

Trådløse lokalnett: Fra test til effektiv drift

Dette er tredje og siste artikkel i en miniserie med fokus på praktisk bruk av trådløse nettverk. De første artiklene var å finne i hhv. nr. 105 og 106.

Mer standardisering

WLAN er fortsatt for fersk teknologi å regne. Derfor er det naturlig at utviklingen er raskere enn på de fleste andre områder vi omgås til daglig: Standarder, produkter, verktøy, anvendelser og så videre. Ingen revolusjoner, men evolusjon i rikelig monn.

Et glimrende eksempel i så henseende er 802.11g-standarden. Utvidelsen av den dominante 802.11b har vært på beddingen i snart to år, med produkter tilgjengelige siden i fjor, men på sensommeren i år ble standarden ratifisert. Denne milepælen er beskjedent i teknisk forstand i og med at forskjellene i forhold til utkastet som har eksistert siden i fjor er beskjedne. I forhold til markedet er hendelsen langt mer betydelig: Usikkerheten knyttet til å kjøpe produkter hvis standard fortsatt er 'tentativ' er borte.

Og produkter som støtter 802.11g, omsettes i raskt voksende volumer. Riktignok har veksten avtatt vesentlig i forhold til forventningene for et år siden, i takt med den generelle nedgangen i IT-markedet. For 802.11-produkter som gruppe, var veksten i 2. kvartal på 6% i volum og 2% i verdi i forhold til 1. kvartal – ifølge Dell'Oro Group. For rene 11b-produkter observerer vi – som ventet – en kraftig nedgang som kompenseres av veksten for 11g.

Fra 802.11b til 11g

Siden de aller fleste 11g-produkter er kombinasjoner som støtter både 11b og 11g, blir det imidlertid misvisende å si at 11b er på tilbaketog. Det hersker liten tvil om at den opprinnelige og robuste 11 Mbps standarden vil representere fundamentet for WLAN i overskuelig fremtid. Videre er det et faktum at selv om produktene som kjøpes i voksende grad dekker begge standarder, er det som regel 11b som brukes: Den dekker behovene, er relativt robust og støttes i alle sammenhenger der WLAN finnes. Markedet kjøper 11g-produkter fordi de oppfattes som mer avanserte og tillegget i pris er beskjedent. Dessuten – og kanskje like viktig – markedsføres de ferske 11g-produktene hardt fra leverandørsiden. De har lyktes i å skape et bilde av at første generasjons 11b-produkter er modne for utskifting, hvilket kun unntaksvis er tilfelle.

Som vi også har vært inne på tidligere i denne serien, er forvirringen stor med hensyn til hva 11g-produktene betyr i praksis – ikke minst fordi markedsføringen i så sterk grad fokuserer på en hastighetsgevinst som i de fleste tilfeller er teoretisk. Følgende punkter – som har sin opprinnelse fra praktiske tester av 11g-utstyr tidligere i år – avklarer en del av de faktiske forhold:⁴

- ✓ Kompatibilitet med dagens 802.11b-produkter er på den ene siden en grunnleggende legitimering og samtidig hemmende for såvel ytelse som rekkevidde. Det er i ren 11g-modus, med kompatibiliteten bortkoblet, den høyere båndbredden kommer til sin rett.
- ✓ Maksimal bitrate for 11g er 54 Mbps, mens den typisk reelle overføringshastigheten er ca. 15 Mbps. De beste produktene nærmer seg 25 Mbps effektivt. Produkter fra leverandøren D-Link er kommet spesielt bra ut av testene.
- ✓ Mange av produktene på markedet, støtter ikke den høyeste hastigheten, men stopper ved bitraten 22 Mbps.
- ✓ Først på forsommeren kom den nye sikkerhets-standarden fra Wi-Fi (WPA, *Wi-Fi Protected Access*) med som en selvfølgelig del av 11g-produktene (og andre WLAN-produkter). Eldre produkter kan i mange tilfeller oppgraderes via nettverket. Hvilken konsekvens WPA har for de ulike produktenes effektive ytelse, er fortsatt ukjent, men et forhold det er viktig å være oppmerksom på.
- ✓ Rekkevidden er forbausende god – i ren 11g-modus. Kombineret modus gir dårligere rekkevidde. Samtidig er forskjellen mellom produktene stor – ca. 60 meter for de svakeste og over 100 meter for de beste.

To observasjoner er særlig viktige i denne forbindelse: Reduksjonen i effektiv hastighet i kombinert modus er ikke et forbigående fenomen, men en nødvendighet – en følge av hvordan teknologien fungerer. Dessuten – rekkevidden for 11g er bedre enn for konkurrerende 11a-produkter, men kun så lenge det er lite konkurranse om plassen i eteren. Når DECT-telefoner, alarmsystemer, mikrobølgeovner og *Bluetooth* blander seg inn, blir situasjonen raskt den motsatte.

802.11a inn i varmen

Utbredelsen av 11a-produkter fortsetter på lavgir – beskjeden, men stødig vekst i et avventende marked. Bortsett fra kombinerte produkter som vi kommer tilbake til nedenfor, har lite skjedd på teknologi-fronten. WPA har kommet til i nye produkter og bedre antennteknologi har økt rekkevidde og overføringsstabilitet noe.

Det betyr ikke at suksesshistoriene rundt 11a-teknologien mangler, kun at det er færre av dem. 11a koster mer, har mindre rekkevidde og har minimal tilstedeværelse i offentlige IP-soner. På den andre siden er båndbredden vesentlig høyere og robustheten større fordi vi har flere kanaler å spille på.

Markedet ønsker fordelene, men ikke ulempene – i beste Ole Brumm stil, og for en gangs skyld er 'ja takk, begge deler' et ønske som snart kan oppfylles.

⁴ Ytterligere detaljer om 11g og de andre WLAN-standardene finnes i temaheftet "Trådløse lokalnett: Fra trussel til frigjort energi", som er gratis tilgjengelig fra www.mellvik.no.



Allsidige klienter

Ingen overraskelse, men en interessant milepæl: Klient-adaptore (PC-kort) som dekker alle WLAN-standardene er tilgjengelig, fra blant andre 3Com. Produktet kom på markedet i sommer, og dekker 802.11a/b/g i tillegg til de nye sikkerhets-standardene. Energiforbruket sier annonseringen imidlertid ingen ting om, en faktor som for det første er av stor betydning og for det andre vil bli et viktig element i konkurransen mellom leverandørene. I løpet av høsten forventes tilsvarende produkter fra en håndfull andre leverandører, og mot slutten av året burde praktiske testresultater være tilgjengelige. Følg med!

Ja takk, alle tre!

I løpet av året har det dukket opp både aksesspunkter og klient-adaptore som dekker tre WLAN-standarder – 802.11a/b/g. Produktene har fått god mottagelse i markedet og 1. generasjon har demonstrert i praksis at dette er mer enn en *gimmick*. Brukermiljøene forteller at radio-planleggingen er vesentlig enklere i tillegg til at fleksibiliteten er stor. Videre blir det påpekt at forenklingseffekten av å støtte alle standardene i samme enhet er viktig. Forutsetningen er dog at verktøyene som styrer systemet, er tilstrekkelig sofistikerte. Dessuten blir uttellingen fullstendig først når klientene også støtter alle standardene, slik at en intelligent 'trådløs svitsj' – se forrige artikkel, nr. 105 side 17 – kan administrere både båndbredde og spektrum/kanaler på en optimal måte.

Det er imidlertid ikke rimelig å forvente noen stor bølge av disse kombinasjonsproduktene i første omgang. For det første er kostnaden for 11a-teknologien fortsatt høy i forhold til hva markedet oppfatter som den reelle nytteverdien. Dessuten er utfordringene knyttet til strømforbruk fortsatt uløst. Det betyr at mens det ikke er urimelig å foreta en teknologi-gardering på aksesspunkt-siden, er det et godt stykke frem til 11a-baserte bærbare klienter vil utgjøre noen betydelig andel av totalen.

På litt lengre sikt – 2-3 år – kan situasjonen se annerledes ut, ikke minst som en følge av at ITU ser ut til å komme i mål med en global utvidelse av det tilgjengelige spektrum for 802.11a. Dersom foreliggende forslag blir ratifisert, hvilket er sannsynlig på bakgrunn av eksisterende konsensus, kan dagens 8 ikke-overlappende kanaler bli utvidet til 19 for hele verden og 25 i USA. Dermed øker både kapasitet, tilgjengelig båndbredde og robusthet mellom konkurrerende teknologier i samme spektrum. Likeledes øker avstanden til 11b/g med sine 3 ikke-overlappende kanaler dramatisk, et forhold som ikke kan unngå å påvirke konkurranseforholdet teknologiene imellom.

En svitsjende bølge

Trådløse svitsjer var blodfersk teknologi da den ble presentert i denne seriens første artikkel (Mellvik-Rapporten nr. 105). Siden har bølgen tiltatt vesentlig, som vi var inne på i foregående avsnitt. En rekke leverandører har presentert slanke eller tynne aksesspunkter som i enkelte tilfeller ikke er stort mer enn en radiosender/mottaker, en antenne og en Ethernet-kontakt. Til en pris av noen hundrelapper er slike aksesspunkter i ferd med å bli bruk-og-kast teknologi i tilstrekkelig grad til at enkelte miljøer like godt installerer to på hvert punkt. Det koster mer å finne og bytte ut et defekt punkt enn å doble antallet og derigjennom etablere redundans. Intelligensen som blant annet kan velge bort et svakt eller defekt aksesspunkt til fordel for en sovende reserve-enhet, finnes lenger bak i nettverket.



Nykommeren Airespace [www.airespace.com] leverer aksesspunkter av den enkle og rimelige varianten – antenne, radio-sender/mottaker og Ethernet-kontakt. Selskapet var også tidlig ute med alt-i-ett produkter – støtte for 802.11a/b/g.

Flere standarder

Alfabet-suppen i tilknytning til WLAN fortsetter å ese ut. Ikke før er 802.11g ratifisert, så er en oppfølger i gang. **802.11n** er neste trinn i samme spektrum (2,4 GHz), og lover – eller skal vi heller si indikerer – en bitrate på ca. 100 Mbps. Tekniske detaljer er så langt magre, og 11n skal ikke forårsake søvnløse netter for noen de nærmeste to årene. Faktum er at så overbefolket som 2,4 GHz-båndet er i ferd med å bli, er det ikke innlysende at 802.11n er realiserbart utenfor strengt kontrollerte omgivelser.

En annen variant som dukker opp i fagpressen fra tid til annen, er 802.11h. Denne standarden kunne vi godt ha klart oss uten. Dens eksistens er historisk forårsaket – av europeiske myndigheter som en gang for lenge siden allokerte en del av 5 GHz-spekteret til militære formål. Den praktiske bruken er – såvidt vi har kunnet bringe på det rene – minimal, og eksistensen av utstyr som benytter frekvensene ytterst beskjeden. Ikke desto mindre – **802.11h** er 802.11a modifisert for å ta hensyn til disse militære omstendighetene – i Europa. Kort og godt en europeisk 11a-variant. Hvorvidt det er straffbart å kjøpe 11a-utstyr i USA og bruke det i Europa, er et åpent spørsmål.

Den største ulempen med trådløse svitsjer er at vi blir fullstendig leverandøravhengige. Det finnes ingen standarder for hvordan en svitsj skal kontrollere (kommunisere med) de tilknyttede aksesspunktene. Enhetene må derfor komme fra samme leverandør. Denne situasjonen er grei nok for de største leverandørene, mens den er uønsket for alle andre. Derfor ble det allerede på vårparten i år satt i gang arbeid med en standard for kommunikasjon mellom aksesspunkter og svitsjer. LWAPP, *LightWeight Access Point Protocol*, er resultatet av innsatsen så langt, og foreligger som utkast i Internettets standardiseringsorgan, IETF.

Forslaget blir positivt mottatt av bransjen i sin alminnelighet – med unntak av Cisco, som oppgir mer eller mindre plausible grunner for å reservere seg. Siden målet med standarden er å sørge for interoperabilitet mellom produkter fra ulike leverandører, er det kanskje ikke så forbausende at en dominerende aktør som Cisco vegrer seg. På den andre siden har nettopp Cisco ved en rekke tidligere anledninger vært en pådriver for standardisering. Dessuten har en Cisco-ansatt vært sentral i utviklingen av LWAPP-forslaget.

Ciscos tilbakeholdenhet vil uten tvil bremse standardiseringen på området, men det er et åpent spørsmål om markedet er villig til å la seg diktere. Vi tror fokuseringen på Microsofts gjøren og laden i slike situasjoner de siste årene, vil bidra til at Cisco til slutt velger å følge markedet. Dessuten er det lite som tyder på at Ciscos ønske om å opprettholde 'fete' aksesspunkter er teknisk forsvarlig.

Drivkrefter

I likhet med en lang rekke andre teknologier som har funnet veien inn i vårt IT-utstyr, er den viktigste drivkraften bak WLAN lav pris. Teknologien har fått tilstrekkelig oppmerksomhet til å være oppfattet som 'kul' av markedet generelt. Denne oppfatningen, kombinert med det faktum at tilleggskostnaden for utstyrsleverandørene er marginal, gjør at WLAN i løpet av inneværende år blir standardutstyr i bærbare maskiner av alle kategorier – utenfor det aller mest prisfølsomme segmentet.

Når funksjonaliteten er der, øker sannsynligheten for at den blir brukt eller at brukeren ønsker å benytte den. Dermed er bølgen i gang, behovet er skapt, brukerne oppdager at trådløsheten er så praktisk at de kan tenke seg å forsake høyere båndbredde. Vi får en effekt som har mange fellestrekk med hva vi har sett innen mobiltelefoni. Selv miljøer der det ikke finnes tekniske eller oppgavemessige argumenter for å

benytte trådløshet, gjør seg trådløse fordi brukerne forlanger det, mens motargumentene er for svake eller kompetansen for liten.

I en rekke sammenhenger er dette negativt fordi utviklingen er uten kontroll, og drives av 'superbrukere' som har tatt i bruk teknologien hjemme, og som presser på med argumenter om lav pris, lettvinhet og høyere produktivitet. Utviklingen lar seg ikke stoppe, men må bringes under kontroll – av en rekke årsaker. Én av dem er sikkerhet, som vi skal komme tilbake til nedenfor. En annen er kompleksitet. Uansett hvor enkelt og attraktivt WLAN fortøner seg for privatbrukere, representerer teknologien en kompliserende faktor i et hvilket som helst driftsmiljø. Aksesspunkter skal installeres og drives, feilsituasjoner skal håndteres, klager og problemer fra brukere skal behandles, trafikk skal styres og nettverket skal sikres. De kostnadene dette representerer, må synliggjøres og veies opp mot fordelene det trådløse nettverket gir – om noen.⁵ I mange tilfeller er det egentlige spørsmålet ikke om eller når et trådløst nettverk skal installeres, men når en policy som forteller hva som gjelder, kan være på plass.

Sikkerhet

Praktisk talt helt siden WLAN-produkter kom på markedet, har sikkerhet vært teknologiens verkebyll. Den har variert i størrelse, like mye i takt med skrekkehistorier fra markedet som med teknologiske forandringer og fremskritt. I Mellvik-Rapporten har vi diskutert temaet ved flere anledninger,⁶ og blant annet understreket at mangelfull sikkerhet i de aller fleste tilfeller har hatt sitt utspring i feilkonfigurasjon og skjodesløshet, ikke i teknologiske svakheter. Mens det på det ene siden er et faktum at trådløse nettverk medfører høyere risiko enn sine trådbaserte motparter, er det også innlysende at de samme mekanismene kan benyttes både for autentisering og transportsikring.

Dette er imidlertid ikke godt nok. I såvel trådbaserte lokalnett som i fjernnett sikrer vi gjerne en del, men ikke all trafikk. Det typiske eksemplet er bruken av SSL/TLS i forbindelse med nettlesertransaksjoner, en mekanisme som blir stadig mer populær som alternativ til spesialiserte VPN-løsninger: Det er tjeneren vi kommuniserer med, som bestemmer når sikring skal aktiviseres og når den er overflødig. Dette er både enkelt og optimalt, men ikke tilstrekkelig for trådløse nettverk. Eksponeringen gjør at det er rimelig å forlange at all trafikk alltid sikres. Dessuten er det i teknisk forstand relativt enkelt å sørge for denne sikringen.

Forutsetningene for at en slik grad av sikring skal være gjennomførbar er at:

- ✓ ... mekanismene finnes i utstyr og tilhørende programvare.
- ✓ ... mekanismene er standardiserte og fungerer uten restriksjoner mellom utstyr fra ulike leverandører.

5 Første artikkel i denne serien gjennomgår en del viktige måleparametre i den forbindelse, se Mellvik-Rapporten nr. 105 side 12.

6 Se for eksempel "Sikkerhet i trådløse Ethernet" i Mellvik-Rapporten nr. 84.

- ✓ ... utstyr og implementasjoner er effektive nok til at sikringen ikke går ut over den effektive ytelsen.
- ✓ ... mekanismene er enkle å administrere i både små og store nettverk.
- ✓ ... drifts/sikkerhets-ansvarlige er tilstrekkelig bevisste og kompetente til både å ta i bruk/vedlikeholde mekanismene og å kommunisere viktighet og ansvar til brukerne.

Å tilfredsstille disse forutsetningene er ikke like trivielt som det kan høres. Standarden som tar vare på alle sider av trådløs sikkerhet, IEEE 802.11i, er fortsatt under utvikling og blir ikke ferdig før neste år. I mellomtiden må vi forholde oss til midlertidige løsninger, som riktignok blir en del av 802.11i når den blir ferdig, men som like fullt er midlertidige.

Transportsikring

Inntil for et knapt år siden var WEP, *Wired Equivalent Privacy*, den eneste tilgjengelige standard-mekanismen for transportsikring av WLAN. WEP har med en viss rett fått skylden for at trådløse lokalnett har et frynsete rykte med hensyn til sikkerhet. For det første er mekanismen forholdsvis svak i krypteringsteknisk forstand, og for det andre har selve algoritmen hull som gjør den mindre sikker enn den burde være. Og som om ikke dette var nok, er selve navnet et bidrag til forvirring: Det indikerer at et sikret trådløst nett blir ekvivalent med et trådbasert nettverk. Så er aldri tilfelle!

WEPs svakheter er imidlertid ikke akseptable argumenter for å la trafikken gå ukryptert i eteren. WEP gir god, men ikke meget god sikkerhet, og skal brukes med mindre bedre mekanismer finnes og blir benyttet.⁷ Hovedansvaret for den dårlige sikkerheten i trådløse nettverk, og skrekkehistoriene som har versert i presse og andre media, er ikke WEP, men skjødesløshet – som vi også var inne på ovenfor. All verdens kryptering og beskyttelse har ingen effekt når de ikke brukes, hvilket har vært regelen, ikke unntaket for WLAN.

Den negative oppmerksomheten har bidratt til å bedre forholdene, og til at organisasjoner har tenkt seg om to ganger før de har gitt etter for presset fra ivrige brukere. Fortsatt er imidlertid anslagsvis mer enn halvparten av alle verdens WLAN-installasjoner – inklusive bortimot 100% av alle private WLANs – usikrede.

Utstyr levert i løpet av det siste halve året er i mange tilfeller utrustet med den nye, 802.11i-kompatible mekanismen for transportsikring (kryptering), WPA, *Wi-Fi Protected Access*. WPA gir både bedre kryptering og sikrere og mer fleksible mekanismer for utveksling av krypteringsnøkler.

⁷ Enkelte leverandører har – i påvente av WPA – laget sine egne proprietære sikringsmekanismer med tilhørende infrastruktur og verktøy for å avhjelpe svakhetene i WEP.

Autentisering

Autentisering har to nivåer: Det første er identifikasjon av utstyr – hvilke enheter skal aksepteres som klienter i nettverket og hvilke skal avvises? Vi kan forlange tilsvarende autentisering i trådbaserte lokalnett, men gjør det sjelden – under den antagelse at har du fysisk tilgang, kan du også kommunisere. Dette forholdet er annerledes i et trådløst scenario. Like fullt vegrer imidlertid mange miljøer seg for å innføre slik autentisering. Det er administrativt krevende å skulle vedlikeholde et register med alt utstyr som skal ha tilgang. Dessuten er identifikasjonen som regel basert på hardware-adresse (såkalt MAC-adresse), som lett kan forfalskes.

Ikke desto mindre er slik hardware-basert aksesskontroll å anbefale der det er mulig – og andre metoder ikke benyttes. Om adressene lett kan forfalskes, er det fortsatt en omstendelig affære for en potensiell inntrenger å finne ut hvilke adresser som er registrert og dermed akseptable. Beskyttelsen som ligger i mekanismen, er dermed betydelig – om langt fra perfekt.

Sist, men ikke minst: Dersom automatisk adressetildeling (DHCP) benyttes, kan mulighetene for misbruk reduseres ved å unngå overallokering av adresser. Sett av så mange adresser som trengs, og utvid/innskrenk i takt med behovene. Dermed blir sjansene store for at uønskede noder ikke får tildelt adresser om de forsøker.

Ingen av de to sistnevnte mekanismene kan brukes i omgivelser som aksepterer tilfeldige besøkende. Slike nettverk fordrer spesielle tiltak i forhold til interne nettverk, og bør alltid behandles som om de er like offentlige som Internettet.

Nivå 2 er bruker-autentisering, der det lettvalgte er å slippe alle brukere til på det trådløse nettverket, og overlate til systemer og applikasjoner å kontrollere hvem som er akseptable og hvem som skal avvises. Mens dette er vanlig praksis i LAN-sammenheng, er det ikke akseptabelt i et WLAN, blant annet fordi det blir altfor lett å misbruke ressurser og å skaffe seg urettmessig tilgang til ressurser og tjenester. Derfor har mange profesjonelle miljøer tatt i bruk påloggingsmekanismer basert på RADIUS-standarden⁸ – ikke bare i WLAN, men også i LAN-sammenheng, gjerne som en del av en mer omfattende *single logon* løsning.

802.1x til unnsetning

Løsningen på mange, kanskje de fleste av disse utfordringene finnes i den relativt ferske 802.1x-standarden – som også er inkludert i den tidligere nevnte (kommende) 802.11i.

802.1x er laget for lokalnett generelt, men blir ikke mindre egnet i WLAN-sammenheng av den grunn. Tvert imot er det utelukkende en fordel med en standard og tilhørende mekanismer som går på tvers av

Praktisk og interessant om WLAN-teknologi

Boken "*Building Wireless Community Networks*" av Rob Flickenger høres ut som en øvelse i moderne opportunistisk sosialisme – og er til en viss grad det. Den gir praktiske erfaringer og råd med hensyn til hvordan 802.11-baserte nettverk kan gjøres tilgjengelige i nærrområder for å gi delt Internett-tilgang i boligmiljøer. Uansett hva forfatterens målsetting har vært, er det imidlertid et faktum at boken er spekket med praktiske erfaringer og gode råd som er nyttige for de fleste som arbeider med praktisk WLAN-teknologi. (168 sider, O'Reilly & Associates, 2. utgave juni 2003, ISBN 0-596-00204-1, ca. USD 25).

Videre har det i løpet av året dukket opp minst et halvt dusin fagbøker om kombinasjonen WLAN og sikkerhet. Søk på '802.11' på Amazon.com for en oversikt.

⁸ Se Mellvik-Rapporten nr. 56, tilgjengelig i PDF-format fra vår Web-tjeneste, se side 35 for detaljer.

underliggende fysiske nivåer. Sentrale områder og funksjoner som dekkes av standarden, er:

- ✓ Gjensidig autentisering – klient-til-nett, nett-til-klient
- ✓ Sentralisert identifikasjon av brukere (typisk via RADIUS)
- ✓ Administrasjon av krypteringsnøkler (per bruker, per sesjon, dynamisk utskiftning)
- ✓ Tjenester for logging og avregning av ressursforbruk
- ✓ Støtte for et antall mekanismer og krypteringsstandarder i forbindelse med autentisering av brukere, inklusive EAP/PE-AP, TLS/SSL

En rekke aksesspunkter og systemer, inklusive Windows 2000 og XP, har allerede støtte for 802.1x. Kombinert med en RADIUS-tjener, for eksempel IAS på Windows 2000, har vi det som trengs for å ta mekanismene i bruk. Med intelligente, selvstendige aksesspunkter i det trådløse lokalnettet, kan den administrative utfordringen dette representerer bli formidabel. I svitsjede WLANs, der aksesspunktene er enkle og 'dumme', og intelligensen flyttet lenger bakover i nettverket, blir utfordringen av en annen og langt mer overkommelig størrelsesorden.

I et nettverk der 802.1x regjerer, vil ingen noder eller brukere få tilgang til ressurser uten å ha blitt autentisert. Standarden tar med andre ord vare på begge nivåene vi diskuterte ovenfor, i tillegg til å forenkle utveksling og administrasjon av krypteringsnøkler for transportsikringen (WPA).

Forvansking og forenkling

Standardene bidrar til å forenkle sikringen av både trådløse og trådbaserte nettverk. Samtidig er de kompliserte i seg selv, med de risikoer dette innebærer. Erfaring har lært oss at prosedyrer kan være feil, programmer inneholder feil og mennesker gjør feil. Derfor er det både mulig og sannsynlig at selv nettverk som har tatt i bruk disse mekanismene, kan være usikre – kanskje til og med usikrede – på grunn av en eller annen banal feil. Igjen er det derfor på sin plass å minne om at det ikke er tilstrekkelig å vri om nøkkelen i døren. Den må også kontrolleres. ■

EAP – Extensible Authentication Protocol

PEAP – Protected EAP

TLS – Transport Layer Security

SSL – Secure Socket Layer, utgangspunktet for – og praktisk talt ekvivalent med – TLS

RADIUS – Remote Authentication Dial-In User Service

IAS – Internet Access Services (RADIUS-server på Windows 2000)

MAC – Medium Access Layer

DHCP – Dynamic Host Configuration Protocol