

Analyse, arkitektur og design av nettverk

Dette er 10. og siste artikkel i en serie med fokus på bygging av moderne lokalnett. Vi har gjennomgått behovsanalyse, krav, komponenter, innhold og arkitektur, design og styring.

I forrige utgave gjennomgikk vi en samling overordnede kjøreregler for siste etappe på veien mot et moderne nettverk. Design er kulminasjonen av den relativt lange og omstendelige prosessen vi påbegynte i desember 2002, og er 'veiledningen' for den fysiske implementasjonen av nettverket.

Et poeng som har gått igjen i prosessen, er viktigheten av å vite hvor vi er og hvor vi skal. Det hører med til våre dagligdagse selvfølgeligheter og er på grensen til banalt, men har like fullt lett for å forsvinne i hverdagens støy.

I forbindelse med behovsanalysen gjennomgikk vi blant annet hvordan trafikkanalyser og flytanalyser gir uunnværlig kunnskap om hva som rører seg i nettverket og hvilke behov som må tilfredsstilles i dets neste generasjon. Herunder er det en innlysende forutsetning at vi vet 'hvor vi er': Hvilke løsninger, tjenester og applikasjoner som 'rører seg' i nettverket.

Fra antagelser til viten

En fersk amerikansk undersøkelse⁹ avslører at slik kunnskap og egeninnsikt hører med til unntakene snarere enn regelen i markedet. Av 200 IT-ledere mente 25% å vite eksakt hvilke løsninger som er i aktiv bruk og hvor mye båndbredde de forbruker. I samme undersøkelse sier 60% at de vil øke den tilgjengelige båndbredden dersom de opplever forsinkelser i nettverket eller økte responstider fra applikasjonene. 82% innrømmer at signaler fra brukerne er deres viktigste kilde til informasjon om hvordan helsetilstanden for nettverket er.

25% høres beskjedent ut i en slik sammenheng, men nettverks- og sikkerhetseksperter Marcus Ranum mener i en kommentar at tallet er altfor høyt. "IT-ledere er feil gruppe å stille et slikt spørsmål til. Det er driftsansvarlige som vet hvordan den egentlige situasjonen er", sier han, og fortsetter: "Dersom de forteller sannheten, vil vi få vite at mindre enn 1% av verdens organisasjoner har den fjerneste idé om hva som foregår i deres nettverk."

Marcus Ranum er kjent for sine spissformuleringer og analogier. Ikke desto mindre trekker han frem et viktig poeng: Altfor ofte designes og drives nettverk i blinde – basert på vage antagelser og med 'kast mer båndbredde på problemet' som den normale løsningen når noe er galt. Som vi har vært inne på tidligere, har dette i flere tiår vært en akseptabel fremgangsmåte. Hovedårsaken til at situasjonen nå er annerledes, er først og fremst at nettverkets rolle har forandret seg – fra å være en

⁹ Undersøkelsen er et samarbeid mellom fagbladet Network World og leverandøren Packeteer Inc.

støttekomponent til å bli det mest kritiske elementet i våre IT-systemer.

Det betyr at ingen lenger kan la det skure. Vi må vite hvor problemene befinner seg og hva som forårsaker dem, hvilket forutsetter løpende og pålitelig informasjon om nettverkets helsetilstand. Å kaste båndbredde på problemene har ikke den samme effekten som under gårsdagens forhold, og vil i en rekke situasjoner overhodet ikke ha noen merkbar effekt. Rikelig båndbredde gir ikke pålitelig forutsigbarhet, hvilket går over fra å være et ønske til et krav sammen med introduksjonen av IP-telefoni, IP-baserte videokonferanser og andre forsinkelses-sensitive anvendelser. Nettverket trenger en styringsarkitektur – et poeng vi har vært inne på tidligere, men som det like fullt er verdt å dvele ekstra ved avslutningsvis.

Hvor blir det av ressursene?

Poenget – og problemet – blir aksentuert av hyperaktuelle temaer som virus, ormer og SPAM. Nettverk uten prioriterings-mekanismer og trafikkstyring gir ingen mulighet til å sørge for at forretningskritiske anvendelser har fortrinnsrett når uviktig eller malignant trafikk fosser inn i eller ut av nettverket. Sagt på en annen måte: Effektive styringsmekanismer gir mulighet til å redusere skadevirkningene av virus og SPAM vesentlig når angrepene eller infeksjonene er et faktum. Dette er et argument for introduksjon av trafikkstyring som så langt har fått beskjeden oppmerksomhet.

Både undersøkelsen vi refererte til ovenfor og andre rapporter fra markedet, bringer en rekke andre interessevekkende problem-årsaker frem i lyset. For eksempel kommer det for en dag at bruken av Internettet, som i de fleste tilfeller vil si nettleser og eksterne Web-tjenester – gjerne uten tilknytning til virksomheten, utgjør en betydelig utfordring både på grunn av belastningseffekten og tiden som brukes. Video-strømmer fra nyhetsstasjoner eller fagrelaterte media trekkes spesielt frem i den forbindelse. Likeledes er misbruk av epost et voksende problem med store ressursmessige ringvirkninger: Gigantiske vedlegg uten signifikant nytteverdi forbruker ikke bare båndbredde, men utgjør en vesentlig belastning på epost-tjenere og lagringssystemer. Her avdekkes nok en gang et akutt opplæringsbehov. Fortsatt er det slik at brukere flest aldri har fått opplæring i bruk av epost og heller ikke er gjort kjent med noen organisasjonell policy for hvordan verktøyet skal brukes (akseptabel bruk). Resultatet er innlysende – og problematisk.¹⁰

Problemområder

Områder som i henhold til disse rapportene oppfattes som spesielt problematiske eller som grunnlag for bekymring, bør være av interesse

¹⁰ Kombinasjonen Word og epost benyttes spesielt ofte som eksempel. Brukere som ikke har fått epost-opplæring, skriver gjerne sine epost-meldinger som Word-dokumenter, selv om det kun er noen få linjer. Det som skulle ha vært en mikroskopisk transaksjon ender opp som en melding med vedlegg som i mange tilfeller er 100 ganger større enn den burde ha vært.

for IT-ledere og -ansvarlige flest. De kan oppsummeres slik – i prioritert rekkefølge:

- ✓ Virus og ormer
- ✓ Web-trafikk inklusive nyheter (fra aviser og radio/TV-stasjoner) og nedlastinger
- ✓ Epost med vedlegg (typisk videoklipp, lydklipp, mp3-filer, fotografier etc.), samt filoverføring i tilknytning til øyeblikksmeldinger (*Instant Messaging* – se Mellvik-Rapporten nr. 105). Sistnevnte er riktignok langt mer effektiv i ressursmessig forstand enn bruk av epost til transport av de samme data, men like fullt gjenstand for betydelig misbruk og/eller skjodesløshet.
- ✓ Sanntids datastrømmer (TV, video, radio)
- ✓ Programvare-oppdateringer, *Service Packs*¹¹
- ✓ Filutveksling (såkalte *peer-to-peer* verktøy, som typisk benyttes i forbindelse med legal eller illegal utveksling av musikk, filmer, spill og andre data)
- ✓ Web-konferanser, video-konferanser, andre IP-baserte lyd/video-anvendelser

Undersøkelsene har også avslørt at de fleste miljøer, selv i det vi etter norske forhold vil kalle meget store organisasjoner, ikke har verktøy eller teknologi som kan gi et pålitelig og nyansert bilde av hva som flyter i nettverket. Til tross for dette faktum, gir de forespurte IT-lederne seg i kast med å estimere den ureglementerte eller unødige bruken til rundt 20% av totalen.

Hvor riktig eller galt dette estimatet er, kan vi vanskelig ha noen formening om fordi det er umulig å definere hva som er ureglementert. Der det ikke finnes klare regler og policies som brukerne kan forholde seg til, er i prinsippet alt tillatt.

Gjetninger ut, fakta inn

En slik 'vill vest' situasjon er naturligvis fullstendig uakseptabel – samtidig med at den er faretruende alminnelig. Hovedpoenget i denne sammenhengen er at arbeidet vi har lagt ned i tilknytning til analyse, arkitektur og design med stor sannsynlighet vil gi et mislykket resultat dersom organisasjonen ikke har et bevisst forhold til hvordan ressursene skal brukes. Kommentaren om opplæring på lederplass i forrige utgave er – dessverre – igjen på sin plass.

Forutsetning nummer én er med andre ord å sørge for at brukerne kan sine viktigste verktøy, vet hvilke regler som gjelder og hvilket ansvar som følger med bruken av dem. Før dette er brakt under kontroll, er

¹¹ Det er en interessant konsekvens av dagens lite lystelige tilstand med hensyn til programvarekvalitet at brukere flest jevnlig laster ned oppdateringer mer eller mindre ukontrollert, i mange tilfeller uten å vite hva som foregår fordi applikasjonene automatisk søker etter slike oppdateringer. Her er et betydelig lerret som må blekes før situasjonen kommer under kontroll. Det er ikke urimelig å se for seg sentraliserte løsninger av typen SoftGrid [www.softricity.com] som viktig element i denne prosessen, se forrige utgave av Mellvik-Rapporten side 34-36.

andre tiltak verdiløse. I den forbindelse er det også naturlig å sørge for at verktøy som ikke skal brukes, blir fjernet eller på annen måte deaktivert – på tjenere såvel som hos den enkelte bruker. Når kunnskapen og reglene er på plass, er sjansen dramatisk redusert for at brukerne reverserer en slik oppryddings-prosess på egen hånd, spesielt dersom konsekvensene av å sette seg ut over gjeldende regler er klart kommunisert.

Neste punkt er å skaffe til veie kunnskapen vi etterlyste innledningsvis – om de reelle forholdene i nettverket. Metodene i så henseende har vi vært innom tidligere i denne artikkelserien: Faktiske trafikkmålinger inngikk som en naturlig del av nettverksanalysen (se Mellvik-Rapporten nr. 103 og 104), og sørger for at vi nå vet hva som skal til for å skaffe den nødvendige kunnskapen. Poenget er at å skaffe oppdaterte bilder av virkeligheten ikke lenger er noe vi kan gjøre en gang i blant. For å komme på offensiven i forhold til behovsutviklingen på den ene siden og leveringskvaliteten på den andre, er det nødvendig med et kontrollsystem som kontinuerlig gir fakta og statistikker som viser hvordan nettverket brukes, belastningsbilder totalt og spredt over tid, feilsituasjoner og så videre.

Interessant nok er mange nettverk allerede instrumentert for å kunne levere slik informasjon uten at muligheten er tatt i bruk. Forklaringen er ofte en eller annen variant av 'vi har ikke hatt tid'-syndromet, hvilket kan være reelt nok, men som regel forteller mer om prioriteringene enn om tiden.

Når styrings- og logge-systemer er på plass, hvordan bruker vi denne kunnskapen? Utover de innlysende resultatene – finne flaskehals, avdekke misbruk og underdimensjonering – er det fordelingen mellom ulike anvendelser som er interessant. I forbindelse med nettverksanalysen konstaterte vi for eksempel at trafikkuundersøkelser kan gi indikasjoner om tjenere og/eller tjenester er feilplassert i forhold til brukerne. Likeledes får vi utvetydige hint om hvor replisering av kritiske, sentraliserte data kan være nyttig for responsen eller nettverksbelastningen.

Endelig trafikk-prioritering?

At vi kan måle og deretter analysere hvordan nettverksbelastningen fordeler seg på ulike anvendelser, er en opsjon av relativt ny dato. Den forutsetter pakkeinspeksjon på et nivå som i et nettverk med høy kapasitet og tilsvarende tett trafikk tidligere har vært umulig eller for kostbart. Utviklingen av spesialiserte integrerte kretser for IP-ruting i Gigabit Ethernet (GE) og 10 Gigabit Ethernet (10GE) nettverk, har imidlertid eliminert barrierer i den forbindelse. Ikke bare har vi nå mulighet til å overvåke høyhastighetstrafikk i sann tid, vi kan også i betydelig grad styre trafikken der det trengs eller er nyttig.

I praksis betyr det at diskusjonen om QoS, *Quality of Service* eller trafikkprioritering har fått ny næring. Årsaken til at slik prioritering ikke forlengst er et faktum i IP-nettverk generelt, er at mekanismer for merking av trafikken har manglet. I dag finnes de, men standarder for

hvordan ulike prioriteter skal oppfattes og behandles mangler eller har for liten gjennomslagskraft til å virke utenfor beskjedne enklaver.

Derfor er alternative prioriteringsmekanismer av stor interesse. Når vi er i stand til å overvåke trafikken på et nivå som avslører trafikktype – for eksempel Web-trafikk, epost, floverføringer, IM, CRM-systemer, ERP-systemer og så videre, sier det seg selv at vi også har mulighet til å regulere datastrømmene i forhold til hverandre. Skulle vi ønske å nedprioritere Web-, epost- og IM-trafikk til fordel for (for eksempel) CRM- og ERP-transaksjoner, er muligheten til stede i teknisk forstand. Med det riktige utstyret er det dessuten praktisk mulig. Det amerikanske selskapet Packeteer har spesialisert seg på nettopp dette feltet, og har i flere år levert produkter som regulerer trafikk etter slike parametre. De er ikke alene i dette foreløpig smale segmentet, der Linux er et annet innslag. Siden 2002 har en rekke Linux-distribusjoner hatt tilsvarende mekanismer – som riktignok ikke ytelsesmessig skalerer opp til GE-nivå, men som har fått betydelig utbredelse i forbindelse med for eksempel bredbåndstilknytninger.

Packeteer kan med betydelig rett kalle seg for pionérer i segmentet – uten at forspranget har gitt de forventede økonomiske uttellingene. Det å være tidlig ute er et tveegget sverd, og det har hittil vært vanskelig å overbevise markedet om at slik trafikkprioritering er nødvendig. Selv i 2003 har vi lett for å kaste båndbredde på de fleste nettverksrelaterte problemer og håper at de forsvinner, et forhold vi også var innom ovenfor.

Markedets sendrektighet har mindre med behov enn med frykt for det ukjente å gjøre. Mens de fleste IT-organisasjoner både kjenner problemene og ønsker seg løsninger, er vegringen mot ytterligere komplikasjoner av hverdagen stor. Utfordringen for leverandører som skal lykkes i segmentet er derfor å selge forenkling sammen med optimalisering.

Vi er ikke i tvil om at denne formen for trafikkprioritering har en fremtid, fordi den ikke forutsetter forandringer eller inngrep på protokollnivå i nettverket. Enkelhet er alltid en styrke, og dette er et eksempel på at en 'gammel' utfordring finner en ny løsning nærmest som en sideordnet konsekvens av den generelle ytelsesutviklingen. Vi er imidlertid ikke overbevist om at det må selvstendige bokser/enheter til for å gjøre jobben. Flere bokser gir høyere kompleksitet og mer som skal styres. Videre må slik prioritering, dersom den skal bli effektiv i lokalnettet som helhet, kunne foretas på alle ingress- og egress-punkter i nettverket, hvilket blir u håndterbart med mindre mekanismene kan integreres i det alminnelige konnektivitetsutstyret (svitsjer, rutere etc.)

Veien videre

Avslutningsvis er det nyttig med nok en påminnelse om at en nettverksarkitektur aldri er statisk. At den er ferdig og har avfødte design, betyr at den er optimal i øyeblikket og for den nære fremtiden, men også at den vil trenge tilpasninger til virkeligheten om 6 eller 12 måneder. ■