

Nettverksarkitektur: Nye krav, nye løsninger

At gårsdagens sannhet blir dagens løgn, er ingen indikasjon på at verden har gått av skafet. Sant og usant har aldri vært absolutte begreper, og avstanden mellom dem er omvendt proporsjonal med dynamikken i hverdagen. Større dynamikk betyr kortere 'holdbarhetstid' på ervervet kunnskap og etablerte sannheter.

Denne faktiske situasjonen representerer en trussel og en mulighet, avhengig av hvordan vi velger å angripe den. Trusselen ligger i å ignorere forandringene, se bort fra signalene om at virkeligheten endrer seg – kort og godt 'stikke hodet i sanden'. For oss mennesker er vegring mot forandring en naturlig reaksjon: Stabilitet skaper trygghet, mens kontinuerlig endring rokker ved vårt fundament – faglig, sosialt, miljømessig og/eller på andre måter. Derfor søker vi ikke forandring for dens egen del, men for dens potensiale til også å gi forbedring. Videre er det grenser for hvor mye samtidig forandring vi er i stand til å takle – selv om den er aldri så positiv.

Vi skal la de sosiale og samfunnsmessige konsekvensene av denne situasjonen ligge. Å håndtere teknologiene som yter sitt kontinuerlige bidrag til utviklingen, er en formidabel utfordring i seg selv. Samtidig er det utilfredsstillende å til stadighet måtte 'henge seg på' en trend. Målsettingen bør i mange tilfeller være om ikke i forkant, så i alle fall tidlig ute – slik at vi fra tid til annen kan styre utviklingen i stedet for å bli styrt.

Nettverksarkitektur

Nettverksarkitektur er et tema vi har hatt til behandling en rekke ganger i Mellvik-Rapportens historie – med god grunn. For det første er en effektiv og behovstilpasset nettverksarkitektur en viktig forutsetning for alle IT-tjenester. Den er dessuten i forandring raskere enn noe annet i vår hverdag – ikke fordi nettverksteknologi isolert sett utvikler seg så raskt, men fordi bruken eksploderer: Gamle anvendelser i nye omgivelser og på nye plattformer, nye brukerskarer, nye tjenester som vi tidligere knapt har drømt om – og så videre. Likeledes fortsetter pressene på kritiske ressurser å falle – på båndbredde, masselager og prosesseringskraft for å nevne de viktigste, mens tilgjengeligheten øker parallelt med voksende trådløshet. At brusautomater, kjøleskap, alarmsystemer og ventilasjon skulle på nettet, var langt fra innlysende for 5 år siden. I dag er de her, sammen med telefoni, video, VPN, mobilitet og mye mer.

Tallrike og sterke drivkrefter

For hvert trinn opp i båndbredde og ned i pris, flytter tjenester og tjenesteytere seg lenger unna geografisk, mens brukerne får større fleksibilitet og nye muligheter. Til sammen sørger en betydelig samling mer

eller mindre uavhengige drivkrefter for forandringer med en hastighet som krever at vi re-evaluerer vår nettverksarkitektur årlig.

Blant disse drivkreftene finner vi:

- ✓ **Sikkerhet** – som påvirker alle områdene nedenfor, og i tillegg får betydelige konsekvenser for kapasitetsplanleggingen.
- ✓ **Telefoni** – IP-telefoni og 'blandingstelefoni', gammel og ny teknologi hånd i hånd.
- ✓ **Trådløse teknologier** – først og fremst WLAN og offentlige IP-soner.
- ✓ **Distribuerte brukere** – reisende, hjemmekontorer og småkontorer.
- ✓ **Mobil IP** – en nykommer med stort potensiale og beskjeden praktisk erfaring (se Mellvik-Rapporten nr. 91) som ikke kan unngå å sette spor etter seg i nettverksarkitekturen.
- ✓ **Bruksmønstre, tjenester** – når korte transienter blir til kontinuerlig belastning, har noe dramatisk skjedd: Nye tjenester og nye brukere er en uforutsigbar kombinasjon.

Vi ser at mens enkelte av faktorene er direkte knyttet til teknologi, har andre sitt utgangspunkt i tjenester, bruk og bruksmønstre. Det er på sistnevnte område de store overraskelsene som regel kommer: For eksempel ser vi at private nettsurfere – stikk i strid med forventningene – ikke surfer mer når de får såkalt bredbåndsforbindelse, men benytter den nyervervede båndbredden til nedlastinger: Av musikk, video, spill og andre programmer. Dette påvirker naturligvis belastningsbildet vesentlig. I stedet for kortvarige og relativt sjeldne⁶ topper, blir forbindelsene belastet til grensen av sin kapasitet over lange og sammenhengende perioder. Konsekvensen er at opprinnelige kapasitetsberegninger blir verdiløse. Arkitekturen må legges om og tilpasses virkeligheten.

IP-konvergens

Den viktigste av alle drivkrefter er imidlertid konvergeringen på protokollsiden, som vi også har diskutert tidligere her i Mellvik-Rapporten: "IP over alt, alt over IP" er credo uansett hvor vi vender oss, og legger grunnlaget for en enestående homogenisering og forenkling. At forenklingene i mange tilfeller fremtrer som det motsatte – i første omgang, er uunngåelig: Her er det tradisjoner som skal brytes, vaner som må forandres, og nye tjenester som må kvalifiseres.

Dette tar tid og koster penger, hvilket bringer oss til en viktig kvalifikasjon: Det er ikke nok at en overgang fra eksisterende teknologi til IP-teknologi koster mindre. Besparelsene må være vesentlige – *up front* og på sikt. Derfor har for eksempel IP-telefoni brukt vesentlig lenger tid på å kapre markedsandeler av betydning enn optimistene ventet. Selv i dag anses besparelsene i mange omgivelser til å ligge på rundt 10% i

⁶ I en slik sammenheng er 'sjelden' det samme som 'flere sekunders opphold mellom hver'.

forhold til tradisjonell teknologi (se leder på side 2). Slike tall gir ingen revolusjon.

Kort levetid

Gang på gang i arkitektur-arbeidet er det viktig å minne seg om den forventede levetiden: Ingen nettverksarkitektur overlever uforandret i over 2 år, og som vi påpekte ovenfor, er årlig revisjon en god idé. Det betyr at vi hele veien må konsentrere oss om nåtid og nær fremtid. Ting som kan komme til å skje et par år frem i tiden, er for langt borte til at vi kan ta hensyn til dem i dag – med unntak av helt grunnleggende og opplagte faktorer som båndbredde ('takhøyde'), fiber i stamnett og lignende.

Mange bekker små ...

Vi skal se nærmere på hva disse drivkreftene leder til – deres konsekvenser for arkitekturen på kort og mellom-lang sikt.

Telefoni

Vi begynner med telefoni – som får mye oppmerksomhet i disse dager, men som fortsatt har relativt beskjeden betydning totalt sett. Revolusjonen – som etterhvert har lite revolusjonært og mye evolusjonært over seg – har bare såvidt begynt: Vi aner toppen av isfjellet.

Motivasjonen er å flytte all trafikk over på ett og samme nett – for å forenkle, forbedre og spare penger. Problemet er at verken nettverket eller protokollene er laget for denne type anvendelser. De stiller krav som var fullstendig fremmede da IP, Ethernet og overliggende protokoller ble definert (se Mellvik-Rapporten nr. 62, 75 og 79). Slike utfordringer er imidlertid til for å løses – og løst er de blitt. Det har tatt tid, det kan diskuteres om løsningene er optimale, og ikke alle de involverte standardene er stabile. Samtidig har 4 års praktisk erfaring med IP-baserte telefoni-systemer av varierende størrelse, gitt praktisk innsikt som får 1. generasjons-produktene til å fortone seg som prototyper fra laboratoriet.

Et evig prioriteringsproblem?

Prioriteringsmekanismer i nettverket har vært en av de største utfordringene i forbindelse med IP-telefoni: Taletrafikken er isolert sett beskjeden i sitt båndbreddebehov, men krevende med hensyn til leveringspålidelighet. Frontene har stått steilt imot hverandre: Den ene siden forfekter at prioriteringsmekanismer blir for kompliserte og umulig kan håndteres i omgivelser med ulike jurisdiksjoner som ikke kan stille krav til hverandre. De mener at å kaste båndbredde på problemet er den eneste farbare vei: Å sørge for at takhøyden alltid er rikelig. På den andre siden finner vi tilhengerne av standardbaserte mekanismer og protokoller som regulerer trafikken i nettverket i henhold til dens prioritet. De mener at å kaste båndbredde på problemet aldri kan bli kosteffektivt og heller ikke pålitelig: Det skal bare én storbruker til for å stoppe 1.000 telefonsamtaler.

Vi skal gjøre en lang historie kort og konstatere at IP-telefoni virker utmerket – i beskjedne, kontrollerte omgivelser. Videre viser QoS-diskusjonen ovenfor klare tendenser i retning av en Ole Brumm-løsning – “ja takk, begge deler”: Den ene blir for komplisert å administrere, mens den andre blir for ukontrollert og uforutsigbar. Hva med å regulere (styre trafikken) i kantene av det enkelte nettverk, og sørge for at det aldri slippes inn mer trafikk enn kapasiteten kan dekke? Det betyr at alle rutere i kanten av hvert nettverk må snakke sammen og oppdatere hverandre med hensyn til trafikkbelastningen – en betydelig oppgave som likevel er beskjeden i forhold til alternativet: At alle rutere i hele nettverket kontinuerlig ‘snakker sammen’, og at hver enkelt trafikkstrøm må utstyres med en prioritet. Et ‘nettverk’ i den forbindelse kan enten være bedriftsinternt eller tilhørende én bestemt ISP – eventuelt utvalgte deler av disse. Å sørge for at hvert enkelt nettverk ikke blir for stort, er en innlysende fordel for å gjøre løsningen skalerbar.⁷

I ‘enden’ av nettverket, det vil si ut mot brukerne – sendere, mottakere, telefonapparater, klienter, tjenere – må trafikken reguleres i større grad av detalj, hvilket nye lokalnettbaserte protokoller legger forholdene til rette for.

Denne ‘reviderte’ tankegangen rundt prioriteringsmekanismer i Internettet er interessant nok til å kvalifisere til en egen, grundig gjennomgang – en fristelse vi står imot ved denne korsvei, mens vi konsentrerer oss om konsekvensene: En klarere fokusering på hvor grensene mellom ulike nettverk går, styring av trafikken dem imellom og kapasitetsplanlegging og -kontroll. Toveis trafikk i sann tid krever forutsigbarhet, og dette er så langt den enkleste måten å tilfredsstille kravet på. Teknologi og standarder tilpasset denne tankegangen er underveis, og vil bli diskutert i trendgjennomgangen i Mellvik-Rapportens juni-utgave (nr. 96).

Betyr dette i sin tur at de QoS-mekanismene vi allerede har investert i, er bortkastet? Svaret kommer an på hvor langt vi har kommet og hvilke standarder vi har satset på. Modningen av lavnivå QoS-mekanismer i lokalnett (Ethernet) gjennom standardene 802.1p og 802.1q⁸ gir gode muligheter (kontrollnivåer) til trafikkstyring, og etablerer et godt grunnlag for å imøtekomme telefonisidens behov. Samtidig vokser utstrekningen av lokalnettet i parallell med at Gigabit Ethernet og 10 Gigabit Ethernet (Mellvik-Rapporten nr. 79 og 91) strekker seg kilometer og mil utenfor vårt tradisjonelle lokale domene.

Konsekvensene for arkitekturen kan oppsummeres slik:

- ✓ Introduksjonen av IP-telefoni krever stor kapasitetsmessig romslighet (takhøyde).

⁷ Uttrykk som “The return of the dumb network” og “dumb at the core, intelligent at the edges” brukes i denne forbindelse.

⁸ Vi kommer tilbake til disse standardene i en artikkel som gjennomgår status på QoS i lokalnett i 2. halvår i år.

- ✓ QoS-mekanismer i lokalnettet er en nødvendighet. Det betyr oppgradering og/eller utskifting av utstyr.

Det viktigste poenget også i forbindelse med IP-telefoni er om dens introduksjon kommer innenfor tidsrammen: Ligger den to år frem i tid, glemmer vi den i denne omgang!

Distribuerte brukere

At brukerne flytter på seg har innlysende konsekvenser: Trafikken flytter i andre retninger enn tidligere, belastningen blir mindre på interne nettverk, og tilsvarende større på eksterne. Erfaringen – så lenge ISDN var regelen – pekte mot totalt sett lavere belastning, mens pilen i dag peker den andre veien: Med 'bredbåndsforbindelser'⁹ via TV-kabel eller xDSL, har bruken og belastningsbildet forandret seg vesentlig.

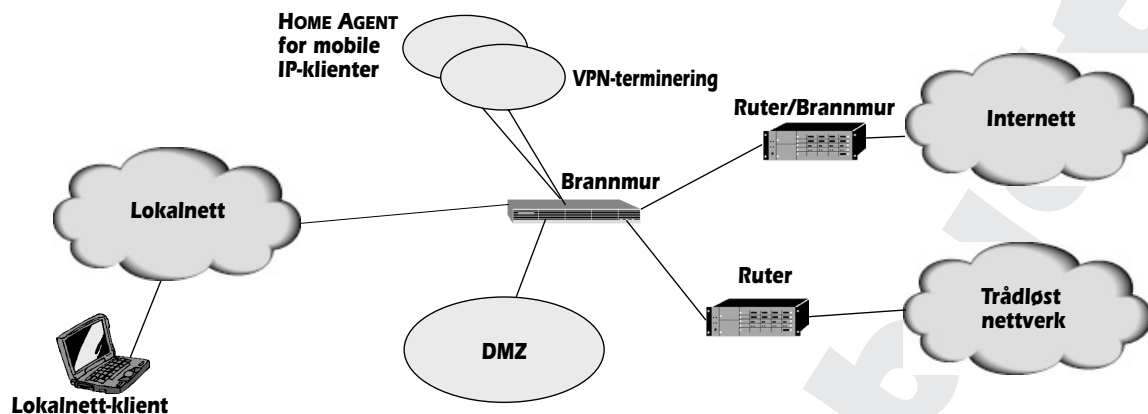
Vi kan oppsummere de viktigste arkitektur-messige faktorene slik:

- ✓ Egne tjenester (linjer, modem, autentiseringstjenere etc.) for oppringte brukere forsvinner, all ekstern trafikk bæres av Internettet.
- ✓ Linjekapasiteten mot Internettet må økes vesentlig – for å håndtere flere brukere, hver med høyere båndbredde og flere tjenester (for eksempel typen *netmeeting*, og etterhvert telefoni) ved siden av større krav til sikkerhet.
- ✓ Parallelt med at båndbredden mot Internettet økes, må brannmur-kapasiteten og andre sikkerhetsrelaterte tjenester følge med. Dette kommer vi tilbake til i forbindelse med sikkerhet.
- ✓ At brukerne blir mer distribuerte og mobile, aksentuerer behovet for sentralisering av IT-ressurser: Det handler om kontroll og kostnader. Likeledes må ressursene plasseres – i nettverksmessig/trafikkmessig forstand – optimalt i forhold til 'konsumentene': Brukerne flytter, belastningene flytter og ressursene tilpasses deretter.
- ✓ Behovet for trafikkstyring aksentueres: Det blir ønskelig, kanskje nødvendig, å skille 'hastetraffic' (tale, video, WTS/Citrix) fra vanlig trafikk (filoverføringer/nedlastinger, epost, surfing) – mot Internettet generelt og mot den enkelte bruker. Dette krever spesialutstyr og/eller programvare – som er lett tilgjengelig og relativt ukomplisert, men i beskjeden bruk i dag.

Trådløse teknologier

Ikke minst av sikkerhetsmessige årsaker får forandringene som drives frem av trådløse nettverk, mye til felles med punktene for distribuerte brukere ovenfor. Det trådløse nettverket kan illustreres som en ekstern 'sky' på linje med Internettet (figur 3), og trafikken behandles på samme måte – med hensyn til sikkerhetsmekanismer og flyt i for-

⁹ Vi setter bredbånd i anførselstegn her fordi mange av disse forbindelsene ligger i området 400 til 700 kbps, hvilket ikke kvalifiserer til betegnelsen.



Figur 3 Både av sikkerhetsmessige og praktiske årsaker er det hensiktsmessig å betrakte det trådløse nettverket som eksternt – på linje med andre eksterne nettverk.

hold til brannmur. Mens det er mulig å tenke annerledes, og å lage et spesielt nivå for det trådløse nettverket, taler både enkelhet og forventet fremtidig utvikling for å velge det vi kan kalle 'Internett-varianten'. Dermed får vi kun to kategorier – interne og eksterne, uansett hvilket eksternt nettverk som er i bruk. Utviklingen i retning av dynamiske, sømløse vandrenett (se Mellvik-Rapporten nr. 91), forlanger – for å unngå overdreven kompleksitet – at alle variantene betraktes som eksterne. At sikkerhetsmekanismene som følger i kjølvannet av et slikt valg, nødvendigvis må spise en merkbar del av båndbredden, blir en liten pris å betale for tryggheten.

Som et trinn på veien mot mobil IP (se nedenfor) og virkelig sømløshet, og for å ivareta sikkerheten, er det kort og godt ønskelig å tilpasse arkitekturen slik at det trådløse nettverket i sin helhet blir eksternt i forhold til lokalnettet.

Mobil IP

Mobil IP er teknologien som gjør det mulig for klienter å beholde konnektivitet mens de er i bevegelse (*roaming*). Mens dette lar seg realisere uten store komplikasjoner innenfor ett og samme WLAN, blir problemstillingen en helt annen når vi flytter oss ut av egen sfære – til offentlige IP-soner, GSM- eller GPRS-nettet eller andre teknologier. Løsningen går i korthet ut på at trafikken kapsles inn på en måte som gjemmer det faktum at en node alltid må ha samme adresse. Alle noder har et hjemsted (på fagspråket en *Home Agent*) som tar imot inngående trafikk og videresender den dit klienten befinner seg for øyeblikket (*Foreign Agent*). Dermed trenger ikke motparten å vite noe annet enn den faste adressen, mens mekanismer i nettverket sørger for at 'agentene' holder styr på hvor vi til enhver tid befinner oss.

Mekanismene har mye til felles med hva som brukes i dagens GSM-nett, og er som sådan modne og velprøvde. For arkitekturen ser vi umiddelbart følgende konsekvenser:

- ✓ All trafikk til de mobile klientene skal innom vårt nettverk – gjennom brannmuren og ut igjen – dobbel dose på sett og vis

[trafikk den motsatte veien går direkte fra klienten til senderen]. Det betyr enda en oppskalering av kapasiteten på brannmur og tilhørende enheter (for eksempel VPN-terminering).¹⁰

- ✓ Når en mobil klient kommer på innsiden av nettverket, oppstår en interessant problemstilling: Nå har vi allerede flyttet vårt WLAN til utsiden, slik at det ikke blir noen logisk forskjell å bevege seg inn i dette. Men hva om vi plugges inn en kabel fra lokalnettet, og forutsetter at sømløsheten skal vedvare? Da må trafikken ut via brannmuren, til vår *Home Agent*, som formodentlig er smart nok til å se at den i øyeblikket også er *Foreign Agent* for denne klienten, videre til VPN-terminering og tilbake til lokalnettet. Dette blir en vesentlig belastning i seg selv, og en dramatisk belastning når vi inkluderer det faktum at båndbredden til klienten plutselig er blitt 100 Mbps.

Utfordringene fortsetter med sikkerhetsmessige aspekter som vi skal komme tilbake til, og som ikke nettopp bidrar til å redusere de arkitektoniske og ytelsesmessige utfordringene. For vår arkitektur ser vi at det igjen er brannmurens plassering og kapasitet som kommer i fokus. Videre må plasseringen av tjeneste-ressurser både på kanten av nettverket (VPN-terminering, autentisering, *Home Agent*) og internt, evalueres. Kort og godt må vi tilbake til tegnebrettet med hensyn til kapasitetsplanlegging.

Neste utgave

I neste utgave avslutter vi gjennomgangen med først å se på tjenestesiden: Hvilke nye tjenester er på vei inn i nettverket og hva er deres konsekvenser? Vi fortsetter med sikkerheten, som vi allerede har nevnt en rekke ganger, og som representerer den største og mest innflytelsesrike faktoren.

Avslutningsvis setter vi opp et eksempel på en (forenklet) arkitektur for et mellomstort miljø som tar høyde for de forholdene vi har diskutert.

■

¹⁰ Hvorvidt det er hensiktsmessig å plassere agenten (*HOME AGENT*) på innsiden av brannmuren eller utenfor, er gjenstand for diskusjon. Sikkerhetsmessige hensyn taler for den innvendige plasseringen.