Datum
21 september 2010

notitie

Verzamelde reacties publieke consultatie IPv6

Lijnparaaf	Medeparaaf	Afschrift aan

De staatssecretaris van Economische Zaken heeft op maandag 17 september 2007 het actieplan open standaarden en open source software aan de Tweede Kamer gestuurd. Het doel van het actieplan is om de informatievoorziening toegankelijker te maken, onafhankelijkheid van ICT leveranciers te creëren en de weg vrij te maken voor innovatie.

Een onderdeel van het actieplan is het opstellen van een lijst met standaarden, die vallen onder het principe "pas toe of leg uit" (comply-or-explain). Het College Standaardisatie spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard. De expertbeoordeling van IPv6 plaatsgevonden tijdens een bijeenkomst op donderdag 22 juli 2010. Conform procedure is het expertadvies vijf weken publiek geconsulteerd. Dit document bevat alle ontvangen reacties op de consultatieronde van IPv6.

In dit document vindt u achtereenvolgens de reacties van:

- Belastingdienst
- e-Overheid voor Burgers
- Gemeente Enschede
- InformatieDesk standaarden Water
- Infinity Networks B.V.
- Inspectie Verkeer en Waterstaat
- InterNLnet
- Kwaliteitsinsituut Nederlandse Gemeenten
- Ministerie van BZK
- Ministerie van Financiën
- Ministerie van Justitie
- Ministerie van LNV
- Ministerie van OCW
- Ministerie van VWS
- NoiV
- Sander Steffann (Vice-voorzitter RIPE Address Policy Working Group)
- WH.v.Goeverden (Ministerie van Defensie)

Reactie Belastingdienst

Datum
21 september 2010

Van: Berlo, GJA (Ger) van (IVB/DH)

Ger van Berlo
Directoraat-generaal Belastingdienst
Afdeling IV-Beleid

Reactie op het expertadvies IPv6.

Vraag 2: aanvullend
IPv6 moet toegepast worden
- voor de onderlinge communicatie tussen eindsystemen *en/of eindgebruikers* van overheids(diensten) onderling, waarbij communicatie over organisatiegrenzen heen plaatsvindt

Vraag 8: opmerking
Bij het uitrollen van IPv6 kunnen plannen gevolgd worden om de netwerkinfrastructuur op natuurlijke (LifeCycle) vervangingsmomenten gefaseerd gereed te maken voor IPv6. Over de tijd heen wordt dan een IPv6 enabled netwerk verkregen zonder merkbare meerkosten.

Vraag 11: opmerking
De vraag verwijst naar 5.3. Deze is niet aanwezig in het expertadvies.

Vraag 12: geen commentaar.

De overige vragen kunnen bevestigend worden beantwoord. We zijn het daarover dus eens met het expertadvies.

Reactie e-Overheid voor Burgers

Datum
21 september 2010

Van: Hans Overbeek

Hoi Bart,

De expertadviezen hebben wij van e-Overheid voor Burgers bestudeerd. Wij zien geen aanleiding om daarop te reageren.

groet,
Hans

Reactie Gemeente Enschede

Datum
21 september 2010

Aan: Bart Knubben
Van: Hans Koenders

Ik heb eerder de vraag uitgezet bij het IMG 100.000+ overleg, bij de VNG en de het Overleg Open Gemeenten (waaraan ook BZK en NOiV deelnemen) en intern in de gemeente Enschede.
In z'n algemeenheid stel ik vast dat de materie niet erg "leeft". Het beeld dat ik aantref is dat óf betrokkenen in de gemeenten toch wel heel erg leken zijn, óf zij de open standaard logisch vinden.

In het Overleg Open Gemeenten is gesproken over de voorgenomen open standaarden. Ik ervaar daar vertrouwen in de adviezen van de experts. Die zijn óók in deze drie gevallen heel goed leesbaar en plausibel. Een korte rondvraag bij deskundigen bij mij in de buurt leert me dat IPv6 volstrekt logisch is en dat SHA-2 inderdaad risico's vermindert.
Het advies omtrent PKI-Overheid getuigt ervan dat de experts zich goed bewust zijn van de grenzen van de open standaarden. Voor mij is PKI zó standaard dat ik me niet meer realiseer dat het een andere typologie van standaard is.

Mijn toets in mijn -natuurlijk beperkte- omgeving leert, dat ik Marcel Meijs, als lid van het College van Standaardisatie graag meegeef in te stemmen met de adviezen.

Met vriendelijke groet
Hans Koenders

IDsW
InformatieDesk standaarden Water

Postbus 17
8200 AA, Lelystad

Forum Standaardisatie
Postbus 84011
2508 AA Den Haag

Onze referentie:	Uw referentie: Consultatie IPv6; PKI; SHA-2	Datum: 13-09-2010

L.S.,

In reactie op de openbare consultatie aangaande:
A: IPv6
B: PKI Overheid
C: SHA-2
het volgende:

Ad a: IPv6

Wij vinden het advies voor IPv6 tweeslachtig, enerzijds wordt voorgesteld deze standaard op de 'pas toe of leg uit' lijst op te nemen, anderzijds is de verwachting dat niemand op korte termijn over zal gaan.

Met name omdat IPv4 momenteel de de-facto standaard is kan niet van 'pas toe of leg uit' worden gesproken zonder substantiële investeringen. Het lijkt daarmee dan ook alleen mogelijk om IPv6 op korte termijn toe te passen door het maken van grote investeringen. Ook binnen de waterwereld zien we deze ontwikkeling en wordt voorzien dat de ontwikkeling in lopende ontwikkelingen wordt meegenomen.

Vanuit dit oogpunt zien we het gebruik van IPv6 als sterke aanbeveling voor toekomstige ontwikkelingen maar zien we ook dat de standaard niet als zodanig op de 'pas toe of leg uit' lijst thuis hoort aangezien dit onvermijdelijk zal leiden tot veel uitleg en geen significant grotere toepassing. Een mogelijk alternatief is opname van zowel IPv4 als IPv6 tot het moment dat voldoende organisaties IPv6 hebben geïmplementeerd.

Ad b: PKI Overheid
Rondom PKI Overheid hebben we een tweeslachtige reactie. Enerzijds juichen wij het vaststellen van standaard methoden voor een betrouwbare communicatie toe. Het voordeel hiervan voor de afnemer is groot doordat deze nog slechts me één methode wordt geconfronteerd.

Anderzijds zien we hiermee ook een keuze die potentieel marktverstorend kan werken doordat het leveranciers niet meer is toegestaan om eigen certificaten etc toe te passen (gedwongen winkelnering). Een nadere definitie van het werkingsgebied (bv basisregistraties) kan hier veel onduidelijkheid wegnemen.

Vanuit deze optiek onderschrijven wij de conclusie van de expertgroep (niet opnemen) maar zien we graag stimuleringsmaatregelen voor de toepassing van PKI Overheid.

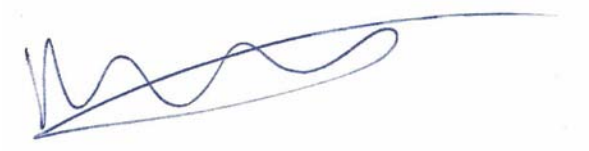
Ad c: SHA-2

De keuze voor SHA-2 tav de huidige standaarden wordt door ons onderschreven.

Met vriendelijke groet,

Myriam de Jong,
Programma manager IDsW

Namens deze,



Huibert-Jan Lekkerkerk
Sr. Projectleider standaarden IDsW

Reactie consultatieprocedure Expertadvies IPv6

Teco Boot
Infinity Networks B.V.
15 september 2010

Vraag: 1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig, bezien vanuit het doel van het document (het Forum en College Standaardisatie voorzien van een inhoudelijk relevante toelichting op IPv6). [paragraaf 1.1 t/m 1.7 van het expertadvies].

Antwoord: Ja.

Pagina 9 onderaan:
voorziet daarbij o.a. in oplossingen voor de structuur en opbouw van de data
Dit is feitelijk onjuist. IPv6 is uitsluitend een protocol voor de OSI layer 3 Networking Layer. IPv6 zegt niets over de opbouw van de data.

Pagina 10:
dat interoperabiliteit tussen systemen op relatief korte termijn (+/- 2 jaar) in grote delen van de wereld niet meer gegarandeerd kan worden
Alleen IPv6 zorgt juist voor een hoge mate van incompatibiliteit met de rest van het Internet. Voor de komende periode (+/- 10 jaar) zullen grote delen van het Internet IPv4-only zijn. Ondersteuning van IPv4 heeft voor de nabije toekomst een veer groter belang dan IPv4.

Pagina 10:
is parallel ook gewerkt aan eenvoudiger beheer, en betere ondersteuning van beveiliging
Dit kan gerekend worden onder de noemer eeuwige beloftes. Voorlopig is IPv6 een extra protocol, hetgeen extra aandacht vereist. Voor eindgebruikers is het omgaan met IPv6 adressen zo goed als ondoenlijk. Voor beheerders is het een stap achteruit, het mondeling overnemen van IPv6 adressen is zeer foutgevoelig.
Er zijn redenen terughoudend te zijn met invoering van IPv6, juist omdat de beveiliging hiervan tekort schiet. Een aantal beveiligingsproducten welke momenteel verkrijgbaar zijn werken niet, of niet goed met IPv6.

Pagina 11:
Beide standaarden kunnen, zullen en moeten naar de mening van de expertgroep naast elkaar binnen hetzelfde netwerk gebruikt worden
Dit is een andere formulering dan wat onder de term ***IPv6*** wordt verstaan. De juiste aanduiding zou zijn: ***IP Dual Stack***.
Voor Internet Service Providers is het zaak zowel IPv4 als ook IPv6 connectiviteit als dienst te leveren. Dit geldt ook voor netwerkdiensten binnen de overheid. Maar wat kan de reden zijn voor een complexe Dual Stack

binnen hetzelfde netwerk? Voor interoperabiliteit is het zaak op het koppelvlak de Dual Stack mogelijkheid aan te bieden. Dit zou bv. geïmplementeerd kunnen worden op gateway systemen, front-end web servers en / of firewalls. End-to-end IP connectiviteit is vanwege beveiliging veelal ongewenst.

Pagina 10:
10 Door de protocol beveiliging, vastgelegd door IPSEC, als integraal onderdeel mee te nemen in het ontwerp
Deze IPv6 requirement is ooit opgenomen als wishfull thinking. Momenteel is er geen reden aan te nemen dat een IPv6 systeem ook daadwerkelijk IPsec ondersteunt. Dit geldt ook voor IPv4, er is geen reden voor een aanname dat een IPv4 systeem geen IPsec ondersteunt. De IETF standaard is hier een papieren waarheid.

2. Bent u het eens met het door de expertgroep geadviseerde functionele toepassingsgebied van IPv6? [paragraaf 2.1 van het expertadvies]

Nee.

Pagina 12:
Voor de communicatie tussen de eindsystemen van (overheids)diensten onderling, waarbij de communicatie over organisatiegrenzen plaatsvindt
Dit advies is brengt hoge kosten met zich mee. Het is niet zinvol een koppeling te realiseren tussen eindsystemen met zowel IPv4 als ook IPv6. Dit zal leiden tot onduidelijkheid welk protocol gebruikt wordt, en daardoor hoge beheerkosten en verhoogde kans op storingen.
Vooralsnog heeft gebruik van IPv4 de voorkeur, dit is veruit kosteneffectief. Nadat IPv6 grootschalig is ingezet op Internet kan dit advies bijgesteld worden, zodat IPv6 de voorkeur geniet. Voorbereiding op gebruik van IPv6 is wel wenselijk.

Pagina 12:
om voorbereid te zijn op toekomstige uitwisseling van data tussen allerhande apparaten. De grootschalige introductie van sensoren in ondermeer mobiliteitsvraagstukken, bij dijkbewaking en in slimme energiemeters moet immers mogelijk zijn voor miljoenen gebruikers in Nederland
De voorbeelden zijn gesloten systemen (dijkbewaking) of staan buiten de overheid (energiemeters). Om beveiligingtechnische redenen is het uiterst ongewenst deze elementen toegankelijk te maken buiten het eigen netwerk. Op zich is het een juiste veronderstelling dat een grootschalige roll-out van sensornetwerken het gebruik van IPv6 een valide keuze is. Ook bij mobiel gebruik zou IPv6 voordelen kunnen bieden. Helaas is er momenteel geen ondersteuning van IPv6 bij mobiele netwerken, het is ongewis of veronderstelde voordelen daadwerkelijk beschikbaar komen.

Pagina 12:
IPv6 geen backwards compatibiliteit biedt met IPv4
Dit is de adder onder het gras, die flink kan bijten.

Pagina 13:
De schaalbaarheid van IPv4 is echter zodanig beperkt dat de transparantie van het Internet en daarmee mogelijkheden voor innovatie op middellange termijn in gevaar komen
Het is de vraag of transparantie van het Internet dermate belangrijk is, dat dit de overgang naar IPv6 rechtvaardigt. Alleen als een overgrote meerderheid van de Internet gebruikers de overgang naar IPv6 door zal voeren, en gebruik van IPv4 zal afstoten, zal een overgang naar IPv6 voor iedere Internet gebruiker aantrekkelijk blijken. Eigenlijk weet niemand wat de toekomst ons brengen zal, en is een zekere terughoudendheid bij invoering van IPv6 op zijn plaats. Dit geldt met name voor gebruik van IPv6 binnen de interne netwerken.

3. Bent u het eens met het door de expertgroep geadviseerde organisatorische werkingsgebied van IPv6? [paragraaf 2.2 van het expertadvies]

Nee.

Ik denk dat hier het onderscheid gemaakt moet worden tussen gebruik van het TCP/IP protocol (gehele werkgebied) en IPv6 / Dual Stack (op koppelvlakken naar het publieke Internet.
Het implementeren van Dual Stack op het koppelvlak naar het Internet is al een enorme klus, waarschijnlijk is dit niet afgerond voordat er daadwerkelijk problemen ontstaan. Om deze reden verdient dit de prioriteit. Daarentegen heeft gebruik van IPv6 binnen eigen netwerken geen hoge urgentie.

4. Bent u het eens met de conclusie van de expertgroep inzake de openheid van IPv6? [paragraaf 3.1 van het expertadvies]

Ja.
De tekst gaat over alle publicaties van IETF. De IETF series kunnen als voorbeeld dienen voor open standaarden.

5. Bent u het eens met de conclusie van de expertgroep inzake de bruikbaarheid van IPv6? [paragraaf 3.2 van het expertadvies]

Nee

Pagina 17:

Er zijn inmiddels voldoende instellingen en organisaties die IPv6 toepassen zowel commercieel als not for profit (Surfnet, universiteiten, SIDN, RIPE NCC, EC). Bij eindgebruikersorganisaties is IPv6 nog relatief onbekend
Binnen de overheid is gebruik van IPv6 zo goed als afwezig. Pogingen tot ondersteuning falen veelal door gebruik van ondersteuning bij aangeschafte producten. Veelal is IPv4 een eis en IPv6 een wens. Producten met Dual Stack zijn duurder, dit geldt zeker voor applicaties. Stelling moet zijn: *Bij de Overheid is IPv6 nog relatief onbekend*.

Pagina 17:
Er zijn productleveranciers (van ondermeer routers, besturingssystemen, etc.) die al jarenlang IPv6 ondersteunen
Er wordt geen voorbeeld genoemd van een leverancier van applicaties. Ook genoemde leveranciers hebben een lijst van producten, waarbij IPv6 ondersteuning gebrekkig of afwezig is. Voorbeeld: Cisco Linksys Wireless router, nieuw uit de doos.
Militaire producten voor tactische netwerken zijn veelal IPv4-only.
De echte problemen zitten in de applicaties. Zie bv. RFC 4038.

pagina 17:
Het gebruik van IPv6 in de nabije toekomst is onvermijdelijk
Er is geen noodzaak voor implementatie van IPv6 binnen een netwerk, mits er voldaan wordt aan de voorwaarde dat er geen belemmeringen zijn voor het kunnen ontsluiten, indien dit gewenst is.
Alleen in gevallen van een open verbinding met het Internet is een Dual Stack implementatie onvermijdelijk.

Pagina 18:
en zal op termijn uitgroeien tot de de facto standaard voor end to end communicatie op basis van het Internet Protocol
Dit is een veronderstelling. Vraag is: wat is op termijn? Moeten we nu kiezen voor hogere kosten van een Dual Stack, terwijl dit in vele gevallen onnodig is en dus geldverspilling?

Pagina 18:
Hiermee is IPv6 theoretisch in staat om ieder persoon op aarde (ongeveer 7 miljard) meer dan $5x10^{28}$ adressen toe te kennen
Dit gaat voorbij aan standaarden voor adresuitgifte. Deze is gebaseerd op een GSE architectuur, waarbij elke persoon slechts een fractie van de genoemde adresruimte krijgt toegewezen.
Groter probleem is de restrictie voor multi-homing. De adresuitgifte heeft soortgelijke restricties als bij IPv4; de prefix is van de provider. Alleen grote organisaties (zoals rijksoverheid) kunnen provider independent prefixes gebruiken. Lagere overheden, die gebruik maken van provider afhankelijke adressen, blijven met renumbering problemen zitten bij een overgang naar een andere provider, door afhankelijkheid van toegekende adressen en de eerder gekozen Internet provider.

Pagina 18:

1. ***Vereenvoudigde adrestoekenning aan apparaten en systemen.***
2. ***Meer flexibiliteit voor opties en uitbreidingen.***
3. ***Uitbreidingen voor veiligheid (authenticatie, integriteit, confidentiality) zijn integraal onderdeel van de standaard.***
4. ***Het feit dat NAT niet nodig is om verder groei van het Internet te realiseren: IPv4 kan alleen verder groeien door inzet van NAT, wat de nodige connectiviteitsproblemen met zich mee brengt.***

Er zijn veel hypes over IPv6. O.a. bovenstaand lijstje.

1) IPv4 heeft DHCP. Dit werkt net zo goed als adrestoekenning bij IPv6. Vaak is DHCP bij IPv6 ook nodig, zodat elk voordeel vervalt.
2) Vele uitbreidingen op IPv6 zijn ook in IPv4 geïmplementeerd.
3) Alle beveiligingsmaatregelen zijn ook beschikbaar in IPv4. Veel IPv6 implementaties zijn minder veilig dan IPv4. IPv6 heeft een privacy probleem, adressen zijn veelal vast toegekend aan de gebruikte hardware (MAC adressen).
4) Er wordt hard gewerkt aan het oplossen van problemen bij gebruik van NAT. Voor particulier gebruik is er geen belemmering, tegenwoordig zit bijna iedereen achter een NAT / NAPT. Dit geldt ook voor grotere bedrijfsnetwerken, deze zijn vrijwel zonder uitzondering afgesloten van het publieke Internet, met firewalls en gateways (bv. mail server, web proxy).

6. Bent u het eens met de conclusie van de expertgroep inzake het potentieel van opname van IPv6 op de lijst met open standaarden? [paragraaf 3.3 van het expertadvies]

Nee

Pagina 19:
neemt de leveranciersonafhankelijkheid dan ook niet toe (maar ook niet af) door opname van IPv6 op de lijst met open standaarden.
Er zijn vast en zeker leveranciers die IPv6 niet of niet goed ondersteunen. Genoemd is de Cisco Linksys apparatuur. Cisco zelf levert gelijksoortige apparatuur, echter tegen minimaal het dubbele van de prijs (in dit geval meer dan tienvoudige ...).

Pagina 19:
De expertgroep stelt vast dat er op moment van schrijven van dit rapport al interoperabiliteitsproblemen zijn aan te wijzen tussen overheidspartijen onderling, die door inzet van IPv6 opgelost zouden kunnen worden.
Het is twijfelachtig of er daadwerkelijk dit soort problemen zijn. Veelal zijn de problemen applicatief, en dient er een gateway geplaatst te worden. Zo een gateway kan prima omgaan met IPv4 en / of IPv6.
Vaak is het nuttig en kosteneffectief eigen autonomie te behouden, en op koppelvlakken de interoperabiliteit aan te bieden. Het IP BGP4 protocol is een goed voorbeeld. Netwerk operators behouden hun eigen netwerk, en zijn op de randen interoperabel met BGP4. Vaak gebruiken ISP's helemaal geen

IPv6 in hun core netwerk. Alle verkeer wordt met MPLS getunneld, en een eigen IPv4 privé IPv4 backbone volstaat. Veilig, flexibel en kosteneffectief.

7. Bent u het eens met de conclusie van de expertgroep inzake de impact van IPv6? [paragraaf 3.4 van het expertadvies]

Nee.

Pagina 19:
De risico's zijn naar de mening van de expertgroep beperkt
De risico's worden onderschat. Het activeren van IPv6 in een netwerk kan gevolgen hebben op het gedrag van de applicaties, met uitval als gevolg. Elke activering van IPv6 dient goed gepland en getest te worden.
(opmerking geldt bij alle uitspraken over risico's)

Pagina 19:
Er zijn overigens ook diensten op de markt die alleen via IPv6 ontsloten worden.
Deze vallen in het niet bij diensten die alleen via IPv4 ontsloten worden.

Pagina 21:
Dat kan privacy problemen opleveren
IPv6 introduceert een levensgroot privacy probleem. Servers kunnen (en zullen!) registreren wie de bezoeker is, aan de hand van de fingerprint van het IPv6 adres. Een netwerkbeheerder zal willen voorkomen dat deze lekkage optreedt, en zal kiezen voor een vorm van adrestranslatie (NAT66 technologie is in discussie bij het IETF, onder druk van enterprise-class gebruikers).

8. Bent u het eens met de overwegingen van de expertgroep ten aanzien van de business case?

Nee

Op zijn zachts gezegd: de business case is boterzacht. Het is evident dat IPv4 adressen schaars zullen worden, en dat het publieke Internet op termijn overgaat naar IPv6. Het is echter de vraag wanneer welke systemen omgezet moeten worden. Dit voorstel adviseert alles om te zetten, opdat dan vele, maar nauwelijks gespecificeerde problemen worden opgelost. Er wordt aangenomen dat systemen binnen de overheid zomaar kunnen worden aangesloten op systemen van andere overheidsinstellingen of aan het openbare Internet. Niets is minder waar, verreweg de meeste systemen bij de overheid draaien in afgeschermde compartimenten. Koppelingen met de (boze) buitenwereld zijn verboden, of verlopen via gecontroleerde koppelingen.

Het advies is: begin daar waar het nodig is. Dit zijn systemen, gekoppeld aan het Internet. Daarna volgt omzetting, daar waar het nuttig is. Dat kan zijn de netwerkdiensten binnen de overheid, en de hieraan gekoppelde systemen. Direct hierop volgend dient een uitfasering van IPv4 in de eigen netwerken plaats te vinden, het leidt geen enkel doel een dure Dual Stack oplossing te voeren in eigen netwerken.

De business case bestaat uit kosten en baten. Kosten zijn verdeeld over drie fases: overgang op Dual Stack, extra kosten Dual Stack en kosten uitfasering IPv4. De TCO voor een IPv6-only omgeving liggen op dit moment waarschijnlijk hoger dan bij IPv4-only (veronderstelling). Dual-stack is altijd duurder.
De baten zijn niet concreet te maken. Dit is een reden de overgang naar IPv6 niet te forceren. Doe het waar het moet, en zorg voor voorbereiding voor een vervolg.

9. Bent u het eens met de samenvatting van de overwegingen van de expertgroep? [paragraaf 5.1 van het expertadvies]

Nee. Argumentatie staat hierboven.

10. Bent u het eens met het advies van de expertgroep aan het Forum en College Standaardisatie? [paragraaf 5.2 van het expertadvies]

Nee. Argumentatie staat hierboven.

11. Bent u het eens met de nadere overwegingen van de expertgroep ten aanzien van het stimuleren van IPv6 binnen de overheid? Heeft u eventueel nadere suggesties of overwegingen? [paragraaf 5.3 van het expertadvies]

????
Er is geen paragraaf 5.3

12. Is/zijn er volgens u nog andere informatie of overwegingen omtrent IPv6 die aan het Forum en College Standaardisatie zou moeten worden meegegeven voor een besluit over het opnemen van IPv6 op de lijst met standaarden?

Deze reactie komt mogelijk wat negatief over. Toch is het zeker niet zo bedoeld. Naar mijn mening is het opwekken van een overtrokken positief beeld van IPv6 juist erg schadelijk voor invoering van IPv6.
Mijn advies:

- wees realistisch en terughoudend
- adviseer IPv6 alleen voor daar waar het noodzakelijk of nuttig is
- gebruik opgedane ervaring bij migraties als hulpmiddel voor een vervolg
- denk na over een IPv6-only beleid, voor de wat langere termijn: netwerk met lage gebruikskosten, lager dan nu bij IPv4
- denk na over een beter, maar ook veiliger netwerk. IPv6 helpt hier niet. Het tegendeel is waar, het wordt met IPv6 gemakkelijker netwerken te koppelen, met mogelijk erg nare consequenties.

Reactie InterNLnet

Datum
21 september 2010

Van: Lucas Kruijswijk

Reactie op "Expertadvies IPv6"

Alle opmerkingen mogen openbaar worden gemaakt, inclusief mijn naam.

3.2 (commentaar op hoofdstuk 1).

1. Nee.

3.3 (commentaar op hoofdstuk 2).

2. Ja.
3. Nee. Mogelijk moet het werkgebied ook uitgebreid worden naar organisaties die subsidie van de overheid ontvangen (zie verder mijn commentaar bij punt 8).

3.4 (commentaar op hoofdstuk 3).

4. Ja
5. Ja
6. Ja
7 Nee. Advies is te beperkt.

Aan het eind van 3.4.1 staat:

"De expertgroep concludeert ten aanzien van migratie dan ook dat de configuratie van IPv6 nu meegenomen moet worden in de vervanging of uitrol van actieve netwerkcomponenten en eindsystemen, inclusief de ondersteuning daarvan. Dit is noodzakelijk om de universele toegang tot de diensten te kunnen garanderen zonder onderbreking van de dienstverlening (of een onevenredig dure inhaalslag later)."

De expertgroep adviseert hier enkel bij aanschaf of vervanging. De expertgroep gaat niet in of er gebieden zijn waar migratie naar IPv6 wenselijk is, ook als er geen sprake is van vervanging van software/hardware. Als enkel IPv6 wordt ingevoerd bij vervanging dan is het niet ondenkbaar dat bijvoorbeeld een site van een gemeente, die recentelijk is opgezet of vernieuwd, de komende 10 jaar enkel via IPv4 te bereiken is.
Dit lijkt me een onwenselijk situatie.

3.5 (commentaar op hoofdstuk 4):

8. Nee, te beperkt.

Niet is meegenomen eventuele juridische consequenties van IPv4 uitputting.

Thans is IPv4 een vrij toegankelijk netwerk. Als de IPv4 adressen op zijn, dan kan hier vraagtekens bij gezet worden. Het netwerk is dan nog steeds "ruim" toegankelijk, omdat miljoenen mensen het nog steeds gebruiken. Maar, nieuwkomers op het internet worden uitgesloten of tenminste benadeeld doordat ze gebruik moeten maken van inferieure NAT-technieken. Daarmee is
IPv4 niet meer vrij toegankelijk.

Zo kan men redeneren dat een site die IPv4-only is, aan "IPv-discriminatie"
doet. Het woord 'discriminatie' klinkt misschien wat zwaar hier, maar dat is het niet. Immers, zou de overheid geen telefoongesprekken accepteren van mensen waar het telefoonnummer eindigt op een 9 of als de overheid geen post wil ontvangen van mensen die een huisnummer hebben hoger dan 1000, dan zou dat niet geaccepteerd worden. Vanuit een juridisch oogpunt is de IPv4/IPv6 problematiek niet verschillend.

Discriminatie is in Nederland verboden bij artikel 1 van de Grondwet.
Dit artikel is een beetje apart, in die zin dat het geen uitputtende lijst van gronden geeft, waarop niet gediscrimineerd mag worden (dit in tegenstelling tot de antidiscriminatie artikelen in Internationale Verdragen). Men kan dus redeneren dat IPv-discriminatie valt onder artikel 1.

In de business case worden de redenen genoemd waarom de overheid IPv6 zou moeten toepassen. Uitgaande van bovenstaande, heeft de overheid niet overal de vrije keus, maar is op sommige gebieden gewoon verplicht om
IPv6 toe te passen.

De verplichtingen die uit het IPv-discriminatie verbod volgen, beperken zich tot de interactie met burgers en bedrijven. Ze hebben geen werking op interne netwerken. Voor de interne netwerken zal de business case vooral bedrijfsmatig moeten zijn.

Indien artikel 1 van toepassing is, dan kan dit verstrekkende gevolgen hebben. In het meest extreme geval heeft dat ook invloed op alle organisaties die subsidie van de overheid krijgen (denk daarbij aan de kwestie rond de subsidie aan de SGP in relatie met vrouwendiscriminatie).

Uitgaande van bovenstaande is het wenselijk om invoering van IPv6 ook te doen als er geen sprake is van vervanging en met de volgende
prioriteiten:

a. IPv6 invoeren overal waar een wettelijke verplichting is van digitale communicatie.

b. IPv6 doorvoeren voor alle overige communicatie met burger en bedrijven.

Het stellen van prioriteiten heeft logische wijze als gevolg dat bepaalde zaken minder prioriteit krijgen. Er is minder noodzaak om interne netwerken direct naar IPv6 te migreren. Daarbij niet gezegd dat die migratie niet gedaan moet worden. De punten uit de business case zijn daar nog steeds geldig.

In de wetten die digitale communicatie verplichten, kan ook nog onderscheid worden gemaakt tussen wetten die digitale "publicatie"
verplichten en wetten met andersoortige communicatie. Zo moeten volgens de Wet Ruimtelijke Ordening alle nieuwe bestemmingsplannen digitaal gepubliceerd worden. Zoals eerder gezegd, als dit met IPv4-only is gedaan, dan is deze informatie ruim toegankelijk, maar niet vrij toegankelijk. Dit kan tot problemen leiden en rechters oordelen meestal erg formeel als het om publicatie gaat.

Het dient daarom de aanbeveling om daar waar een wettelijk verplichting tot digitale publicatie bestaat, daar op tijd IPv6 in te voeren. Daarna kunnen andere diensten volgen, zoals de belastingdienst (daarbij toegevoegd dat er geen reden is, omdat na elkaar te doen).

3.6 (commentaar op hoofdstuk 5)

9. Ja
10. Ja
11. Nee

Ik ben het er mee eens dat IPv6 binnen de overheid gestimuleerd moet worden en promotie daarvan lijkt me ook nuttig.

In het expertadvies is echter onvoldoende gemotiveerd ten aanzien van de aspecten die door de markt opgepakt kunnen worden. Het maakt een te grote specialisatie naar de overheid. Men mag verwachten dat het invoeren van IPv6 in de overheid niet wezenlijk verschilt van het invoeren bij een bedrijf. Ervaringen binnen de overheid zijn nuttig voor het bedrijfsleven en omgekeerd. Vanuit dit oogpunt past het niet om een organisatie te introduceren die zich specifiek richt op de overheid.

Een ICT-organisaties die diensten aan de overheid aanbiedt, zal deze kennis ook bij andere klanten (binnen of buiten de overheid) gebruiken.
Het expertadvies heeft onvoldoende gemotiveerd dat een extra kanaal voor kennisverspreiding nodig is.

Verder heeft het expertadvies uitvoerig gemotiveerd dat IPv6 invoeren eigenlijk allemaal geen probleem is. In paragraaf 5.2

lijkt dat opeens toch niet zo makkelijk te zijn en is er een expertisecentrum nodig.

Een expertisecentrum kan ook contraproductief werken. Een overheidsinstelling vraagt mogelijk een advies van het expertisecentrum en van een marktpartij. Deze zullen verschillen bevatten en daardoor zal vertraging ontstaan.

Alvorens belastinggeld uit te geven aan een expertisecentrum zonder accountability, dient dat beter gemotiveerd te worden, bijvoorbeeld ook met een verwijzing naar een eerdere situatie waarbij een expertisecentrum goed gewerkt heeft.

In plaats van een expertisecentrum, stel ik voor om early-adaptors binnen de overheid financieel te steunen, maar als tegenprestatie een evaluatie te verlangen. Deze evaluaties verzamelen en centraal te publiceren (waarbij opgemerkt dat indien er een evaluatie is, deze opgevraagd kan worden op basis van de Web Openbaar Bestuur. Door evaluaties pro-actief te publiceren, wordt de administratieve last van WOB-verzoeken voorkomen, die bijvoorbeeld studenten kunnen ingediend kunnen worden, die voor hun scriptie onderzoek doen naar invoering van IPv6).

Tenslotte, is IPv6 invoering over heel Nederland mogelijk onnodig duur, als hier weinig sturing aan wordt gegeven.

Met krijgt de situatie dat men van IPv4 naar een chaotische situatie gaat met IPv4-only, NAT technieken, dual-stack en IPv6-only. Daar vandaan wordt de situatie weer eenvoudiger en wordt alles IPv6.

Het is aannemelijk dat een voortvarende invoering, de chaotische situatie van gemengde technieken niet overal nodig is. Zo kan bij een snelle invoering bijvoorbeeld een intern netwerk van IPv4 overgaan naar
IPv6 met NAT, maar zonder dual-stack (dit zal zeker niet overal zo zijn).

Er is daarmee een algemeen belang dat IPv6 over geheel Nederland (en de
wereld) voor alle externe functies, snel wordt ingevoerd. Dit algemeen belang rechtvaardigt een eventuele bemoeienis van de overheid. Ik wil daarom adviseren dat de overheid ook een consultatieronde begint onder de ICT-bedrijven of het wenselijk is om eventuele maatregelen te nemen die IPv6 stimuleren of afdwingen. Daarbij ook gevraagd, welke vorm die maatregelen dan zouden moeten hebben. Als voorbeeld, bij verlenging van een domeinnaam zou een toeslag kunnen worden ingevoerd indien een website nog IPv4-only is.
Deze toeslag kan per jaar verhoogd worden.

Dat waren mijn opmerkingen. Graag een bevestiging van ontvangst,

Datum
21 september 2010

met vriendelijke groet,

Lucas Kruijswijk

Reactie Inspectie Verkeer en Waterstaat

Datum
21 september 2010

Van: Duijne, J. van (Jennifer) - IVW **Namens** Inspecteur Generaal - IVW

Beste Bart,

Jenny Thunnissen heeft geen opmerkingen, het is prima zo.

Groet, Jennifer van Duijne

KWALITEITS INSTITUUT NEDERLANDSE GEMEENTEN

Logius
Bureau forum Standaardisatie
Postbus 84011
2508AA Den Haag

doorkiesnummer	uw kenmerk	bijlage(n)
070 373 8017		
onderwerp	**ons kenmerk**	**datum**
Consultatieprocedure IPv6	100914.001u_AS	14 september 2010

Geachte heer/mevrouw,

Hierbij onze antwoorden op de vragen van de consultatieprocedure IPv6.

Vraag 1: Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig, bezien vanuit het doel van het document (het Forum en College Standaardisatie voorzien van een inhoudelijk relevante toelichting op IPv6). [paragraaf 1.1 t/m 1.7 van het expertadvies]?

Antwoord KING:
De huidige tekst in paragraaf 1.1 van het Expertadvies IPv6 van 9 augustus 2010 zijnde:

> "De opdracht aan de expertgroep was om een advies op te stellen over het wel of niet opnemen van IPv6 op de lijst met open standaarden, al dan niet onder bepaalde voorwaarden. Daarbij heeft de expertgroep, nadrukkelijk gekeken naar de samenhang tussen IPv6 en de huidige, zeer gangbare voorloper IPv4. Bovendien heeft de expertgroep gekeken naar de Business Case."

aanvullen met:

> "Aangezien de risico's bij de standaard IPv6 vooral verbonden zijn met het niet (tijdig) implementeren van deze standaard bij overheidsorganisaties en minder met het verheffen van IPv6 tot overheidsstandaard (de optie niet over te gaan op IPv6 bestaat in feite niet), bevat dit expertadvies tevens adviezen (in hoofdstuk 5) voor een tijdige implementatie oftewel uitrol van IPv6 bij de Nederlandse overheid."

Kwaliteitsinstituut Nederlandse Gemeenten (KING)
Nassaulaan 12
Postbus 30435
2500 GK Den Haag
INFO@KINGGEMEENTEN.NL
WWW.KINGGEMEENTEN.NL

kvk 27348329
Bank 285143662
T 070 373 8017
F 070 363 5682

Vraag 10: Bent u het eens met het advies van de expertgroep aan het Forum en College Standaardisatie? [paragraaf 5.2 van het expertadvies]?

Antwoord KING:
De huidige tekst in paragraaf 5.2 van het Expertadvies IPv6 van 9 augustus 2010 zijnde:

> "Voor een effectieve uitrol van IPv6 binnen de overheid adviseert de expertgroep het Forum daarom aanvullend om:
> - De sense of urgency voor de uitrol van IPv6 te communiceren. Bijvoorbeeld door het gebruik van IPv6 actief te promoten binnen de overheid als een voorwaarde voor interoperabiliteit."

te vervangen door:

> "Voor een effectieve uitrol van IPv6 binnen de overheid adviseert de expertgroep het Forum daarom aanvullend om:
> - De risico's en concrete gevolgen van een niet tijdige uitrol van IPv6 bij overheidsorganisaties te communiceren plus de urgentie van een wel tijdige uitrol."

en aan te vullen met:

> "- Te bevorderen dat op landelijk niveau de advisering ingevuld gaat worden over hoe overheidsorganisaties de uitrol van IPv6 technisch en projectmatig kunnen invullen.".

Met vriendelijke groet,
Kwaliteitsinstituut Nederlandse Gemeenten

Adrie Spruit, adviseur gemeentelijke informatiearchitectuur

Reactie Ministerie van BZK

Datum
21 september 2010

Geachte heer Knubben,

Hierbij ontvangt u vanuit BZK de reactie op de openbare consultatieronde voor IPv6, PKIOverheid en SHA-2. Hierbij zijn de 3 adviezen in 1 document opgenomen.
Mocht u vragen hebben, dan verneem ik dat graag.

Met vriendelijke groet, mede namens Nicole Stolk,

Hylke Wierda
plv. CIO

Standaarden

IPv6

IP staat voor Internet Protocol en daarmee is direct de reikwijdte benoemd van deze standaard. Het protocol voorziet (onder andere) in de adressering van verschillende infrastructuurcomponenten in een netwerk.
Het huidige protocol IPv4 dateert uit het midden van de vorige eeuw en de grenzen van schaalbaarheid zijn inmiddels nagenoeg bereikt.
IP is louter een technisch communicatieprotocol waardoor de implementatie van deze standaard enkel op ICT beheersorganisaties impact zal hebben.
Door de markt is deze standaard inmiddels ruimschoots omarmd.

Echter de impact moet ook niet onderschat worden, het IP protocol vormt de basis van vrijwel alle netwerkfunctionaliteiten, het migratietraject zal dan ook een langdurig iteratief karakter hebben.

De eerste migratiestappen zullen zich met name richten op de communicatie "naar buiten", intranetten kunnen voorlopig nog uitstekend gefaciliteerd blijven middels IPv4.

Zie bijlage 1 voor de beantwoording van de door het Forum Standaardisatie gestelde vragen.

Bijlage 1: Beantwoording vragen IPv6

Links naar:
Consultatiedocument
Expertadvies

1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig, bezien vanuit het doel van het document (het Forum en College Standaardisatie voorzien van een inhoudelijk relevante toelichting op IPv6). [paragraaf 1.1 t/m 1.7 van het expertadvies].
    a. Nee
2. Bent u het eens met het door de expertgroep geadviseerde functionele toepassingsgebied van IPv6? [paragraaf 2.1 van het expertadvies]
    a. Nee, hoewel in het functioneel toepassingsgebied veel aandacht wordt besteedt aan het iteratief karakter en de verwachte doorlooptijd van de migratie van IPv4 naar IPv6 sluit de

uiteindelijke definiering deze weer uit. Wenselijker zou zijn ook in de definiering rekening te houden met deze fasering.

3. Bent u het eens met het door de expertgroep geadviseerde organisatorische werkingsgebied van IPv6? [paragraaf 2.2 van het expertadvies]
    a. Ja
4. Bent u het eens met de conclusie van de expertgroep inzake de openheid van IPv6? [paragraaf 3.1 van het expertadvies]
    a. Ja
5. Bent u het eens met de conclusie van de expertgroep inzake de bruikbaarheid van IPv6? [paragraaf 3.2 van het expertadvies]
    a. Ja
6. Bent u het eens met de conclusie van de expertgroep inzake het potentieel van opname van IPv6 op de lijst met open standaarden? [paragraaf 3.3 van het expertadvies]
    a. Ja
7. Bent u het eens met de overwegingen van de expertgroep ten aanzien van de business case?
    a. Ja, zie ook de beantwoording van vraag 2, er is feitelijk geen directe interne business case, de huidige netwerkinfrastructuur van de Rijksoverheid (met name externe elementen zoals proxyservers, firewalls, routers) zijn reeds IPv6 ready, met name omdat de industrie deze keuze reeds heeft gemaakt. Voor de consumenten/MKB markt zal dit een grotere impact hebben.
8. Bent u het eens met de samenvatting van de overwegingen van de expertgroep? [paragraaf 5.1 van het expertadvies]
    a. Ja, echter zal de invoering van IPv6 geen direct zichtbare verbeteringen in de dienstverlening van de Rijksoverheid bieden, de invoering van de standaard dient voornamelijk preventief overwogen te worden vanuit het oogpunt van de onvermijdelijk naderende schaalbaarheidsgrenzen van IPv4.
9. Bent u het eens met het advies van de expertgroep aan het Forum en College Standaardisatie? [paragraaf 5.2 van het expertadvies]
    a. Ja, mits voldaan wordt aan de opmerking bij vraag 2.
10. Bent u het eens met de nadere overwegingen van de expertgroep ten aanzien van het stimuleren van IPv6 binnen de overheid? Heeft u eventueel nadere suggesties of overwegingen? [paragraaf 5.3 van het expertadvies]
    a. Ja
11. Is/zijn er volgens u nog andere informatie of overwegingen omtrent IPv6 die aan het Forum en College Standaardisatie zou moeten worden meegegeven voor een besluit over het opnemen van IPv6 op de lijst met standaarden?
    a. Nee

Reactie Ministerie van BZK

Datum
21 september 2010

Van: Andersen, Olaf

Reactie op expertadvies IPv6

Hierbij mijn reactie op het expertadvies Ipv6.

3.2 Doel

De reden om IPv6 voor te dragen voor opname op de lijst van open standaarden volgens het "comply or explain" principe van het College Standaardisatie was, dat de overheid zwaar achter liep bij het invoeren van IPv6.
Opname op de lijst van het College Standaardisatie zou (was ook de gedachte van de Tweede Kamer) de urgentie benadrukken en bovendien de organisaties van de overheid verplichten in nieuwe aanbestedingen (waarbij IPv6 relevant is) het kunnen hanteren van IPv6 als eis op te nemen.
Er is geen discussie over, dat de overheid op korte termijn IPv6 compliant moet zijn: anders is communicatie van de overheid met IPv6 systemen en van IPv6 systemen met de overheid niet mogelijk. (zie 1.5 blz. 10 van het advies) Hierbij is dus ook geen "explain"mogelijk.
De datum, waarop uitsluitend IPv6 nummers zullen worden uitgegeven, omdat de IPv4 nummers op zijn komt steeds dichterbij (mede door "hamstergedrag"van ISP's en andere grote bedrijven). Naar schatting zal dit al in mei of juni 2011 het geval zijn.
De overheid moet dus heel snel zorgen, dat ze IPv6 compliant is (zoals boven beschreven). Het gebruik van IPv6 wordt daarmee vooral een vereiste op het koppelvlak van de organisatie, aan de buitenkant (2.1 blz. 12 van het advies).

Het nu voorliggende advies lijkt een stap verder te gaan door niet het compliant zijn aan IPv6 (d.w.z. met IPv6 systemen kunnen communiceren), maar het migreren naar en volledig zelf gebruiken van IPv6 verplicht te stellen,

Dit laatste kan nooit de bedoeling zijn, omdat er voor een volledige migratie naar IPv6 geen business case is (blz. 23 en 24 van het advies). Zo'n migratie kan de overheid naar schatting honderden miljoenen gaan kosten. Hoewel op blz. 23 en op blz. 6 ook de niet onderbouwde stelling wordt geponeerd, dat een latere (wanneer?) overgang naar IPv6 onevenredig duur cq. buitenproportioneel hoog zou zijn.
IPv6 is een wat aparte standaard, omdat de voorganger IPv4 naar schatting nog heel lang in gebruik zal blijven (het expert advies noemt een periode van 10 tot 20 jaar). Bij volledige overgang door de overheid naar IPv6 zou overigens communicatie met IPv4 daarom nog steeds mogelijk moet blijven.

Het verplichte doel moet dus zijn "kunnen communiceren met IPv6 systemen" (compliancy).
Een volledige migratie naar IPv6 moet worden overgelaten aan de organisaties zelf en zal o.a. worden gestuurd door de behoefte aan en voordelen van andere en intensievere communicatie. Hiervoor moet geen verplichte explain worden opgelegd.

3.3 Functioneel toegangsgebied en werkingsgebied

Vraag 2: Op blz. 12 staat heel dwingend, dat IPv6 **moet** worden gebruikt voor vier genoemde gebieden (streepjes). Om compliant te zijn voldoen de gebieden achter eerste en de derde gedachtestreep. Voor de twee andere gebieden zie ik niet in, waarom dat nú verplicht zou moeten worden. IPv4 blijft immers nog tientallen jaren bestaan en gebruikt worden.
Het functioneel toegangsgebied wordt daardoor nu heel breed gedefinieerd. Als daarvoor IPv6 gebruik verplicht wordt, wordt impliciet een volledige migratie naar IPv6 verplicht. Dat gaat te ver; zie ook onder 3.1

Vraag 3: het werkingsgebied is akkoord.

3.4 toetsing van de standaard aan de criteria

Vraag 4: eens met conclusie over openheid

Vraag 5: IPv6 is voldoende bruikbaar (en onontkoombaar) en biedt ook voordelen ten opzichte van IPv4. Om deze voordelen te behalen is echter een zeer kostbare migratie nodig (zie eerder ontbrekende business case).

Vraag 6 (potentieel van de standaard) : geen opmerkingen

Vraag 7 (impact): ook hier lopen compliancy en volledige migratie door elkaar heen in het advies. Dit zou helderder moeten worden opgesteld. Termen moeten beter worden gedefinieerd: wat versta je onder uitrol? Als voorbeeld wordt genoemd zorgen, dat nieuwe apparatuur geschikt is voor IPv6. Is dat uitrol?
Heel kort door de bocht: compliancy (zoals boven gedefinieerd) heeft nauwelijks impact. Volledige migratie heeft grote impact en leidt tot heel andere (inzet van) netwerken. Daarom is daar ook geen business case voor. Ook zijn er nog niet veel praktijkvoorbeelden van grote organisaties, die geheel zijn gemigreerd of dat gaan doen.

De “best practice” op dit moment is zorgen, dat je organisatie aan de buitenkant met IPv6 kan communiceren (compliant is). Dat moet dus verplicht worden en meer niet. Met bestaande partners en binnen de organisatie blijf je voorlopig IPv4 “praten”.
Deze twee trajecten zouden in het hele advies beter naast elkaar moeten worden uitgewerkt.

3.5 Business case

Vraag 8 (conclusies Business Case) .
Een echte conclusie ontbreekt, dus ook een business case.
Overigens welke business case? Voor compliancy of voor migratie? Algemeen stellen de experts, dat er nu geen positieve Business case voor een migratie naar IPv6 is. En compliancy moet een verplichting voor de overheid zijn: je mag systemen met een IPv6 nummer niet uitsluiten van communicatie met de overheid. Wel wordt zonder onderbouwing gewaarschuwd, dat door het niet opnemen op de lijst de kosten van invoering (ook dat is nergens goed omschreven) later bovenproportioneel zullen toenemen.

Het is duidelijk, dat het verplicht opnemen in aanbestedingen van de eis dat alle ICT-componenten (ook) geschikt voor IPv6 moeten zijn, de kosten van migratie in de toekomst zullen beperken. Dat moet de kern van het doel van het opnemen van IPv6 op de lijst van het College zijn. Schrijf dat ook helder op.

3.6 Advies aan Forum en College

Vraag 9 (samenvatting): zie eerdere opmerkingen

Vraag 10 (eens met advies): opnemen van IPv6 op de lijst is prima, met de inperking, dat het comply alleen geldt voor het compliant maken van je organisatie. Een explain voor het niet volledig migreren naar IPv6 moet niet nodig zijn. (zie eerdere opmerkingen).
Dit impliceert feitelijk, dat explains voor het niet compliant zijn niet mogelijk moeten zijn.

Pas op met het teveel optuigen van allerlei organisaties, die zich met deze materie bezighouden. Kennis op dit gebied is volop aanwezig (kijk maar op het internet). Het is meer een bestuurlijk probleem. Stel daarom een datum vast (suggestie: 1-7-2011), waarop alle organisaties binnen het werkingsgebied compliant moeten zijn en laat hen daarover rapporteren.
Bevorder daarnaast dat alle overheidsorganisaties hun ICT diensten en producten IPv6 compliant inkopen. (verplichte aanbestedingstoets?)

Reactie Ministerie van Financiën

Datum
21 september 2010

Beste Bart,

Het Ministerie van Financien heeft verder geen aanvullende opmerkingen of vragen over het gedegen onderzoek van de expertgroepen over de respectieve onderwerpen PKIoverheid. IPV6 en SHA-2.
Minfin kan instemmen met de adviezen. (PKIoverheid nog geen Open standaard, het belang van IPV6, ook de Overheid zal deze standaard moeten gaan invoeren om connectiviteit te behouden, SHA-2 ipv MD-5 t.b.v. authenticatie en integriteitscontrole)

MinFin ziet het belang van de introductie IPV6 en zal de activiteiten ook in haar roadmap gaan opnemen om als departement haar connectiviteit te behouden.

Met vriendelijke groeten,

Frank van Linden

Reactie Ministerie van Justitie

Datum
21 september 2010

Beste Bart,

Justitie is het eens met de uitkomsten van de expertgroep
Hierbij het ingevulde consultatie document op de nieuwe
standaard IPv6 ingevuld met behulp van Justitie achterban.

Mvg

Roland Groustra
ICT-adviseur/EA-architect

3.1 Inleiding
Onderstaand wordt een aantal vragen aan u gesteld omtrent het expertadvies IPv6. Gelieve in uw beantwoording dezelfde nummering aan te houden. Graag, zoals al eerder opgemerkt, waar mogelijk ook de onderbouwing van uw antwoord bijvoegen zodat inzichtelijk wordt op basis waarvan u tot een (eventueel afwijkend) oordeel komt.

3.2 Vragen over hoofdstuk 1 van het expertadvies ("Doelstelling expertadvies")
Hoofdstuk 1 geeft een beschrijvende toelichting op IPv6.
Vraag:
1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig, bezien vanuit het doel van het document (het Forum en College Standaardisatie voorzien van een inhoudelijk relevante toelichting op IPv6). [paragraaf 1.1 t/m 1.7 van het expertadvies].
=> NEEN

3.3 Vragen over hoofdstuk 2 van het expertadvies ("Toepassings- en werkingsgebied")
Hoofdstuk 2 gaat achtereenvolgens in op het voorgestelde functionele toepassingsgebied van IPv6 en het voorgestelde organisatorische werkingsgebied.
Vragen:
2. Bent u het eens met het door de expertgroep geadviseerde functionele toepassingsgebied van IPv6? [paragraaf 2.1 van het expertadvies]
=> JA
3. Bent u het eens met het door de expertgroep geadviseerde organisatorische werkingsgebied van IPv6? [paragraaf 2.2 van het expertadvies]
=> JA

3.4 Vragen over hoofdstuk 3 van het expertadvies ("Toetsing van de standaard aan de criteria")
Hoofdstuk 3 gaat achtereenvolgens in op de aspecten en criteria van openheid, bruikbaarheid, impact en potentieel, gebaseerd op een aantal subcriteria.
Vragen:
4. Bent u het eens met de conclusie van de expertgroep inzake de

openheid van IPv6? [paragraaf 3.1 van het expertadvies]
=> JA
5. Bent u het eens met de conclusie van de expertgroep inzake de bruikbaarheid van IPv6? [paragraaf 3.2 van het expertadvies]
=> JA
6. Bent u het eens met de conclusie van de expertgroep inzake het potentieel van opname van IPv6 op de lijst met open standaarden? [paragraaf 3.3 van het expertadvies]
=> JA
7. Bent u het eens met de conclusie van de expertgroep inzake de impact van IPv6? [paragraaf 3.4 van het expertadvies]
=> JA

3.5 Vragen over hoofdstuk 4 van het expertadvies ("Business Case")

In hoofdstuk 4 formuleert de expertgroep een korte analyse van kosten en baten van implementatie en ingebruikname van IPv6.
Vragen:
8. Bent u het eens met de overwegingen van de expertgroep ten aanzien van de business case?
=> JA

3.6 Vragen over hoofdstuk 5 van het expertadvies ("Advies aan Forum en College")

In hoofdstuk 5 formuleert de expertgroep onder zijn conclusie de overwegingen en zijn advies aan het college.
Vragen:
9. Bent u het eens met de samenvatting van de overwegingen van de expertgroep? [paragraaf 5.1 van het expertadvies]
=> JA
10. Bent u het eens met het advies van de expertgroep aan het Forum en College Standaardisatie? [paragraaf 5.2 van het expertadvies]
=> JA
11. Bent u het eens met de nadere overwegingen van de expertgroep ten aanzien van het stimuleren van IPv6 binnen de overheid? Heeft u eventueel nadere suggesties of overwegingen? [paragraaf 5.3 van het expertadvies]
=> JA

3.7 Resterende inhoudelijke opmerkingen

Vraag:
12. Is/zijn er volgens u nog andere informatie of overwegingen omtrent IPv6 die aan het Forum en College Standaardisatie zou moeten worden meegegeven voor een besluit over het opnemen van IPv6 op de lijst met standaarden?
=> Er is een dubbele stack Ipv6 en Ipv4 nodig om interoperabel te blijven met burger en bedrijf

Reactie Ministerie van LNV

Datum
21 september 2010

Beste Bart,

Bij deze de reactie op de openbare consultatie van LNV.

Met vriendelijke groet.

Pieter Rood

IPv6

Vragen over hoofdstuk 2
Omdat het surfgedrag van een ieder eenvoudiger te volgen wordt, zijn er met IPv6 wellicht extra risico's op het gebied van privacy. De nadruk zou minder op iedere individuele gebruiker moeten komen te liggen. Dit betekent voor het functionele toepassingsgebied in de richting van:
"communicatie op netwerkniveau tussen alle organisaties, apparaten, diensten en sensoren. In voorkomende gevallen ook naar individuele gebruikers"
Overigens schuilt er in het woord "netwerkniveau" veel meer dan alleen het laag 3 protocol IPV6 dat hier genoemd wordt.

Vragen over hoofdstuk 3
Hier wordt veel melding gemaakt van het verdwijnen van de NAT-constructie door de beschikbaarheid van een groter aantal adressen. NAT heeft ook een functie heeft in de beveiliging en afscherming van delen van het netwerk. De NAT-constructie moet niet worden afgeschaft voordat er alternatieve oplossingen voor dit beveiligingsprobleem worden gevonden.

Vragen over hoofdstuk 4
Bij de invoering van IPV6 moet niet licht nagedacht worden over de impact die dat heeft op de bestaande infrastructuur. Slechts een deel van de infra is geschikt (te maken) voor het gebruik van IPV6. Het is maar de vraag of een vervanging van huidige infra tegen redelijke kosten realiseerbaar is. Beter is het om voor een geleidelijke invoering van IPV6 en daarmee de geleidelijke uitfasering van IPV4 te kiezen. In concreto; nieuw op basis van IPV6 en oud op basis van IPV4 met een goede gateway ertussen. Uiteindelijk faseren de IPV4 systemen zichzelf uit.
Het genoemde voordeel in beheer moet duidelijker onderbouwd worden. Het beheer van IPV6 wordt eerder complexer dan eenvoudiger. De opbouw van IPV6 is veel complexer, waar vroeger slechts met "enkele" IP adressen aan de buitenkant werd gewerkt, zal dat nu veel meer worden. De opmerking dat het firewall beheer minder zal worden moet daarom beter onderbouwd worden Daarnaast zal voor de berekening van subnets etc. tooling nodig zijn.

Reactie Ministerie van OCW

Datum
21 september 2010

Beste Bart,

Bij deze laat ik je weten dat OCW akkoord gaat met de voorgestelde standaarden.

Vriendelijke groeten,

Bram Gaakeer

Reactie Ministerie van VWS

Datum
21 september 2010

Van: Haveman, dhr. drs. H.B.

Bart

Ter info; onze VWS-informatie is voldoende ingebracht en verwerkt via de expertmeetings
Akkoord dus.

Hans

Reactie NOiV

Datum
21 september 2010

Beste,

dank voor de uitnodiging te reageren op de consultatie IPv6, PKIoverheid en SHA-2 standaarden.

Wij hebben de expertadviezen doorgenomen en hebben geen opmerkingen. We kunnen ons dus vinden in de aanbevelingen van de expertgroepen voor de drie standaarden.

Met vriendelijke groet,

Piet Hein Minnecre
Projectleider Open Stanndaarden
NOiV

Reactie Sander Steffann
(Vice-voorzitter RIPE Address Policy Working Group)

Datum
21 september 2010

Bij deze reageer ik op het consultatiedocument betreffende IPv6. Mijn betrokkenheid bij IPv6 komt voort uit mijn ervaringen gedurende de de laatste 15 jaar als internet specialist, mijn functie als vice-voorzitter van de RIPE Address Policy Working Group welke belast is met het creëren van beleid voor de uitgifte van onder andere IPv4 en IPv6 adressen en mijn betrokkenheid bij de Nederlandse IPv6 task force.

Ik zal het document per vraag behandelen:

1: Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig, bezien vanuit het doel van het document?
Nee. De expertgroep heeft dit mijns inziens correct en volledig geformuleerd.

2: Bent u het eens met het door de expertgroep geadviseerde functionele toepassingsgebied van IPv6?
Het functioneel toepassingsgebied lijkt mij prima geformuleerd. Enige beperking van het toepassingsgebied zal op de lange termijn invoering van IPv6 hinderen en hogere kosten met zich mee brengen.

3: Bent u het eens met het door de expertgroep geadviseerde organisatorische werkingsgebied van IPv6?
Hiervoor geldt hetzelfde antwoord als op vraag 2.

4: Bent u het eens met de conclusie van de expertgroep inzake de openheid van IPv6?
Ja.

5: Bent u het eens met de conclusie van de expertgroep inzake de bruikbaarheid van IPv6?
Ja.

6: Bent u het eens met de conclusie van de expertgroep inzake het potentieel van opname van IPv6 op de lijst met open standaarden?
Ja.

7: Bent u het eens met de conclusie van de expertgroep inzake de impact van IPv6?
Ja.

8: Bent u het eens met de overwegingen van de expertgroep ten aanzien van de business case?
Ja.

9: Bent u het eens met de samenvatting van de overwegingen van de expertgroep?
Ja.

10: Bent u het eens met het advies van de expertgroep aan het Forum en College Standaardisatie?

Ja. Ik kan mij ook uitstekend vinden in de aanvullende aanbevelingen die door de expertgroep gegeven worden.

11: Bent u het eens met de nadere overwegingen van de expertgroep ten aanzien van het stimuleren van IPv6 binnen de overheid? Heeft u eventueel nadere suggesties of overwegingen?
Deze vraag refereert naar sectie 5.3, welke niet bestaat. Ik neem aan dat u verwijst naar het laatste deel van sectie 5.2, waar ik mij uitstekend in kan vinden. Naast de gegeven aanbevelingen lijkt mij bijscholing van personen die met systeem- of netwerkbeheer belast zijn een waardevolle aanvullen. Hierdoor kunnen implementatie- en beheerfouten voorkomen worden. Ook voor het handhaven van het beveiligingsbeleid zal deze kennis noodzakelijk zijn. Ik stel voor om hierover de Nederlandse IPv6 task force in ieder geval te raadplegen. Binnen deze task force is alle benodigde kennis hierover aanwezig. Het versterken van de task force zodat deze de benodigde kennis ook buiten de overheid onder de aandacht kan brengen is mijns inziens noodzakelijk.

12: Is/zijn er volgens u nog andere informatie of overwegingen omtrent IPv6 die aan het Forum en College Standaardisatie zou moeten worden meegegeven voor een besluit over het opnemen van IPv6 op de lijst met standaarden?
Nee. Het rapport van de expertgroep sluit prima aan bij mijn eigen visie.

Met vriendelijke groet,
Sander Steffann

Reactie WH.v.Goeverden (Ministerie van Defensie)

Datum
21 september 2010

Van: WH.v.Goeverden

Geacht forum,

Hierbij stuur ik u een opmerking naar aanleiding van het Expertadvies IPv6 (op persoonlijke titel, omdat ik niet in de gelegenheid was om voor de sluiting van de consultatieprocedure dit punt formeel af te stemmen). Ik heb van Bart Knubben begrepen, dat de consulatieprocedure was verlengd t/m 15 september.

Aandachtpunt
Het Expertiseadvies geeft aan dat RFC 4862 "IPv6 Stateless Address Autoconfiguration" als essentiële RFC wordt gebruikt. Het gebruik hiervan impliceert dat het MAC-adres van een object, gekoppeld aan het netwerk (b.v. een PC), wordt opgenomen in het IP-adres van het betreffende netwerkobject. Hierdoor is het in theorie mogelijk om, op basis van zijn IP adres een specifiek object te traceren en na te gaan waar het zich bevindt. De vraag is, of dit wenselijk is en of dit niet strijdig is met bestaande wet- en regelgeving. Het antwoord op deze vraag weet ik niet.

Een alternatief is, dat gebruik wordt gemaakt van DHCP voor IPv6. In het Expertiseadvies wordt DHCP wel genoemd (paragraaf 1.6, blz. 10), maar wordt de bijbehorende RFC (meest recente RFC 5494 "IANA Allocation Guidelines for the Address Resolution Protocol (ARP)") niet vermeld als essentiële RFC.

Het Expertiseadvies doet geen harde uitspraken over het gebruik van Stateless Address Autoconfiguration dan wel het gebruik van DHCP. De indruk wordt gewekt dat IPv6 Stateless Address Autoconfiguration op zijn minst is toegestaan en mogelijk zelfs de voorkeur heeft.

Aanbeveling
Stel zeker dat als onderdeel van een mogelijk besluit om IPv6 verplicht te stellen expliciet wordt gemaakt welke adresformaten zijn toegestaan en of er mogelijk beperkende wet- en regelgeving van toepassing is.

Achtergrond informatie
Onderstaande informatie heb ik één op één overgenomen uit de wikipedia (http://en.wikipedia.org/wiki/IPv6_address) en biedt wat achtergrondinformatie. Hieruit blijkt in het bijzonder dat een IP adres, indien gegenereerd op basis van het MAC adres, zowel routing informatie bevat als informatie van het betreffende object (namelijk zijn MAC adres).

Met vriendelijke groeten,
Wout van Goeverden

---- Start citaat ---
Unicast address format

Unicast and anycast addresses are typically composed of two logical parts: a 64-bit network prefix used for routing, and a 64-bit interface identifier used to identify a host's network interface.

General unicast address format

bits	48	16	64
field	*network prefix*	*subnet identifier*	*interface identifier*

The *network prefix* is contained in the most significant set of bits of the address. The recommended allocation to end users is a 48-bit routing prefix. In this scenario, the 16 bits of the *subnet identifier* field are available to the network administrator to define subnets within the given network. The 64-bit *interface identifier* is **either automatically generated from the interface's MAC address** using the modified EUI-64 format, **obtained from a DHCPv6 server**, automatically established randomly, or assigned manually.
--- Einde citaat ---