

Vandrenett: Sømløs, permanent konnektivitet

Drømmen nærmer seg virkelighet: Enkelte har snakket om 'IP over alt' siden tidlig på 90-tallet, og møtte til å begynne med hoderysting og skepsis: "Det er ikke mulig" var credo fra ulike hold, og argumentene var både tallrike og velfunderte.

Utviklingen har vist oss noe annet: Til tross for sin alder og sine tallrike begrensninger, har IP-protokollen funnet veien inn i de mest usannsynlige anvendelser. Hindringer og svakheter er overvunnet med kreativitet og nyutvikling. Selve protokollen har gjennomgått flere mindre ansiktsløftninger som ikke har ødelagt kompatibiliteten med historien, hvilket sier sitt om den grundighet og fleksibilitet den fikk med seg i fødsels gave.

Vår virkelighet, innenfor og utenfor Internettet, må fortone seg som den rene *science fiction*-historie i forhold til situasjonen da TCP/IP fikk sin form på 70-tallet. Vi har gått fra rene dataoverføringer over relativt saktegående linjer, til telefoni, videokonferanser, radio og TV-overføringer, fjernmedisin og underholdning. Det hersker ikke lenger tvil om at IP blir bærer av alle typer informasjon i praktisk talt enhver sammenheng innen overskuelig fremtid. Fra de tusen hjem til den største bedrift vil denne konvergeringen gjøre IP like selvsagt og allestedsnærværende som elektrisitet. IP-basert telefontrafikk, kabel-TV, interaktive underholdningstjenester vil flyte inn i våre hjem. Forbindelser internt – med og uten tråd – for styring av alarmsystemer, TV, musikk-anlegg, varme, lys, kjøkkenutstyr og så videre, vil finne seg godt til rette med IP som utgangspunkt.

Frihet uten en tråd

Våre ambisjoner og krav stopper imidlertid ikke der. Inspirert av mobiltelefonenes frihet og tilgjengelighet, og trådløse lokalnett som eliminerer kabler og andre fysiske restriksjoner, vokser kravet om at også våre datamaskiner, det være seg PDAer av ulike slag eller alminnelige, bærbare maskiner, skal være 'på nett' konstant – uavhengig av tid, sted og fysiske tilkoblingsmuligheter.

Noen av oss har fått praktisk erfaring med bruk av offentlige trådløse Internett-tilkoblinger – på hoteller, kongressentre, utstillinger og messer i inn- og utland. Dette gir mersmak: Vi har fått høyere båndbredde og lettere tilgjengelighet i og med at vi slipper å lete etter nærmeste telefonkontakt, men vi må fortsatt 'koble opp' og logge oss på når vi kommer innenfor dekningsområdet. Det naturlige neste trinn er å hoppe over denne forsinkelsen og å øke tilgjengeligheten ytterligere – kort og godt realisere drømmen om *always on line*.

Vi kan avfinne oss med at båndbredden varierer, og med den hvilke oppgaver som kan la seg utføre. Det skal imidlertid ikke være vår opp-

gave som brukere å verken vite hvilke tilkoblingsmuligheter som finnes, å foreta de håndgrep som må til for å bytte fra det ene til det andre, eller å velge oppgaver i forhold til tilgjengelig båndbredde. Det er slikt vi har datamaskiner til – å sørge for optimal bruk av tilgjengelige ressurser som vi verken forstår eller har ambisjoner om å forstå. I høyden kan vi strekke oss til å plugge inn en fysisk nettverkskabel der dette er eneste – eller det optimale – alternativ.

Målsettingen er kort og godt å alltid være ON LINE med den maksimalt tilgjengelige båndbredde. Om den aktuelle forbindelsen er WLAN, Bluetooth, GSM, GPRS, UMTS eller noe annet, overlater vi til utstyret å bekymre seg om. Likeledes ønsker vi at programvaren er intelligent nok til å ikke sette i gang overføring av PowerPoint-presentasjoner på 50 MB når båndbredden er under 50 kbps, men automatisk kører opp slike jobber til forholdene ligger til rette. Og sist, men ikke minst forventer vi at sikkerheten skal være godt ivaretatt – uavhengig av transportmedium og teknologi.

Ambisiøst? Javisst, men det er nettopp ambisjoner og vyer om forbedring som driver utviklingen fremover. Dessuten er vi kommet til et punkt der teknologien for å realisere drømmene burde finnes. Vi har sågar sett eksempler på leverandører som hevder å kunne realisere drømmen.

Spørsmålene er imidlertid tallrike: Hvor sømløst og usynlig kan det bli, hvor effektivt er det, hva koster det og ikke minst: Hvordan er de tilsynelatende uovervinnelige utfordringene med å kombinere IP og mobilitet løst?

Komplisert frigjøring

Mens de øvrige anvendelsesområdene vi nevnte innledningsvis, ikke representerer noen utfordring av betydning for transportprotokollen, er det motsatte tilfelle med mobile anvendelser – noder i bevegelse: Adresseringsmekanismene i IP er basert på at veien frem til den enkelte node er fast og forutsigbar, og ikke forandrer seg så lenge noden er aktiv i nettverkssammenheng.

Navlestrengen kuttet

Med en fysisk kabel plugget til brukerutstyret, er dette problemfritt: Topologien er fast så lenge konnektiviteten finnes, dvs. så lenge kablet er på plass og applikasjonene aktive. Om mediet er et modem, en ISDN-linje, Ethernet eller noe annet, spiller ingen rolle. Når vi slår av maskinen og pakker den sammen eller stikker den i lommen, terminerer vi forbindelsen, og er fullstendig *off line* mens vi flytter til et nytt punkt (hotell, kontor, hjem, etc.). Her etablerer vi en ny forbindelse med en ny adresse, og starter applikasjonene på nytt.

Likeledes representerer trådløse forbindelser via GSM-modem ingen utfordring: Den trådløse delen av ligningen simulerer et stasjonært modem, og holder den faktiske trådløsheten ute av syne for transportprotokollen – og utstyret forøvrig. Tilsvarende gjelder for trådløse lokalnett: Basestasjonene kommuniserer seg imellom omtrent på

Viktige Internett-standarder knyttet til mobil IP:

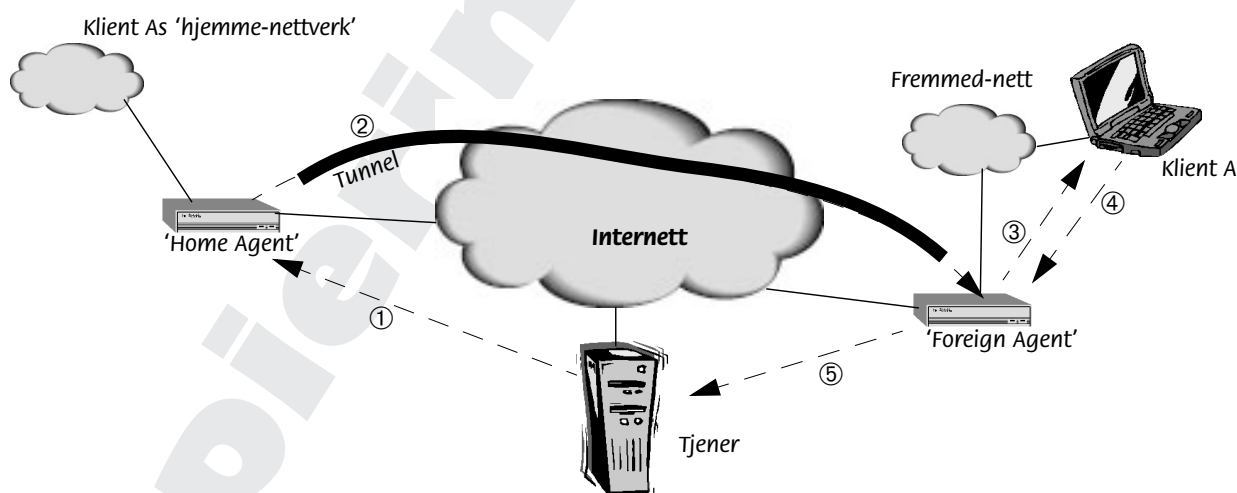
- **RFC 3115** - *Mobile IP Vendor/Organization-Specific Extensions* (april 2001)
- **RFC 3024** - *Reverse Tunneling for Mobile IP (revised)* (januar 2001)
- **RFC 3012** - *Mobile IPv4 Challenge/Response Extensions* (november 2000)
- **RFC 2977** - *Mobile IP Authentication, Authorization, and Accounting Requirements* (oktober 2000)
- **RFC 2794** - *Mobile IP Network Access Identifier Extension for IPv4* (mars 2000)
- **RFC 2344** - *Reverse Tunneling for Mobile IP* (mai 1998)
- **RFC 2290** - *Mobile-IPv4 Configuration Option for PPP IPCP* (februar 1998)

samme måte som GSM-nettets aksesspunkter, og overfører klientene seg imellom sømløst når de flytter seg. At slik *roaming*, som det heter på fagspråket, i mange tilfeller kun fungerer mellom basestasjoner fra én og samme leverandør, er en situasjon vi har lært å leve med, og som på sikt vil forandre seg.

Usynlig mobilitet

Vi ser at mobilitet ikke representerer noe teknisk problem så lenge den er usynlig for transportprotokollen. Denne observasjonen viser hvor vi må lete etter generelle løsninger som kan ekspanderes utover singulære teknologier: Det må etableres mekanismer som strekker mobiliteten videre til et nivå der vi bytter transport-teknologi uten at dette påvirker aktive forbindelser og pågående kommunikasjon. Robustheten må være på samme nivå som for utstyr med høy tilgjengelighet (HA, *High Availability*): Disker, prosessorer, strømforsyninger og så videre kan byttes mens utstyret er i full drift.

Problemstillingen kom for alvor på banen midt på 90-tallet, og forårsaket langvarige og grundige evalueringer og diskusjoner blant eksperter verden over – ikke minst i Internettets spesialistfora og standardiseringsorganer (IETF, *Internet Engineering Task Force*). Resultatet ble '*Mobile IP* – en spesifikasjon av hvordan *roaming*, autentisering og andre mekanismer knyttet til klienter i bevegelse kan foregå innenfor rammene av IP-protokollen. Dens offisielle liv startet i 1998, og har siden blitt raffinert og supplert med standarder for støttemekanismer av ulike slag. Per 2001 er *Mobile IP* en anbefalt Internett-standard som er implementert av de fleste store ruterleverandørene i markedet.



Figur 2

Eksempel på mobil IP-trafikk mellom en tjener i fastnett og en mobil klient: 1: Tjener X sender pakken til klientens hjemme-nett. 2: Der blir den fanget opp av en agent, som kapsler den inn og formidler den videre til klientens sist registrerte fjernagent. 3: Her pakkes den ut, legges i en nivå-2 pakke (f.eks. en Ethernet-ramme eller en 802.11b-ramme (Wireless Ethernet)) og sendes til klienten. 4: Klienten svarer med en pakke direkte til tjeneren, som formidles av en ruter – i dette tilfelle samme boks som også er fjernagent. 5: Ruterens sender pakken videre i internettet der den finner veien frem til tjener X.

Mobile IP

I korte trekk er mekanismen grunnlagt på samme tankegang som VPN-løsninger: Etablering av dynamiske tunneller i nettverket som gjemmer det faktum at klienten er i bevegelse. Klienter får faste adresser akkurat som mobiltelefoner har faste nummer. Dette impliserer at klienter også har et fast hjemsted (et 'hjemmenettverk' i IP-terminologi), uavhengig av deres fysiske plassering. All trafikk til klienten går først til hjemmenettverket, der en agent (typisk en ruter) holder styr på den fysiske plasseringen, pakker inn trafikken og sender den til en 'fjernagent' (se figur 2)⁶. Denne befinner seg på samme fysiske nett som klienten, og pakker ut den innkapslede trafikken før den i likhet med annen lokal trafikk legges i fysiske 'rammer' tilpasset mediet (Ethernet-rammer, Wireless Ethernet-rammer, PPP-pakker via GPRS og så videre).

På klienten sørger et stykke programvare (*Mobile IP Client*) for de administrative funksjonene med registrering i nettverket, bytte av grensesnitt når det er nødvendig og andre detaljer, godt ute av syne for brukeren. Operativsystemet og øvrige programmer på klienten ser ikke noe annet enn at trafikk kommer på vanlig måte til den registrerte, faste IP-adressen, og er godt fornøyd med det. Trafikk i motsatt retning – utgående fra klienten, trenger ingen av disse mekanismene, men sendes på vanlig måte til nærmeste ruter og videre inn i den store skyen, som vi antar er Internettet, men gjerne kan være et annet sammensatt, IP-basert nettverk.

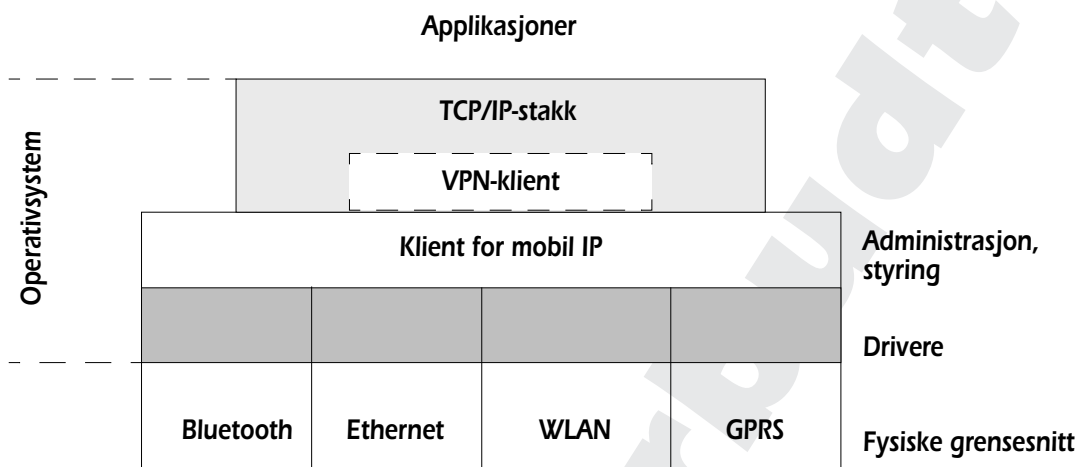
Dette kan høres komplisert ut, og forteller i virkeligheten kun en liten del av historien. Her er det en rekke mer eller mindre åpenbare komplikasjoner som må være godt ivaretatt før det hele kan fungere. Konseptet er imidlertid relativt enkelt. Dessuten – og enda viktigere: Kompatibiliteten er 100%: For såvel klienter som tjenere ser verden ut som før. *Mobile IP* ligger utenpå tradisjonell IP, og håndteres av avanserte rutere fra de fleste leverandører på markedet. Løsningene krever både administrative og tekniske ressurser, men fungerer godt i praksis, og har gjennom ca. 2 års bruk bevist sine kvalifikasjoner.

Sømløs programvare

Den sømløsheten – eller automatikken – vi drømte om innledningsvis, forutsetter *Mobile IP*, men kravene stopper ikke der. Vi ønsker ikke bare å kunne bevege oss uten å miste forbindelsen, men forlanger også at utstyret automatisk skal velge den optimale infrastrukturen på våre vegne. Som figur 2 viser, betyr dette at vår klient-programvare må kunne aktivt styre, kontrollere og administrere alle fysiske grensesnitt på maskinen – gjerne opptil en håndfull.

Slike klienter er kommet på markedet det siste året fra flere leverandører, inklusive norske Birdstep, men er fortsatt for unge til å kunne kalles 'modne'. De skal kunne brukes om hverandre så lenge de støtter

⁶ Slik innpakning og viderefremføring av trafikk kalles 'tunnel': Det etableres en virtuell kanal mellom sender og mottaker. Samme mekanisme benyttes i forbindelse med VPN.



Figur 3 En mobil IP klient er et stykke programvare som introduseres mellom drivere og protokollstakk på systemer som skal benytte seg av konnektivitet basert på MOBILE IP standarden. Programvaren vil normalt også få ansvaret for å håndtere overgangen mellom ulike media, og automatikken i den forbindelse. Dens samspill med VPN-klienten er kritisk – og i mange tilfeller vanskelig, fordi også denne ønsker å sitte nærmest driverne i hierarkiet. Dette problemet håndteres ved enten å forandre VPN-klienten eller å sørge for at IP-klienten ser ut som og ter seg som en driver overfor neste nivå, og dermed 'lurer' VPN-klienten til å tro at den er 'sjef'.

standarden fullt ut. Samtidig er det åpenbart betydelig rom for kreativitet og variasjon med hensyn til hvordan for eksempel automatikk i valg av grensesnitt fungerer.

En annen interessant effekt i denne forbindelse er at IP-klienten, som forutsetningsvis må være robust og pålitelig, bidrar til å øke den generelle påliteligheten i systemet. Mange har erfart at trådløse forbindelser er vel og bra, men sporadiske brudd i konnektiviteten fører lett til at operativsystem eller applikasjoner henger seg eller terminerer. En av IP-klientens oppgaver er å sørge for at slike sporadiske brudd ikke blir synlige på høyere nivå (se figur 3), og erfaring tilsier at denne forventningen er korrekt.

Sikkerhet i fokus

Videre fører en 'alltid on line' løsning gjerne til bedre sikkerhet: VPN-basert sikring er en forutsetning for all kommunikasjon mellom eksterne og interne nettverk, men representerer gjerne en komplikasjon for brukeren, fordi selve påloggingen tar merkbart lengre tid, og i enkelte tilfeller er komplisert i seg selv. Når klienten aldri kobles ned, reduseres hyppigheten med hvilken vi må gjennom denne prosessen vesentlig.

Samtidig dukker det opp en uventet utfordring: VPN-klienter har vesentlig lengre fartstid i markedet enn klienter for *Mobile IP*. Deres foretrukne plassering i programvarestakken (figur 3) er rett under IP-stakken, og med direkte kontakt mot drivernivået. Her må imidlertid den nye IP-klienten inn, fordi den skal kontrollere drivere og grensesnitt på en helt annen måte enn tidligere.

Resultatet blir at en rekke velprøvde VPN-klienter på markedet ikke lenger fungerer. De er ikke laget for å eksistere i slike omgivelser, og

VPN – Virtual Private Network
WLAN – Wireless LAN
WEP – Wired Equivalent Privacy

må gjennom betydelige forandringer hos sine respektive leverandører før de våkner til liv igjen.

En annen relevant betraktning i tilknytning til sikkerhet er at forbindelser som er autentisert og sikret via VPN, eliminerer problemstillingene rundt WLAN-teknologiens egne sikkerhetsmekanismer, som fikk mye negativ oppmerksomhet i presse og andre media i 2001.⁷ Svakhetene i den opprinnelige WEP-krypteringen som fulgte første generasjons WLAN-produkter, er et faktum – og historie. Mekanismen har ikke lenger noen signifikant verdi når VPN er i bruk, og må fjernes helt for å muliggjøre den bevegelsesfriheten vi ønsker i forbindelse med 'vandrenett'.

Hvor står vi?

Hvor står vi så ved inngangen til 2002 – kan drømmen realiseres? Til tross for at de nødvendige standardene er etablert og teknologien finnes, er svaret i beste fall et betinget 'ja'. Store leverandører som Cisco og Nortel, vil gjerne ha oss til å tro at alt som skal til er å anskaffe deres løsninger, så går resten av seg selv. Og om vi nedskalerer drømmen et stykke, kan det argumenteres for at de har rett: Har vi et internt nettverk som strekker seg over flere geografiske lokasjoner, med både WLAN og tradisjonell LAN-teknologi, kan tilgjengelig utstyr og programvare gi oss sømløs konnektivitet fra WLAN til GSM/GPRS når vi forlater lokalnettet. Løsningene kan også ta oss inn i varmen igjen når vi kommer til neste 'avdeling'.

Skulle vi imidlertid ha mistet forbindelsen over lengre tid på vår ferd, er idyllen brutt. Dessuten, og for de fleste den viktigste innvendingen: Vi får ikke benyttet IP-soner og andre offentlige kommunikasjonsmuligheter som måtte finnes langs vår vei – på hoteller, restauranter, konferanselokaler og så videre.

En slik bedriftsintern løsning er med andre ord i beste fall tilfredsstillende for en beskjeden nisje av kunder, og ikke harmonisk med målsettingen vi skisserte innledningsvis.

Paddehatter

Nettopp offentlige IP-soner, områder der en eller annen leverandør har funnet det for godt å etablere tilgang til Internett via WLAN, representerer en joker i utviklingen: Sonenes eksistens gjør det attraktivt å utnytte dem, gitt at prisen er riktig. For tilbyderne er dette enten en potensiell direkte inntektskilde eller et agn for å trekke kunder – for eksempel til serveringssteder, hoteller og konferanseområder.

At sonene finnes er imidlertid ikke det samme som at vi får tilgang til dem: De har ulike aksessmekanismer, benytter ulike krypterings- og autentiseringsmekanismer og har forskjellige måter å identifisere seg på. På enkelte steder finnes det sågar flere tilbydere på samme område, men hvilken skal vi velge og hvorfor? Dette begynnende kaoset må konsolideres før det kan bli orden på sømløsheten, og sannsyn-

7 Se "Wireless Ethernet: Et åpent sikkerhetshull?" i Mellvik-Rapporten nr. 84.

ligheten er stor for at vi ender opp med en situasjon som ligner til forveksling på GSM-nettet: To eller kanskje tre hovedleverandører som leier kapasitet eller har såkalte *roaming*-avtaler med de mindre aktørene med fotfeste i enkeltområder. Denne krigen er i full gang, med Telenor og NetCom som hovedaktører, og en rekke gullgravere som haster avgårde for å stikke ut sine skjerp. Det vil imidlertid ta tid før virksomheten kan gi avkastning, hvilket peker i retning av at kun de største vil overleve når gullrushet er over.

Karakteristisk for dagens situasjon er at IP-sonene dukker opp som paddehatter, og gir trådløs konnektivitet med god hastighet, men representerer isolerte øyer som tele-aktørene søker å binde sammen med verdiøkende tjenester. Per januar 2002 har Telenor 29 slike som er fordelt over store deler av landet, med 16 nye under planlegging. NetCom har et mindre antall, men lignende tjenester.

Fra drøm til virkelighet

Både disse to og flere andre – i ulike samarbeidskonstellasjoner – arbeider mot å realisere drømmen om optimal, permanent konnektivitet i bevegelse. Som vi har sett, er utfordringene ikke først og fremst av teknologisk art, men en blanding av praktiske, politiske og programvaremessige problemstillinger.

Dessuten står de overfor den høyst relevante problemstilling å etablere et nytt marked: Hvem er kundene, hva er de villige til å betale og hvilke tjenester er de primært interesserte i? Hvor mye er det rimelig å investere før inntektene begynner å tikke inn, og hvilken funksjonalitet må være på plass før den første kunden kommer?

Helt på bar bakke starter de riktignok ikke: IP-sonene genererer allerede inntekter, som typisk avregnes per byte overført, i motsetning til per tidsenhet, som er vanlig i andre sammenhenger. Segmentet preges imidlertid av liten modenhet, og både praktiske og økonomiske sider vil forandre seg sterkt de neste to årene.

I behovsvurderingen er det også høyst relevant å reflektere over hvilke erfaringer vi har gjort med andre *always on* tjenester, for eksempel WAP: Er det nyttig med en slik ekstrem grad av tilgjengelighet, eller er det hemmende å aldri gi seg selv anledning til å sette tankene fri? Svaret avhenger naturligvis av hvem vi er, hva vi gjør og hvilke oppgaver og ansvarsområder vi skal ta vare på. Å stille spørsmålene blir imidlertid ikke mindre viktig av den grunn.

Konklusjon

Drømmen nærmer seg virkelighet. I løpet av inneværende år vil vi kunne realisere betydelige deler av den – med en kombinasjon av interne WLAN-forbindelser, GSM/GPRS-forbindelser og offentlige IP-soner. Når vi er i bevegelse over større områder, er det ikke til å komme forbi at GPRS blir vårt eneste alternativ i overskuelig fremtid. Den beskjedne båndbredden vil begrense anvendeligheten og markedet, men samtidig bidra til å demonstrere teknologiens anvendelighet.

En annen faktor er utviklingen på PDA-markedet, som på den ene siden vil ha stor innflytelse på etterspørselen etter mobil og permanent konnektivitet, og på den andre siden holder båndbreddebehovet i tømme: Enkle anvendelser har beskjedne behov, også med hensyn til båndbredde.

Konnektivitet fra fly er et område som gir mindre grunn til optimisme. Sjansene for store positive forandringer de neste to årene er rett og slett minimal. Markedet har rast sammen som følge av terrorfrykten, og med den investeringsviljen hos flyselskapene. Samtidig er teknologien som skal til for å gi individuell konnektivitet med akseptabel båndbredde og responstid via satelitt, fortsatt for kostbar til at vi ser for oss noen kortsiktig progresjon.

Det er bokstavelig talt nødvendig å stikke fingeren i jorda og erkjenne at forutsatt god bakkekontakt kan drømmen om permanent konnektivitet realiseres i løpet av de neste 12-18 månedene. Allerede inneværende år vil vi se interessante demonstrasjoner som vil bidra både til å stimulere interessen, og ikke minst til å katalysere nye anvendelser. Vi følger utviklingen her i Mellvik-Rapporten, og kommer tilbake til temaet mot slutten av året. ■

Produkter

I neste utgave, i spalten Godbiter, diskuterer vi vandrenett-produkter som er på beddingen i det norske markedet.