

## NAT: Nettverksmagi med bivirkninger

Se også artikkelen "Network Address Translation: Nødvendighet eller problem?" i Mellvik-Rapporten nr. 59.

*NAT – Network Address Translation – er moderne nettverksmagi. Vi plugges inn en boks til 400-500 kroner, og kan plutselig dele én offisiell Internett-adresse mellom flere titalls, kanskje hundretalls, brukere. Funksjonen er transparent – for brukerne, applikasjonene og tjenestene som kontaktes. Med på kjøpet får vi sågar en brannmur.*

Med utgangspunkt i en slik beskrivelse er 'magi' et nærliggende adjektiv for NAT. Og beskrivelsen er udiskutabelt korrekt – om ikke akkurat fyllestgjørende. Nettverkskompetente lesere vil nok heller karakterisere den som villedende, korrektheten til tross. Årsaken til paradokset er at NAT ble laget for helt andre omgivelser og for å løse andre problemer enn hva dagens Internett-hverdag karakteriseres av.

### En underlig historie

I så måte er det nærliggende å minne om at det samme er tilfelle med de fleste Internett-protokollene. At de har overlevd betyr at deres opprinnelige design har vært enkel, robust, fleksibel og ikke så rent lite forutseende. At mange av dem – inklusive TCP/IP – vanskelig kan karakteriseres som egnet for formålene de benyttes til i dag, er også et faktum. På den andre siden er *the proof of the pudding* fortsatt *in the eating*: Det faktum at de ikke bare eksisterer og brukes, men mangler reell konkurranse, overskygger kritikken.

### Problemet som forsvant

NAT kom til verden helt i begynnelsen av 90-tallet, i kjølvannet av sterk bekymring for tilfanget av Internett-adresser. I all sin enkelhet har NAT bidratt til at vi mer enn ti år senere, og etter en kolossal vekst i spredning og bruk av Internettet, i dag har omtrent like store adresse-reserver som for 10-12 år siden.<sup>7</sup>

På den tiden hersket det bred konsensus om at dagens Internett-protokoll var ved slutten av sin levetid, og at etterfølgeren – IPv6 – ville overta før årtusenskiftet. NAT ble derfor ansett for å være en midlertidig mekanisme for å løse et akutt problem. Innsatsen som ble lagt i å ruste NAT-mekanismen for eventuelle fremtidige behov, var tilsvarende beskjeden.

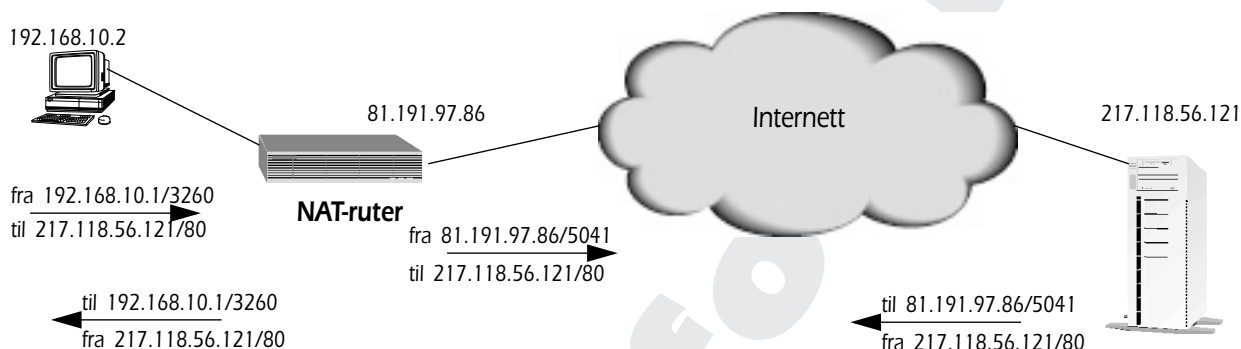
Siden har det teknologiske verdensbildet forandret seg betydelig, og vi ser ikke lenger noen slutt for dagens Internett-protokoller. Riktignok øker bruken av IPv6 jevnt og trutt, spesielt i Asia, men ingen tar lenger på seg å spå om eller når arvtakeren eventuelt tar over. Uansett hva vi måtte mene om akkurat det, ligger tidspunktet for langt inne i fremtiden til å spille noen rolle for de evalueringer og valg vi gjør i dag og i morgen.

<sup>7</sup> NAT er naturligvis ikke alene om æren for denne situasjonen, men uten tvil en vesentlig bidragsyter.

Dermed blir også NAT med oss videre fremover, og utfordringene teknologien forårsaker, må løses uten å skape konflikter i forhold til spesifikasjoner og eksisterende implementasjoner.

## Enkelt, men ikke så greit

Men hvor komplisert kan det egentlig være? Skal ikke NAT ganske enkelt oversette interne adresser til eksterne, og passe på at inngående trafikk havner på riktig sted? Jovisst, og i utgangspunktet er oppgaven enkel – som illustrert på figur 2 nedenfor. For å holde styr på



**Figur 2** En adresse/port-oversetter har i utgangspunktet en enkel oppgave – å omskrive pakkehoder og holde styr på tabeller som forteller hvor innkommende trafikk skal rutes. Oppgaven kompliseres av at den kan løses på mange forskjellige måter og at et voksende antall anvendelser ikke følger den tradisjonelle klient/tjener-modellen.

forbindelsene og kanalisere inngående trafikk til riktig mottaker, bruker NAT-ruteren en tabell der hvert innslag inneholder (opptil) 5 elementer: Avsender-adresse og -port, hvilken port dette ble oversatt til, samt mottaker-adresse og -port. Innkommende trafikk som klaffer på alle 5 punkter, slipper igjennom, annen trafikk forkastes.

### Kilde til forviklinger

Her starter imidlertid også komplikasjonene: Hva om den eksterne tjeneren som kontaktes, overfører svaroppgaven til en annen tjener, hvilket blir stadig mer alminnelig? Dersom mekanismen fungerer som ovenfor, vil svar-trafikken bli forkastet. Skal vi for å imøtekomme dette behovet, si at all innkommende trafikk til en port som finnes i 'aktivtabellen', og som dermed har initiert en slik forbindelse, slipper igjennom? Eller skal vi forlange at også (den eksterne) avsenders portnummer er det samme som den opprinnelige?

En lang rekke slike spørsmål dukker opp når vi graver dypere i materien, og svarene finnes ikke i spesifikasjonen, RFC-1631 fra 1994. Oppklaringer i RFC-2663 (1999) og RFC-2776 (2000) hjelper, men forandrer ikke på det faktum at implementasjonene som er i bruk i dag, benytter alle tenkelige vari-

### NAT vs. NAPT

Mens NAT støttes av de fleste rutere som selges i dag, med priser fra NOK 350 og oppover, brukes funksjonen sjelden. Det som brukes er NAPT – *Network Address and Port Translation* – som er en del av samme spesifikasjon, men ikke det samme. NAT forutsetter et én-til-én forhold mellom interne og eksterne adresser, altså at ruteren har tilgang til en samling offisielle Internett-adresser som kan benyttes når det trengs.

Dagens typiske situasjon er imidlertid at vi får tildelt én offisiell adresse og må klare oss med den. NAPT tar vare på denne én-til-mange situasjonen, og overskygger fullstendig NAT i praktisk bruk. Denne realiteten er årsaken til at begrepene har forandret betydning. Når NAT brukes i dag, er det som regel i betydningen NAPT. Enkelte leverandører bruker også betegnelsen SUA, *Single User Account* for det samme. Den egentlig NAT trenger dermed et nytt navn, og kalles gjerne *True NAT* eller *Real NAT*.

anter av de åpne problemstillinger som finnes.

Årsaken til at denne tilsynelatende forvirringen ikke har manifestert seg i enorme konnektivitetsproblemer, er at den opprinnelige mekanismen fungerer bra for de mest alminnelige anvendelsene – epost og surfing med nettleser. Disse to – og mange flere – følger den tradisjonelle klient/tjener-modellen, som NAT opprinnelig ble laget for: Klienten spør (initierer forbindelsen), tjener svarer, klient sender data, tjener sender data tilbake. Innkommende trafikk som ikke kan kobles til en utgående forespørsel av ny dato (typisk *timeout* 2-5 minutter), blir forkastet.

Her er NATs største styrke og svakhet. Siden forbindelser kun kan initieres innenfra – fra klienten, fungerer NAT-enheten som en enkel brannmur: Den slipper kun igjennom trafikk som en eller annen klient på innsiden har bedt om. At dette ikke er nok til å stoppe virus, som gjerne transporteres via epost eller Web-sider, forandrer ikke det faktum at NAT blokkerer tilfeldig, uinvitert trafikk utenfra. Andre viktige fordeler er enkelheten vi allerede har vært inne på, som gjør at en NAT-boks kan plasseres uten videre nærmest hvor som helst mot klienter i nettverket.

En signifikant svakhet er at klient/tjener-modellen ikke lenger dekker våre behov. En jevnt voksende andel av tjenestene vi etterspør og benytter, forutsetter at tjenesten kan kontakte klienten uten direkte invitasjon som NAT forutsetter. Alle P2P- (*peer-to-peer*) anvendelser hører hjemme i denne kategorien. Det samme gjelder telefoni – som er

inne i en eksplosiv utvikling, spill, ulike tjenester for øyeblikksmeldinger og så videre. Dessuten er tjenersiden ikke lenger 'stabil' i nettverksmessig forstand. Flere tjenere kan være involvert i leveringen av samme tjeneste – for eksempel i en lastfordelings-konfigurering eller i en kompleks ehandels-løsning. Videre dukker det stadig opp nye såkalte multiparty- (samarbeids-) anvendelser, ikke bare i forbindelse med spill, men også i profesjonell sammenheng.

### UPnP, NAT og sikkerhet

Det er en utbredt misforståelse at UPnP, *Universal Plug and Play*, har noe med NAT å gjøre. Årsaken til misforståelsen er at UPnP kan forandre måten NAT fungerer på, eller mer spesifikt: Besørge konfigurasjonsendringer på en NAT-ruter.

UPnP er en konfigurasjonsmekanisme og har ingen ting med verken NAT eller ruting å gjøre. Initiativet til teknologien kom i 1999 fra Microsoft som svar på det de oppfattet som en trussel fra Sun: JINI. Hensikten er å gjøre det enkelt for nettverksprodukter (rutere, aksesspunkter, PCer, telefoner, alarmer etc.) å konfigurere seg selv, uten å involvere brukere – som er uten forutsetninger for å bidra til en slik konfigurasjonsprosess.

Microsoft fikk med seg en enorm samling leverandører i UPnP Forum, og spesifikasjonen ble ferdig på rekordtid. Siden er det imidlertid blitt relativt stille. UPnP støttes riktignok av mange nettverksprodukter for konsumentmarkedet, men anvendelse og dermed nytteverdi er det smått med.

Ikke overraskende kom det nemlig raskt for en dag at UPnP representerer en betydelig sikkerhetsrisiko. Forkortelsen fikk på rekordtid en ny betydning i tekniske kretser: *UnPlug and Pray*. I løpet av vinteren 2001/2002 gikk bølgene høyt rundt UPnP og svakheter i Windows XP. Microsoft ble gang på gang hengt til tørk for å feilinformere markedet om både svakheter og konsekvenser. Saken ble etterhvert så belastende at selskapet i februar 2002 satte i gang sin store sikkerhetsoffensiv – *Thrustworthy Computing*. Resultatene av tiltaket overlater vi i denne omgang til leseren å mene noe om, men for UPnPs vedkommende kom massefarten aldri tilbake.

Det hersker i dag bred konsensus hos sikkerhets-eksperter om at teknologien er risikabel og bør slås av der den finnes. Dermed er det også innlysende at dens praktiske betydning er beskjeden.

### Et usynlig problem

Dessuten, som vi har vært inne på tidligere (Mellvik-Rapporten nr. 59), representerer NAT et betydelig problem for VPN-tunneller med IPSec, som riktignok lar seg omgå,<sup>8</sup> men som er langt fra trivielt og på en eminent måte illustrerer hvilke komplikasjoner en slik

usynlig 'hjelper' i nettverket kan føre med seg. En NAT-boks fjerner den direkte koblingen mellom adresse og endepunkt som de fleste Internett-tjenester tar for gitt. Og utfordringene på teknisk nivå stopper ikke her, men en fullstendig analyse av dem havner utenfor temaet for denne artikkelen.<sup>9</sup>

Usynligheten var i sin tid en viktig forutsetning for at NAT overhodet skulle kunne anvendes. Dens eksistens måtte være fullstendig transparent for både klient og tjener. Anvendelsene som nå banker på døren, har andre behov som vanskelig kan tilfredsstilles uten at applikasjonene eller tjenestene vet om det finnes en NAT-oversetter på veien, og eventuelt hvordan den fungerer. Usynligheten har gått fra å være en nødvendighet til å bli et problem. Dersom NAT-enheten kunne forespørres på et standardisert vis, ville mange av utfordringene vi nå står overfor være langt mer overkommelige.

Med millioner av enheter i drift, er det åpenbart for sent å forandre på grunnleggende karakteristika for NAT. Som tilfellet har vært med en rekke andre Internett-protokoller, må det finnes alternative veier rundt utfordringene – og det har ikke manglet på forsøk i så henseende de siste årene. Enkelte applikasjoner har klart utfordringen rimelig bra, med telefoni-tjenesten Skype (se Mellvik-Rapporten nr. 123) og spillet CS (CounterStrike) som nærliggende eksempler. At slike leverandør- eller applikasjons-spesifikke mekanismer fungerer, bringer oss imidlertid ikke nærmere en generell løsning på problemene.

På standard-siden er STUN (*Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*, RFC-3489) et nærliggende eksempel og et hederlig forsøk, men løser fortsatt kun en del av problemet. Bare navnet er tilstrekkelig til å fortelle at dette er komplisert – og mekanismen introduserer en grad av kompleksitet som vi egentlig forsøker å unngå, både i Internettet og i andre sammenhenger.

## Mot kanten av stupet?

Gitt alle utfordringene vi har presentert, hvordan kan det ha seg at de fleste av oss i en eller annen sammenheng bruker NAT i løpet av en dag eller en uke uten å merke noe til dem? Forklaringen er først og fremst at vi i teknisk forstand har tilpasset vår verden til de muligheter og begrensninger som finnes, og NAT er en av dem. For å komme rundt det faktum at NAT-bokser hindrer Internett-brukere flest fra å motta oppkoblinger utenfra, har – som vi var inne på ovenfor – en rekke applikasjoner og tjenester tatt skjeen i egen hånd. De har fått sine egne mekanismer som for det første avslører om en NAT-boks finnes, og dernest benytter såkalte rendezvous-mekanismer for å 'invi-

8 Hvordan IPsec kan sameksistere med NAT er beskrevet i IETF-dokumentet RFC-3715 (mars 2004). En etterhvert alminnelig måte å kortslutte problemstillingen på, er å la NAT-enheten også være VPN-endepunkt, hvilket selv billige rutere for konsument-markedet nå tilbyr. Dette gir imidlertid ikke samme grad av sikkerhet som full ende-til-ende sikring.

9 En glimrende og grundig gjennomgang av NAT i går, i dag og i morgen er å finne i artikkelen "Anatomy" av den kjente australske Internett-eksperten Geoff Houston i *The Internet Protocol Journal* vol.7 nr. 3 ([www.cisco.com/ipj](http://www.cisco.com/ipj)).

tere' de nødvendige eksterne koblingene og derigjennom koble sammen mange samtidige brukere eller noder.

At det er mulig å komme rundt problemene, forandrer imidlertid ikke det faktum at NAT ødelegger fundamentale grunnpillarer i Internettet: Alltid konnektivitet ende-til-ende, at selve nettverket er uten egen intelligens og at endepunkter (IP-adresser) representerer pålitelige identifikatorer. Det finnes også andre teknologier som setter én eller flere av disse elementene på prøve, men ingen av dem representerer en like stor utfordring som den usynlige NAT.

Spørsmålet som uvegerlig dukker opp, blir dermed om vi egentlig er på vei mot stupet – mot en nettverksteknisk katastrofe hvis utkomme må bli en storstilt overgang til IPv6 over hele verden?<sup>10</sup> Eller er det mulig å få utviklingen inn på et spor som holder oss på riktig side av stupet og på sikt øker avstanden til avgrunnen? Sikkert er det i alle fall at det er for sent å fjerne NAT fra Internettet, og det mangler ikke på 'glupe' hoder som arbeider med å finne akseptable og gjennomførbare løsninger på utfordringen.

### En ny NAT-standard?

Den mest sannsynlige – og dessuten ønskelige – veien videre går via en ny standard. Årsaken til at Internettets standardiseringsorganisasjon IETF ikke har engasjert seg med forbedringer av NAT de siste 10 årene (utover de dokumentene vi allerede har nevnt), er at teknologien har vært kategorisert som midlertidig. Innsats for raffinering av det midlertidige kunne bidra til ytterligere aksept av NAT, hvilket ikke var ønskelig.

NAT trengte imidlertid ingen slik støtte for å bli praktisk talt allesteds nærværende, og som vi har sett, er situasjonen overmoden for nettopp en innsats. Markedet har behov for en 'NAT2' eller 'NATv2', som for det første spesifiserer alle detaljene som ble utelatt i første omgang, og derigjennom har skapt dagens uholdbare situasjon. Dernest må en ny NAT-utgave sørge for at implementasjonene blir funksjonelt forutsigbare, og at NAT-bokser blir synlige komponenter i nettverks-administrativ forstand. Det må bli mulig å signalisere spesielle behov for ulike applikasjoner og å gjøre enhetene til en styrbar del av en sikkerhetspolicy. Slik situasjonen er i dag, motarbeider NAT-enheter gjennomføring av overordnede sikkerhetstiltak, bidrar – i motsetning til hva som er den generelle oppfatningen – til å svekke sikkerheten i stedet for å styrke den.

## Konklusjon

Vi kan ønske NAT dit pepperen gror av utallige gode, tekniske årsaker, men det blir som å ønske seg et nytt politisk system i Norge. Vi må leve

10 Det er i denne sammenhengen verdt å nevne at IPv6 ikke eliminerer NAT, selv om behovet for konservering av adresser blir borte. Tvert imot er det lagt opp til private adresse-områder også i IPv6, og det kan lett finnes situasjoner hvor NATing kan være ønskelig. Imidlertid er det ingen grunn til å tro at bruken av NAT i en IPv6-verden vil bli særlig utbredt. Dessuten befinner bruken av denne kombinasjonen seg på et tilstrekkelig tidlig (beskjedent) stadium til at det fortsatt er mulig å foreta tilpasninger som fjerner hovedproblemene vi sliter med i dagens IPv4-NAT.

med det vi har, og må gjøre det beste ut av situasjonen, hvilket blant annet betyr tilpasninger til realitetene.

NAT er på vei dit, men det skjer ikke over natten. En arbeidsgruppe i IETF-regi under navnet *Middlebox Communication Working Group* har tatt fatt i noen av problemstillingene, som ikke bare gjelder for NAT, men også for ulike proxyer, trafikk-'komprimatorer', brannmurer og trafikk-releer.

Håpet er at gruppen vil få et bredere mandat i forhold til NAT, og i løpet av de neste 18 månedene kan komme opp med en anbefalt spesifisering for en ny NAT-generasjon. At prosessen er brolagt med kontroverser og tekniske utfordringer, er det liten tvil om. Men alternativet er verre. Det er god motivasjon for både innsats og kompromisser.

I mellomtiden lever vi videre med den NATen vi har, der kunnskap om realitetene setter oss i stand til å gjøre veivalg som er optimale i forhold til behovene. Knappt noen implementasjoner er 100% like, og mens de fleste er formelt korrekte i forhold til gjeldende standard, er det ikke umiddelbart innlysende hvilke som er i stand til å dekke våre behov. Derfor er kunnskap makt også i denne sammenheng. ■