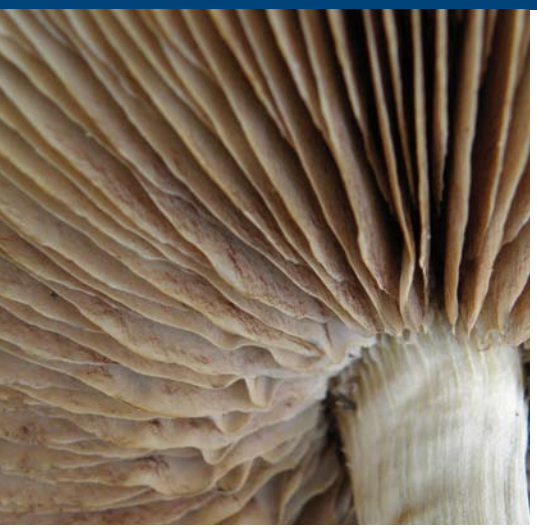


Internet groeit uit zijn jasje

Dr. ing. S. Klous
heeft meer dan tien jaar ervaring in grootschalige dataverwerking en is lid van de IPv6 Task Force. Hij is bij KPMG Advisory Senior Manager bij CT Informatie Technologie, waar hij de service line Gedistribueerde systemen onder zijn hoede heeft met onder andere dienstverlening op het gebied van cloud computing.

klous.sander@kpmg.nl

Drs. T. Balint
is expert op het gebied van IT-infrastructuur en cloud computing. Zij heeft diverse complexe migraties succesvol begeleid en afgerond, en is onder andere betrokken bij de ontwikkeling van de KPMG Cloud Performance monitor.

balint.tunde@kpmg.nl

Drs. J.M.A. Koedijk CISA CISM
is al jaren actief op het gebied van software engineering (winnaar NK ICT-architectuur 2006) en internetstandaarden. Hij is verantwoordelijk voor opdrachten op het gebied van softwarekwaliteit en heeft een fors aantal ICT-systemen beoordeeld op vele aspecten in de application lifecycle.

koedijk.joost@kpmg.nl

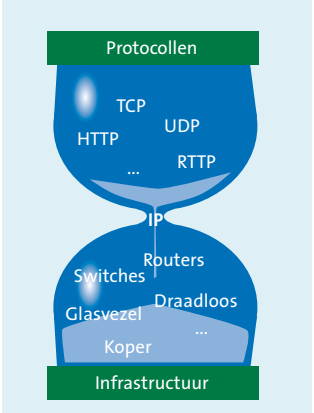
Dr. ing. Sander Klous, drs. Tünde Balint en drs. Joost M.A. Koedijk CISA CISM

Versie 4 van het Internet Protocol (IP)-adres is door de jaren heen vrijwel de enige constante factor gebleken in internetcommunicatie. Toch is het moment inmiddels gekomen dat internet met deze versie niet nog meer gebruikers kan ondersteunen. Nieuwe gebruikers zullen daarom alleen versie 6 van het adres ontvangen (IPv6). In dit artikel leggen we uit waarom deze transitie als een sluipmoordenaar op de loer ligt en de concurrentiepositie van uw organisatie bedreigt. U zal uw IT-landschap nu geschikt moeten maken voor de komst van IPv6. Alleen op die manier kunt u zich ervan verzekeren dat uw organisatie op tijd klaar is voor de ontwikkelingen in de komende jaren.

Inleiding

Op het internet zien we een wildgroei van allerlei communicatieprotocollen (TCP, UDP, HTTP, FTP, SMTP, etc.) en infrastructuurcomponenten (switches, routers, glasvezel, koper, draadloos, etc.). Over de jaren heen is de diversiteit steeds verder toegenomen, tot een niveau waarbij er voor een buitenstaander geen touw meer aan vast te knopen is. Er is echter één constante factor in deze enorme vergaarbak en dat is het Internet Protocol (IP)-adres.

Het IP-adres ([DARP81]) is een unieke code om een apparaat (pc, server, televisie, koelkast, etc.) op het internet aan te sluiten, vergelijkbaar met de unieke combinatie postcode/huisnummer die TNT Post nodig heeft om een pakketje af te kunnen leveren op de juiste locatie. Figuur 1 bevat een grafische weergave van de bovenstaande situatie in het zogenaamde zandlopermodel ([CSTB94]). De centrale rol die IP speelt in internetcommunicatie is daarin duidelijk zichtbaar.



Figuur 1. **Het zandlopermodel voor internetcommunicatie.**

Ondanks dat het IP-adres (versie 4 om precies te zijn, IPv4) door de jaren heen vrijwel de enige constante factor is gebleken in internetcommunicatie, weten we al sinds eind jaren tachtig dat de 32 bits die binnen IPv4 voor het adres beschikbaar zijn (en resulteren in ruim 4

miljard adressen), onvoldoende zijn om in de groeiende behoefte aan adresruimte te voorzien. Als reactie op deze constatering heeft de Internet Engineering Task Force (IETF) in de jaren negentig een nieuwe 128 bits-versie van het IP-protocol ontwikkeld, IPv6 ([NWG98]).

In de afgelopen tien jaar zijn er verschillende voorspellingen gedaan over de exacte datum waarop de adressen echt op zouden zijn, maar op 3 februari 2011 was het dan eindelijk zover: het internet kan met IPv4 niet nog meer gebruikers bedienen ([NITF11]).

Probleemstelling

Nu de IPv4-adressen op zijn, rijst de vraag hoe ernstig deze situatie is. Om een inschatting te maken van de consequenties, zullen we eerst beschrijven wat de mogelijkheden zijn voor verdere ontwikkeling van het internet. Daarna gaan we verder in op de barrières in deze ontwikkeling en de impact op uw bedrijfsvoering. Als laatste trekken we de conclusies over een mogelijke aanpak en keuzen die u de komende jaren zal moeten maken aangaande uw IT-landschap, gerelateerd aan de overgang naar de nieuwe versie van het internetprotocol.

Verdere ontwikkeling van het internet

Zelfs nu de Internet Assigned Numbers Authority (IANA) niet meer beschikt over IPv4-adressen heeft dat nog geen directe consequenties voor IP-adresaanvragen van eindgebruikers en van Internet Service Providers (ISP's). De Regional Internet Registries (RIR's) hebben nog een voorraad waarmee bijvoorbeeld het Europese Coördinatie Centrum (Reseaux IP Européens – RIPE) tot ongeveer het midden van 2011 toekan ([Hust11]). Daarnaast is er nog een aantal vrijwel ongebruikte 'legacy blocks': grote blokken met IP-adressen, die in het verleden direct aan organisaties zijn toegewezen. Als deze blokken worden herverdeeld, zal het iets langer duren voordat de eindgebruikers in Europa geen IPv4-adressen meer kunnen aanvragen ([Vego08]).

Als ultieme noodmaatregel voor het oprekken van de IPv4-beschikbaarheid is er nog de mogelijkheid om binnen uw organisatie de infrastructuur te optimaliseren. Door middel van Network Address Translation (NAT) kan ervoor worden gekozen om grote delen van uw netwerk niet (direct) toegankelijk te maken vanaf het internet ([NWG01]). U wijst dan adressen toe die alleen van binnen uw organisatie te bereiken zijn en legt dus minder beslag op publieke IP-adressen. De systemen kunnen overigens zelf wel van toegang tot het internet worden voorzien, ze zijn alleen niet (direct) benaderbaar vanaf het internet.

Overgang naar IPv6

Alle eerdergenoemde maatregelen zijn eindig. Voor verdere ontwikkeling is een overgang naar de nieuwe versie van het internetprotocol noodzakelijk. Het laatste blok met ongeveer 17 miljoen IPv4-adressen dat RIPE beschikbaar heeft, wordt dan ook gebruikt om de overgang naar de nieuwe versie van het internetprotocol (IPv6) te faciliteren. In de andere regio's van de wereld zijn vergelijkbare afspraken gemaakt. In de praktijk zal dat betekenen dat deze IP-adressen niet beschikbaar zijn voor eindgebruikers en ISP's, maar zullen worden verdeeld volgens speciale richtlijnen ([Smit10]).

Nu bijna alle adressen oude stijl zijn vergeven, rest geen andere mogelijkheid meer dan het maken van de overstap naar IPv6. Daarbij moeten we ons realiseren dat de nieuwe versie niet in staat is te communiceren met de oude versie en omgekeerd: IPv4 en IPv6 zijn twee volledig gescheiden parallelle netwerken ([DARP81], [NWG98]).

IPv6 bevat een aantal interessante verbeteringen ten opzichte van IPv4 met betrekking tot veiligheid en schaalbaarheid ([NWG98]). Zo is standaardondersteuning voor dataencryptie (met IPsec) ingebouwd en kunnen IPv6-systemen zichzelf door communicatie met hun omgeving (via ICMPv6) automatisch op de juiste manier configureren op het netwerk (stateless address autoconfiguration). Verder is routering geoptimaliseerd, zodat relatief nieuwe concepten als multicast (het sturen van informatie naar meerdere ontvangende systemen) sterk worden vereenvoudigd.

De oplossing voor een vloeiende overgang van IPv4 naar IPv6 ligt in de zogenaamde dual-stack protocolimplementatie ([NWG05]). Met andere woorden, internetinfrastructuurcomponenten moeten beide protocolversies (gaan) ondersteunen. Moderne dual-stack implementaties bieden de mogelijkheid om applicaties te ontwikkelen die gebruikmaken van zogenaamde hybride poorten, zodat deze direct geschikt zijn voor beide protocollen. Niet alle systemen bieden echter deze mogelijkheid. Op bijvoorbeeld Windows XP en Server 2003 moeten expliciet twee gescheiden poorten worden geopend voor dual-stack ondersteuning ([Micr]), wat leidt tot extra ontwikkelinspanningen.

Om het belang van de overstap naar IPv6 te benadrukken is, in opdracht van het ministerie van Economische Zaken, de Nederlandse IPv6 Task Force opgericht. Het doel van de Nederlandse IPv6 Task Force is om bewustwording te creëren betreffende het nut en vooral de noodzaak van IPv6, kennis uit te wisselen over de toepassing van IPv6 en afstemming te bereiken met betrekking tot de invoering van IPv6. Deze Task Force is ondergebracht bij het ECP-EPN-platform voor de informatiesamenleving.

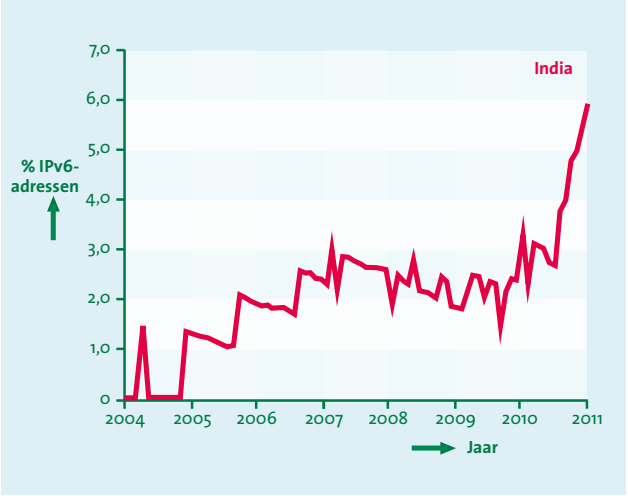
Impactanalyse

Als de dual-stack oplossing zo voor de hand ligt, waarom zijn we dan nog niet overgestapt? Wachten tot het laatste IPv4-adres is vergeven, is toch niet nodig! Er zijn twee facetten die daar een belangrijke rol in spelen.

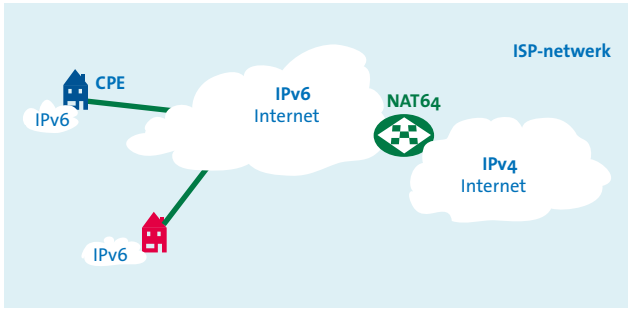
- Een verandering naar een standaard die niet compatibel is met zijn voorganger is altijd een ingewikkelde klus. Zeker als de standaard een fundamenteel en wijdverspreid onderdeel is van de bestaande goed werkende infrastructuur. Vergelijk het maar met een beslissing om met zijn allen links op de weg te gaan rijden in plaats van rechts. Daar moet echt heel wat voor gebeuren.
- Er is heel lang geworsteld met het kip-ei-probleem. Iedereen had de beschikking over IPv4, dus er was (nog) geen noodzaak om te investeren in het aanbieden van diensten via IPv6. Aan de andere kant, als alle diensten worden aangeboden over IPv4, waarom zouden eindgebruikers dan investeren in IPv6?

Het kip-ei-probleem is door de uitputting van de IPv4-adrespool inmiddels doorbroken. Met name in Azië gaan de ontwikkelingen snel en worden op dit moment op grote schaal IPv6-infrastructuren uitgerold (zie bijvoorbeeld figuur 2). Daarmee ontstaat de situatie dat binnenkort (grote) delen van het internet alleen nog via IPv6 beschikbaar zijn. Dat is een belangrijke stimulans voor aanbieders van internetdiensten (en in mindere mate ook voor eindgebruikers) om op dual-stack over te schakelen. De internetreuzen zoals Google en Facebook hebben al IPv6-varianten van hun portals, bijvoorbeeld op http://ipv6.google.com.

Op infrastructuurgebied zijn we er in Europa nog lang niet (zie ook http://v6asns.ripe.net/v/6). Hoewel een aantal ISP's al pro-



Figuur 2. **Trendbreuk in India, explosieve toename van IPv6-adressen sinds eind 2010.**



Figuur 3. **Segmentering van het internet in gebieden met IPv4 en IPv6.**

actief bezig is met de ondersteuning van IPv6, zijn grote delen van het internet nog niet ontsloten. Probeer thuis of op het werk maar eens of de Google of Facebook IPv6-portal toegankelijk is, grote kans dat u eindigt met een 'Network Error'.

Om de ontsluiting van IPv6 te bespoedigen is er een aantal technieken beschikbaar. Bij zogenaamde IPv6-over-IPv4-tunnels worden IPv6-pakketjes verpakt in IPv4-pakketjes ([NWG05]). Op die manier kunnen twee afzonderlijke IPv6-delen van het internet elkaar bereiken door een IPv4-gebied heen. Er zijn diverse automatische tunneltechnieken in gebruik (bijvoorbeeld Teredo) om de bereikbaarheid van IPv6-sites te vergroten ([NWG10]).

Een andere belangrijke techniek voor het faciliteren van de overgang naar IPv6 is een variant op de al eerder genoemde Network Address Translation (NAT). Figuur 3 toont een schematische weergave van een IPv6- en een IPv4-gedeelte van het internet. Via een speciaal daarvoor ingerichte server (in dit geval gebruikmakend van NAT64) kan aan de eindgebruikers op het IPv6-netwerk toegang worden verschaft tot het IPv4-netwerk (maar niet andersom!) door de IPv4-adressen te vertalen in IPv6-adressen ([BWG10]). Deze technieken worden nu al toegepast in de wereld van de mobiele communicatie. Zie bijvoorbeeld de public beta-tests door T-Mobile op http://groups.google.com/group/tmoipv6beta.

Opvallend aan eerdergenoemde oplossingen voor de transitie van IPv4 naar IPv6 is dat er voldoende mogelijkheden zijn om vanaf systemen met alleen het nieuwe protocol toegang te verkrijgen tot delen van het internet met alleen het oude protocol. Andersom zijn de mogelijkheden echter zeer beperkt. Eindgebruikers met alleen de beschikking over een IPv4-adres zijn niet in staat om gebruik te maken van nieuwe IPv6 only-diensten. Voor die groep zijn er twee oplossingen. Zelf overschakelen op dual-stack, waarbij aan de ISP duidelijk moet worden gemaakt dat deze ondersteuning noodzakelijk is, of aandringen op dual-stack bij de leverancier van de dienst. De eerste oplossing zal daarbij in toenemende mate haalbaar zijn omdat dit voor ISP's een concurrerende factor wordt. De tweede oplossing daaren-

tegen wordt met het beperkte aantal beschikbare IPv4-adressen steeds onwaarschijnlijker.

Conclusie

Organisaties en eindgebruikers zullen in toenemende mate worden geconfronteerd met de schaarste aan IPv4-adressen. Hoewel er door verschillende belanghebbenden proactief wordt gewerkt aan de uitrol van IPv6 (zie bijvoorbeeld [SURF11]), is er nog een lange weg te gaan.

IPv6 ligt als een sluipmoordenaar op de loer en bedreigt de concurrentiepositie van uw organisatie. De ontwikkeling voltrekt zich op dit moment nog grotendeels buiten uw gezichtsveld. Immers, het IPv4-netwerk blijft gewoon functioneren en IPv6 only-delen van het internet ontstaan vooral in gebieden waar relatief weinig contact mee is, zoals Azië. Zolang er in Europa nog internetadressen te verkrijgen zijn, lijkt er geen directe noodzaak voor een dual-stack implementatie.

Het probleem ontstaat als Europa dan ook eindelijk overgaat op IPv6. Plotseling krijgt u de massale concurrentie te verwerken van bedrijven die al geruime tijd in die markt actief waren op tot dan toe onbereikbare delen van het internet. Met recht wordt u op dat moment geconfronteerd met een remmende voorsprong van formaat. Naarmate de IPv6 only-gebieden van het internet groter worden, wordt het voor uw organisatie steeds belangrijker om dual-stack te ondersteunen.

De belangrijkste conclusie is om proactief om te gaan met de komst van IPv6. Bij iedere verandering in uw IT-landschap moet u zich afvragen of er de mogelijkheid is voor dual-stack ondersteuning. Dit geldt niet alleen op netwerkbeheergebied, maar ook bij de vervanging van applicaties of het afsluiten van nieuwe contracten met ISP's of andere IT-partners, zoals bijvoorbeeld cloud-serviceproviders. Alleen op die manier kunt u zich ervan verzekeren dat uw organisatie op tijd klaar is voor de ongekende mogelijkheden van IPv6.

IPv6-beveiliging

De introductie van IPv6 roept vragen op over de beveiligingsaspecten die bij implementatie een rol spelen. Doordat tijdens de ontwikkeling van IPv6 goed is nagedacht over beveiliging is IPv6 intrinsiek veiliger is dan IPv4. Deze ontwikkeling vond echter al weer vijftien geleden plaats, waardoor de standaard nog kwetsbaar kan zijn voor recentere aanvalstechnieken. Met name tijdens de transitieperiode van IPv4 naar IPv6 zal goed moeten worden nagedacht over de beveiligingsimplicaties.
Op lange termijn wordt vooral verbetering verwacht op het gebied van beveiliging door de toename in adresruimte, waardoor poortscanning (een techniek die nu vaak door kwaadwillenden wordt gebruikt om potentiële kwetsbaarheden van een systeem bloot te leggen) een lastige opgave wordt ([Sotio6]). Verder kan IPsec door de standaardondersteuning in IPv6 verder worden uitgerold en helpen de neighbour discovery en automatische adresconfiguratietechnieken in ICMPv6 tot verdere verbeteringen op het gebied van beveiliging ([Sotio6]).
Het belangrijkste aandachtspunt voor uw veiligheidsbeleid op korte termijn is het gebrek aan kennis over IPv6 in de meeste organisaties. Als gevolg daarvan kunnen tijdens de transitie lekken ontstaan in het IT-landschap die er nu nog niet zijn ([IPTF]). Zo maken veel organisaties op dit moment gebruik van Network Adress Translation (NAT, zie tekst), waardoor interne servers niet bereikbaar zijn vanaf het internet. Bij introductie van IPv6 krijgen deze servers waarschijnlijk publieke adressen. Om ook in de nieuwe situatie toegang vanaf het publieke internet te blokkeren moet de configuratie van de firewall worden aangepast. In het algemeen is aandacht vereist om ervoor te zorgen dat in het veiligheidsbeleid eisen voor IPv6 en IPv4 gelijk worden getrokken en gehouden.
Een ander belangrijk aspect is het gebrek aan volwassenheid in de IPv6-software stack. Deze stack zal waarschijnlijk nog een flink aantal kwetsbaarheden bevatten die naar boven komen als in de komende jaren het gebruik toeneemt ([IPTF]). De situatie is vergelijkbaar met de introductie van virtualisatie een aantal jaren geleden. Ook virtualisatie biedt een aantal nieuwe mogelijkheden op het gebied van beveiliging en de software stack voor ondersteuning van virtualisatie was (en is) eveneens nog volop in ontwikkeling. Het is dus van belang om het verandermanagementproces in uw organisatie goed op orde te hebben, zodat uw systeem altijd kan worden voorzien van de laatste beveiligingsupdates.
Ook wijzen we graag op de specifieke beveiligingsproblemen die optreden in een hybride landschap met IPv4 en IPv6. In die hybride omgeving zullen componenten worden opgenomen voor vertaling tussen IPv4- en IPv6-delen van het internet en voor het tunnelen van IPv6-verkeer door IPv4-delen van het internet, zoals beschreven in de tekst. Met de inzet van die componenten en de manier waarop ze worden gebruikt moet zeer zorgvuldig worden omgesprongen omdat ze uw IT-landschap kunnen blootstellen aan risico's die bij afzonderlijk gebruik van IPv4 of IPv6 niet aan de orde zijn ([IPTF]). Kwaadaardige IPv6-pakketjes kunnen bijvoorbeeld via een IPv4-tunnel door een firewall worden geloodst.
Overbodig te stellen dat alle netwerkcomponenten onder een gedegen configuratie- en changemanagementregime moeten staan om ongewenste effecten van wijzigingen door instabiele IPv6-stacks tegen te gaan. Door uw IT-landschap op tijd geschikt te maken voor IPv6 door middel van een dual-stack implementatie (zie tekst) kunt u in ieder geval een deel van bovengenoemde problemen voorkomen.

Literatuur

[BWG10] Behave Working Group, *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 servers (Draft)*. s.l. : Internet Engineering Task Force (IETF), 2010.

[CSTB94] Computer Science and Telecommunications Board, *Realizing the Information Future: The Internet and Beyond*. Washington D.C.: National Academy Press, 1994.

[DARP81] DARPA, *Internet Protocol Specification (RFC 791)*. s.l. : Internet Engineering Task Force (IETF), 1981.

[Hust11] Geoff Huston, IPv4 Address Report. *Potaroo*. [Online] February 03, 2011. http://www.potaroo.net/tools/ipv4/index.html.

[IPTF] IPv6 Task Force, *Technical and Economic Assessment of Internet Protocol, Version 6 (IPv6)*. s.l. : U.S. Department of Commerce, National Telecommunication and Information Administration (NTIA).

[Micr] Microsoft, Dual-Stack Sockets. *Microsoft Developers Network*. [Online] http://msdn.microsoft.com/en-us/library/bb513665(v=VS.85).aspx.

[NITF11] Nederlandse IPv6 Task Force, Press Release. *IPv6 Task Force*. [Online] February 03, 2011. http://www.ipv6-taskforce.nl/.

[NWG98] Network Working Group, *Internet Protocol, Version 6 (IPv6) Specification (RFC 2460)*. s.l. : Internet Engineering Task Force (IETF), 1998.

[NWG01] Network Working Group, *Traditional IP Network Address Translator (RFC 3022)*. s.l. : Internet Engineering Task Force (IETF), 2001.

[NWG05] Network Working Group, *Basic Transition Mechanisms for IPv6 Hosts and Routers (RFC 4213)*. s.l. : Internet Engineering Task Force (IETF), 2005.

[NWG10] Network Working Group, *Teredo: Tunneling IPv6 over UDP through Network Address Translations (RFC 4380)*. s.l. : Internet Engineering Task Force (IETF), 2006, updated 2010.

[Smit10] Philip Smith en Alain Bidron, *Allocations from the last /8*. s.l. : RIPE, 2010.02.

[Soti06] Samuel Sotillo, *IPv6 Security Issues*. s.l. : East Carolina University, 2006.

[SURF11] SURFnet, *IPv6-nummerplan opstellen*. s.l. : SURFnet, 2011.

[Vego08] Leo Vegoda, *Recovering IPv4 Address Space*. s.l. : Internet Corporation for Assigned Names and Numbers (ICANN), 2008.