

DEN – Directory Enabled Networking

Directory Enabled Networking – umiddelbart kan det høres ut som en opprømsing av begreper uten sammenheng. Så ille er det ikke. Tvert imot har ideen etterhvert hatt god tid til å bli kjent – om ikke kjær – gjennom et antall år.

Helt siden katalogtjenester, halvparten av det teknologiske fundamentet, kom på banen i siste halvdel av 90-årene, har drømmen om å kombinere dem med nettverks-styring og -drift vært voksende. Temaet har vært perifert berørt her i Mellvik-Rapporten ved tidligere anledninger (se nr. 66), blant annet i diskusjoner om forenkling: Praktisk talt alle elementer rundt oss vokser i antall og kompleksitet. Forenklet styring og kontroll er en forutsetning for å komme videre, og *Directory Enabled Networking* er – slik verden ser ut i dag – et viktig virkemiddel i den retning.

Reservasjonen ovenfor er overlagt – for å understreke at det fortsatt er et stykke frem: Som vi skal se i denne artikkelen, er potensialet stort og behovet akutt, mens de praktiske resultatene så langt på ingen måte er oppsiktsvekkende.

Utfordringer

Grunnlaget for utfordringen er skalerbarhet: Nettverkene eksploderer, antall 'bokser' som sørger for at det hele henger sammen og fungerer, vokser eksponensielt, og verktøyene som skal besørge styring og kontroll, er i beste fall delvis kompatible med hverandre. Videre fører vår avhengighet av at nettverk og systemer alltid er operative, til nye krav som ikke kan tilfredsstilles etter dagens modell.

Etter den siste tids terror-aksjoner er for eksempel katastrofeberedskap blitt hyperaktuelt: Hva gjør vi dersom store deler av nettverket blir satt ut av spill? Kan vi med et håndgrep sperre all trafikk som ikke er livsnødvendig, og derigjennom reservere den gjenværende båndbredde til den mest kritiske trafikken? Få organisasjoner kan svare ja på spørsmålet, mens en riktig kombinasjon av DEN, et effektivt regelverk og riktige verktøy, er ideelt for å håndtere også slike situasjoner.

Kjernen i utfordringen kan oppsummeres slik:

- ✓ Vi har behov for å styre tjenester og 'bokser' på samme måte som vi styrer brukere.
- ✓ Vi skal koble sammen brukere, applikasjoner og tjenester på den ene siden, til bokser og nettverk på den andre.
- ✓ Brukere og nettverkstjenester er i mange tilfeller på plass i katalogtjenesten, men informasjonen er vanskelig å utnytte: Det finnes ingen standard representasjon (skjema) for bruke-

re og applikasjoner, og ei heller for tjenester og nettverks-elementer (bokser).

Løsningen – trinn 1

En ypperlig kilde til dybdekunnskap om DEN er boken **Directory Enabled Networks** (John C. Strassner, Fred Baker), New Riders Publishing, ISBN 1578701406.

DMTF – *Distributed Management Task Force*, industrigruppering som utarbeider standarder for distribuerte nettverksomgivelser (www.dmtf.org). Organisasjonen ble opprettet i 1992, og forkortelsen sto opprinnelig for *Desktop Management Task Force*, men ble endret i 2001 for å reflektere reelle oppgaver og interesser.

LDAP – *Lightweight Directory Access Protocol* – se Mellvik-Rapporten nr. 44 og 57, begge er tilgjengelige fra vår Web-tjeneste, se side 35.

Løsningen – i et overordnet perspektiv – er innlysende og krevende:

- ✓ En 'informasjonsmodell' som definerer abstraksjoner (modeller) av og representasjoner for:
 - ✗ Utstyr, protokoller og tjenester
 - ✗ Hvordan brukere og applikasjoner benytter tjenestene
 - ✗ Hvordan utstyret må konfigureres for å støtte tjenestene
- ✓ Dette gir oss en enhetlig, standardisert modell for å 'koble' sammen brukere, applikasjoner og nettverkstjenester. Samtidig etableres et fundament med de riktige bestanddelene for videre utvidelser og utvikling.

Vidløftig høres det ut, og blir gjerne luftig med et så overordnet perspektiv. For å flytte det hele nærmere hverdagen, og etablere forbindelsen mellom idé, teori og virkelighet, er det nyttig med noen definisjoner:

- ✓ **Informasjonsmodell:** En abstraksjon og representasjon – beskrivelse om vi vil – av elementene i et styrt system, deres egenskaper, funksjoner og grensesnitt (forhold til omverden). Informasjonsmodellen er uavhengig av lagringsform, anvendelse, protokoll og plattform.

- ✓ **Datamodell:** Noe forenklet en konkret forekomst av en informasjonsmodell, tilpasset omgivelsene den skal lagres i og protokollene den skal aksessereres med.

- ✓ **CIM – Common Information Model:** En objekt-orientert definisjon av hvordan informasjonsmodeller kan presenteres i praksis. CIM er en standard utviklet av DMTF, med bred markedsaksept. Standarden inneholder skjemaer for representasjon av systemer, nettverk, sammenkoblingselementer, applikasjoner og mer. Nye skjemaer utvikles kontinuerlig.

Tid for DIRECTORY ENABLED NETWORKING

Terroraksjonene mot USA har ikke bare aksentuert behovet for katastrofeberedskap: En hel verden vegrer seg for å dra på lange flyreiser og strammer inn på sine reisebudsjetter, mens flyselskapene øker prisene i takt med fallende trafikk. Videokonferanser og tilhørende utstyr havner nærmest automatisk på agendaen – spesielt i organisasjoner som strekker seg over landegrensene.

Tradisjonelle løsninger har fordret spesielle nettverk og kostbart utstyr – utenfor rekkevidde for andre enn de største. ISDN-baserte alternativer har vært fine å se på, men for dårlige og for kostbare. Med billige kameraer, kraftige prosessorer og god støtte for toveis lyd, har alminnelige PCer lenge utpekt seg som den optimale plattform for videotelefoni og -konferanser. Utstyret er billig og tilgjengelig, og programvaren likeså, fra Microsoft og andre leverandører. Den gjenstående utfordringen har vært nettverket: Hvordan sikre tilgjengelig båndbredde og pålitelighet når den trengs, og uten å legge beslag på store ressurser når de ikke benyttes?

Den tekniske løsningen på utfordringen diskuterte vi i forrige utgave, i artikkelen "Prioritering av nettverkstrafikk": Teknologien finnes og virker, men er vanskelig å implementere i nettverk som dekker 'mange jurisdiksjoner' – som Internettet. Umulig er det imidlertid ikke, og når de økonomiske incentivene er store nok, er det utrolig hva som lar seg gjøre.

Teknologi er imidlertid ikke tilstrekkelig. En minst like stor utfordring er å administrere og styre det hele, slik at ressursene allokeres når de trengs, og frigis når de ikke lenger brukes. I et stort nettverk er det – som vi også var inne på i nevnte artikkel – umulig å gjøre dette på tradisjonelt vis. Her må det pålitelig automatikk til, og DEN er veien til målet.

CIM – Common Information Model

CIM er ikke bare en måte å representere en informasjonsmodell på, men en standard. Eksistensen av en slik standard er én av forutsetningene for at DEN skal kunne realiseres i praksis. Utover å definere CIM-standardene og en rekke skjemaer tilpasset ulike utstyr- og system-typer, har DMTF også laget overgangsregler ('mappinger') mellom CIM og andre informasjonsmodeller som er relevante i nettverkssammenheng. Dermed er forholdene tilrettelagt for pålitelig og entydig utveksling av data mellom CIM og MIB (MASTER INFORMATION BASE, benyttes av styringsverktøy og tilhørende agenter grunnlagt på SNMP-protokollen) og MIF (MANAGEMENT INFORMATION FILE, som er dataformatet knyttet til DMI-standardene).

DMI – DESKTOP MANAGEMENT INTERFACE, det første resultatet av arbeidet i DMTF-gruppen

SNMP – SIMPLE NETWORK MANAGEMENT PROTOCOL, standard etablert av IETF, INTERNET ENGINEERING TASK FORCE

Dermed har vi grunnlaget for en enkel definisjon av *Directory Enabled Networks*:

DEN: En tilpasning (mapping) av CIM til et format som kan lagres i en katalog via LDAP-protokollen.

Så enkelt – og samtidig så komplisert. Vi ser at CIM er selve grunnlaget for DEN, og at organisasjonen DMTF har spilt en nøkkelrolle i utviklingen av standardene som danner fundamentet for konseptet.

DMTF har følgende tre punkter som visjon og mål for DEN:

- ✓ Utnytte mulighetene moderne katalogtjenester tilbyr til å styrke nettverkstjenestene
- ✓ Gjøre CIM tilgjengelig som katalogskjemaer
- ✓ Legge grunnlaget for samspillende, standardiserte nettverkstjenester via LDAP

Dette handler om anvendelse av teknologi i langt større grad enn utvikling: DMTF lager standarder og spesifikasjoner, ikke teknologi. Dessuten – og like viktig for de fleste av oss – som hører hjemme på kundesiden i bildet: De fleste elementene og standardene er ute av syne for oss: Vi trenger ikke å se dem eller kjenne til detaljene i dem, men å vite at de støttes og hva det betyr i praksis.

Forbi teknologien

Om vi fjerner alle forkortelsene og de tekniske frasene, er målsettingen kort og godt å kunne beskrive nettverket med alle dets komponenter og sammenhenger, i en database som aksesseres via LDAP-protokollen. Her er alle elementene like viktige – lenker i én og samme kjede: Å kunne beskrive nettverket i en database har liten verdi med mindre a) beskrivelsen er standardisert, slik at hvem som helst kan forstå den og bruke informasjonen, og b) aksessmekanismen er standardisert, slik at informasjonen er lett tilgjengelig for alle som måtte ha bruk for den.

Forenklingen vi kan oppnå gjennom å benytte de samme mekanismene for å styre rutere og tjenere, svitsjer og klienter, telefonsentraler og printere er innlysende. Dessuten og vel så viktig: Det blir mulig å innføre grader av automatisering som tidligere har vært fullstendig utenfor rekkevidde. Reservering av ressurser, som vi diskuterte i forrige utgave, er et nærliggende eksempel: Å sette opp en videokonferanse mellom et dusin eller flere deltagere på ulike geografiske steder, forutsetter at flere titalls bokser i nettverket får sine instruksjoner og vet hva de betyr, og at involverte systemer og klienter vet hvordan trafikken skal håndteres.

Med mindre hele denne operasjonen er automatisert, slik at ressursene kan reserveres og frigjøres med enkle håndgrep, er det innlysende at video-konferanser vil høre til sjeldenhetene. Situasjonen for de fleste organisasjoner i dag er at dette enten er umulig, for tidkrevende – eller muliggjort gjennom en hårdhendt homogenisering av nettverket, med alt utstyr og tilhørende programvare fra én og samme leverandør. En slik *en gros* utskifting av utstyr og plattformer er kun unntaksvis mulig – og aldri ønskelig.

Fra teknologi til politikk

SLA – Service Level Agreement

MIB – Management Information Base

CLI – Call Level Interface

Directory Enabled Networking gir med andre ord det teknologiske grunnlaget for å komme et viktig skritt videre i retning av effektiv kontroll og styring av nettverksressurser: Den gir mekanismene til å styre – rorpinnen og gass-spaken om vi vil. Men hva skal vi styre etter? Hvor er kartet og forklaringene på hvordan kartet skal leses? Se det forteller DEN lite om. Vi har fått kjøretøyet, men ingen kjøreopplæring.

Helt innlysende er det kanskje ikke, men retningslinjene for disponering av ressursene er å finne i organisasjonens regler og rutiner: Her spesifiseres det hva som gjelder, hva som er viktig, hvordan vi skal prioritere og hvilke mål vi skal nå. Dersom detaljeringsgraden er utilstrekkelig for å imøtekomme behovene i forbindelse med bruk av ulike IT-ressurser, må den utvides og tilpasses dagens behov. En slik situasjon er regelen snarere enn unntaket, selv i 2001: Få organisasjoner har funksjonelle og oppdaterte policy-dokumenter, verken generelt eller på IT-området.

Når regelverket er på plass, gjenstår utfordringen med å koble sammen regelverket med teknologien: Hvordan omsette regler og policy i konfigurasjoner og kommandoer for det fysiske utstyret, som til slutt styrer trafikken og prioriteringene?

Trinn 2: Regelverket

Løsningen, som slett ikke er umiddelbart opplagt, er først og fremst å akseptere at et regelverk ikke må oppfattes som en lovtekst, men som et spekter der målet alltid er det samme, men der form og innhold må tilpasses hvem brukeren er og i hvilken sammenheng de skal benyttes. At bruker X har rettigheter Y, begrensninger Z og IP-adresse W kan stå i et dokument, men er uegnet til å styre nettverk og systemer: Disse trenger en annen representasjon av samme innhold. Forholdet illustreres i figur 3.

Et forenklet eksempel illustrerer hvordan dette fungerer i praksis – når relevant informasjon og regler er tilgjengelig i katalogen:

- ✓ En bruker starter Microsoft NetMeeting, og forsøker å etablere kontakt med 2 kolleger.
- ✓ Forespørselen registreres på tjenersiden, som i første omgang forespør katalogtjeneren om dette er en tjeneste brukeren har tilgang til.
- ✓ Gitt at svaret er positivt, undersøkes det hvilket nivå brukeren tilhører. Typisk etableres det tre eller flere nivåer med



Figur 3 Regler, retningslinjer og mål for virksomheten må kunne omformes og tilpasses ulike sammenhenger for å brukes som grunnlag for automatisering og styring av infrastrukturen.

- hensyn til ressursforbruk: Standard (de fleste), sølv (storbrukere, ledere), gull (toppledere, brukere med spesielle behov).
- ✓ Et verktøy oversetter disse og flere parametre til nettverks- og utstyrsspesifikke verdier, kommandoer og konfigurasjoner ved hjelp av 'mapping' som allerede finnes i katalogen.
- ✓ Det samme eller et annet verktøy instruerer den underliggende infrastrukturen om hvordan trafikken som tilhører denne forespørselen skal håndteres.
- ✓ En mekanisme i applikasjon eller infrastruktur sørger for å frigjøre ressursene når de ikke lenger brukes eller trengs.

Selv dette enkle eksemplet demonstrerer at oppgaven er omfattende, og samtidig at resultatets praktiske verdi er stor: Dette er en type funksjonalitet (automatisering) vi ikke bare trenger, men snart vil være avhengige av. Samtidig er status på området høyst utilfredsstillende: Både mekanismer og metoder mangler ferdige standarder, og henger et par år etter DEN i så henseende. Verktøyene som finnes er interessante, men mangelfulle.

På den positive siden kan vi anføre at det arbeides frenetisk på området, i standardiserings-organisasjoner og hos leverandører. IETF – Internettets standardiseringsorgan – er en av aktørene, og en håndfull tentative spesifikasjoner finnes (tilgjengelige på Internettet – se www.ietf.org). Utgangspunktet er en vedtatt standard som definerer en generisk modell for regelverket: RFC 3060 – *Policy Core Information Model - version 1 Specifications*.

Vi innser også raskt at fagfeltet eller segmentet i seg selv fortjener og forlanger oppmerksomhet langt utover denne introduksjonen. Derfor vil vi komme tilbake til *Policy Based Networking* her i Mellvik-Rapporten på nyåret, med en mer inngående introduksjon og ikke minst en status-rapport.

Konklusjon

Styret i DMTF-organisasjonen er sammensatt av de mest prominente aktørene i IT-bransjen:

- Intel
- IBM
- Compaq
- HP
- Sun
- Microsoft
- Novell
- Symantec
- 3Com
- Cisco
- BMC Software

DEN er langt mer enn et konsept; det er en standard – med tre unike egenskaper:

- ✓ Konseptet definerer både en informasjonsmodell og en samling tilpasninger til ulike datamodeller.
- ✓ Modellen er tilstrekkelig omfattende og utvidbar til å dekke de behov for styring, rapportering og kontroll vi kan se, inklusive muligheten til å knytte regler til parametrene – for eksempel: Mellom kl. 0100 og 0400 på hverdager skal 70% av båndbredden på linje X reserveres for trafikktype Y.
- ✓ Mens andre modeller står alene, kan DEN kombinere informasjon fra en rekke ulike standarder.

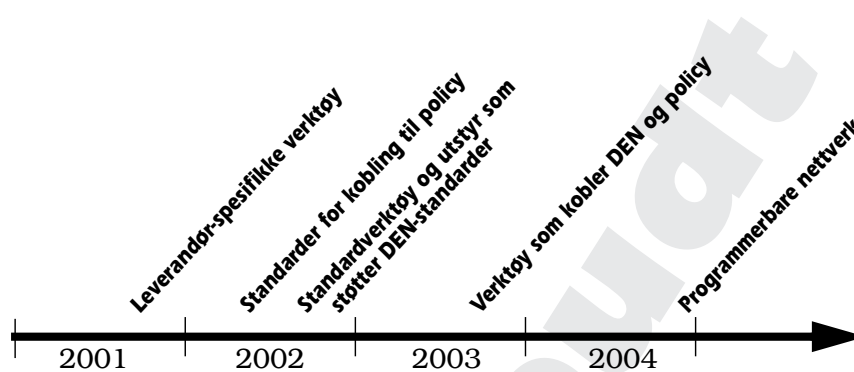
Dermed blir DEN en fellesnevner og en katalysator som får sin egen massefart gjennom å tilby muligheter hele markedet er ute etter: Leverandørsiden i like stor grad som kundesiden. Videre har organisasjonen DMTF tilstrekkelig bredde bak seg til at spesifikasjonene sjelden skaper politiske problemer i bransjen. Veien fra papiret til praktiske implementasjoner blir dermed relativt kort.

Hvor står vi så i dag? Situasjonen kan oppsummeres i følgende korte punkter:

- ✓ Konsensus i markedet om behovet for og viktigheten av DEN er øredøvende.
- ✓ Standardene er ferske, uprøvde og i enkelte tilfeller mangelfulle.
- ✓ Katalogtjenester er fortsatt under utprøving i mange organisasjoner, og det er for tidlig å ta deres tjenester i bruk på bred basis. Active Directory i Windows 2000 representerer en milepæl i så henseende, men møter skepsis i deler av markedet på grunn av sin tette integrasjon med operativsystem og andre elementer.
- ✓ Verktøyene er underutviklet og leverandørspesifikke.
- ✓ Effektive koblinger mellom policy og katalogens datamodeller er mangelfulle.
- ✓ De eneste løsningene som i noen grad virker, er leverandørspesifikke.

Dermed blir konklusjonen slik vi antydnet innledningsvis, at vi trygt kan ile langsomt – *hurry up and wait*, som det heter. Ikke desto mindre er det nyttig å se fremover, og skaffe seg et bilde av hva som er på horisonten. Det vi trenger er kort sagt et programmerbart nettverk. På lengre sikt er det ønskelig at også applikasjonene videreutvikles, slik at de blir i stand til å fortelle nettverket om sine behov, undersøke hvilke ressurser som er tilgjengelige og tilpasse seg til disse – ikke én gang, men hver gang.

Et programmerbart nettverk leverer automatiserte tjenester til sine klienter, og blir i høy grad selvstyrt, i noen grad selv-reparerende – og er verdiløst uten applikasjoner som kan utnytte dets egenskaper. For oss som arbeider med infrastruktur til vanlig, høres dette ut som en drøm



Figur 4 Estimat for utviklingen i retning av programmerbare nettverk.

der fordelene er innlysende og formidable, men der vi avfeier det hele med at dette ikke er mulig. Hva som er mulig og ikke kommer imidlertid an på perspektivet. Slik verden og trendene avtegner seg i dag, kan de viktigste milepælene fremover estimeres som vist i figur 4. ■