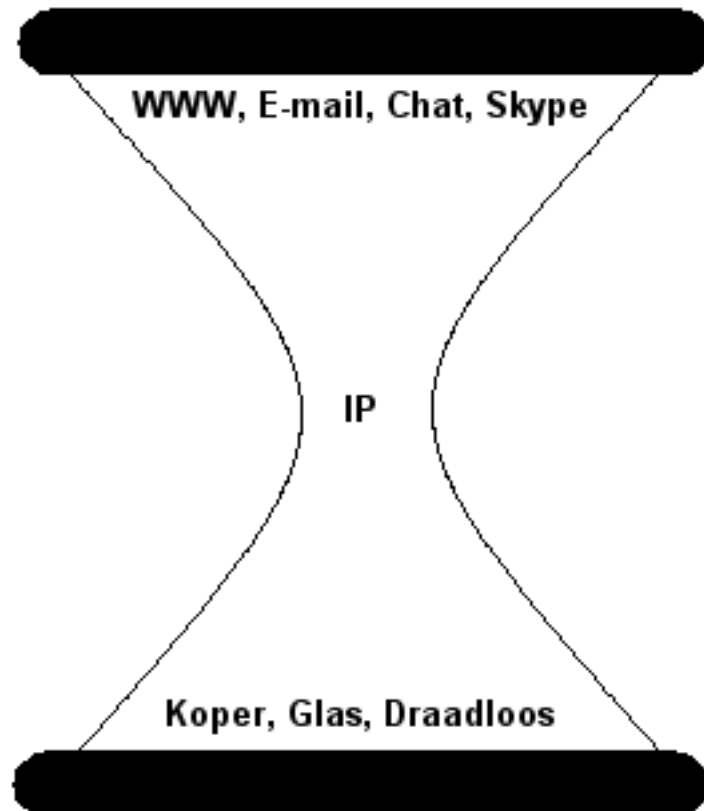


De noodzaak van IPv6

Erik Huizer
3-1-2008

Wat is het Internet Protocol?

Het Internet Protocol (IP) is 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, Skype, Youtube, Internet-shoppen etc. Anderzijds kan het Internet Protocol over allerlei infrastructuren worden gebruikt, zoals ADSL, Kabel-TV, glasvezel, mobiele telefoon, Wifi, etc. Het Internet Protocol is daarmee het kleinste gemene veelvoud in de wereld van de communicatieprotocollen (een gemeenschappelijke "taal" in een wereld van vele "talen"), waardoor communicatie met een willekeurige andere Internetgebruiker en met elke Internetsdienst mogelijk is. Zo ontstaat het in Internet-kringen gangbare zandloper model (National Research Council, 1994, blz. 53 [1]). 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.



Figuur 1: Vereenvoudigd zandlopermodel

Als een toepassing of dienst niet (langer) aanslaat dan kun je direct kiezen voor een alternatief.. De keuze in toepassingen en diensten is vrij en overdadig en wordt gestuurd door gemak, beschikbaarheid, toepasbaarheid en kosten. Dankzij IP zijn alle op Internet ontwikkelde diensten direct voor iedere gebruiker beschikbaar.

Wanneer een infrastructuur niet levert wat jij als gebruiker wilt (of te duur is). Dan neem je een andere. Kabel in plaats van ADSL (of vice versa) voor toegang thuis. Draadloos Internet 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.

Een consequentie van dit principe is dat elk op het Internet aangesloten systeem een uniek adres moet hebben. Zonder dat is het niet mogelijk dat iedereen met iedereen kan communiceren. Elke computer op het internet heeft zo'n IP-adres. Door deze IP-adressen weten computers elkaar te vinden en is er dus communicatie over het internet mogelijk. Om er voor te zorgen dat iedereen hiervoor dezelfde afspraken hanteert, is in de jaren 70 het Internet Protocol versie 4 (IPv4) ontwikkeld. Dit protocol biedt maximaal ruimte aan vier miljard adressen (door gebruik voor gereserveerde toepassingen is de werkelijke beschikbare adresruimte veel kleiner).

Wat is het probleem?

Vier miljard adressen was toentertijd ruim voldoende (de PC was toen nog niet eens uitgevonden!), maar met een toenemend aantal machines dat met het internet verbonden wordt - pc's, mobiele telefoons, Personal Digital Assistants (PDA's) en zelfs huishoudelijke apparatuur - neemt de behoefte aan IP-adressen toe. Daarbij komt de opkomst van internet in regio's als China, India en Afrika met hun miljarden inwoners. Door deze ontwikkelingen dreigt een tekort aan IP-adressen.

Internet-adressen dreigen dus schaars te worden. Nu worden ze volgens strikte regels uitgedeeld om te zorgen dat beschikbare adressen niet worden verkwist. Iedere organisatie, waar ook ter wereld, met een duidelijk omschreven behoefte kan vooralsnog zoveel IPv4-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 medio 2010. Daarna is de centraal beschikbare adresruimte op. Decentraal zijn er dan op diverse plekken in de wereld nog wel buffers met adressen, maar ook die zullen spoedig opraken. Op dat moment ontstaat schaarste en verwachten economen dat er een markt in werking gaat treden waarbij adresruimte economisch verhandeld zal gaan worden. Het effect van een dergelijke markt voor IP-adressen is lastig te voorspellen. Maar er zullen zeker niet meer adressen beschikbaar komen, die zijn er in IPv4 domweg niet. Meest waarschijnlijk is dat het verschil tussen rijke en armere gebieden zich zal gaan affekenen in de beschikbaarheid van Internet.

Op het moment dat de IPv4-adressen opraken, kunnen bestaande Internetgebruikers (vooral dus de westerse wereld) gewoon doorgaan met Internetten. Google en Youtube blijven bereikbaar en e-mail blijft werken. Maar men zal niet meer iedereen en elke dienst kunnen bereiken. Want elders in de wereld zullen nieuwe ondernemers en nieuwe gebruikers niet de beschikking hebben over IPv4-adressen. Langzaamaan zal het Internet zoals we dat nu kennen daarmee verdwijnen.

Nieuwe bedrijven met nieuwe toepassingen zullen niet meer zondermeer het netwerk op kunnen, maar zullen eerst adresruimte moeten financieren. Daarmee verschaalt één van de aantrekkelijke kanten van het Internet, namelijk dat ondernemers met een goed idee (waar dan ook ter wereld) dat zeer laagdrempelig op Internet kunnen uitvoeren. Daarnaast zal in die regio's waar de Internetgroei nog in de kinderschoenen staat (Afrika, China, India) deze groei afnemen door een gebrek aan (betaalbare) IPv4-adressen. Daarmee gaat een ander aspect van het Internet verloren, namelijk uniforme groei waarbij iedereen elke andere gebruiker kan bereiken, onafhankelijk van waar men zich bevindt. Kortom door het opraken van adressen dreigt het Internet zijn openheid, zijn rol als wereldwijd bindende factor en de rol van innovatiemotor te verliezen, ook voor mensen die nu al een IPv4-adres hebben.

Wat is de oplossing?

De internationale groep die het Internet Protocol ontwikkeld (IETF) voorzag het opraken van de IPv4-adressen al geruime tijd geleden. Vandaar dat er begin jaren 90 een nieuwe versie van het Internet Protocol werd ontwikkeld: IP versie 6. 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. Het resultaat is dat IPv6 erg veel lijkt op de huidige versie, IPv4, maar dan met meer adresruimte (2 tot de macht 128 adressen, hetgeen in praktijk nagenoeg oneindig veel adressen

zijn). 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.

Zo biedt IPv6 nieuwe mogelijkheden op het gebied van geïntegreerde autoconfiguraties voor plug-and-play mogelijkheden. Apparatuur die overweg kan met IPv6 zal in staat zijn om zichzelf te configureren, waardoor het gebruik van IP (door bijvoorbeeld je mobiele telefoon of je koelkast) eenvoudiger wordt. Verder biedt IPv6 nieuwe mogelijkheden op het gebied van beveiliging. Zo ondersteunt IPv6 standaard IPsec (Secure IP) dat het mogelijk maakt om data versleuteld te verzenden. Hierdoor wordt het zeer moeilijk gemaakt om zonder toestemming gevoelige data te onderscheppen en te bekijken, en neemt de betrouwbaarheid van Internet toe.

Ondersteuning voor IPv6 is inmiddels al geruime tijd beschikbaar in infrastructuurcomponenten (routers, switches, firewalls etc.) en software (Windows XP, Vista, Apple, Linux etc.). Eindgebruikers en dienstverleners (servers) hebben de mogelijkheid om gedurende een transitieperiode zowel IPv4 als IPv6 te ondersteunen (dual-stack). Daarmee is gegarandeerd dat zij iedereen op het Internet kunnen blijven bereiken.

Helaas blijft de operationele ondersteuning voor IPv6 sterk achter bij de implementatie in infrastructuur- en software. Weinig Internet Service Providers (ISP, zowel leveranciers van Internettoegang als backbone/transit providers) in de wereld ondersteunen al IPv6. Er is een gebrek aan duidelijke meerwaarde van IPv6 (zolang er nog IPv4-adressen zijn), om ISPs te bewegen IPv6 te implementeren. Een ISP moet investeren in IPv6 voor een meerwaarde die in de toekomst ligt (vergelijk het met investeren in een brandtrap). In een markt waar de marges afnemen en de concurrentie hoog is, is dat geen goede motivatie voor een implementatie hier en nu.

Door het gebrek aan operationele ondersteuning is er ook geen bekendheid bij eindgebruikers. Dat leidt er weer toe dat er geen vraag naar IPv6 komt vanuit eindgebruikers en zo is de cirkel rond. Gevolg is bijvoorbeeld dat thuisrouters (voor ADSL of Kabel) die verkocht worden nagenoeg geen van alle zijn voorbereid op IPv6.

IPv6 is de enige reële oplossing die de groei en het karakter van het Internet kan waarborgen. Maar met de implementatie van IPv6 als operationele dienst is het nog slecht gesteld.

Alternatieven?

Het meest gebruikte alternatief op het huidige Internet is Network Address Translation (NAT).

Bij gebruik van NAT krijgen computers op een lokaal deel van het netwerk allemaal niet-unieke IPv4-adressen (zogenoemde private adressen). Indien een systeem op het lokale netwerk een verbinding wil opzetten met de rest van het Internet, gaat die verbinding door een NAT-Box. De NAT-box vervangt voor de verbinding tijdelijk het niet-unieke private IP-adres door een publiek IP-adres, 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 [2]). Een aantal toepassingen werkt niet via een NAT. Als de IPv4-adressen opraken is het mogelijk dat service providers NAT gaan toepassen op meer plaatsen in hun netwerken dan alleen in lokale delen. Daarmee worden inderdaad IPv4-adressen uitgespaard en dus het opraken van de adressen uitgesteld. De toename van de complexiteit van Internet-verbindingen is echter significant en de operationele gevolgen (denk alleen al aan de belasting van de helpdesk) zijn niet te overzien. Het ligt voor de hand dat de daarmee gepaard gaande kosten die van een IPv6-implementatie veruit zullen overstijgen. Daarnaast zullen diverse toepassingen simpelweg niet meer werken als de Internet-verbinding door een serie van NAT-boxen heenloopt.

Last but not least blijven er bij gebruik van NAT IPv4-adressen noodzakelijk. NAT wordt al ruimschoots toegepast en heeft de groei van het adresgebruik nauwelijks doen minderen. Uiteindelijk is NAT dus geen oplossing.

Hoe nu verder?

Het enige redelijke alternatief met kans op succes lijkt dus ondersteuning van IPv6. ISPs, leveranciers van apparatuur en diensten dienen zo snel mogelijk IPv6 ondersteuning te implementeren. Maar ook het bedrijfsleven, de overheid en eindgebruikers moeten IPv6 gaan gebruiken. Alleen op die manier kunnen de voordelen van het huidige Internet worden gehandhaafd.

De EU heeft al jaren geleden het belang van een goede transitie naar IPv6 ingezien. Het heeft er voor gezorgd dat in alle lidstaten een IPv6 Task Force is opgezet om de implementatie van IPv6 dienstverlening te bevorderen. Tot nu toe hebben deze Task Forces geprobeerd om ISPs en bedrijven ervan te overtuigen IPv6 te implementeren, zonder daarbij paniek te zaaien. Dit heeft helaas tot bijster weinig resultaat geleid. De tijd begint te dringen en de enige weg voorwaarts is om zo snel mogelijk IPv6 te ondersteunen. Essentieel daarbij zijn de ISPs die de schakel vormen tussen alle gebruikers (organisaties, bedrijven en eindgebruikers).

De Task Force IPv6 doet een zeer dringend beroep op alle Nederlandse ISPs om zo snel mogelijk IPv6 ondersteuning te bieden, op minimaal hetzelfde niveau als de IPv4 ondersteuning. Schaf geen apparatuur of diensten meer aan zonder IPv6 ondersteuning, neem geen personeel meer aan zonder kennis van IPv6 en stuur het huidige personeel naar IPv6 trainingen. Maak een plan voor de vervanging van alle in omloop zijnde ADSL/kabelrouters die geen IPv6-ondersteuning hebben. Een IPv6-keurmerk voor thuisrouters zou helpen bij de bewustwording van consumenten en zou de fabrikanten van dergelijke apparatuur stimuleren om aandacht te besteden aan IPv6 ondersteuning.

Voor bedrijven en organisaties met (grote) netwerken geldt dezelfde oproep. Schaf geen apparatuur of diensten aan zonder IPv6-ondersteuning. Maak een IPv6-implementatieplan. Het boek "Running IPv6" [3] kan daarbij behulpzaam zijn.

De overheid moet op meerdere manieren helpen om de implementatie van IPv6 te bevorderen:

- Als klant. De overheid is zelf een grote klant en moet in alle relevante offerte-aanvragen IPv6 opnemen als een verplichting.
- Als netwerkbeheerder. De overheid heeft zelf diverse met het Internet gekoppelde netwerken. Deze netwerken dienen z.s.m. gereed te worden gemaakt voor IPv6.
- Als informatieaanbieder. De overheid dient alle informatiediensten (webservices) die zij heeft ook beschikbaar te maken over IPv6.
- Als regelgever. De overheid moet overwegen om een deadline te stellen waarop ISPs IPv6 moeten ondersteunen. Daarmee wordt voor ISPs een 'level playing field' geschapen.

[1] Computer Science and Telecommunications Board, National Research Council, "Realizing the Information Future: The Internet and Beyond", National Academy Press, Washington, D.C. 1994

[2] T. Hain, Architectural implications of NAT, 2000, RFC 2993
(<ftp://ftp.rfc-editor.org/in-notes/rfc2993.txt>)

[3] I. van Beijnum, Running IPv6, APress, 2006, ISBN: 1-59059-527-0