

Trådløse lokalnett: Fra test til effektiv drift

Dette er andre artikkel i en miniserie med fokus på praktisk bruk av trådløse nettverk. Tredje og siste artikkel i serien kommer i august-utgaven (nr. 108).

Vi fortsetter der vi slapp i forrige utgave – med gjennomgangen av ulike sider ved WLAN-teknologi – et segment som forandrer seg nærmest fra måned til måned: Hvem hadde for 6 måneder siden hørt om 'trådløse svitsjer', som i dag er en selvfølge i tilknytning til WLAN-prosjekter?

Vi har tidligere diskutert WLANs tallrike barnesykdommer, hvorav en rekke med letthet kunne ha vært unngått. De har vært forårsaket av forvirring som både teknologer og markedsførere må ta ansvaret for. I sin iver etter å alminneliggjøre teknologien, ble den opprinnelig solgt inn som en 'forlengelse av kabelen' – en utvidelse av lokalnettet, en implikasjon som også ligger i navnet WLAN. Mens det kan argumenteres for en slik fremstilling i logisk forstand, ser vi i ettertid at den gjorde langt mer skade enn gagn.

Mens sikkerhet og sikkerhetsproblemer har fått mest oppmerksomhet det siste året, spenner årsakene til denne forvirringen langt videre – fra kapasitet og hastighet (som vi var inne på i forrige utgave) til stabilitet og pålitelighet. At sikkerhet får mest interesse er ufortjent, men ikke urimelig – og har sin åpenbare årsak i det forholdet at sikkerhet er det mest synlige.

Like fullt starter vi med noen betraktninger knyttet til nettopp sikkerhet, før vi griper fatt i en oversikt over mindre opplagte teknologiske forhold som må være med i ligningen når et større nettverk skal planlegges.

Nye ideer – nye anvendelser

Den mest spennende konsekvensen av rimelige trådløse lokalnett har med nye anvendelser å gjøre. Å fjerne kabelen mellom utstyr og nettverk er vel og bra, men introduserer lite nytt i seg selv. Det er å utnytte den nyvunne friheten som virkelig blir spennende. Eksempelene dukker opp på løpende bånd, og har ofte med det vi kan kalle yrker i bevegelse å gjøre. Håndverkere, transportbransje, lov og orden, teknisk service – for å nevne noen. I mange tilfeller er det mindre viktig hvilken teknologi som benyttes – om det er GPRS, WLAN, WLL eller andre varianter. Der konstant konnektivitet er et krav, må mobiltelefoni-nettverket benyttes, mens der bevegeligheten er mindre eller kravene til løpende konnektivitet beskjedne, er *hot-spots* og WLAN ideelt. Oakland politidistrikt i Nord-California er et godt eksempel på det siste: Alle politibilene har i en periode hatt bærbare PCer med trykkfølsomme skjermer installert. Diverse registre oppdateres et par ganger i uken slik at oppslag i forbryterarkiv (ettersøkte fjes), stjålne kjøretøyer og så videre, går raskt. Data-oppdateringen er imidlertid tungvint, og oppdatering av programvare likeså: Hver enkelt bil må 'behandles' manuelt.

Oppsetting av en liten håndfull WLAN aksesspunkter i byen har imidlertid løst problemet billig og effektivt. PCene laster automatisk ned det som måtte finnes av oppdateringer når bilene er i nærheten av et aksesspunkt. Oppdateringen tar i høyden et par minutter per dag, og gevinsten er lett å kvantifisere i og med at de manuelle oppdateringene er borte. Videre har konstablene dagfersk informasjon til enhver tid, hvilket gir flere arrestasjoner og færre feiltagelser. Og flere aksesspunkter kommer, etter at prøveperioden nå er over og de praktiske resultatene kan dokumenteres. Her er det ideer å hente for noen og enhver!

Konnektivitet, mobilitet og sikkerhet

Sikkerhetskysteriet i tilknytning til WLAN er omsider avtagende etter å ha nådd øredøvende høyder i en periode. Noen – men ikke mange – har fått med seg at sikkerhetsproblemene, her som ellers, i første rekke har hatt med mennesker og sløvhet å gjøre, og i andre rekke med teknologiske svakheter. Nå er teknologien rettet opp, bevisstheten omkring risikoen hevet, og sikkerheten blitt generelt bedre.

Avstanden er imidlertid stor fra 'litt bedre' til 'mye bedre'. Lerretet som skal blekes, er fortsatt stort. At teknologi ikke lenger kan brukes som unnskyldning for å 'la sløvheten råde' har i forbausende liten grad påvirket situasjonen. Nye aksesspunkter dukker opp over en lav sko med minimal eller fraværende sikkerhet. I privatmarkedet er det lite å gjøre med forholdet – inntil Internett-leverandørene (ISPene) tar affære overfor sine kunder og pålegger dem (eller tilbyr hjelp til) å sørge for grunnleggende sikkerhet.

I bedriftsmarkedet er forholdet annerledes: Grunnleggende sikkerhet må ivaretas straks, hvilket forutsetter to konkrete tiltak utover å sørge for at riktig teknologi finnes og tas i bruk. Etablering av en klar policy for bruk av trådløs kommunikasjon,⁴ og aktiv scanning av nettverket etter brukerinstallerte aksesspunkter. Relativt enkle logistikkverktøy

som kartlegger og kategoriserer alle noder på nettverket er alt som skal til, samt at informasjonen faktisk brukes. I den forbindelse er det viktig å huske at brukerne sjelden er så dumme som de selv vil ha det til. I motsetning til hva som synes å være alminnelig konsensus, viser praktisk erfaring at de fleste brukere som setter opp 'pirat-aksesspunkter', vet at dette ikke er akseptabelt, og har 'rutiner' for ikke å bli oppdaget: De slår av aksesspunktene når de ikke selv er på kontoret – og når de har mistanke om at kontroll foregår. Forholdet burde være håndterbart gjennom en klar policy, men slik alminnelig

Offer for sin egen popularitet

Wi-Fi utstyr har havnet i kategorien 'nesten gratis', og er i en del miljøer blitt like selvfølgelig som fjernkontroll til TVen. Dermed går det som med motorveien, det blir kø og dårlig fremkommelighet. I enkelte boligkomplekser, spesielt i USAs store byer, opplever brukerne voksende problemer med å kunne bruke sitt eget trådløse nettverk. Når alle leilighetene – som ikke er spesielt store – har sitt eget aksesspunkt, kanskje flere, blir de tre tilgjengelige kanalene i 802.11b-standarden lite å dele på. Bedre blir det ikke når den ene etter den andre både snakker i sin trådløse telefon, lager middag i mikrobølgeovnen og nylig har installert alarm med trådløse følere. Her er gode råd om ikke dyre så i alle fall nødvendige, og veien ut for WLAN-brukerne er enkel, om ikke alltid ønskelig: 802.11a har flere kanaler, lav tetthet og beskjeden rekkevidde – det siste er normalt en ulempe, men i denne sammenhengen en fordel. I praksis betyr det at veien ligger åpen for kombinasjons- (*dual band*) grensesnitt, som gjør det rimelig enkelt å bytte fra det ene til det andre. Under slike forhold – som vi kan garantere blir mer alminnelige i tiden fremover – har 802.11g lite å by på.

En annen vei ut av uføret er å sentralisere trådløsheten. I slike leilighetskomplekser er det optimalt å tilby trådløs Internett-aksess som en tjeneste. Tjenesteleverandører og eiere har vært forbausende sendrektige med å oppdage denne muligheten, hvilket er årsaken til situasjonen vi beskrev ovenfor. Spørsmålet er om toget nå har gått. Når 'alle' har skaffet seg sitt eget utstyr, er incentivet for fellesløsninger beskjedent. Her burde imidlertid 802.11a ha betydelig potensiale. Mot slutten av inneværende år vil et flertall av PC-leverandørene tilby innebygget 11b/g/a i sine bærbare maskiner. Da er det programvaren som avgjør hvilke løsninger som vinner. Her er det enkleste også det beste.

praksis er her til lands, er konsekvensene minimale for selv alvorlige forseelser. Effekten av regler og tiltak er deretter, og må følges av handling. Konsekvensene av overtredelser må gjøres godt kjent – gjentatte ganger, og den praktiske håndhevelsen må være synlig for alle.

⁴ En policy som kort og godt sier nei til trådløse lokalnett, er sjelden hensiktsmessig og praktisk talt alltid unyttig. Den vil fungere som en invitasjon til 'POWER USERS' om å ta saken i egne hender.

Bedre sikkerhet med konnektivitet

Sikkerhetsproblemene vi har vært vitne til gjennom media og praktisk erfaring, må ikke brukes som unnskyldning for ikke å ta i bruk trådløse nettverksteknologi. Som vi har sett, kan autentisering og kommunikasjon gjøres så sikker som behovene tilsier. Dessuten – og like viktig – er konstant konnektivitet i mange tilfeller grunnlag for bedre sikkerhet i stedet for det motsatte. Vi har lett for å glemme at bærbart utstyr, det være seg mobiltelefoner, PDAer, PCer eller spesial-terminaler (se figur 3), er notoriske sikkerhetsrisikoer i seg selv. De er små og lette, og tilsvarende enkle å stjele og skjule. Dersom de inneholder verdifulle data, hvilket er regelen for utstyr som ikke er konstant *on line*, er risikoen spesielt stor. Ved å ta i bruk trådløse nettverk og gjøre utstyret om til bevegelige terminaler som kun overfører data, ikke lagrer noe lokalt, er risikoen vesentlig mindre, selv der data-transporten ikke er sikret. Er også overføringene sikret, hvilket er regelen i dag, gir den nyvunne konnektiviteten en vesentlig forbedring av den totale sikkerheten.



Figur 3 Eksempler på trådløse spesial-terminaler (bilder fra Symbol Technologies).

Vi kommer tilbake til praktiske sikkerhetstiltak – alternativer, prioriteringer og konsekvenser – i seriens siste artikkel (Mellvik-Rapporten nr. 108).

Planer og arkitektur

Et kosteffektivt og funksjonelt trådløst lokalnett forutsetter planlegging. Hva vi ønsker å oppnå (målsetting, forventninger), hvordan (teknologi, arkitektur, prosjekt, spesifikasjoner, leverandører) og hva det skal koste (budsjett). Planen blir ikke mindre viktig om vi allerede har en del av nettverket installert. Det koster langt mer å flikke på et dårlig utgangspunkt enn å skrote det som finnes, og starte på ny frisk.

Uttrykket arkitektur hører naturlig inn i denne sammenhengen, men blir stadig misbrukt av WLAN-leverandører – i markedsføringsmateriale og presentasjoner, og blir derfor lett misforstått (se definisjon av arkitektur i artikkelserien på side 20). For anledningen kaller vi oppgaven ganske enkelt for planlegging, og poengterer følgende punkter som hører hjemme i den tidlige planleggingsfasen:

- ✓ Ethvert prosjekt handler til slutt om kosteffektivitet – som ikke alltid kan kvantifiseres, men som i alle fall må sannsynliggjøres. Kostnadene (investeringer og driftskostnader) kan imidlertid alltid kvantifiseres, og må fordeles på antall bru-

- kere. Sørg for at brukerantallet er reelt: Ikke alle, eller 'noen', men et antall som det er overveiende sannsynlig vil benytte tjenestene – hele tiden eller deler av tiden.
- ✓ Bruksfrekvens: Hvor hyppig og hvor mye vil tjenestene bli benyttet? Vær realistisk – og kritisk. Dersom brukerne har et alternativ allerede, må det nye være vesentlig bedre, enklere eller begge deler for at det skal bli tatt i bruk. Løsninger som kommer i veien, velges bort der det lar seg gjøre.
 - ✓ Hva blir kostnadene sammenlignet med andre alternativer (i dette tilfellet fast lokalnett)? Dersom det faste nettverket finnes allerede, blir dette spesielt interessant. Vi må kvantifisere tilleggsverdien. Samtidig sørger det eksisterende nettverket for at utplassering av aksesspunkter er enkelt og rimelig. Noen virksomheter og oppgavetyper egner seg åpenbart bedre for trådløshet enn andre. Transiente arbeidsplasser – for eksempel anleggskontorer – er et godt eksempel.
 - ✓ Fokuser på de mest åpenbare og relevante faktorene: Produktivitet/effektivitet, teknologi-styring (forenklinger, kostnadsreduksjoner), tilgjengelighet (utvidet og forbedret infrastruktur), forenkling av arbeidsprosesser (for eksempel at data registreres på direkten i stedet for 2 eller flere ganger).

Tekniske observasjoner

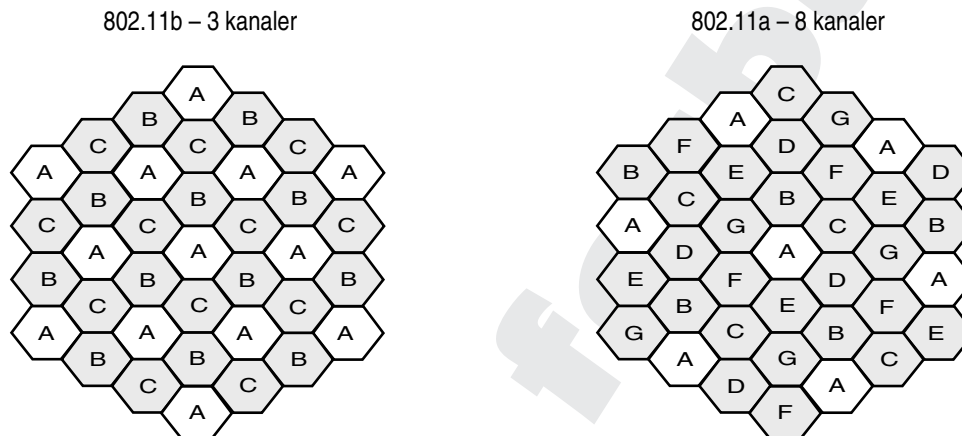
WLAN-produktene som kommer på markedet i disse dager, tilhører tredje generasjon, hvilket er en rekord i seg selv i et dynamisk marked. 3 generasjoner på like mange år. Generasjonsskiftene bærer med seg forandringer og forbedringer med utgangspunkt i erfaringer fra tusenvis av installasjoner siden 2000. Mens mange av disse erfaringene og de tilhørende løsningene er godt ute av syne for brukere flest, er de høyst relevante for oss som skal velge leverandører, teknologi og produkter. Her er det i enda større grad enn ellers dyrt å handle 'kjapt og billig' – og av beskjeden nytte med avanserte produkter dersom leverandøren ikke forstår eller har kunnskap om dem.

Punktene nedenfor sammenfatter en del slike praktiske erfaringer fra en lang rekke WLAN-installasjoner, med vekt på forhold som har lett for å bli oversett i planleggingsfasen. Når de dukker opp – i forbindelse med pilottesting eller praktisk bruk, blir det gjerne kostbart og/eller tidkrevende å foreta justeringer.

- ✓ Grundig radioplanlegging er en forutsetning for pålitelighet, stabilitet og fornuftig utnyttelse av den tilgjengelige båndbredden. Radioplanlegging er ikke for amatører, og påvirkes av en lang rekke mer og mindre opplagte forhold – for eksempel bygningsmaterialer (i vegger, tak, gulv, veggflatens vindusareal osv.), antenne-teknologi, brukertetthet og støykilder. Planleggingen begynner på papiret, men må alltid substansieres av praktiske målinger.
- ✓ Pålitelighet har mange sider. For eksempel er det rimelig å forlange at bortfall av et aksesspunkt knapt skal merkes av

brukerne. Det betyr blant annet at svitsjene som styrer aksesspunktene, automatisk flytter brukere til nærmeste funksjonelle punkt i tilfelle feil, og at tettheten er stor nok til å tillate dette.

- ✓ Et beslektet forhold er hva som skjer dersom ryggradsnettverket 'går ned': Kan svitsjene sørge for en regulert frakobling av klientene til konnektiviteten er gjenopprettet? Er det ønskelig at konnektivitet mellom klientene opprettholdes?



Figur 4

Fordelingen av radiokanaler gjøres slik at aksesspunkter med samme kanal plasseres så langt borte fra hverandre som mulig. Der avstanden blir så tett at merkbar interferens oppstår, må sender-effekten justeres ned, eventuelt i kombinasjon med bruk av retningsspesifikke antenner. I 2,4 GHz-området (11b, 11g) har vi kun 3 separate kanaler til disposisjon, hvilket gjør plasseringen spesielt vanskelig i store miljøer. Dette forholdet reduserer teknologiens skalerbarhet. Dette blir vesentlig enklere for 11a, der vi har 8 kanaler til disposisjon.

- ✓ Interferens er et kontinuerlig problem i trådløse omgivelser. Nærliggende aksesspunkter kan ikke unngå å påvirke hverandre selv om fordelingen av kanaler gjøres etter alle kunstens regler (se figur 4). Derfor er det optimalt for aksesspunktene å kunne regulere signalstyrken automatisk, og å kunne fortelle klientene hvilken styrke de skal bruke. Dette er et område som mangler skikkelig standardisering, med tilhørende samspillproblemer mellom leverandører.
- ✓ Radioplanleggingen indikerer hvor det er optimalt å plassere aksesspunktene – eller deres antenner. Dersom planleggingen er gjennomført for 11b-teknologi, er det rimelig å ta høyde for en fremtidig fortetning i forbindelse med at 11a-teknologi blir tatt i bruk. Å 'ta høyde for' i denne sammenhengen betyr fremføring av eller tilrettelegging for kabler.
- ✓ Av praktiske hensyn er det et krav at aksesspunktene strømforsynes via parkabelen – gjerne fra nærmeste svitsj. Hittil har vi manglet en standard på dette området, og vært henvist til leverandørenes egne mer eller mindre kompatible løsninger. I disse dager legger imidlertid IEEE siste hånd på PoE-standard (Power over Ethernet, IEEE 802.3af, se www.ieee802.org/3/af/).
- ✓ Som vi allerede har vært inne på (forrige artikkel), er bruk av trådløse svitsjer en nødvendighet – av en rekke årsaker: Au-

- tomatisk *failover* (driftssikkerhet, se ovenfor), *roaming*, last-balansering – for å nevne noen få.
- ✓ Typiske PC-anvendelser er ofte krevende med hensyn til båndbredde, og konsumerer alt som gjøres tilgjengelig. En lang rekke anvendelser klarer seg imidlertid med langt mindre enn de maksimale 3-6 Mbps for WLAN. For å spare energi i mobile enheter er det nødvendig å tilpasse båndbredden til behovet. Dette blir viktigere etterhvert som flere utstyrstyper med WLAN-aksess kommer til (PDAer, telefoner, spesial-terminaler). Derfor er det nødvendig at aksesspunktene kan tilpasse seg klientenes behov og egenskaper, og kan 'svitsje ned' bitraten uten at dette gir negative 'følgeskader'.
 - ✓ 802.11a-teknologien er attraktiv av en rekke årsaker, men det er viktig å være klar over at spesial-terminaler kun unntaksvis har kapasitet til – eller behov for – å støtte denne standarden. I mange tilfeller betyr det at valget ikke står mellom 11a og 11b, men mellom 11b og 11b+11a.
 - ✓ WLAN-teknologi er ideell for sammenkobling av nettverk mellom bygninger over korte avstander – og over lengre avstander med spesialantennene (se forrige utgave). Sørg imidlertid for en grundig evaluering av båndbreddebehovene: Det har lite for seg å sette opp slike forbindelser dersom de reelle behovene kun kan tilfredstilles med kabel eller fiber.
 - ✓ Telefoni over WLAN kommer. Derfor er det riktig å bygge inn eller legge til rette for mekanismer for trafikkprioritering (QoS) i nettverket allerede nå.

Neste artikkel

Siste artikkel i denne miniserien kommer i august (Mellvik-Rapporten nr. 108), og tar for seg sikkerhetstiltak – hva er nødvendig, hvilke valgmuligheter har vi og hvilke muligheter finnes for forenkling i et bilde som synes å bli stadig mer uoversiktlig?

Flere konkurrenter til 3G mobiltelefoni

Mens dødsdommene hagler over den forventede 3G-mobilteknologien, samler 'gribbene' seg for å overta markedet. Og om 802.11-teknologi er den mest synlige og utbredte, finnes det alternativer som har betydelig massefart og leverandører som mener å ha bedre forutsetninger enn WLAN for oppgaven. Vi nevnte noen av disse i artikkelen "Trådløshet truer telefonlinjene" i Mellvik-Rapporten nr. 104, med hovedvekt på den ferske 802.16-standard.

Her står spesielt 802.16e-standard sentralt: Den spesifiserer mobilitet for trådløse teknologier som hittil har vært stasjonære – i lisensierte deler av 2GHz til 6GHz området. Mens 802.16e er fersk, har arbeidet med selve transport-standard 802.16 – som også går under navnet *Wireless Local Loop* eller WLL – vært i arbeid en stund. Her blir veien til mens vi går, og leverandørene oppdaget først i 2002 at deres teknologi kunne ha potensiale langt utover det opprinnelige segmentet.

Ambisjonene vokser, og utfordringene for 3G-teknologien har gitt blod på tann for WLL-klanen, som i desember 2002 fikk satt i gang en arbeidsgruppe i IEEE for spesifisering av en utvidet 802.16-standard, under navnet 802.20 og med frekvensområde 0,5 til 3,5 GHz, som overlapper hele GSM og 3G spektrene. Målsettingen er åpenbar: Å konkurrere med og forhåpentlig erstatte 3G-teknologien, som av stadig flere blir ansett for å være *too little, too late*.

802.20 er blodfersk – på papiret, men de ivrigste leverandørene, Flarion og ArrayCom, har for det første allerede demonstrert hvordan den fungerer og for det andre vist automatisk samspill med 802.11 (WLAN) nettverk. Dette begynner virkelig å lukte *business*. Vi kommer tilbake til Flarion og 802.20-teknologien i neste utgave av Mellvik-Rapporten (se baksiden).

Videre skal vi diskutere de siste trendene på området, ikke minst i kjølvannet av nyheter fra Networld+Interop messen i Las Vegas i begynnelsen av mai måned. Når kommer telefonien – og kombi-telefonene – for alvor? Hva med den effektive båndbredden – har vi mer å hente? ■

Kopiering forbudt