Het ongewenste einde van end-to-end Internet?*

Dit artikel is verschenen in nummer 2 van het Tijdschrift I&I (jaargang 2000) en in geactualiseerde vorm in de jubileumuitgave van I&I "nieuwe media in perspectief" (2003).

door Erik Huizer

Het mist de sex-appeal van het World Wide Web en het mist de politieke lading van telecominfrastructuur. Toch vormt het Internet Protocol (IP), zoals de naam al zegt, de kern van het Internet. Jarenlang heeft IP in alle stilte onveranderlijk bijgedragen aan de ongeëvenaarde groei van het Internet. De laatste tijd is het Internet Protocol onder technische en commerciële druk aan het veranderen en de gevolgen zijn verstrekkend.

Inleiding

In de pers verschijnen regelmatig artikelen over ontwikkelingen op het Internet en de economische, sociale of maatschappelijke gevolgen. Deze artikelen betreffen vrijwel zonder uitzondering bepaalde toepassingen of diensten op het Internet of de onderliggende transmissie-infrastructuur. Een voorbeeld van het eerste is de uitgebreide aandacht voor e-commerce en van het laatste het geharrewar van de OPTA en KPN Telecom over de toegang tot het Internet via het telefoonnetwerk.

Waar je, behalve in de vakpers, weinig over leest of hoort is wat er tussen deze twee componenten zit en wat meestal wordt aangeduid met de term "TCP/IP protocol". Door Internet Service Providers (ISP) wordt dit ook wel infrastructuur genoemd, Telecom operators noemen het een dienst en netwerk-puristen noemen het de transport- en netwerklaag. Voor de meeste Internet-gebruikers is het niet meer dan een onbegrijpelijk abracadabra wat ze alleen te zien krijgen als ze in hun Windows instellingen per ongeluk op het netwerk icoon hebben geklikt.

In werkelijkheid is het Internet Protocol (IP) de bindende factor die alle Internet gebruikers ter wereld in staat stelt met elkaar te communiceren. Enerzijds zijn over het Internet Protocol ontelbare toepassingen en diensten mogelijk, zoals E-mail, WWW, Telefoon, TV, E-commerce etc. Anderzijds kan het Internet Protocol over allerlei transmissie-infrastructuren en dragers worden gebruikt, zoals telefooninfrastructuur, Kabel-TV infrastructuur, glasvezel, GSM, laserstralen, infrarood, etc. Zo ontstaat het in Internet-kringen gangbare zandloper model (National Research Council, 1994, blz. 53). Een vereenvoudigde weergave van dit model is weergegeven in figuur 1. Uit het model blijkt duidelijk dat IP het kleinste gemene veelvoud is in de wereld van de communicatieprotocollen (een gemeenschappelijke "taal" in een wereld van vele "talen"), waardoor communicatie met een willekeurige andere Internet gebruiker mogelijk is.

Als een toepassing of dienst niet aanslaat in de markt (of niet (langer) goed functioneert, of door nieuwe regelgeving wordt gehinderd) dan zal er onmiddellijk een alternatief beschikbaar komen in de markt dat voor iedereen snel te gebruiken is. De keuze in toepassingen en diensten is vrij en overdadig en wordt gestuurd door gemak, beschikbaarheid, toepasbaarheid en (vooralsnog in veel mindere mate) kosten. Dankzij IP kun je blijven communiceren, met elke applicatie en dienst naar keuze.

Wanneer een transmissie-infrastructuur niet levert wat de gebruiker wil (hier wordt de keuze wel in sterke mate bepaald door de factor kosten)? Dan neem je een andere. Kabel in plaats van telefoon als toegang thuis. Draadloos in plaats van Ethernet op kantoor. Je kunt het wijzigen zonder dat alle andere gebruikers op het Internet dat op hetzelfde moment ook moeten doen. Dankzij IP kun je blijven communiceren.

Het end-to-end model

Het Internet Protocol is ontwikkeld in de jaren zestig in opdracht van het Amerikaanse ministerie van defensie. Het ministerie had behoefte aan een communicatieprotocol dat flexibel en snel inzetbaar was, ongeacht de beschikbare infrastructuur (ofwel: in tijden van oorlog). Alle netwerken die er tot dan toe waren (voornamelijk telefoon) gingen er van uit dat je een verbinding over het netwerk opzet tussen de twee communicatiepartners, waarbij alle tussenliggende netwerkcomponenten (kabels, schakelaars, centrales etc.) voor de duur van de verbinding aan die verbinding worden toegewezen (dit wordt een "circuit-schakeling" genoemd).

Het bijzondere aan IP is dat het heeft gebroken met deze traditie van circuit-geschakelde netwerken. Bij het Internet Protocol wordt pakket-schakeling gebruikt. Hierbij verdelen de communicatiepartners (meestal computers) de communicatie in kleine delen (IP-pakketten) die stuk voor stuk worden voorzien van een geadresseerde en een afzender. De pakketten worden vervolgens op het netwerk "gegooid" waar ze zelf hun weg naar de eindbestemming dienen te vinden. Groot voordeel van deze methode is dat bij een probleem op een bepaalde verbinding de IP-pakketten onmiddellijk een andere route zullen nemen en daardoor de verbinding niet wordt verbroken. Circuit-schakeling is goed te vergelijken met treinen en het spoornet in Nederland, terwijl pakket-schakelen het best vergeleken kan worden met auto's en het wegennet.

Op basis van het Internet protocol kunnen netwerken gemakkelijk aan elkaar worden gekoppeld. Aangezien IP geen centrale toewijzing van middelen vereist is er geen centrale autoriteit vereist. Men koppelt een netwerk aan het Internet zonder daarbij de autoriteit over het eigen netwerk uit handen te geven. Het is met name deze eigenschap van het Internet protocol die de oorzaak is geweest van de sterke groei van het Internet.

Dit Internet Protocol ontwikkelde zich in de loop van de jaren zeventig tot een uitermate flexibel protocol. Bij communicatie tussen twee op een IP-netwerk aangesloten systemen worden er daadwerkelijk IP-pakketten uitgewisseld tussen die twee systemen. Het netwerk zelf verandert niets aan de IP-pakketten die onderweg zijn, het zorgt er slechts voor dat ze te bestemder plaatse arriveren. In Internet kringen wordt dit het end-to-end principe genoemd. Het tussenliggende netwerk is inherent "dom", gezien vanuit het perspectief van de eindstations (computers). Het enige dat het netwerk doet is de IP-pakketten afleveren, zonder zich om de inhoud te bekommeren.

Adressering en routering

Een duidelijke consequentie van het end-to-end principe is dat elk op het Internet aangesloten systeem een uniek IP-adres moet hebben. Zonder dat is het voor IP-pakketten niet mogelijk om eenduidig naar hun eindbestemming gerouteerd te worden. In theorie zijn er ruim 4 miljard van deze IP-adressen beschikbaar in de huidige versie van het Internet Protocol (IP versie 4).

De Internet infrastructuur bestaat uit verbindingen die op knooppunten in zogenaamde routers bij elkaar komen. Als een IP-pakket over een verbinding bij zo'n router aankomt moet de router besluiten via welke verbinding het IP-pakket verder moet om zo snel mogelijk bij de eindbestemming te komen. Dit noemen we routeren. Een router in het Internet moet dus van elke mogelijke bestemming (dus van elk IP-adres) weten waar het zich bevindt. Er zijn echter zoveel IP-adressen in omloop dat het bijhouden van een route per IP-adres zelfs voor de meest krachtige routers ondoenlijk is.

IP-adressen worden dan ook aan organisaties (en ISPs) toegekend in blokken van opeenvolgende adressen. Op deze wijze hoeven de routers niet te onthouden waar elk individueel adres zich bevindt, het is nu voldoende dat de routers weten waar een blok van adressen zich bevindt. Hoe groter de blokken van adressen, des te minder blokken en dus des te minder het netwerk (de routers) hoeft bij te houden.

Tot begin jaren negentig waren er slechts drie categorieën van adresblokken die werden uitgedeeld aan gebruikers (organisaties met een eigen netwerk, Internet toegang providers en andere ISPs). Men had de keuze uit:

een blok met ruim 16 miljoen adressen;

een blok met ruim 65000 adressen; of

een blok met 256 adressen.

De adresblok indeling werd ontwikkeld ver voor dat de eerste PC op de markt kwam, in een tijd dat nog maar zeer weinig mensen vermoedden dat er wereldwijd behoefte was aan meer dan enkele tientallen computers. De opkomst van de PC, het modem en niet lang daarna het lokale netwerk (LAN) maakte dat de groei van het aantal aangesloten computersystemen op het Internet veel harder ging dan men had durven denken. Vanaf ca. 1983 verdubbelt het aantal aangesloten systemen elk jaar. Bedrijven installeren LANs met enkele honderden van Pc's en vragen adresruimte aan. Zij krijgen noodgedwongen een blok uit categorie B (categorie C is te klein, A is veel te groot). Door deze inefficiënte manier van blokken adressen uitdelen krijgt een organisatie heel veel IP-adressen die het niet gebruikt.

Begin jaren negentig werd al snel duidelijk dat verreweg alle adresaanvragen noodgedwongen in categorie B werden ingedeeld en dat het aantal adresblokken in deze categorie daardoor rond het eind van 1994 op zouden raken als er geen actie werd ondernomen. Bovendien dreigde door de inefficiënte verdeling de totale adresruimte op te gaan raken rond 2008.

In eerste instantie lijkt het alternatief om organisaties in plaats van een groot blok uit categorie B meerdere kleine blokken van adressen uit categorie C te geven. Dit zou de verspilling van adresruimte en het opraken van blokken in de categorie B voorkomen. Echter dat zou tot gevolg hebben dat de hoeveelheid informatie in het netwerk (een route voor elk blok) exponentieel zou stijgen, hetgeen de routers niet aan zouden kunnen. Er werden door de Internet Engineering Task Force (IETF, het standaardisatie-orgaan van het Internet) twee oplossingen ontwikkeld om deze problemen het hoofd te bieden.

De korte termijn oplossing omvatte het afschaffen van de adrescategorieën en het efficiënter toewijzen van adressen. Een organisatie die nu adresruimte aanvraagt krijgt een op maat gesneden adresblok dat voldoende groot is om aan de wensen van de organisatie tegemoet te komen. Bovendien werd het uitdelen van adressen zo gestructureerd dat de routers in het Internet makkelijk adresblokken kunnen samenvoegen tot één route, hetgeen de explosieve groei van de routeringstabellen binnen de perken hield. Deze oplossing vereiste nogal wat technische maatregelen (alle router software en host software op het Internet moest vervangen worden), operationele maatregelen (alle ISPs moeten hun netwerken er op afstemmen) en organisatorische maatregelen (opzetten organisatie efficiënt uitdelen van adressen). Mede door de duidelijke noodzaak en dankzij een flexibele transitie (niet alles hoefde tegelijk te gebeuren) is deze oplossing in enkele jaren verwezenlijkt.

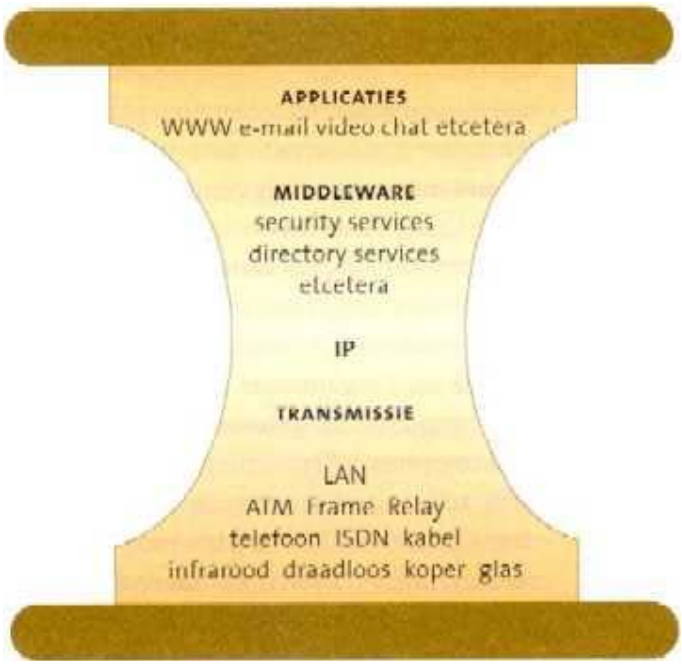
Dit heeft geleid tot de situatie waar we ons nu in bevinden met het Internet. Internet-adressen zijn dus niet erg schaars, maar worden nu alleen volgens strikte regels uitgedeeld om te zorgen dat ze niet schaars worden. Iedere organisatie met een duidelijk omschreven behoefte kan zoveel adressen krijgen als er noodzakelijk zijn. Op basis van deze situatie en de huidige groei van het Internet geven de laatste voorspellingen aan dat we nog voldoende adressen hebben tot ver in de 21ste eeuw.

De tweede oplossing die de IETF heeft uitgewerkt is voor de langere termijn en bestaat

uit een nieuwe versie van het Internet Protocol (IP versie 6 ofwel IPv6). De ontwikkeling van dit protocol is een zware strijd geworden tussen de "innovators" die hun kans schoon zagen om allerlei nieuwe toeters en bellen in het nieuwe protocol in te bouwen en de "operators" de mensen die verantwoordelijk zijn voor de stabiliteit en de beschikbaarheid van het Internet die geen nieuwe dingen willen die niet bewezen zijn in een operationele omgeving. IPv6 lijkt daarom erg op IPv4 met meer adresruimte (2 tot de macht 128 adressen, ofwel 50.000 IP-adressen per vierkante centimeter aardoppervlakte). Zaken die nu reeds beschikbaar zijn als toevoeging aan het bestaande IPv4 protocol zoals beveiliging (IPsec), mobiliteit en automatische adresconfiguratie zijn ingebouwd in het IPv6 protocol.

De huidige situatie

Het succes van de korte termijn oplossing heeft er toe geleid dat de motivatie om IPv6 te implementeren niet zo groot is. De onmiddellijke noodzaak is immers niet langer aanwezig. Dat IPv6 op de lange termijn nog zeker de beste (en noodzakelijke) oplossing is wordt duidelijk beschreven in (King et al., 1999). Er wordt door alle gerenommeerde software-, hardware- en Internet-leveranciers hard gewerkt aan de IPv6 oplossing en er zijn reeds volop producten beschikbaar die deze versie van het Internet Protocol ondersteunen. Diverse ISPs bieden inmiddels ook de mogelijkheid om met het Internet te koppelen op basis van IPv6.



Figuur 1: Vereenvoudigde weergave van het 'zandlopermodel' De korte termijn oplossing heeft echter ook een andere effect tot gevolg gehad dat door de markt is ontwikkeld en dat nu ruimschoots wordt toegepast: Network Address Translation (NAT).

NAT is gebaseerd op het principe dat niet alle op een lokaal netwerk aangesloten systemen tegelijkertijd een verbinding met de rest van het Internet actief hebben. Een organisatie met een dergelijk LAN geeft alle aangesloten systemen een IP-adres uit een niet uniek blok van IP-adressen (private address space, Rekhter et al. 1996). Daarnaast vraagt de organisatie een formeel blok van publieke (en dus wel unieke) IP-adressen aan voor het LAN dat voldoende is om het geschatte aantal gelijktijdig op het Internet actieve systemen van een adres te voorzien. Tussen het LAN en de verbinding met de rest van het Internet wordt een zogeheten NAT-box geplaatst. In de NAT-box wordt het blok met verkregen publieke adressen opgeslagen. Indien nu een computersysteem op het LAN

een verbinding wil opzetten met een systeem op het Internet, worden de IP-pakketten opgevangen door de NAT-box. De NAT-box vervangt in elk IP-pakket het niet-unieke private IP-adres door een IP-adres uit het blok van publieke IP-adressen, en zorgt er zo voor dat het systeem tijdelijk een uniek IP-adres krijgt toegewezen.

Hoewel NAT diverse nuttige toepassingen kent, zijn er vele nadelen aan verbonden (zie Hain, 1999), waarvan de belangrijkste is dat het end-to-end principe dat de basis vormde voor het Internet zoals we dat kennen overboord wordt gegooid. De argumentatie om NAT te gebruiken is vaak oneigenlijk:

Het is niet mogelijk voldoende publieke (unieke) IP-adressen te verkrijgen; Zoals hierboven al is uitgelegd is dit niet correct. Wel dient men duidelijk te kunnen aangeven waar IP-adressen voor nodig zijn, maar er is voldoende adresruimte beschikbaar.
Het draagt bij aan de beveiliging; NATs worden vaak gecombineerd met Firewalls die het lokale netwerk tegen ongewenste toegang moeten bewaken. Een "hacker" kan door het toepassen van een firewall niet rechtstreeks doordringen tot een systeem op het LAN, maar zal eerst door de firewall heen moeten. Natuurlijk is het zo dat als een hacker door de firewall heen weet te breken de schade niet wordt beperkt door het gebruik van private (niet unieke) adressen op het LAN.
Ach, we hebben het toch op de firewall zitten.
De meeste mensen die deze argumenten (en dus NAT) gebruiken zijn zich niet goed bewust van de nadelen. Een en ander wordt natuurlijk versterkt door het feit dat hardware en software leveranciers met NAT in hun productportfolio graag bijdragen aan het verspreiden van de mythes die aan deze misverstanden ten gronde liggen.
De toepassing van IPv6 kent deze problemen niet. Sterker nog IPv6 voegt allerhande voordelen (zoals autoconfiguratie) toe, die het opzetten en beheren van netwerken een stuk eenvoudiger maken, terwijl de transparantie voor de gebruiker behouden blijft. Daartegenover staat dat de introductie van IPv6 natuurlijk een forse inspanning vergt die (binnen een organisatie of ISP) ondersteund moet worden door een goede visie op de lange termijn voordelen van dit nieuwe protocol.

Gevolgen

Naast NAT zijn er inmiddels andere ontwikkelingen die maken dat het end-to-end principe niet meer geldt en dat het Internet steeds minder transparant wordt voor gebruikers. Sommige hebben te maken met beveiliging (firewalls, proxy, Application Level Gateway, etc.) sommige hebben te maken met efficiëntie en besparen van bandbreedte (caching, load-sharing-switches, etc.). Waar vroeger op het Internet een IP-pakket ongestoord van het de ene computer naar de andere ging is dat dus tegenwoordig vaak niet meer het geval. Meestal zonder dat de gebruiker het weet (of het beseft) worden de IP-pakketten geopend, geïnterpreteerd, veranderd of zelfs vernietigd.

Het netwerk is intelligenter geworden. Lag vroeger de intelligentie alleen bij de eindsystemen, nu is het netwerk ook intelligent en "denkt mee" met de datastromen die er in omloop zijn. Deze trend wordt natuurlijk versterkt doordat naast de originele ISPs inmiddels de traditionele telecom maatschappijen zich ook op de Internet markt hebben begeven. Deze maatschappijen redeneren traditioneel vanuit een perspectief dat je alleen (een goede) service kan leveren als je een intelligent netwerk tot de beschikking hebt, en sturen vanuit deze opvatting de markt. Het Internet begint daardoor qua architectuur steeds meer trekjes te vertonen van de traditionele telecom datanetwerken. Dat heeft nogal wat gevolgen die niet alleen technisch zijn:

1. **Eilandvorming**
   Allereerst ontstaat er op deze wijze een Internet dat uit geschakelde eilanden bestaat in plaats van één groot transparant netwerk. Als

gevolg daarvan is het niet meer eenduidig te voorspellen wie met wie kan communiceren en of dat in omgekeerde richting ook werkt.

2. **Kwetsbaarheid**
   In het klassieke Internet kon elk afzonderlijk IP-pakket zijn eigen weg zoeken, het maakte niet uit via welke weg de eindbestemming werd bereikt. Als er een verbinding uitviel zocht het netwerk onmiddellijk een alternatieve weg voor het IP-pakket. In de nieuwe situatie moeten IP-pakketten via verplichte punten (NAT, Firewall etc.) die elk op zich een "single point of failure" vormen. Het is door deze gedwongen routering niet altijd mogelijk voor pakketjes om een alternatieve weg te zoeken indien er een verbinding niet werkt. Het netwerk wordt dus kwetsbaarder. Bovendien brengt de intelligentie in het netwerk veel ingewikkelder software met zich mee, en software is zelden foutloos. Meer intelligentie betekent dus ook een veel grotere kans op fouten.

3. **Controle**
   Meer intelligentie in het netwerk betekent meer controle over de verschillende datastromen. Natuurlijk is die controle handig ten behoeve van het bewaken van de kwaliteit van de service, maar het betekent ook dat de eindgebruiker geen controle meer heeft over zijn/haar datastroom. Het geeft bijvoorbeeld totalitaire regimes de mogelijkheid om de IP datastromen van en naar hun land te beperken of te filteren, of aan bedrijven om datastromen met een bepaalde inhoud (b.v. informatie over product X) te vertragen, zodat de gebruiker concurrerende informatie (b.v. over product Y) sneller en beter ontvangt.

4. **Aftappen**
   Doordat in het klassieke Internet de IP-pakketten elk hun eigen weg konden kiezen was aftappen eigenlijk alleen mogelijk op de toegangslijn van de eindgebruiker (local loop). Verderop was het immers niet mogelijk om te garanderen dat alle IP-pakketten van een bepaalde bron daar ook langs zouden komen. In de nieuwe situatie met de intelligentie in het netwerk is het eenvoudig om op elk van de punten die "iets met een IP-pakket" doen een tap aan te brengen. Dit maakt het voor overheden eenvoudig om een strikt aftapbeleid te voeren (b.v. het Amerikaanse Echelon spionagenetwerk, Klaver, 1999).

5. **Beveiliging**
   Het IPsec protocol is bedoeld om (geheel transparant voor de gebruiker) de datastroom tussen twee eindstations geheel te versleutelen en op die manier te beveiligen tegen afluisteren of verminken. Dit is met name handig voor thuiswerkers die via hun lokale ISP willen werken op het LAN van hun werkgever. Algemeen geldt dat met het toenemende belang van veilige communicatie over het Internet IPsec een efficiënte en, voor de gebruiker, transparante manier van beveiligen is. IPsec is een toevoeging aan het huidige Internet Protocol. In IPv6 zit IPsec ingebouwd. IPsec beschermt de communicatie tussen twee systemen door ervoor te zorgen dat:
   de identiteit van de betrokken systemen wordt geverifieerd; Het wordt zeer moeilijk om een systeem op het Internet zich te laten voordoen als een ander systeem. Dit kan bijvoorbeeld helpen bij het voorkomen van de in februari 2000 op Yahoo en E-bay uitgevoerde "Denial of Service" aanvallen.
   de communicatie niet is af te luisteren; De inhoud van alle IP-pakketten wordt versleuteld, zodat deze alleen voor de beide eindsystemen leesbaar zijn.

de integriteit van de communicatie wordt gewaarborgd. Er wordt voorkomen dat er "onderweg" iets aan de IP-pakketten wordt veranderd.
Het zal duidelijk zijn dat IPsec moeilijk toepasbaar is in een netwerk met NATs en dergelijke die gebaseerd zijn op het kunnen lezen, snappen en soms zelfs veranderen van IP-pakketten. Als IPsec niet kan worden toegepast door dergelijke intelligentie in het netwerk is het aan de gebruiker om zelf actie te ondernemen en zijn/haar communicatie te versleutelen. Dat vereist momenteel nog veel technische kennis en kunde en zal dus meestal niet gebeuren, met alle risico's van dien.

6. **Nieuwe applicaties**
   In het klassieke Internet was het mogelijk voor een klein bedrijf of zelfs een individu, om een nieuwe applicatie te ontwikkelen en die snel te verspreiden. Elke gebruiker die dat wilde installeerde de nieuwe applicatie en een nieuwe dienst was geboren. Indien de dienst aansloeg (WWW, Real, ICQ) was de verspreiding bijna onmiddellijk (killer application). Nu zullen vele van de intelligente netwerkcomponenten de snelle verspreiding van een nieuwe applicatie op het Internet blokkeren. Het is niet langer alleen aan de gebruiker om een applicatie te installeren en te gebruiken, ook de ISPs moeten hun netwerkapparatuur vaak aanpassen. Dit geeft grote spelers op de markt van de ISPs de mogelijkheid applicaties te vertragen of te versnellen en daarmee de markt te bespelen.

7. **Nieuwe communities**
   De kracht van het Internet zit niet alleen in de aanwezige informatie, maar vooral ook in de communicatie en de daaruit voortvloeiende "global communities". Gebruikers met dezelfde interesses groeperen zich ongeacht geografische barrières en tijdzones. In het klassieke Internet ontstaan deze communities spontaan doordat communicatie en informatie zich ongehinderd over het Internet kan plaatsvinden. In de nieuwe situatie is dit minder vanzelfsprekend. Het vormen van een community en het ondersteunen van een community met diverse applicaties kan niet langer zonder meer spontaan plaatsvinden. Meer en meer is overleg nodig met de ISPs van de betreffende gebruikers om bepaalde zaken te regelen.

Wat kan IPv6 doen?

Veel van de toevoegingen aan IPv4, zoals NAT, zijn in IPv6 overbodig. Er is in IPv6 voldoende adresruimte om adrestranslatie overbodig te maken. IPv6 maakt goede authenticatie van communicerende systemen mogelijke waardoor de beveiliging wordt verbeterd. Daarnaast voegt IPv6 allerhande voordelen (zoals autoconfiguratie) toe, die het opzetten en beheren van netwerken een stuk eenvoudiger maken, terwijl de transparantie voor de gebruiker behouden blijft. IPv6 is zo ontworpen dat het geen onnodige intelligentie aan het netwerk toevoegt en dus geen van de nedelene heeft die allerlei toevoegingen aan IPv4 (zoals NAT) wel hebben.

IPv6 zal, ondanks voldoende adressen en geïntegreerde beveiliging, niet voorkomen dat op diverse plaatsen NAT's en firewalls worden toegepast. Wel zal de noodzaak vor dergelijke intelligentie in de infrastructuur sterk verminderen in een IPv6-netwerk. Daartegenover staat dat de introductie van IPv6 natuurlijk een forse inspanning vergt die (binnen een organisatie of ISP) ondersteund moet worden door een goede visie op de langetermijnvoordelen van dit nieuwe protocol.

Conclusies

De IP-laag vormt de kern van het Internet en is de basis van het succes van dit wereldwijde netwerk. Het is wenselijk om deze kern te ontwikkelen met behoud van de bestaande functionaliteiten en eigenschappen. Dit is bijvoorbeeld goed mogelijk door de introductie van IPv6, dat nieuwe eigenschappen als beveiliging (IPsec), mobiliteit en automatische adresconfiguratie toevoegt terwijl de bestaande eigenschappen behouden blijven. De ontwikkeling in de markt gaat echter een kant op waarbij de kern steeds meer intelligentie krijgt. Hierbij worden enerzijds eigenschappen toegevoegd aan het Internet Protocol die nogal wat nadelen met zich meebrengen en anderzijds wordt een groot deel van de bestaande functionaliteit en eigenschappen van het Internet Protocol tenietgedaan.

Deze ontwikkeling is niet meer te stoppen en zal ook bij een succesvolle introductie van IPv6 doorzetten. Een snelle en succesvolle introductie van IPv6 zal de schade echter flink kunnen beperken. Meer organisaties zouden zich dan ook bewust moeten worden van het belang van de invoering van IPv6. Daarbij moet echter wel gekeken worden naar het belang op de lange termijn, terwijl in de nieuwe economie het korte-termijn belang de voorkeur lijkt te hebben.

Deze ontwikkelingen dwingen de Internet Architecture Board en de IETF tot een heroverweging van de Internet architectuur. De strategische visie waar deze organisaties aan werken zal in deze fase van het Internet helaas niet veel invloed meer hebben. Hoogstens draagt ze bij aan het begrip rond de technische ontwikkelingen op het Internet. Het sturen van die ontwikkelingen gebeurt tegenwoordig vanuit Wall street en niet vanuit een doorwrochte op consensus gebaseerde strategische visie.

De (maatschappelijke) gevolgen voor de gebruikers zijn significant. Waar de gebruiker in het geval van diensten en toepassingen zelf nog kan kiezen en sturen is dat bij het Internet Protocol niet het geval. De gevolgen zijn dan ook ingrijpend door het hele Internet heen. Het nieuwe Internet dat hieruit naar voren komt zal vele nieuwe diensten en toepassingen kennen, maar zal ook veel verloren hebben van de vrijheid die het zo aantrekkelijk maakte.

Literatuur

Computer Science and Telecommunications Board, National Research Council, "Realizing the Information Future: The Internet and Beyond", National Academy Press, Washington, D.C. 1994
Hain, "Architectural implications of NAT", in voorbereiding als RFC, concept beschikbaar op: http://www.ietf.org/internet-drafts/draft-iab-nat-implications-04.txt, 1999.
Huitema, "IPv6: The New Internet Protocol," Prentice-Hall:Upper Saddle River, NJ, 1998.
King et al., "Case for IPv6", in voorbereiding als RFC, concept beschikbaar op: http://www.ietf.org/internet-drafts/draft-ietf-iab-case-for-ipv6-05.txt, 1999.
Klaver, "Echelon pesten", I&I jrg. 17 no 4, 1999.
Rekhter et all, "Address Allocation for Private Internets", RFC-1918, 1996.

Prof.dr. ir. Erik Huizer is hoogleraar Internet-toepassingen aan de Universiteit Twente en directeur business development bij het NOB. Daarnaast is hij lid van de Internet Architecture Board en voorzitter van de Internet Research Task Force. Dit artikel is geschreven toen hij werkzaam was als directeur van het SURFnet ExpertiseCentrum bv.