

# Nettverksarkitektur: Nye krav, nye løsninger

*I første artikkel spente vi opp lerretet: Vi gjennomgikk drivkreftene bak den akselererende forandringen og farene ved å ignorere utviklingen. Videre presenterte vi teknologier og tjenester som hver for seg bidrar til å 'forsure' dagens arkitektur: Den knaker i sammenføyningene og er faretruende ofte gått ut på dato. Dette kan vi ikke leve med i lengden.*

## Ny arkitektur, nye muligheter

### Hva er en nettverksarkitektur?

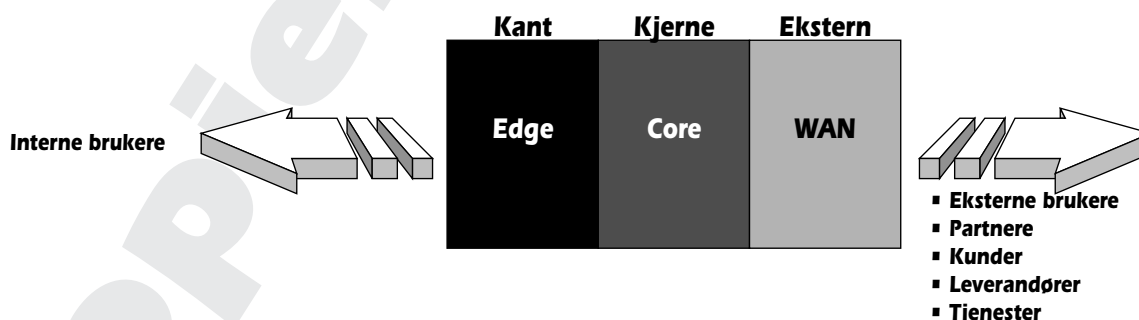
«En nettverksarkitektur er en overordnet målsetting og et sett spesifikasjoner nettverket blir bygget rundt. I tillegg må arkitekturen – og planene som baseres på den – angi løsninger og/eller løsningsalternativer som dekker tre hovedområder: Fysisk arkitektur (konnektivitet og kabling), interoperabilitet (protokoller og tjenester) og systemer/prosedyrer for overvåking, styring og kontroll av nettverket.»

Sitatet er hentet fra spesialrapporten "Datanettverk: Arkitektur og teknologi" (Team Mellvik as, 1994).

Det er kun én måte å angripe utfordringene på: Brette opp armene og ta fatt – armert med god oversikt over dagens arkitektur, trafikkstatistikk og forventet utvikling på en rekke viktige områder, hvorav de viktigste ble diskutert i forrige artikkel:

- ✓ Vekst i organisasjonen
- ✓ Ekstern bruk, distribuerte brukere (SOHO)
- ✓ E-handelsløsninger
- ✓ Nye internsystemer på beddingen
- ✓ Systemarkitektur (tjenere, lagring, lagringsnettverk etc.)
- ✓ Telefoni
- ✓ Trådløse teknologier, mobil IP

Under fortutsetning av at en gjennomarbeidet nettverksarkitektur allerede eksisterer, blir hovedoppgaven å finne hvor forandringene kommer (eller er kommet), og hvilke konsekvenser de skal eller kan få. Her er det viktig å huske at konsekvensene ikke er gitt: De kommer ikke alltid av seg selv, men er resultater av de valg vi gjør. Lar vi være å foreta valgene, styres utviklingen av tilfeldigheter, hvilket neppe er akseptabelt for noen.

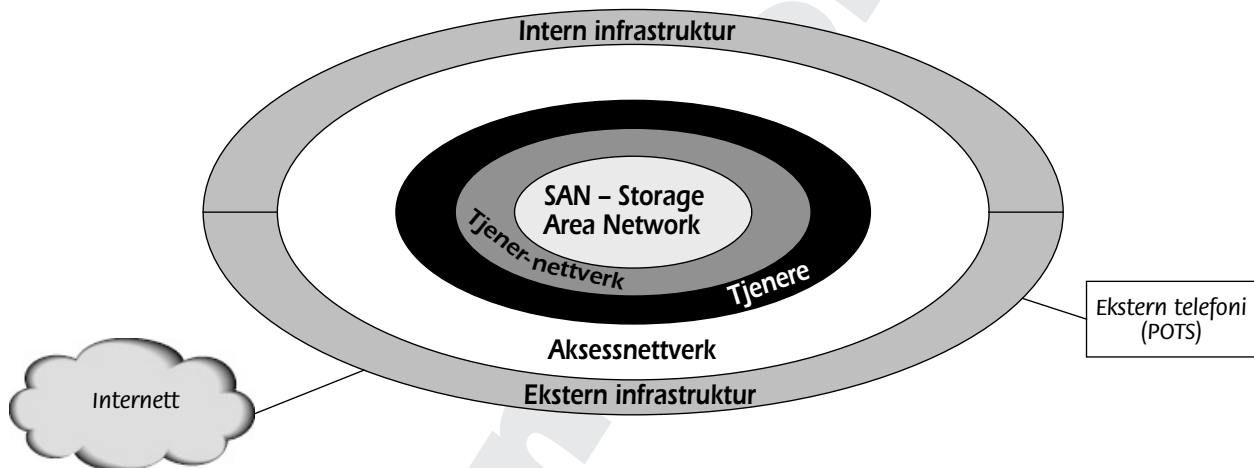


**Figur 3** Den grunnleggende tredelte nettverksmodellen er fortsatt anvendelig, men vi ser at vektfordelingen forandres, mot færre interne og flere eksterne brukere.

### Vi 'eksternaliseres'

Figur 3 viser en tradisjonell forenkling av nettverkets dekningsområder, med tre deler: Ryggradsnett (*core*) i midten, kantnett (*edge*) mot interne brukere og WAN mot eksterne tjenester og brukere. Modellen er fortsatt gyldig, og den viktigste forandringen vi ser i disse dager er at vekten flytter seg: Vi får færre interne og flere eksterne brukere.

Endringen kan ikke unngå å få store konsekvenser for trafikkflyten: Trafikken i det tradisjonelle interne aksessnettverket blir ikke nødvendigvis mindre, men flater ut, fordi veksten i trafikk per bruker kompenseres av færre brukere. På den motsatte siden blir forandringen voldsom: En eksplosiv trafikkvekst som ikke kan unngå å få konsekvenser både for måten vi tenker på og mekanismene vi tar i bruk for å beholde kontroll og et tilfredsstillende kvalitetsnivå.



**Figur 4** Forenklet prinsippsskisse av en moderne system- og nettverksarkitektur. Klare grenser mellom de ulike 'nivåene' er kritisk – for sikkerhet, enkelhet, skalerbarhet og ikke minst for fleksibilitet: Det gir oss mulighet til å flytte på – i fysisk forstand – én eller flere av ringene uten å påvirke de andre, en aktuell problemstilling i forbindelse med outsourcing, katastrofeplanlegging eller store organisasjonelle forandringer.

De viktigste drivkreftene i denne 'folkevandringen' er:

- ✓ Hjemmekontorer og mobile brukere er sjeldnere 'inne' – en jevnt voksende del av jobben utføres der de måtte befinne seg, fordi det er praktisk mulig.
- ✓ Bruken av trådløse nettverk (WLAN) eksploderer. Samtidig øker sikkerhetsbevisstheten: Det er blitt naturlig og nødvendig å behandle WLAN-brukere på linje med eksterne, uansett hvor de fysisk måtte befinne seg. Sist, men ikke minst, dukker behovet for å tilby trådløs konnektivitet til besøkende stadig opp. Når det trådløse nettverket er kategorisert som eksternt, blir slike behov lette å imøtekomme. Enkelhet gir ikke bare bedre sikkerhet, men også lavere kostnader.
- ✓ Handelstrafikk: Papirløst samarbeid med partnere, leverandører og kunder bidrar alene til en vesentlig trafikkøkning på den eksterne siden, sammen med behov for å administrere, styre og sikre trafikken.

### Folkevandring og trafikkeksplasjon

Følgene av denne forflyttingen gir en bortimot eksponensiell trafikkvekst til og fra Internettet – som tiltar ytterligere dersom vi velger å prioritere sikkerhet og enkelhet på bekostning av båndbreddeforbruk:

- ✓ Eksterne brukere kan – og bør – få sin Internett-aksess via virksomhetens nettverk i stedet for direkte fra sin egen PC. Dette er vår eneste pålitelige mulighet til å sørge for skikkelig sikkerhet gjennom filtrering og kontroll av datastrømmene, hvilket vi gjør for interne brukere i alle fall. Tjenesten er like viktig for eksterne brukere: De representerer forlengelsen av det interne nettverket. Dette vil bidra til en vesentlig økning i Internett-trafikken og dermed belastningen på eksterne forbindelser. Gode *Web-cache*-løsninger er viktige for å optimalisere disse datastrømmene. At Internett-trafikken dermed kanaliseres inn i brukernes VPN-kanal, bidrar også til å øke belastningen, både trafikkmessig og på VPN-løsningen.
- ✓ ISDN-forbindelser for eksterne brukere forekommer stadig sjeldnere. TV-kabel og ulike DSL-varianter overtar raskt – med dramatiske konsekvenser for belastningsbildet – på linjer, VPN-systemer og tjenerbelastning generelt. At brukerne er eksterne forandrer ikke deres behov for og bruk av interne tjener- og lagringsressurser, ofte tvert imot. Med permanente forbindelser til eksterne nettverk, kompliseres også sikkerhetsbildet, hvilket gjør det enda viktigere å prioritere kontroll med datastrømmene til og fra SOHO-brukere.
- ✓ Tilsvarende konsekvenser følger i kjølvannet av å flytte WLAN-brukerne ut av lokalnettet.
- ✓ Som vi var inne på i forrige artikkel, vil vandrenett-teknologi og mobil IP aksentuere problemstillingen ytterligere: Slike brukere er alltid å betrakte og behandle som eksterne, selv når de kobler seg fysisk til det interne nettverket. Sømløsheten har sin pris – i dette tilfellet at all trafikk til og fra klienten må ut gjennom brannmuren og tilbake igjen.

Gang på gang ser vi at valgene dukker opp: Skal vi koste på oss båndbredde og dramatiske trafikkøkninger for å imøtekomme krav til sikkerhet og enkelhet? I de fleste tilfeller vil svaret automatisk være ja, fordi summen på bunnlinjen blir positiv. Uansett hva båndbredde og utstyr måtte koste, blir det billigere enn personell-økninger og lavere sikkerhetsnivå.

### Øding av ressurser

Denne prioriteringen representerer en viktig trend i seg selv: Vi er blitt vant til å ødsle med ressurser i IT-sammenheng – prosessorkapasitet, hukommelse, masselager og så videre. Turen er kommet til båndbredde, og argumentene er enda sterkere – og lettere å demonstrere.

Spesielt gjelder dette i forbindelse med sikkerhet: Vi har erfart hva som skal til – og tatt konsekvensen av erkjennelsen: Eksterne brukere benytter VPN, *end of discussion*. Nå folder vi WLAN-brukere inn i

SOHO – *Small Office, Home Office*

samme rammeverk, og fjerner både en brukerkategori og en risikogruppe. Dermed står vi igjen med to kategorier – interne og eksterne. Samtidig vet vi at interne brukere i de fleste sammenhenger representerer like stor risiko som eksterne. Dermed er veien kort til å fjerne distinksjonen og forlange samme grad av trafikksikkerhet og autentisering for interne som for eksterne brukere. Det betyr ikke at brannmurer, grenser eller dybdeforsvar blir mindre viktig, men at vi har forenklet hverdagen og hevet sikkerhetsnivået enda et betydelig hakk. Samtidig har vi økt belastningen på en rekke elementer i infrastrukturen: VPN-terminatorer, brannmurer, rutere, linjer, lastfordelere og så videre.

### **Hardware som utgår på dato**

Før en slik homogenisering kan realiseres, må det med andre ord en teknologisk oppgradering til – først og fremst på VPN-siden: Dagens løsninger er for tunge, kostbare og lite behovstilpasset: Med distinksjonen mellom eksterne og interne brukere borte, hvor skal VPN-forbindelsene termineres? Om vi tar utgangspunkt i figur 4, ser vi at grensen mellom aksessnettverket og tjenerressursene blir det naturlige skillet mellom indre og ytre rom, mellom sikret og usikret trafikk. Dagens VPN-løsninger er ikke kapasitetsmessig klare for en slik oppgave i store organisasjoner. Derfor ligger overgangen et par års tid inn i fremtiden, og får ikke effekt for den arkitekturen vi arbeider med i denne omgang.

Også brannmurene kommer under sterkt press i forbindelse med en slik forandring: I dag termineres VPN-forbindelsene typisk i en såkalt demilitarisert sone utenfor hoved-brannmuren, slik at brannmuren kun får ukryptert trafikk til behandling. Dette er en forutsetning for dens funksjon: Den må kunne se det virkelige (ukrypterte) innholdet i trafikken for å analysere og eventuelt blokkere mistenkelige pakker. En slik konstellasjon blir kunstig og lite optimal etter en 'eksternalisering' av det aller meste av trafikken. Derfor ser vi for oss en betydelig forandring i måten sikkerhetsprodukter settes sammen på i løpet av de to-tre neste årene. Det er på mange måter en underlig ironi at vi trolig vil få løsninger der langt mer prosesseringskraft går med til sikring og kontroll av nettverkstrafikk enn til virksomhetens IT-oppgaver. Igjen havner vi imidlertid på utsiden av det tidsrommet som er relevant for dagens arkitektur.

## **Konklusjon**

En arkitektur handler om prioriteringer og valg – optimale valg i forhold til virksomhetens behov og ressurser, ikke i forhold til en eller annen mal: Fasitsvar finnes ikke, mens optimale og mindre optimale veivalg for den foreliggende situasjonen finnes.

Vi har sett at en rekke av veivalgene får store konsekvenser for den resulterende arkitekturen, og må gjøres tidlig i prosessen. Målet er riktig kvalitet til best mulig pris i sluttproduktet.

“Forenkling og automatisering er viktige målsettinger for enhver nettverksarkitektur.

Fra spesialrapporten  
NETTVERKSARKITEKTUR FOR DET 21.  
ÅRHUNDRE, Team Mellvik 2000.

Samtidig har vi en samling grunnleggende regler og forutsetninger som også legger føringer på veivalgene – for eksempel sikkerhet, skalerbarhet, enkelhet og ressursmessig romslighet. Blant disse er det naturlig å begynne med kapasiteten: Om nettverket ikke har tilstrekkelig kapasitet til å håndtere trafikken, er de øvrige kravene meningsløse. Riktig kapasitet får vi etter en øvelse som først kartlegger dagens volum, og deretter stipulerer utviklingen fremover med utgangspunkt i de faktorene og valgene vi diskuterte ovenfor.

Neste punkt er kvalitet – som har mange fasetter: Leveringskvalitet, pålitelighet, forutsigbarhet og tilgjengelighet – for å nevne noen. Egenkapene bygges inn i nettverket delvis gjennom mekanismer og delvis gjennom styringsverktøy. Her kommer begreper som DEN, QoS og SLM inn – i den grad vi har valgt å ta dem i bruk som hjelpemidler på veien mot ønsket kvalitet. Valgte vi dem ut ved forrige korsvei, kan det like fullt være tid for å foreta en ny vurdering denne gang, spesielt med hensyn til QoS – i kombinasjon med telefoni.

Skalerbarhet påvirkes av en rekke valg på mange nivåer. Det mest grunnleggende er fysisk kapasitet (kabling), som vi ikke diskuterer i denne sammenheng, men antar finnes på plass. Lenger oppe i kjeden finner vi styringsprotokoller og -løsninger, ved siden av produkt-, leverandør- og teknologivalg. Helt på toppen finner vi policy: Hvilke valg har vi gjort med hensyn til hvordan brukerne kan eller skal benytte ressursene? Vi diskuterte eksempler på slike valg og deres konsekvenser innledningsvis: Å forlange at eksterne brukere skal ha sin Internett-aksess via virksomhetens nettverk, kan lett bety en dobling av trafikkbelastningen inn til og ut av nettverket.

Tilsvarende gjelder for sikkerheten: Den påvirkes av valg vi gjør på alle nivåer. Samtidig påvirker våre sikkerhetsmessige valg nettverksarkitekturen – de to må stemme overens – harmonere – dersom resultatet skal bli optimalt. Vekselvirkningen mellom sikkerhet og nettverksarkitektur forutsetter at de utvikles i parallell – gjennom en iterativ prosess.

### Den nye arkitektur

Vår nye nettverksarkitektur preges av følgende hovedpunkter:

- ✓ Klarere grenser, enklere struktur.
- ✓ Voldsom vekst i ekstern trafikk – med tilhørende fokus på trafikkstyring – lastfordeling, *caching*, behovsstyring av ressurser (*policy-based networking*).
- ✓ Mer fokus på sikkerhet – med tilhørende økning i bruk av VPN-teknologi i nye sammenhenger.
- ✓ Dramatisk belastningsøkning på sikkerhetsutstyret: Brannmurer og VPN-terminatorer – som i de fleste tilfeller står foran en oppgradering eller utskifting.
- ✓ Introduksjon av QoS-mekanismer i kantnettverket for å ivareta IP-telefoni.<sup>11</sup>

**QoS** – Quality of Service

**DEN** – Directory Enabled Networking, se Mellvik-Rapporten nr. 88.

**SLM** – Service Level Management, se Mellvik-Rapporten nr. 67-73.

**POTS** – Plain Old Telephone System

En interessant, men ikke innlysende konsekvens av utviklingen, er at plasseringsfleksibiliteten øker: Klare grenser, høyt sikkerhetsnivå over hele linjen og fokus på forenkling og sikkerhet – med båndbredde og andre ressurser som innsats, gjør det lettere å flytte deler av systemet: Til mer optimale steder i organisasjonen, eller kanskje til eksterne tjenesteleverandører. Ballen ruller, og lar seg ikke stoppe. ■

11 På noe sikt skal også IP-telefoni over på det trådløse nettverket. Dette forutsetter introduksjon av QoS-mekanismer i link-protokollen, men ligger tilstrekkelig langt frem i tid til at vi ikke kan ta hensyn til det i denne omgang.