.

Hvor vi begynner er som kjent helt avgjørende for resultatet, og nettopp på grunn av presset vi nevnte ovenfor, har tallrike WLAN-prosjekter endt opp som rene katastrofer. Som vi påpekte i forrige utgave av Mellvik-Rapporten: WLAN er ikke LAN – selv om det prøver hardt å være nettopp det. Misforståelsen er hovedårsaken til de fleste feilslåtte prosjektene.

Når markedsstatistikker og utviklingstrender for trådløse nettverk blir presentert, får vi inntrykk av en eksplosiv utvikling og en gigantisk suksess. Mens tallenes tale er uomtvistelig, er det samtidig et faktum at det finnes få virkelig store WLAN-installasjoner. Kompleksiteten vokser gjerne eksponensielt i forhold til antall aksesspunkter, og når antallet passerer noen få titall, har praktiske og driftsmessige forhold sørget for effektivt å stoppe veksten. Dette har naturligvis ikke bare med teknologiens egenskaper å gjøre, men er også i stor grad knyttet opp mot produktenes modenhet, og de verktøy som finnes for å kontrollere og styre systemene. Her foregår det fortsatt intens utvikling og konsolidering innen segmentet, et forhold vi har vært inne på tidligere i Mellvik-Rapporten.

### Små tuer velter store lass

I denne artikkelen skal vi rette søkelyset mot en samling problemstillinger som i henhold til erfaring ofte skaper forviklinger i slike prosjekter. Helt i tråd med ordtaket om at 'liten tue kan velte stort lass' dukker tilsynelatende ubetydeligheter opp og forstyrrer eller forsinker prosjektene – ofte i tilknytning til idriftsetting eller slutt-testing.

### Sikkerhet

Vi har ved flere anledninger proklamert at WLAN-sikkerheten nå er under kontroll – bare den brukes. Bedre algoritmer og større nøkler gjør at de innebygde krypteringsmekanismene gir tilstrekkelig transportsikring for alminnelige behov.

Sikkerhet har imidlertid flere sider, og problemstillingene blir helt annerledes i en større sammenheng med mange brukere og ditto aksesspunkter, enn med et par punkter og en håndfull brukere. Vi trenger løsninger som for det første er skalerbare, og for det andre lar seg integrere sømløst med eksisterende mekanismer og tjenester. Derfor må følgende punkter avklares allerede i planleggingsfasen:

- ✓ Hvilke mekanismer for brukerautentisering er optimale, hva trengs av ekstra utstyr eller programvare for å koble sammen og synkronisere brukernavn og passord med eksisterende systemer?
- ✓ Gir autentisering mot nettverket automatisk autentisering mot bakenforliggende tjenester/tjenere (SSO)?
- ✓ Trenger vi aksesskontroll på brukernivå, eller er det tilstrekkelig å kunne tillate/stenge for grupper?
- ✓ Hvordan kontrollerer og administrerer vi sikkerheten i systemet?
- ✓ Er mulighetene for logging og sporing av aktiviteter tilstrekkelige?

Det optimale er å kunne integrere policystyring og aksesskontroll med eksisterende mekanismer, knyttet opp mot en katalogløsning. RADIUS utpeker seg som den foretrukne og allerede dominerende standarden for autentisering, og lar seg integrere med de fleste systemer.

I forbindelse med planlegging av sikkerheten er det også viktig å ta hensyn til bruken av VPN (eller SSL, se side 28). Dersom alle WLAN-brukere benytter VPN, er det sannsynligvis hensiktsmessig og praktisk å droppe bruken av løsningens egen krypteringsmekanisme.

### Se opp for spesialløsninger

Det er fristende å se på det trådløse nettverket som et nett for seg selv, og separere det fra øvrige lokalnett, for eksempel gjennom VLAN-mekanismer. Dette er i de fleste tilfeller unødvendig og kompleksitetsdrivende. Vel skal vi ta spesielle forholdsregler og hensyn i forbindelse med WLAN-tilkoblinger, men når dette er gjort, er det riktig å betrakte teknologien på linje med annen såkalt *link-layer* teknologi, dvs. resten av Ethernettet:

- ✓ “Vi må se på det trådløse nettverket som et eksternt nettverk” hører vi ofte. Påstanden er kun riktig dersom vi lager en offentlig IP-sone. Med sikkerhets- og autentiseringsmekanismer på plass, er det rimelig og riktig å se på et WLAN som en del av lokalnettet.

- ✓ I og med at alle lokalnett i dag er svitsjede i alle fall, er det lite å tjene på å separere *roaming*-trafikk (administrativ trafikk mellom aksesspunktene) til sitt eget nett. I den forbindelse er det viktig å verifisere at aksesspunktene kommuniserer seg imellom på nivå 3 (IP), ikke på nivå 2, og at protokollene som benyttes er compatible fra én leverandør til den neste.

Det skal med andre ord gode argumenter til for ikke å benytte den eksisterende infrastrukturen (kabelnettet) som den er for aksesspunktene. At kabel i enkelte tilfeller må fremføres til nye steder, er en annen sak.

### **Mer er ikke alltid bedre**

Dekning og effektiv hastighet er ikke proporsjonalt med antall aksesspunkter. Å sette opp 5 punkter i nærheten av hverandre femdobler ikke kapasiteten, men kan i stedet redusere den til en brøkdel. Frekvensspekteret som benyttes av 802.11b, er snevert og inneholder kun 3 helt separate kanaler. Trafikken forstyrres av annet utstyr, og påvirkes av antenner, antenntyper og signalstyrke. Når flere aksesspunkter plasseres nær hverandre, brukes en betydelig del av tilgjengelig båndbredde til å administrere (slåss om) kanalene dem imellom. Derfor er følgende punkter viktige i planleggingen:

- ✓ Sørg for å få god oversikt over 'radio-miljøet' gjennom en grundig RF-kartlegging, utført av spesialister. Bruk resultatet som veiledende, men gjennomfør også praktiske tester for å kontrollere riktigheten. En slik undersøkelse tar neppe hensyn til mikrobølgeovnen som ble installert i kaffekroken i forrige uke, eller en kollega som kjøpte mobiltelefon med Bluetooth i går.
- ✓ Velg aksesspunkter og antenner med rekkevidde og dekning i henhold til kartleggingen.
- ✓ Sørg for å justere signalstyrken slik at overlappingen blir optimal. Kraftig signal er vel og bra på egen hånd, men ikke når det forstyrrer naboen (dvs. nærmeste aksesspunkter). Velg klientutstyr som synkroniserer signalstyrke mot aksesspunktet: Det har lite for seg at aksesspunktet kan justeres til optimal signalstyrke dersom brukerne fortsetter med 'full pedal'.

Samspill er nøkkelen – og utfordringen, og forutsetter at utstyret er sofistikert nok til å kunne tilpasse seg omgivelsene.

### **Begrenset båndbredde**

Det er lett å glemme at brukerne er bortskjemte – med 100 Mbps dedikert båndbredde og tilsvarende responstider. Når de skal dele en 11 Mbps-forbindelse hvis effektive hastighet er 6 Mbps, er det ikke til å unngå at det kommer klager. En forutsetning for suksess er derfor å kartlegge behov og krav før brukere overføres til trådløse forbindelser. En rekke anvendelser er rett og slett for båndbreddeintensive til å kunne kjøres med dagens trådløse teknologi.

I andre tilfeller er båndbredden tilstrekkelig dersom den brukes og fordeles optimalt. Derfor har 802.11e-standarden for prioritering av trafikk på link-nivå dukket opp i trådløst utstyr det siste året. Mer administrasjon betyr imidlertid mer arbeid, og å utvide kapasiteten med 802.11a (54 Mbps) i enkelte områder, kan være en mer optimal løsning. Kombinerte basestasjoner har vært på markedet siden 2. kvartal i år, mens klient-utstyr (PCMCIA-kort) som støtter begge standarder, blir tilgjengelige i disse dager.

Den ferske 802.11g-standarden, som utvider dagens 11 Mbps-standard til 22 Mbps eller mer, kan også bli et alternativ, og har den fordel at den er kompatibel med 802.11b. Den kjemper imidlertid om plass i et frekvensbånd som blir stadig tettere befolket, og det er ikke opplagt at teorien lar seg omsette i praksis. Slik markeds- og teknologibildet ser ut i dag, er 802.11a en langt sikrere vei til høyere båndbredde enn 802.11g.

### Standard med variasjoner

WI-FI-standarden fra WECA er katalysatoren som har gjort 802.11b-suksessen mulig. Å sørge for at utstyret er sertifisert av WECA er derfor en selvfølge. Det er imidlertid grenser for hva som kan standardiseres, og en rekke leverandører har utviklet sine egne 'forbedringer' og tillegg til standarden.

Disse utvidelsene skaper naturligvis kompatibilitetsproblemer som det er umulig å styre unna: Selv om vi bestemmer oss for å holde oss til én bestemt leverandør, vil besøkende som skal ha konnektivitet og utstyr med innebygget WLAN-støtte uvegerlig skape komplikasjoner. Viktige observasjoner i den forbindelse er derfor:

- ✓ Hold hodet kaldt når selgere markedsfører de 'uvurderlige utvidelsene' deres produkt kan by på. Spør hvordan de kan utnyttes i et heterogent miljø.
- ✓ Unngå utstyr som krever spesiell programvare på klientsiden. En driver er uunngåelig, mens alt annet bør være overflødig og skaper ekstra driftskostnader.
- ✓ Styring og kontroll av det trådløse nettverket skal kunne gjøres fra nettverket, ikke via en av basestasjonene. Mekanismer og protokoller skal fortrinnsvis være leverandøruavhengige.

I løpet av det siste året har det dukket opp styringsverktøy for WLAN fra uavhengige leverandører, som utnytter en del av utvidelsene de største leverandørene har innført. Ved hjelp av et slikt 'mellomlag', gjemmes inkompatibilitetene, samtidig med at vi får en rekke funksjoner – blant annet logg-analyser og policy-styring – som er meget attraktive. Ideelt sett skulle disse verktøyene ha vært moduler som 'plugges inn' i vår eksisterende styrings-infrastruktur, men segmentet er for ungt til at så har skjedd. Først om et par års tid vil dette være regelen i stedet for unntaket.

WI-FI – 'Wireless Fidelity'  
WECA – Wireless Ethernet Compatibility Alliance [www.wi-fi.org]

### **Forandring er regelen**

Mens dagens WLAN-marked ser relativt ryddig ut, kan vi love at fremtiden blir det motsatte. Utviklingen følger mønsteret etter Ethernet, men komprimert i tid: Spredningen er eksplosiv, komponentprisene synker med rekordfart, og nye utstyrstyper og kategorier kommer til over en lav sko. Om kort tid skal vi i tillegg til bærbare maskiner med 802.11b-kort, forholde oss til tablet-PCer, PDAer, printere, kopimaskiner, kaffemaskiner, telefoner, Bluetooth, 802.11g, 802.11a, 802.11a+ og så videre. Det er nærliggende å bruke amerikanernes uttrykk: "You ain't seen nothing yet!" Vi kan ikke planlegge for alle disse enkeltteknologiene og produktene, men vi kan legge forholdene til rette for forandring. Det betyr å unngå å overinvestere i eksisterende teknologi, men i stedet å følge behovskurven tett. Sjansene for at vi i løpet av to år vil ha behov for å bytte basestasjoner er stor.

Likeledes er det viktig å være bevisst de begrensningene som finnes, og å se etter optimaliseringer. For eksempel ser vi at til tross for at den effektive båndbredden i trådløse nettverk øker, vil båndbredde forbli en flaskehals i overskuelig fremtid. Derfor er det naturlig å se etter løsninger og produkter som optimaliserer bruken av både denne og andre begrensede ressurser.

### **Fremtiden kan ingen gjemme seg fra**

Frykt er å finne blant de mest alminnelige utviklingsbremser, og nettopp frykt – for blant annet sikkerheten – har bremset spredningen av trådløse nettverk i profesjonell sammenheng. Mens det i enkelte tilfeller kan argumenteres for å være tilbakeholden, er det alltid en fare for å havne bak sine egne brukere.

Vi så hvilke konsekvenser en slik situasjon kan få i forbindelse med Internett-bølgen på 90-tallet. I organisasjoner som ikke skaffet egen Internettforbindelse, satt annenhver bruker med sitt eget modem og Internett-abonnement, med den følge at det interne nettverket sto åpent for hvem som helst – store deler av døgnet. Samtidig tikket kostnadene avgårde på en måte som ikke kunne spores, men som ikke desto mindre skulle dekkes.

Tilsvarende skjer med trådløse nettverk i disse dager. De er blitt tilstrekkelig billige til at brukerne tar saken i egne hender: Armert med erfaring fra hjemmenettverket, kjøper de aksesspunkt, plugges inn – og er 'på nett': En IT-avdelings mareritt og som regel en regulær katastrofe i sikkerhetsmessig forstand. At problemet kan reduseres ved å ha god kontroll på adresse-utdelingen i nettverket (DHCP), hjelper lite når dette kun unntaksvis er tilfelle.

Løsningen er innlysende: Å ha godt synlige holdninger og planer for ny teknologi tilstrekkelig tidlig til at slike overtramp blir mindre fristende, og å sørge for at brukerne er kjent med konsekvensene. Selv om planene finnes eller trådløse nettverk allerede er på plass, er det fortsatt god grunn til å ha en aktiv holdning til 'pirat-aksesspunkter': De kommer og går, og er alltid like risikable.

## Oppsummering

Planlegging og installasjon av trådløse nettverk er en jobb for eksperter: I forhold til radiobølger er kabler for en trivialitet å regne. Bølger reflekteres, forsterkes, dempes og forstyrres. De passerer uhindret gjennom noen materialer, blokkeres av andre og er lett 'synlige' for alle som er innen rekkevidde.

Utfordringen med å etablere store nettverk må håndteres deretter, og ingen kunnskap kan konkurrere med erfaring. Likeledes må erfaringen være lokal: Byggeskikker, materialvalg, standarder og forskrifter varierer fra land til land, hvilket har store konsekvenser for hvordan radiobølgene sprer seg i rom av tilsvarende størrelse.

Vi har diskutert 7 gjengangere i forbindelse med etablering av trådløse nettverk i profesjonelle miljøer: 7 viktige påminnelser om hvor fort gjort det er å havne galt ut på ulike trinn i prosessen:

- ✓ **Sikkerhet** – er langt mer enn mekanismer. At den finnes er ikke det samme som at den er tilstrekkelig eller i bruk.
- ✓ **Kompleksitet** er en fiende – og spesialløsninger skaper kompleksitet. Spesialløsninger for WLAN er sjelden nyttige.
- ✓ **Mer er ikke alltid bedre:** Kapasitetsproblemer kan kun unntaksvis løses gjennom flere aksesspunkter i samme område.
- ✓ WLAN har **begrenset båndbredde:** 802.11b gir effektivt 6 Mbps med en innendørs rekkevidde fra 20 til 100 meter. Dette er magert i forhold til hva brukere flest er vant med i våre dager, og utilstrekkelig for en rekke anvendelser.
- ✓ **WI-FI standarden** er viktig, men de fleste leverandørene har utvidelser. Disse er sjelden kompatible leverandørene imellom og må brukes med omtanke.
- ✓ **Forandring** er regelen, og det vi installerer i dag må trolig byttes eller endres i løpet av 2 år. Legg forholdene til rette for kontinuerlige endringsprosesser.
- ✓ **Fremtiden kommer** uansett – ikke vent til brukerne kommer med den – bakveien.