Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

IP versie 6

Versie 2.0

IP versie 6

Versie 2.0

Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
T 070 751 55 55 | F 070 888 75 50
www.ncsc.nl | info@ncsc.nl

Oktober 2013

Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met het geven van expertise en advies, response op dreigingen en het versterken van de crisisbeheersing. Daarnaast voorziet het in informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie. Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.

Het NCSC is een onderdeel van de Directie Cyber Security van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Samenwerking en bronnen

Dit Whitepaper is opgesteld door het NCSC. In een samenwerking met meerdere deskundigen uit publieke en private organisaties is dit whitepaper gerealiseerd. Hun bijdragen, de inhoudelijke reviews alsmede openbaar toegankelijke bronnen hebben in sterke mate bijgedragen aan de inhoud van dit whitepaper. In Bijlage E – Referenties worden de individuele deskundigen die een bijdrage geleverd hebben met naam vermeld.

Managementsamenvatting

Het Internet Protocol versie 6 (IPv6) is de opvolger van het Internet Protocol versie 4 (IPv4). De ontwikkeling van IPv6 is in de jaren 90 met name gestart om met een oplossing te komen voor een dreigend tekort aan IP-adressen. Dit tekort werd in eerste instantie veroorzaakt door een toename en een grotere dichtheid van Internet aansluitingen wereldwijd, maar wordt de laatste jaren versneld door een enorme ontwikkeling in consumentenapparatuur die aan het Internet gekoppeld moet worden.

Tussenoplossingen

Tussenoplossingen verlengen de levensduur van IPv4 met enkele jaren maar in andere delen van de wereld, bijvoorbeeld in Azië, worden IPv4 adressen niet meer uitgegeven. Door deze ontwikkelingen kunnen Europa en de rest van de wereld niet achterblijven en het gebruik van IPv6 zal gaan toenemen. Op 14 september 2012 is RIPE NCC, de instantie die in Europa verantwoordelijk is voor de uitgifte van IP adressen, begonnen aan de laatste range IPv4 adressen[1]. Er worden alleen nog in beperkte mate IPv4 adressen uitgegeven als de aanvrager ook beschikt over een IPv6 allocatie[2]. In nieuwe hard- en software is het gebruik van IPv6 inmiddels geïntegreerd.

Naast de aanpak van de beperkte adresruimte zijn vele verbeteringen aangebracht in IPv6. Zo is een groot aantal nieuwe functies toegevoegd en is de structurering van IP-adressen duidelijker geworden. Uiteindelijk zijn de basisfunctionaliteit en de werking hetzelfde gebleven als die van IPv4.

Beveiliging

Qua beveiliging zijn op detailniveau een aantal problemen opgelost. Een belangrijk beveiligingsaspect is dat het verplicht is om IPsec te ondersteunen in IPv6. Dit zal de toepassing van IPsec, beveiliging in de vorm van o.a. authenticatie en versleuteling op IP-niveau, ten goede komen. Anderzijds moet bij de introductie van IPv6, net als bij veel implementaties van nieuwe technologie, rekening gehouden worden met het feit dat nog kwetsbaarheden gevonden zullen worden.

Veel apparatuur en software zijn al geschikt om IPv6 te gebruiken en een van de risico's is dat IPv6 steeds vaker standaard al aan staat, ook als daar niet expliciet voor gekozen is. Als een organisatie zich hier niet bewust van is zal een beveiligingsprobleem ontstaan. Vooral als de beveiligingsorganisatie en geïmplementeerde maatregelen volledig ingericht zijn op IPv4 en IPv6 communicatie ongemoeid laten.

Migratie

De migratie van IPv4 naar IPv6 zal niet op één moment plaats vinden. Jarenlang zal een situatie bestaan waarin beide protocollen naast elkaar gebruikt worden. Om dit te realiseren zijn verschillende migratiemethoden ontwikkeld zodat verbindingen mogelijk zijn tussen IPv4- en IPv6-systemen.

Op dit moment lijkt voor veel organisaties nog steeds geen dringende noodzaak te ontstaan om over te stappen. Het is niet te verwachten

1 http://www.ripe.net/internet-coordination/ipv4-exhaustion

2 http://www.ripe.net/internet-coordination/ipv4-exhaustion/business-and-enterprise

dat alsnog een gewilde toepassing ('killer application'), die IPv6 vereist, zal komen. Toch is het sterk af te raden om 'niets' te doen, vanwege de toename van het mondiale gebruik van IPv6 en de ontwikkelingen op het gebied van IPv6 in infrastructurele componenten en software. Het negeren van IPv6 zal op termijn dus extra complexiteit en kwetsbaarheden veroorzaken. Daarnaast zullen ook issues ontstaan op het gebied van performance en beschikbaarheid en kunnen de totale netwerk- en beheerskosten stijgen. IPv6 in een later stadium alsnog implementeren zal complexer zijn dan weloverwogen in een vroeger stadium een migratie of in gebruik name in gang zetten. Het is verstandig om als organisatie een besluit te nemen en plannen te ontwikkelen om te voorkomen dat in een te laat stadium acties opgepakt moeten worden waardoor risico's en security-incidenten ontstaan door tijdsdruk en onvoldoende doordachte ontwerpen. «

Executive summary

Internet protocol version 6 (IPv6) is the successor to internet protocol version 4 (IPv4). The main reason why IPv6 was developed in the 1990s was to solve the problem of the impending shortage of IP addresses. This shortage was initially caused by an increase and higher density of internet connections worldwide. In recent years, it has been accelerated by the rapid developments in consumer appliances with an internet connection.

Interim solutions

Interim solutions have extended the lifecycle of IPv4 by several years, but in other parts of the world, such as Asia, IPv4 addresses are no longer issued at all. Due to these developments, Europe and the rest of the world cannot lag behind. Therefore, the use of IPv6 addresses is expected to increase. On 14 September 2012, RIPE NCC, the European coordination centre that is responsible for the allocation of IP addresses, started issuing IPv4 addresses from the final range[3]. IPv4 addresses are now limitedly issued and only if the applicant also has an IPv6 allocation[4]. IPv6 is already fully integrated into new software and hardware.

While IPv6 was mainly created to solve the shortage of IP addresses, it also contains many improvements. For instance, a great many new functionalities have been added and the structure of IP addresses is more clear now. The basic functionality, however, is the same as that of IPv4.

Security

In terms of security, several problems have been solved on a detailed level. One of the most important security aspects is that it is compulsory to support IPsec in IPv6. This will be beneficial to the application of IPsec, which is security in the form of authentication and encryption on an IP level. On the other hand, as with any new technology, it should be taken into account that the introduction of IPv6 will be accompanied with vulnerabilities.

Many appliances and software programs are already compatible with IPv6 and one of the risks is that IPv6 is automatically on, whereas the user is not aware of it of has not explicitly chosen to turn it on. If an organization is not aware of this feature, this will result in security issues. This is particularly true if the security organization and implemented measures are fully geared towards IPv4 and not towards IPv6 communication.

Migration

The migration from IPv4 to IPv6 will not take place at one moment. It is likely that both protocols will be used simultaneously for several years. In order to realize the migration, several migration methods have been developed to connect the IPv4 and IPv6 systems.

For the moment, it seems that many organizations do not see the urgency of migrating. It is not expected that a much-desired application (killer application) that requires IPv6 will be released in the short term. Yet, we recommend not to do 'nothing', because

3 http://www.ripe.net/internet-coordination/ipv4-exhaustion

4 http://www.ripe.net/internet-coordination/ipv4-exhaustion/business-and-enterprise

of the worldwide increase in IPv6 use and because of the developments in the area of IPv6 infrastructural components and software. Ignoring IPv6 will therefore eventually result in complex problems and vulnerabilities. In addition, issues in the area of performance and availability may arise and the total network and management costs may increase. Implementing IPv6 at a later stage will be more complex than migration or initiation at an early stage. Organizations are therefore advised to take timely decisions and to develop plans to avoid having to take remedial actions at a later stage, which would result in risks and security incidents due to time pressure and ill-considered plans.

Inhoud

1 Inleiding

Het doel van dit whitepaper is de lezer te informeren over IPv6, de kansen en mogelijkheden die het biedt en de beveiligingsaspecten waarmee rekening gehouden moet worden. Het whitepaper is bedoeld voor het business- en ICT- management van organisaties en bedrijven en moet voldoende basis leveren om weloverwogen besluiten te kunnen nemen over het beleid en de strategie die gevolgd moet worden ten aanzien van IP versie 6.

1.1 Leeswijzer

Dit document beschrijft het Internet Protocol versie 6 (IPv6). In **Hoofdstuk 1** wordt een algemene introductie gegeven met de historische achtergrond over het Internet Protocol (IP). Omdat niet iedere lezer gelijke technische kennis bezit wordt in de bijlagen A en B respectievelijk de werking van IP en de verschillen tussen IPv4 en IPv6 beschreven.

Hoofdstuk 2 beschrijft de kansen die ontstaan door gebruik te gaan maken van IPv6 en ook de mogelijke risico's. In **hoofdstuk 3** wordt dieper ingegaan op beveiliging in relatie tot IPv6. **Hoofdstuk 4** beschrijft de inbreng voor een business case. Technische aspecten en migratie komen aan de orde in **hoofdstuk 5**. Tot slot worden in **hoofdstuk 6** conclusies getrokken en aanbevelingen gedaan.

1.2 Publiek-private samenwerking

Dit whitepaper is een update van het whitepaper dat in 2007 is geschreven en gepubliceerd voor de deelnemers van de voorloper van het NCSC, GOVCERT.NL. In mei 2010, is dat whitepaper publiek gemaakt.
In 2013 is op initiatief van de Managed Service Providers ISAC en met behulp van 14 deskundigen uit publieke en private organisaties, met verschillende aandachtsgebieden, dit vernieuwde whitepaper tot stand gekomen.

1.3 Achtergrond

Eind jaren zestig van de twintigste eeuw is bij de ontwikkeling van het internet een protocolsuite ontstaan die TCP/IP wordt genoemd. Deze protocolsuite maakte het voor het eerst mogelijk om op brede schaal verschillende systemen met elkaar te laten communiceren. Als basis voor deze communicatie dient het Internet Protocol (IP). Elk apparaat dat is aangesloten op het Internet of een netwerk heeft een uniek nummer om zich te identificeren (IP-adres). Er is een verschil tussen interne IP-adressen die alleen geschikt zijn om te communiceren op een intern netwerk en publieke IP-adressen die nodig zijn voor communicatie op het Internet. De Interne IP-adressen worden verstrekt door systemen op het interne netwerk. De publieke IP-adressen worden verstrekt aan bedrijven door Internet Service Providers (ISP).

IPv4 bestaat uit adressen van 32 bits waardoor theoretisch bijna 4,3 miljard adressen mogelijk zijn. In de praktijk ligt dit aantal lager omdat een aantal reeksen gereserveerd zijn voor bijvoorbeeld het gebruik in interne en private netwerken of omdat ze gereserveerd zijn voor een andere toepassing.
Doordat het aantal en de dichtheid van Internetaansluitingen en dus de uitgifte van IPv4 adressen toeneemt, komt het totale aantal beschikbare adressen in het gedrang. Ook door een enorme toename van aan Internet gekoppelde consumentenelektronica, het zogenaamde 'Internet of things[5]', die allemaal een of soms zelfs meerdere publieke Internetadressen nodig hebben, is IPv4 uiteindelijk niet meer toereikend[6].

De Internet Engineering Task Force (IETF)[7], met als taak de standaardisatie van protocollen voor Internet, heeft in 1994 besloten een opvolger voor IPv4 te ontwikkelen[8]. Deze werd in eerste instantie IP Next Generation (IPng) genoemd en later IP versie 6 (IPv6). IP versie 5 is in de praktijk maar weinig gebruikt en om verwarring te voorkomen overgeslagen.

IPv4 adressen raken op

De eerste prognoses over het opraken van IPv4 adressen stammen uit 1994 en gaven toen 2008 als kritieke datum. Het verwachte moment waarop het dreigende tekort aan IPv4-adresruimte werkelijkheid wordt is in de loop van de tijd enigszins bijgesteld. Ironisch genoeg komen door het overgaan op IPv6 ook weer IPv4-adressen vrij. Dit aantal weegt echter niet op tegen de al maar groeiende behoefte aan adressen.

Het uitgeven van IPv4-adressen verloopt in meerdere stappen. De Internet Assigned Numbers Authority (IANA), de organisatie die wereldwijd verantwoordelijk is voor de uitgifte van IP-adresreeksen, heeft op 1 februari 2011 de laatste blokken IP-adressen uitgegeven aan Regionale Internet Registrars (RIR)[9]. De APNIC, de RIR voor Azië, Oceanië en Australië, is in april 2011 als eerste begonnen aan de uitgifte van de laatste beschikbare klasse van IPv4-adressen. In deze regio is het gebruik van IPv6 dan ook inmiddels gemeengoed. Op 14 september 2012 is RIPE NCC, de registrar voor Europa, begonnen

5 http://en.wikipedia.org/wiki/Internet_of_Things

6 Zie Hoofdstuk 5 – Hyperconnectiviteit, Cybersecuritybeeld Nederland 2013. https://www.ncsc.nl/actueel/nieuwsberichten/cybersecuritybeeld-nederland-kwetsbaarheid-van-ict-onverminderd-hoog.html

7 [http://www.ietf.org]

8 In Bijlage C is een overzicht te vinden van relevante RFCs met betrekking tot IPv6. Een Request For Comments (RFC) is een specificatie van een protocol dat door de IETF wordt opgesteld.

9 Organisaties die zorgdragen voor de allocatie en registratie van IP-adressen in een specifieke regio (APNIX, ARIN, LACNIC, RIPE NCC en AfriNIC)

aan de laatste reeks van IPv4 adressen. Een groep IPv4 adressen wordt alleen nog verstrekt aan organisaties die ook een IPv6 allocatie bezitten. Tenslotte zullen ook de Internet Service Providers, de bedrijven die organisaties en bedrijven toegang tot het internet bieden, door hun voorraad adressen raken. Wanneer dit zal plaatsvinden, verschilt per ISP.
Geoff Huston van APNIC (Asia-Pacific Network Information Centre) houdt een teller bij die voorspelt wanneer de voorraad IP-v4 adresblokken van de RIR's op zal zijn[8].

Dat er langer IPv4-adressen uitgegeven konden worden dan de eerdere verwachting dat in 2008 geen IPv4-adressen beschikbaar zouden zijn, is grotendeels te danken aan de tussenoplossing in de vorm van toepassen van Network Address Translation (NAT). Hiermee kunnen meerdere systemen op het internet worden aangesloten via één publiek IP-adres. «

IPv4 rapport

Report generated at 08-Oct-2013.

IANA Unallocated Address Pool Exhaustion	
	Exhaustion Date
	03-Feb-2011

Projected RIR Address Pool Exhaustion Dates:		
RIR	**Projected Exhaustion Date**	**Remaining Addresses in RIR Pool (/8s)**
APNIC	**19-Apr-2011**	0.8311
RIPE NCC	**14-Sep-2012**	0.8624
ARIN	**16-Jan-2015**	1.7434
LACNIC	**26-Apr-2015**	1.8914
AFRINIC	**14-Aug-2022**	3.5642

Figuur 1-1. Bron: Geoff Huston, IPv4 adress report.

10 Zie http://www.potaroo.net/tools/ipv4/index.html

2 Kansen en risico's van IPv6

In de inleiding is te lezen dat IPv6 in soft- en hardware geïntegreerd wordt/is, dat in delen van de wereld websites en onlinediensten in toenemende mate overgaan op communicatie via IPv6 en dat overheidsdiensten, bijvoorbeeld in de VS, al gefaseerd over gaan. Hierdoor is duidelijk dat de ontwikkelingen doorgaan en als men niet in een communicatie isolement terecht wil komen of onvoorziene beveiligingsrisico's wil lopen een besluit over IPv6 genomen moet worden.

2.1 Kansen

Een van de belangrijkste redenen om over te stappen op IPv6 is het geringe adressenbereik van het huidige IPv4-protocol. Nieuwe publieke IPv4-adressen worden in zeer beperkte mate uitgegeven. Zeker als de volgende "disruptive technology" zijn opwachting maakt: het "Internet of Things, anything connected". Het koppelen van bijvoorbeeld koelkasten, auto's, elektriciteitsmeters en dergelijke aan het internet zal een grote vlucht nemen naarmate steeds meer apparaten op afstand uitgelezen en/of bediend moeten kunnen worden. Al deze apparaten moeten kunnen communiceren met achterliggende Internetdiensten, bijvoorbeeld om informatie uit te wisselen of nieuwe firmware te laden, waardoor een unieke kans ontstaat voor vernieuwende businessmodellen.

In een groot deel van Azië en Australië zijn IPv4-adressen op en worden bijvoorbeeld nieuwe gebruikersdiensten gekoppeld via IPv6. Raadplegen van de 'oude' IPv4 websites en diensten is daardoor moeilijk. Als een bedrijf of organisatie zaken doet met deze regio is het zeker van belang om een migratie in gang te zetten. Business partners in deze regio's zullen al grotendeels overgeschakeld zijn.

Nieuwe technische ontwikkelingen worden waarschijnlijk primair op IPv6 gebaseerd en ondersteuning voor IPv4 zal dan worden afgebouwd. Echter zullen ook oudere applicaties of apparatuur, die niet met IPv6 overweg kunnen, voorlopig in gebruik blijven. De meeste migraties bevatten daarom het plan om een periode 'dual stack' te acteren waarmee bedoeld wordt dat IPv6 en IPv4 naast elkaar gebruikt worden.

2.2 Risico's

Het grootste risico is dat IPv6 wordt beschouwd als 'gewoon een update van IPv4', en dat het daarom slechts een technische aangelegenheid is. IPv6 is weliswaar ontwikkeld als vervanging van IPv4, maar is dusdanig anders, dat het hele business model van een organisatie en de wijze waarop de dienstverlening is ingericht mogelijk geraakt wordt door implementatie. Een migratie zonder al te veel problemen moet daarom goed doordacht en gepland worden waarvoor een tijdige start noodzakelijk is.
IPv6 verschilt wezenlijk van IPv4 waardoor het zeer waarschijnlijk is dat binnen de organisatie onvoldoende kennis voor implementatie en beheer aanwezig is. Implementatie van IPv6 vanuit de kennis over IPv4 kan leiden tot situaties waarin men onvoldoende in control is over in- en uitgaand netwerkverkeer. Dit risico werkt ook door in de aanschaf van nieuwe netwerkapparatuur die al IPv6 'ready' is en verbindingen toestaat over dit protocol zonder dat de organisatie daarvan op de hoogte is. Hierdoor kan het zijn dat het beveiligingsniveau van de ICT infrastructuur via IPv4 weliswaar voldoende is maar dat het via IPv6 onbedoeld 'open' staat. Op pc's en laptops, die uitgerust zijn met Microsoft Windows 7 of 8, staat IPv6 standaard aan. Omdat IPv6 in die installaties de voorkeur heeft boven IPv4,
zal communicatie in eerste instantie met IPv6 opgestart worden. Dit wordt mogelijk gedaan door gebruik te maken van encryptietunnels, waarbij IPv6 verkeer over het bestaande IPv4 netwerk wordt geleid in een versleutelde IPv4 tunnel, waardoor veel firewalls niet eens doorhebben dat IPv6 communicatie opgezet wordt en ook de inhoud niet kan controleren.

Nummerplan

De opbouw van IP-adressen van IPv6 is complexer dan IPv4. Voor de start van de ingebruikname is het daarom noodzakelijk om een goed doordachte architectuur uit te werken. SURFnet heeft hiervoor een nummerplan[9] document opgesteld dat een leidraad en hulpmiddel hierbij kan zijn.

Conventionele beveiligingstechnieken en middelen die gestoeld zijn op IPv4 moeten geconfigureerd worden om ook IPv6-verkeer te monitoren dan wel te analyseren. Apparaten kunnen bijvoorbeeld over meerdere IPv6-adressen beschikken en omdat de opbouw van IPv6-adressen complexer en moeilijker te herleiden is dan bij IPv4 is het ook moeilijker om te bepalen in een log welk adres bij welk apparaat hoort?

2.3 Analyse

Belangrijkste vraag is welke impact IPv6 heeft op de bedrijfscontinuïteit van de organisatie. Door groei van (zakelijke) toepassingen en gekoppelde apparaten neemt die impact alleen maar toe. IPv6 is een 'technology push' met grote invloed op ICT- en, door nieuwe diensten en functionaliteiten, ook bedrijfsprocessen. Hoewel het binnen bedrijfsprocessen voornamelijk om 'functionaliteit' gaat is IPv6 een technische component die invloed daarop uitoefent en dus merkbaar is. Het is ondoenlijk om hier een opsomming van alle mogelijke risico's te geven. Dit hangt uiteraard ook sterk af van de

11 http://www.surfnet.nl/documents/rapport_201309_IPv6_numplan_NL.pdf

organisatie, maar om de risico's in beeld te krijgen en om een besluit over de te volgen strategie te plannen volgt hier een (beperkte) opsomming van afwegingen:

- Wat doen mijn klanten/leveranciers/partners/outsourcingpartijen/concurrenten? Gaan zij of hebben zij gepland om over te gaan op IPv6 en zo ja, wanneer?
- Is er voldoende kennis intern of moet personeel getraind worden of ingehuurd?
- Wat doen de leveranciers van netwerkapparatuur, systemen en applicaties? Kunnen deze ondersteuning verlenen voor de implementatie / uitrol van IPv6?
- Wat zijn de eisen van de betreffende toezichthouder (bijvoorbeeld De Nederlandsche Bank (DNB), Autoriteit Consument en Markt (ACM), enz.?
- Welke apparatuur en software zijn al aanwezig of in gebruik met IPv6-technologie?
- Kunnen de standaard of maatwerkapplicaties omgaan met IPv6?
- Welke activiteiten komen er uit business development?
- Wat is de verwachte groei in ICT diensten?
- Zijn er integraties (fusies) te verwachten? «

3 IPv6 en beveiliging

IPv6 heeft niet alleen technische consequenties voor beveiliging maar ook gevolgen voor de organisatie van beveiliging. Door het in gebruik nemen van IPv6 ontstaat de mogelijkheid om nieuwe toepassingen of diensten te ontwikkelen waardoor een herziening van het beveiligingsbeleid en de risicoanalyses noodzakelijk zijn. Met IPv6 ontstaat de mogelijkheid om een veelvoud aan apparatuur aan het Internet te koppelen waardoor de perimeter, de punten waarop het bedrijfsnetwerk met Internet is gekoppeld, veranderd. De wijze waarop beveiliging is ingericht en waarop security management is georganiseerd zal daarom herzien moeten worden.

Risicoanalyses

In de risicoanalyses die een organisatie uitvoert moet terdege rekening worden gehouden met communicatie via IPv4 én IPv6. Daarbij moet ook meegenomen worden dat er communicatie via andere dan de tot nog toe gebruikelijke wegen plaatsvindt. Zo kunnen meer en/of andere apparaten aan het Internet gekoppeld zijn die ook bedrijfsgegevens bevatten of ook met het interne netwerk communiceren. Apparaten kunnen meerdere IP-adressen bezitten en die gebruiken voor verschillende toepassingen zoals tegelijkertijd intern en extern communiceren. In de schadescenario's van een risicoanalyse heeft dit invloed op de wijze en de kans waarop schade ontstaat. Uit de risicoanalyses kan bijvoorbeeld blijken dat een situatie is ontstaan waarbij de beveiliging van de 'buitenkant' van het interne netwerk lastiger is uit te voeren omdat een diversiteit aan apparatuur aan het Internet gekoppeld is die ook op enigerlei wijze connectie kan maken met de interne ICT infrastructuur. Het beveiligingsbeleid en de toekenning van autorisaties aan apparatuur en gebruikers moeten goed worden doordacht en opnieuw worden opgezet.

De technische security assessments, bijvoorbeeld penetratietesten, zijn tot nu toe voornamelijk gericht op IPv4 communicatie en diensten. Als deze assessments periodiek worden uitgevoerd moet hierin ook rekening gehouden worden met IPv6.

Dreigingen

Dreigingen waaraan netwerken, internet diensten en apparatuur bloot gesteld worden veranderen niet bij het gebruik van IPv4 of IPv6 en dat geldt ook voor de beveiliging. Aanvallen zoals sniffing, flooding en man-in-the-middle-aanvallen, zijn voor beide versies relevant. Ook aanvallen op de applicatielaag en het gebruik van illegale apparatuur op het netwerk (rogue devices) zijn in IPv6 net zo goed mogelijk als in IPv4.

In het gebruik van IPv6 schuilen echter een aantal gevaren die niet spelen bij IPv4. Niet alle in gebruik zijnde firewalls ondersteunen op dit moment volledig IPv6 of zelfs helemaal niet. De vraag is dan wat er met IPv6-verkeer gebeurt, met andere woorden wat is de standaard instelling van de firewall voor IPv6? Er bestaan voorbeelden van firewalls die IPv6 niet ondersteunen maar het IPv6-verkeer wel doorlaten. Daarnaast bestaan er beveiligingssystemen die IPv6 wel ondersteunen en ook standaard aan hebben staan. In dat geval is het van belang te weten wat de standaard instellingen zijn en op welke wijze dit verkeer wordt bewaakt en gefilterd. Een gerelateerd probleem is dat veel systemen, waaronder werkstations, al IPv6 ondersteunen. Het is in dit geval wellicht mogelijk om IPv6-verkeer te 'verpakken in een versleutelde tunnel die op het IPv4 netwerk door de beveiligingssystemen naar buiten en naar binnen communiceert. De firewall en andere beveiligingssystemen kunnen dan de inhoud van het verkeer niet beoordelen waardoor een open verbinding naar het internet gerealiseerd wordt.

Beveiligingsvoordelen

Een van de voordelen van IPv6 is dat geëist wordt dat IPv6-systemen met IPsec-encryptie en tunneling kunnen omgaan. Dit leidt tot een bredere toepassing van IPsec. Dit IPsec-protocol zorgt voor betere beveiliging tegen aanvallen als 'IP-spoofing' en 'TCP sequence number prediction'. Echter, het is niet zo dat IPsec een algemene oplossing is voor alle beveiligingsproblemen, hoewel het wel vaak gezien wordt als zodanig. Een van de belangrijkste factoren die de sterkte van een op vercijfering gebaseerde oplossing bepalen is het sleutelbeheer. Voor IPsec in IPv6 zijn geen eisen vastgelegd. IPsec zelf beschrijft wel een aantal methoden voor sleutelbeheer die gebruikt kunnen worden. Bij het implementeren van IPsec op basis van IPv6 moet het sleutelbeheer dus op een goede manier geïmplementeerd worden[10].

Daarnaast bestaan talloze andere beveiligingsprotocollen die veel gebruikt worden zoals SSL/TLS en Kerberos. Deze zijn hetzelfde gebleven aangezien ze geïmplementeerd worden bovenop het Internet Protocol.

Nieuwe ontwikkelingen

IPv6 maakt veel nieuwe ontwikkelingen mogelijk, het is meer geschikt voor mobiliteit van draagbare apparatuur en zogenaamd ad-hoc netwerken. Deze zullen naar verloop van tijd steeds meer ondersteund worden, maar zullen, zoals elke nieuwe toepassing, ook mogelijk nieuwe dreigingen introduceren. Wel geldt dat bij de

12 NIST publication: Guidelines for the Secure Deployment of IPv6. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=907211

ontwikkeling van nieuwe toepassingen steeds meer aandacht komt voor beveiliging.

Beveiliging en IPv4 – IPv6 transitie

De transitie van een puur IPv4 netwerk en een netwerk waarbinnen IPv4 en IPv6 gebruikt worden creëert een aantal aandachtspunten ten aanzien van beveiliging die nader onderzocht moeten worden. Als beveiligingsmaatregelen enkel ingesteld zijn op IPv4 zijn deze vaak niet effectief voor IPv6 communicatie. Ook de eerder beschreven tunneling van IPv6 verkeer via IPv4 is een aandachtspunt waartegen maatregelen toegepast moeten worden. Meer beveiligingsoverwegingen met betrekking tot deze situatie zijn opgesomd in het IETF paper: 'IPv6 Transition/Co-existence Security Considerations'[11].

Als hard- en/of software die in een IPv4-netwerk aanwezig zijn, (standaard) IPv6 ondersteunen, kan het zo zijn dat via 'stateless autoconfiguration' ongemerkt IPv6-verbindingen worden opgezet. Hierdoor ontstaan mogelijk gaten in de beveiliging, bijvoorbeeld door een inadequaat filter in een firewall.
Sommige leveranciers van producten die nu al IPv6 ondersteunen, geven aan dat het uitschakelen van IPv6 tot problemen in ondersteuning zou kunnen leiden. Dit vereist dat een weloverwogen architectuur wordt opgezet en hard- en softwarecomponenten bewust geconfigureerd worden vanwege eerder genoemde security-implicaties.

Het belangrijkste aandachtspunt ten aanzien van de veiligheid van IPv6 is dat het nog relatief nieuw is. Hoewel veel onderzoeken naar kwetsbaarheden in IPv6-implementaties hebben plaatsgevonden, waarbij ook kwetsbaarheden zijn gevonden, is de kans groot dat in de nabije toekomst nog nieuwe fouten worden ontdekt zoals dat bij iedere nieuwe technologie gebeurt. «

13 http://www.ietf.org/rfc/rfc4942.txt.pdf

4 Inbreng voor Business case

Adoptie van IPv6 door de gehele organisatie is cruciaal. Ondersteuning voor een doelgerichte aanpak door het opstellen van een business case kan daarmee helpen.

IPv6 is geen doel op zich maar een middel voor communicatie en dienstverlening en zou als zodanig deel uit moeten maken van een bedrijfsbrede strategie. Een overzicht van het applicatielandschap helpt bij het in kaart brengen van de specifieke wensen en risico's. Ook zullen alle stakeholders geïdentificeerd moeten worden om die in een vroeg stadium bij de plannen te kunnen betrekken.

In de business case kunnen de geïdentificeerde kansen opgenomen worden (denk bijvoorbeeld aan verbetering van netwerkperformance of mogelijkheden voor nieuwe diensten en werkmethodes) maar ook de onderkende risico's. Zorg dat in de business case rekening gehouden wordt met het opbouwen van benodigde kennis rondom IPv6. Laat commerciële argumenten van leveranciers niet leidend zijn maar baseer de business case op realistische en voor de business relevante argumenten.

4.1 Scenario's

Er zijn drie scenario's denkbaar over hoe om te gaan met IPv6:

Niets doen

Het eerste scenario, niets doen, is eigenlijk geen optie meer. Nieuwe apparatuur en software ondersteunen standaard al IPv6 waardoor beveiligingsrisico's ontstaan. IPv6 uitschakelen heeft vaak gevolgen voor ondersteuning door de leverancier. Uiteindelijk zullen ook leveranciers, klanten en andere organisaties de stap zetten naar communicatie m.b.v. IPv6 waardoor de organisatie geïsoleerd raakt.

'Big bang'

Het tweede scenario is een zogenaamde 'big bang' waarbij alles in één keer volledig gemigreerd wordt van IPv4 naar IPv6. Dit scenario lijkt alleen mogelijk voor kleinere organisaties met relatief weinig ICT-middelen en een goede en accurate configuratiedatabase (CMDB). Voor het besluit tot dit scenario zal een gedegen risicoanalyse uitgevoerd moeten worden om te beoordelen of alle apparatuur en software geschikt is om communicatie via IPv6 te laten verlopen en of communicatie in de (primaire) bedrijfsprocessen problemen gaat ondervinden als in één keer wordt gemigreerd.

'Dual-stack'

Het derde en meest waarschijnlijke scenario bestaat uit een 'dual-stack' periode. Een tijdlang zullen IPv4 en IPv6 naast elkaar gebruikt worden. Beide protocollen kunnen naast elkaar op dezelfde infrastructuur bestaan. Wel zullen ondersteunende ICT-diensten als DNS en DHCP aangepast moeten worden om ook IPv6 te ondersteunen. IPv6 zal in deze situatie meestal voor externe communicatie gebruikt worden en IPv4 voor de interne communicatie.

Proof of Concept

Bij het toepassen van een van de scenario's is het raadzaam om in eerste instantie te beginnen met een 'Proof of Concept' (PoC) waarbij in een kleine, begrensde omgeving kennis en ervaring rondom de inrichting en beheer van IPv6 wordt opgebouwd. Het is daarbij wel van belang dat de hele keten van netwerk, operating system en applicatie een goed beeld geven van de totale infrastructuur en in de PoC worden meegenomen. Nadat de PoC gedraaid heeft volgt een evaluatie waarna de business case en een verdere aanpak worden uitgewerkt.

In hoofdstuk 5 wordt op technisch gebied nader ingegaan op de scenario's en migratie aandachtspunten.

4.2 Ondersteuning migratie IPv6

Om een volledige migratie naar IPv6 mogelijk te maken is het noodzakelijk dat op verschillende niveaus het protocol wordt ondersteund. Op de lagen onder IP, dus de linklaag en de fysieke laag, hoeft meestal niets te gebeuren. Voor switches, hubs, netwerkkaarten en dergelijke is het IP-protocol namelijk niet zichtbaar. Sommige switches (layer 2,5 switches) en andere apparatuur maken wel gebruik van IP, namelijk voor beheertoepassingen.

Moderne routers ondersteunen IPv6, zij het niet altijd voor alle toepassingen en ook niet altijd in alle mogelijke configuratiecombinaties. Voor firewalls geldt een vergelijkbare situatie. Vaak is het zo dat IPv6-ondersteuning in de configuratie-interface is weggestopt.

Voor besturingssystemen geldt dat de meeste Unix-varianten zoals Linux (waaronder Ubuntu, Fedora etc.), Sun Solaris, FreeBSD, en OpenBSD al jaren een stabiele IPv6-ondersteuning geïntegreerd hebben. Voor andere besturingssystemen is dit een ander verhaal. Windows ondersteunt IPv6 in Windows Vista, Windows Server 2008, Windows server 2008 R2, Windows server 2012, Windows 7 en Windows 8. Mac OS X is gebaseerd op BSD en ondersteunt dus ook IPv6 op vergelijkbaar niveau als Free- en OpenBSD.

De meeste applicaties op de verschillende Unix versies ondersteunen IPv6 vaak volledig. Een statusoverzicht van de ondersteuning van IPv6 op Unix is te vinden op http://www.deepspace6.net/docs/ipv6_status_page_apps.html. Dit betreft veelal opensource-applica-

ties. Belangrijke serverapplicaties zoals Apache (webserver), Bind (DNS server), Sendmail, Postfix (mailservers), SSH (secure remote access); maar ook belangrijke clientapplicaties zoals Firefox (web browser), Kmail, Evolution (mail clients) ondersteunen IPv6. Voor commerciële applicaties geldt dat ondersteuning in het algemeen een stuk minder is.

De veelgebruikte Windows applicaties kunnen ook met IPv6 omgaan, zoals Exchange 2010 en 2013, Web Server (IIS) en Internet Explorer 6 (en hoger). Let op: de juiste werking van maatwerk-software of zelf ontwikkelde applicaties zal uiteraard uitvoerig getest moeten worden.

Voor diensten op internet geldt dat de meeste nog op basis van IPv4 beschikbaar zijn. Wel is het op het moment mogelijk om DNS-diensten wereldwijd aan te bieden op basis van IPv6.

Task Force IPv6

In opdracht van het ministerie van Economische Zaken is de Nederlandse Task Force IPv6 opgericht. Het doel van de task force is om bewustwording te creëren over het nut en de noodzaak van IPv6. Ook wil de task force een platform zijn om kennis over de toepassing en invoering van IPv6 uit te wisselen. Informatie over de Nederlandse Task Force IPv6 is te vinden op de website[12].

14 http://www.ipv6-taskforce.nl

5 Technische aspecten

Hoewel beide, IPv4 en IPv6, bedoeld zijn om datapakketjes van een afzender richting een ontvanger te krijgen, zijn de verschillen dusdanig groot dat een IPv4 aanpak niet zal werken op een IPv6 omgeving. Enkele belangrijke aspecten zijn dat IPv4 en IPv6 een andere adressering hanteren en daardoor niet zondermeer uitwisselbaar zijn, dat IPv6 sterk leunt op het gebruik van DNS, dat een DHCP-server niet per se nodig is om connectiviteit te verkrijgen en dat één systeem meerdere IP-adressen kan gebruiken. Daarom is het noodzakelijk goed na te denken als het scenario van 'voorlopige dual stack' gevolgd wordt of gemigreerd wordt van IPv4 naar IPv6.

5.1 Toelichting

Veel netwerk apparatuur en software is "IPv6-Ready", maar wat is dat eigenlijk? Hier is geen standaard voor en dat kan zorgen voor nogal wat hoofdbrekens bij de technische implementatie. In sommige gevallen wil "IPv6-Ready" zeggen dat een dual-stack aanwezig is, dus dat IPv4 en IPv6 naast elkaar draaien. Daarbij kan het zijn dat IPv6 al standaard aan staat met een aantal default instellingen, of dat IPv6 aangezet kan worden. "IPv6-Ready" kan ook betekenen dat het betreffende apparaat technisch (hardware) in staat is om IPv6 te praten, maar de daarvoor benodigde software (nog) niet bevat. Ook andersom, het kan zijn dat de software al wel met IPv6 kan omgaan, maar de onderliggende hardware nog niet optimaal is, waardoor u wordt geconfronteerd met verminderde performance en minder features. U moet zich dus goed inlezen op de specificaties van in te zetten apparatuur en software om een gedegen technische implementatie aanpak te kunnen opstellen. Opbouwen van benodigde kennis kan via de Nederlandse Task Force IPv6 of via cursussen, conferenties en internet fora (maar probeer wel mythe van werkelijkheid te scheiden, vooral bij internet fora).

5.2 Oplossingsrichtingen

Op dit moment is het gebruik van IPv6 nog beperkt. Doordat in Europa en in andere delen van de wereld IPv4 adressen niet meer uitgegeven worden zal naar verwachting het gebruik toenemen. Het is zeer onwaarschijnlijk dat er een moment komt waarop het hele internet zal worden omgeschakeld naar IPv6. Om toch migratie naar IPv6 te laten plaatsvinden, op een wijze zoals de in hoofdstuk 5 omschreven scenario's, zijn een aantal oplossingen ontwikkeld.

1. De belangrijkste eigenschap is dat IPv4 en IPv6 naast elkaar kunnen bestaan binnen een netwerk. Ze functioneren onafhankelijk van elkaar en storen elkaar niet. De meeste netwerken die IPv6 ondersteunen, ondersteunen ook IPv4. Sterker nog, dit geldt ook op systeemniveau. Wanneer systemen zowel IPv4 als IPv6 kunnen gebruiken spreekt men van een *dual stack*. Applicaties kunnen dus kiezen of ze gebruik maken van IPv4 of IPv6. Echter, wanneer een applicatie IPv6 ondersteunt, kan dit volledig transparant zijn en is het afhankelijk van de partij waarmee het communiceert of IPv4 of IPv6 wordt gebruikt. De socket API[13] voor IPv6 handelt dit transparant af. Met deze aantekening dat de functies die hiervoor gebruikt worden, anders zijn dan van de oude socket API voor IPv4. Dit betekent dat de applicatie gewijzigd moeten worden.

2. Wanneer IPv6-functionaliteit aan het netwerk wordt toegevoegd, is het ook noodzakelijk dat alle ondersteunende diensten (zoals DNS en DHCP) IPv6 gaan ondersteunen. Voor DNS betekent dit dat een 'vertaling' nodig is tussen hostnamen en IPv6-adressen en vice versa. Hiervoor is een nieuw type DNS-entry gedefinieerd, het AAAA-veld (quad-A). DHCP echter kan in dezelfde vorm gebruikt worden voor IPv6, of er kan gebruik gemaakt worden van stateless autoconfiguratie.

3. Daarnaast moeten intelligente netwerkelementen zoals routers ook IPv6 ondersteunen, onder andere in verband met de benodigde nieuwe routeringsprotocollen. IPv6 gebruikt bijvoorbeeld geen IGMP-berichten[14] meer voor multicast-routering, waardoor oudere switches het multicastverkeer niet doorsturen. IPv4-routeringsprotocollen zoals OSPFv2 moeten ook upgraden (naar OSPFv3).

4. In het nummerplan moet rekening worden gehouden met het feit dat bij de keuze voor public range IP-adressen, alle systemen rechtstreeks met andere IPv6-systemen op het internet kunnen communiceren. De afscherming met internetverkeer dat bij private range IPv4-adressen hoort is dan niet meer aanwezig en dat zal via een firewall gecompenseerd moeten worden.

15 De Socket API is de programmeerinterface die door applicaties kan worden gebruikt om functionaliteit voor netwerkcommunicatie op basis van onder andere TCP/IP aan te roepen.

16 Internet Group Management Protocol. IPv6 gebruikt wel een soortgelijk protocol: Multicast Listener Discovery(MLD)

5.3 Migratie op netwerkniveau

Op netwerkniveau bestaan verschillende manieren om IPv6-netwerken te koppelen zonder dat alle tussenliggende systemen het ondersteunen. De belangrijkste zijn:

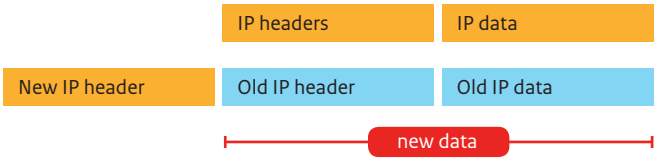
- Tunnelen;
- Network Address Translation and Protocol Translation (NAT-PT, NAT64, DNS64);
- Proxying;
- IPv4-mapped-IPv6-adressen.

5.3.1 *Tunnelen*

Het verpakken van het ene type verkeer in een ander type verkeer wordt tunnelen genoemd. Dit is een generieke methodiek die ook voor IPv6 kan wordt toegepast. Om twee IPv6-netwerken te kunnen koppelen over een IPv4-verbinding moet een tunnel opgezet worden zodat de IPv6-pakketten worden geëncapsuleerd in IPv4 pakketten. Het is ook mogelijk om dit op systeemniveau toe te passen. Tunnelen is een eenvoudige oplossing die volledig transparant is voor applicaties en weinig tot geen beperkingen oplevert. Dit is momenteel de meest gebruikte manier om IPv6-netwerken te koppelen. Er zijn verschillende methoden om tunnels op te zetten:

- Configured. Hierbij worden handmatig tunnels geconfigureerd tussen verschillende eindpunten.
- Teredo. Een door Microsoft ontwikkelt tunneling protocol. Dit systeem tunnelt IPv6-verkeer in UDP-pakketten die met IPv4 worden verstuurd. Dit protocol maakt het ook mogelijk om door NAT-apparaten te tunnelen. Overigens zijn er naast Teredo nog meerdere tunnelingprotocollen[15].
- 6to4. Dit is een methode voor het automatisch tunnelen van IPv6-verkeer over IPv4-verkeer.
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). Dit protocol kan binnen een site tunneling van IPv6 over IPv4 automatiseren, zonder dat op IPv4 niveau multicast vereist is.

Ook is het mogelijk om IPv4-verkeer in IPv6 te tunnelen. Hoewel dit nu weinig voorkomt, zal het in de toekomst vaker noodzakelijk zijn vanwege de schaarste aan IPv4-adressen. Wanneer dan nieuwe systemen aan internet moeten worden gekoppeld, kan dit alleen nog op basis van IPv6. Om het toch mogelijk te maken dat dergelijke systemen via IPv4-systemen kunnen praten is een IPv4 in IPv6-tunnel een oplossing.



Figuur 5-1 IP-tunnelling.

Er schuilt wel een risico in het gebruik van tunnelen, hoewel dit niet specifiek is voor IPv6. Bij uitwisselen van getunneld verkeer, heeft een firewall meestal geen of beperkt inzicht op wát wordt uitgewisseld. Tunnels kunnen dan 'covert channels' worden. Het kan dan zomaar gebeuren dat informatie wordt uitgewisseld zonder dat beveiligingsmaatregelen dit waarnemen. Ook kunnen allerlei diensten die de firewall normaliter tegenhoudt wel via een tunnel aangeboden worden. Het gebruik van bijvoorbeeld Teredo, of andere tunneltechnieken, versterkt dit gevaar doordat het automatisch tunnels kan opzetten die firewalls passeren.

5.3.2 *NATPT en proxying*

Vergelijkbaar met NAT is het ook goed mogelijk om IPv6-pakketten te vertalen in IPv4-pakketten en vice versa. Hiervoor is een systeem (een gateway of router) noodzakelijk die de vertaling uitvoert. Op deze manier kan een IPv4-host met een IPv6-host communiceren. Dit proces wordt Network Address Translation and Protocol Translation (NAT-PT) genoemd, maar dit wordt tegenwoordig als verouderd en achterhaald beschouwd[16].

Gebruik maken van proxies is een vergelijkbaar principe en het is een bruikbare optie. Een proxy moet dan aan de ene kant IPv6 ondersteunen en aan de andere kant IPv4. Het verschil tussen deze twee oplossingen is dat NAT-PT de vertaling voor alle toepassingen regelt en dat dit redelijk transparant is voor applicaties. Proxies zijn applicatiespecifiek met als gevolg dat applicaties moeten kunnen omgaan met proxies en daarvoor dus geconfigureerd moeten worden.

5.3.3 *IPv4-mapped-IPv6*

Een andere oplossing is dat IPv4-mapped-IPv6-adressen het mogelijk maken om IPv6-applicaties op een simpele manier met IPv4-applicaties te laten communiceren. IPv4-adressen worden in het IPv6-systeem omgezet in IPv6-adressen. Hiervoor is een specifieke range van adressen gereserveerd, waarin het IPv4-adres is geëncapsuleerd. Dit heeft de vorm ::ffff:<ipv4adr>. Bijvoorbeeld het IPv4 adres 192.0.2.12 wordt dan ::ffff:192.0.2.12.

5.4 Ondersteuning IPv6 in applicaties

Voor applicaties die IPv6 willen ondersteunen, betekent dit dat specifieke functieaanroepen in de broncode moeten worden omgeschreven naar de nieuwe socket API die ook IPv6 ondersteund. Voor veel implementaties is dit proces grotendeels te automatiseren[17]. Het gaat namelijk om een beperkt aantal functies en datastructuren die veranderd zijn en die op een beperkt aantal plaatsen gebruikt worden. Deze nieuwe API maakt het dan tevens mogelijk om vrijwel transparant te kiezen uit IPv4 of IPv6, al naar gelang wat de wederpartij ondersteunt.

17 Zie voor een overzicht aan tunnelingprotocollen: http://tools.ietf.org/pdf/draft-steffann-tunnels-04.pdf

18 Zie http://tools.ietf.org/html/rfc4966, "Reasons to Move NAT-PT to Historic Status"

19 In de meeste gevallen zal het met behulp van een automatisch script eenvoudig om te zetten zijn. Echter er kunnen aspecten in de code voorkomen die niet direct te mappen zijn. Hierbij valt bijvoorbeeld te denken aan het gebruik van broadcast-adressen.

5.5 Mogelijk migratiepad

Het meest gehoorde argument voor migratie naar IPv6 is 'Internet presence', of anders wel communicatie met IPv6-websites op het internet. Deze functionaliteit kan relatief kleinschalig ingevoerd worden aan de rand van de infrastructuur, en kan als springplank gebruikt worden voor navolgende implementaties. Een ander voordeel is dat hiermee praktische ervaring wordt opgedaan. De realisatie hiervan kan door een 'dual stack' DMZ te maken, of het toepassen van 6to4 gateways. Voordeel hiervan is dat de geleverde diensten IPv6 enabled kunnen zijn zonder dat een operationeel risico wordt genomen door de rest van het, vaak veel complexere, interne netwerk te migreren.

Vervolgens kan de volgende stap in het migratiepad zijn om het interne netwerk te migreren naar een dual stack. Dat wil zeggen dat infrastructuurcomponenten zoals routers en besturingssystemen, waar mogelijk, geschikt gemaakt worden voor IPv6 zodat deze voorzien kunnen worden van een dito adres. Er moet dan een IPv6-nummerplan voor het hele netwerk komen. Houdt er rekening mee dat IPv6-adressen in principe altijd globaal zijn en dus rechtstreeks met andere systemen op het internet kunnen communiceren. Dit is een rechtstreeks gevolg van het niet meer in gebruik zijn van NAT.

IPv6 adressen zijn er ook in de lokale variant (zogenaamde unique local adresses) waarbij communicatie met systemen op het internet via deze IPv6 adressen niet mogelijk is. Het bijzondere aan IPv6 is dat apparaten meerdere IPv6 adressen (kunnen) hebben, een mix van lokale en globale adressen. Edge firewalls kunnen de communicatie naar systemen op het internet over IPv6 nog steeds blokkeren, zoals dat ook kan op IPv4.

Vervolgens dienen zoveel mogelijk basisdiensten te migreren naar een oplossing die zowel IPv4 als IPv6 ondersteunt. Het betreft hier voornamelijk de onderdelen als DNS, interne mail-servers en beheerapplicaties.

Daarna kunnen ook de overige interne services worden opgewaardeerd. Stap voor stap kan zo de migratie getest worden zonder de huidige faciliteiten te verstoren. Als de migratie intern geregeld is kan een organisatie een IPv6-verbinding naar het internet realiseren. Daarmee kan een organisatie eventueel diensten aanbieden en afnemen op basis van IPv6.

Een directe aanleiding om IPv6 te implementeren bestaat, vanuit ICT beheer gezien, niet voor de meeste netwerkomgevingen. Wel is het verstandig om alvast een migratie voor te bereiden, omdat het op enig moment, gedreven vanuit de bedrijfsprocessen, het zover zal komen. Houd bij de voorbereiding in ieder geval rekening met:

- kennisopbouw;
- inventariseren van te migreren spullen;
- IPv6-support van de infrastructuurcomponenten.

NB. Houd bij de aanschaf van nieuwe diensten en applicaties alvast rekening met een migratie naar IPv6. Dit geldt vooral voor componenten die voor langere tijd aangeschaft worden. Nieuwe routers en switches zijn al gereed voor IPv6. Een aandachtspunt daarbij is welke diensten (services) over deze netwerkcomponenten getransporteerd moeten worden. Dit is namelijk van invloed op de benodigde firmware van deze componenten.

Voor ISP's staat in [RFC 4779] beschreven hoe IPv6 wordt geïmplementeerd.

6 Conclusies

Met nieuw aangeschafte apparatuur en software is IPv6 geïntroduceerd in de ICT-infrastructuur. Ondanks dat vanuit ICT-beheer gezien de noodzaak tot een migratie niet aanwezig lijkt moet vanuit beveiligingsoogpunt wel rekening ermee gehouden worden. Security management, risicoanalyses en technische security assessments kunnen niet meer om IPv6 heen en zullen moeten worden aangepast aan de situatie om te voorkomen dat kwetsbaarheden ontstaan doordat IPv6 communicatie 'onder de radar' plaatsvindt.

De grootste drijfveer voor organisaties en bedrijven om IPv6 in gebruik te nemen is dat IPv4 adressen niet meer of zeer beperkt worden uitgegeven. In Europa, Azië en Australië is dit al het geval waardoor het aandeel van IPv6 websites en diensten in deze regio's gaat toenemen. Om te zorgen dat communicatie en bereikbaarheid binnen deze gebieden optimaal blijft is het belangrijk om een plan te ontwikkelen voor het gebruik van IPv6.

IPv6 in gebruik

IPv6 biedt ook kansen voor het ontwikkelen van nieuwe diensten doordat de hoeveelheid mogelijke adressen bijna onuitputtelijk is en alle mogelijke apparatuur aan het Internet gekoppeld kan worden met één of meerdere IP-adressen. Nieuwe toepassingen en diensten, van leveranciers of afnemers of naar aanleiding van wensen van klanten, zullen het gebruik van IPv6 gaan afdwingen.

Een combinatie van IPv6 en IPv4, dual stack, lijkt de meest voor de hand liggende oplossing om te migreren en het is waarschijnlijk dat deze combinatie zeer lange tijd naast elkaar zal blijven bestaan. Om deze combinatie mogelijk te maken, zijn een groot aantal migratiemogelijkheden voor IPv6 ontworpen, waarbij elke migratievorm voor- en nadelen heeft. De keuze voor een migratievorm is sterk afhankelijk van de situatie.

Beveiliging

Wat beveiliging betreft: Het is belangrijk de wijze van risicoanalyses en security assessments aan te passen en rekening te houden met de (latente) aanwezigheid van IPv6. Nieuwe vormen van communicatie door bijvoorbeeld apparatuur die aan het Internet gekoppeld is of nieuwe diensten die gebruik maken van IPv6 vergen ook een ander beveiligingsbeleid en uitvoerende procedures.
Daarnaast is het belangrijk te onderzoeken welke (beveiligings) systemen die in gebruik zijn, zoals firewalls, IPv6 ondersteunen. Ook is van belang hoe zij zich gedragen als IPv6 verkeer aangeboden wordt. Een firewall zou zo maar standaard door kunnen laten bij IPv6, terwijl deze een totaal andere beveiligingsinstelling heeft voor IPv4. Analyseer dus wat de mogelijke risico's van IPv6 zijn, ook al wordt het binnen de organisatie nog niet (bewust) toegepast. Verder heeft IPv6 momenteel nog een beperkte gebruikersgroep en zal het dus nog moeten blijken in hoeverre IPv6 veiliger is dan IPv4! Een voordeel van IPv6 is wel dat IPsec een verplicht onderdeel is wat het gebruik van IPsec wellicht ten goede komt.

Bijlage A Werking IP

Deze bijlage beschrijft globaal de werking van het Internet Protocol en TCP/IP-referentiemodel.

Internet Protocol

Het Internet Protocol maakt het mogelijk, om onafhankelijk van de onderliggende techniek, systemen in verschillende netwerken met elkaar te laten communiceren. IP zorgt ervoor dat de onderliggende communicatieprotocollen, waaronder Ethernet, ATM, en Token Ring, transparant zijn.

In feite werkt het Internet Protocol heel eenvoudig; dit geldt voor zowel versie 4 als versie 6. Een netwerk is opgebouwd uit verschillende systemen en elk van deze systemen heeft een uniek IP-adres. Als het systeem een stuk informatie (een IP-pakket) naar een ander systeem wil sturen, zet hij het IP-adres van de bestemming in het pakket, evenals zijn eigen adres en stuurt dit het netwerk op. Er kan grofweg onderscheid gemaakt worden tussen twee typen systemen op internet, namelijk routers en hosts. Het verschil is dat hosts alleen pakketten versturen die afkomstig zijn van henzelf en alleen pakketten ontvangen die bestemd zijn voor henzelf. Routers daarentegen kunnen ook pakketten doorsturen die afkomstig zijn van andere systemen; routers hebben dan ook meerdere netwerkaansluitingen. Routers bepalen op basis van het bestemmingsadres waar het pakket heen wordt gestuurd.

Het Internet Protocol is een best-effort protocol. Het Internet Protocol zelf geeft namelijk geen enkele garantie dat pakketten aankomen of dat de volgorde waarin ze zijn verzonden dezelfde is als waarin ze worden ontvangen. Daarnaast geeft het ook geen garanties over het al dan niet gewijzigd zijn van de inhoud gedurende het transport. Alle gewenste zekerheid moet komen van de bovenliggende protocollen, zoals TCP, SCTP en UDP. Qua werking is het verschil tussen IPv4 en IPv6 vrij gering. Voor een uitgebreid overzicht van de werking van IP, zie referenties[7][3][8].

TCP/IP-referentiemodel

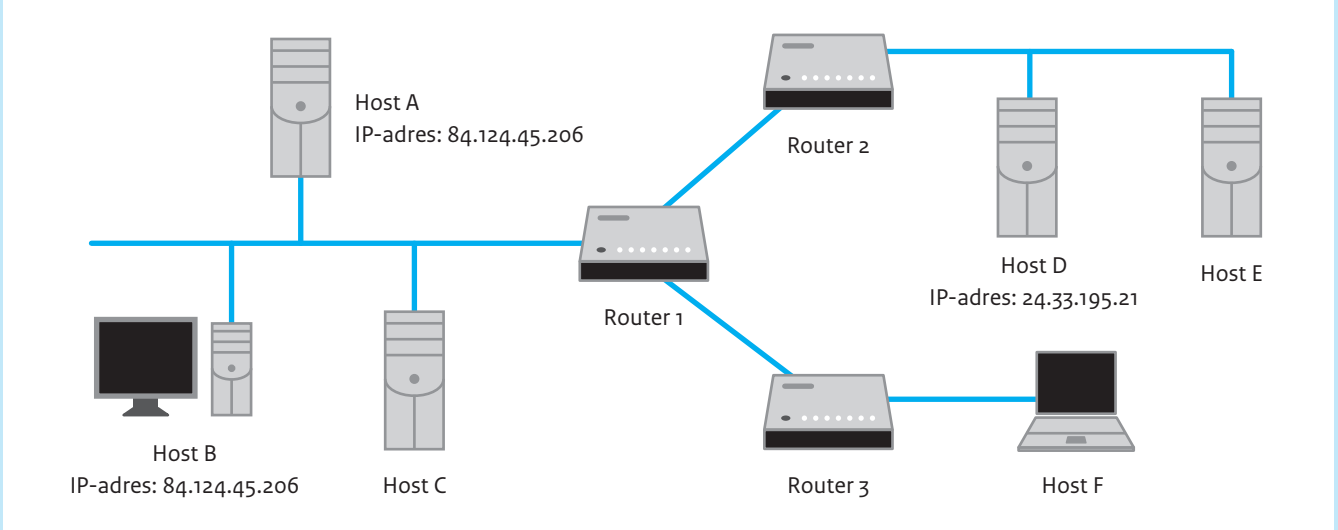
De TCP/IP-suite wijkt af van het bekende ISO-OSI referentiemodel dat bestaat uit zeven lagen. De IETF gebruikt een ander model, namelijk het TCP/IP-referentiemodel, zie tabel 4-1[7]. Dit model bestaat uit vier lagen waarbij de hardwarelaag als gegeven wordt beschouwd. Op iedere laag worden protocollen gebruikt die diensten leveren aan protocollen op aansluitende lagen.

TCP/IP-referentiemodel	
Applicatielaag	HTTP, SSL, TLS, SMTP, FTP
Transportlaag	TCP, UDP, SCTP
Netwerklaag	IP, ICMP, IGMP
Datalinklaag	IEEE 802.3, WLAN, Token Ring
(Hardwarelaag)	(fysieke medium)

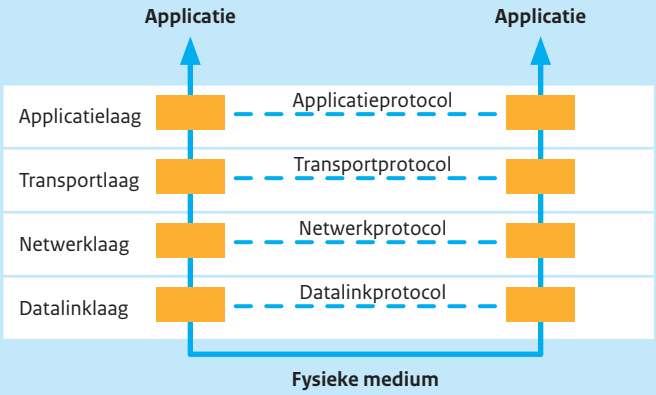
Tabel A-1 Het TCP/IP-referentiemodel met voorbeeld protocollen

De protocollen voor de datalinklaag worden niet door de IETF ontwikkeld. Het TCP/IP-referentiemodel wordt ook wel het zandlopermodel genoemd. IP (de netwerklaag) vormt hier het smalle deel van de zandloper en is het verbindende protocol tussen vele protocollen in de hogere en lagere lagen.

Figuur A-1 Een voorbeeld van gekoppelde, op IP-gebaseerde netwerken



Het principe van beide referentiemodellen is dat informatiestromen vanuit de applicatie worden doorgegeven aan het protocol op de applicatielaag. Deze bewerkt de informatie om het protocol te kunnen laten werken en geeft het op zijn beurt door aan de laag daaronder. Dit principe wordt herhaald tot de hardwarelaag is bereikt. De ontvanger loopt in omgekeerde volgorde de lagen door totdat de oorspronkelijke informatie is verkregen en geeft dit door aan de applicatie. De zender en ontvanger communiceren binnen een laag uitsluitend met elkaar op dezelfde laag. Dit proces is weergegeven in figuur A-2.



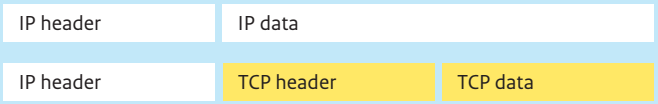
Figuur A-2 Communicatie in het TCP/IP-referentiemodel

Bijlage B Verschillen met IPv4

Deze bijlage beschrijft de verschillen tussen versie 4 en versie 6 van het Internet Protocol en gaat ook in op beveiligingsconsequenties. Referentie[5] beschrijft in detail de verschillen tussen IPv4 en IPv6.

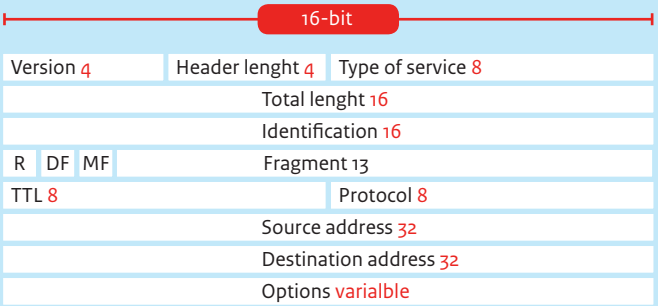
Headers

Een IP-pakket bestaat altijd uit twee delen: een header en data (in het Engels ook wel payload genoemd). De header is noodzakelijk voor de afhandeling van het protocol, waaronder routering. Hierin staat in het geval van IP onder andere wie de zender en de ontvanger zijn. Het datagedeelte bevat de feitelijke data die worden getransporteerd. Voor vrijwel alle protocollen in het TCP/IP-model geldt, dat deze een dergelijk onderscheid tussen header en data maken, zoals TCP en UDP. Omdat de administratieve afhandeling van deze protocollen anders verloopt, is de inhoud van deze headers ook verschillend. De TCP- of UDP-header vormt samen met de TCP- of UDP-data het dataveld in een IP-pakket. Dit proces wordt ook wel encapsulatie genoemd.

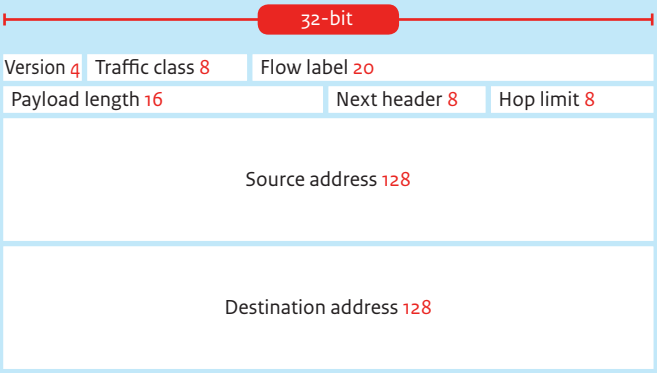


Figuur B-1 Een IP-pakket bestaat uit een header en een dataveld. Het dataveld zelf kan weer uit een header en dataveld van het bovenliggende protocol bestaan.

Hoewel de IPv6-header een stuk minder informatie bevat dan een IPv4-header, is deze toch 2x zo groot geworden (20 bytes voor IPv4 en 40 bytes voor IPv6). Dit komt volledig voor rekening van de grotere IP-adressen. Ten opzichte van de totale pakketgrootte (1500 bytes voor Ethernet) is dit echter een verwaarloosbare toename in de overhead.



Figuur B-2 IPv4-header met het aantal bits per veld.



Figuur B-3 IPv6-header met het aantal bits per veld.

Adresnotatie

Het belangrijkste verschil tussen IP versie 4 en versie 6 is de adresruimte. Voor versie 4 bestaan de adressen uit 32 bitsgetallen. Dit resulteert in ruim 4 miljard adressen die gebruikt kunnen worden, zij het dat een deel ervan is gereserveerd voor andere doelen. Voor IP versie 6 zijn er 128 bits gebruikt om een adres aan te duiden. Dit komt neer op circa 3,4 × 1038 adressen.

De adressen worden in IPv4 voornamelijk in de zogenaamde *dotteddecimal* notatie opgeschreven, bijvoorbeeld 192.0.2.12 Voor IPv6 is er voor gekozen om deze in een achttal groepen van vier hexadecimale cijfers[18] gescheiden door dubbele punten te noteren – de zogenaamde *colon hexadecimal notation.* Hierbij mogen voorloopnullen worden weggelaten evenals één reeks van opeenvolgende nullen. In het laatste geval worden hiervoor in de plaats twee dubbele punten geplaatst. De hier onderstaande adressen zijn dus gelijk.

```
2001:DB:0000:0000:0000:0001:169f:0666
2001:DB:0:0:0:1:169f:666
2001:DB:0::1:169f:666
2001:DB::1:169f:666
```

Net als in IPv4 zijn IPv6-adressen opgedeeld in een netwerkgedeelte en een host gedeelte. In IPv4 wordt dit weergegeven door het netwerkadres en een netmasker. In IPv6 vormen de laatste 64 bits van een adres het host gedeelte, terwijl de eerste 64 bits het netwerkdeel vormen. Het netwerkdeel wordt veelal prefix genoemd. De prefix kan worden opgesplitst in verschillende subnetten. De lengte van de prefix specifiek voor een netwerkdeel, wordt weerge-

20 Hexadecimale cijfers zijn cijfers die gevormd worden met grondtal 16, in plaats van 10. Hierdoor is het mogelijk om 16 waarden (0 tot 15) in een 'cijfer' te stoppen. De letters A-F worden gebruikt voor de waarden 10-15. De waarde van een byte kan daardoor met 2 hexadecimale getallen worden weergegeven.

geven door een slash gevolgd door de lengte van de prefix. Bijvoorbeeld:

```
2001:DB::1:169f:666/64
```

In URL's, zoals die bijvoorbeeld gebruikt worden in webbrowsers, worden vierkante haakjes om het adres geplaatst, bijvoorbeeld:

```
http://[ 2001:DB::1:169f:666]
```

Door de lengte van de IP-adressen wordt het wel steeds moeilijker om deze adressen praktisch te gebruiken; ze zijn nauwelijks meer te onthouden. Dit betekent dat IP-adressen zelf steeds minder zullen worden toegepast. In plaats daarvan zal er meer gebruik gemaakt worden van DNS (Domain Name System) en van alternatieve methoden, zoals autoconfiguratie.

Type adressen

Binnen IPv6 wordt een drietal types adressen onderscheiden:

- Unicast adressen. Deze worden gebruikt om een pakket naar precies één systeem te sturen;
- Multicast adressen. Een multicast adres wordt toegekend aan meerdere systemen. Wanneer een pakket naar dit adres wordt gestuurd zullen alle systemen met dit adres het pakket ontvangen;
- Anycast adressen. Een anycast adres wordt aan meerdere systemen toegekend. Wanneer een IP-pakket wordt verstuurd naar dat IP-adres is er uiteindelijk één systeem dat het pakket ontvangt. Welk systeem dat is, wordt op basis van routeringscriteria vastgesteld.

Het broadcastadres zoals dat in IPv4 gebruikt wordt, bestaat in IPv6 niet meer; dit wordt voornamelijk opgevangen door gebruik te maken van multicast. Multicast is dan ook een standaard onderdeel van IPv6 geworden terwijl het bij IPv4 nog optioneel is. Het ontbreken van broadcast heeft wel als voordeel dat amplificatie-aanvallen, zoals de smurf-aanval[19], niet meer zo eenvoudig zijn uit te voeren.

Unicastadressen worden verdeeld in drie categorieën: Link local, private range en global:

- Global unicastadressen zijn adressen die over internet gebruikt kunnen worden en dus internetwijd gerouteerd kunnen worden.
- Private range adressen zijn specifiek voor een privénetwerk en behoren niet te worden gerouteerd over het internet.
- Link local adressen zijn adressen die uitsluitend op één link worden verstuurd en dus nooit voorbij een router komen.

Adreshiërarchie

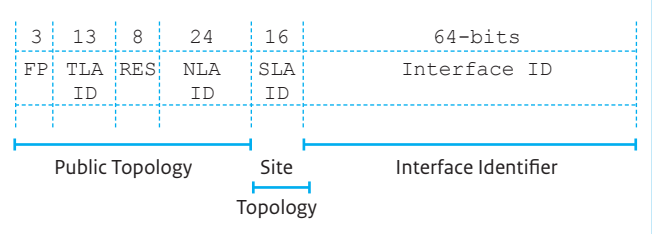
Globale unicast adressen worden hiërarchisch toegekend. Bij IPv4 is het zo dat momenteel altijd ranges van 256 adressen worden uitgegeven (een zogenaamde /24 range). Deze ranges worden echter relatief willekeurig uit de beschikbare ranges geselecteerd. Alle routers op het internet moeten voor al deze ranges bijhouden via welke route, pakketten met een doeladres in die range, moeten worden gestuurd. Het gevolg hiervan is dat de routetabellen in de routers enorm groot worden, wat de doorvoersnelheid van de routers niet ten goede komt. In IPv6 is dit opgelost door aggregatie van globale unicast adressen toe te passen[RFC 2374]. Dit houdt in dat degenen die IPv6-adressen uitgeven altijd ranges onderverdelen in delen van hun eigen range. Hiervoor zijn binnen het IP-adres drie niveaus aangegeven van aggregatie: toplevel (/16), nextlevel (/48) en sitelevel (/64). In figuur B-4 is weergegeven hoe een global unicast IPv6-adres wordt opgedeeld. De eerste 3 bits is de format prefix; dit geeft aan welk type pakket het is (bijvoorbeeld *unicast*, *multicast*). De TLA-ID is de toplevel aggregation. Dit wordt gevolgd door 8 bits die gereserveerd zijn. De NLA-ID is de nextlevel aggregation van 24 bits, gevolgd door een SLA-ID, de sitelevel aggregation.

21 Bij een Smurf-aanval worden PING pakketten, voorzien van een gespoofed source adres, gestuurd naar het broadcast adres van een netwerk. Alle systemen op dat netwerk sturen dan een antwoord (ECHO Reply) naar het (gespoofde) source adres.

22 De genoemde tegenhanger heeft niet altijd exact dezelfde definitie, maar in de praktijk is het gebruik vergelijkbaar.

Tabel B-1 IPv6 speciale adressen en prefixen.

IPv6 adres	Omschrijving	IPv4 tegenhanger
::1/128	Local host adres	127/8
fc00::/7	Private range adres	192.168/16; 10/8; 172.16/12 [RFC 1918]
fe80::/10	Link local adres	Geen – Zet de time-to-live waarde in het pakket op 1.
2000::/3	Global unicast adres	0.0.0.0/0
ff00::/8	Multicast adres	224.0.0.0/8 – 239.0.0.0/8 (Class D adres)
::<ipv4 adr>	IPv4 compatible IPv6 adres	<ipv4 adres>
::ffff:<ipv4adr>	IPv4-mapped IPv6 adres	<ipv4 adres>
2001:db::/32	adres voor documentatie gebruik	192.0.2.0/24



Figuur B-4 IPv6 Adresstructuur in termen van aggregatieniveaus.

Goodbye ARP

Ten aanzien van adressen zijn nog twee andere aspecten gewijzigd. In de eerste plaats is het Address Resolution Protocol (ARP) niet meer aanwezig in IPv6. Dit protocol wordt in versie vier gebruikt om het Media Access Control (MAC) adres (op linklaag niveau, bijvoorbeeld het Ethernet adres) behorende bij een IP-adres te bepalen. Hiertoe wordt gebruik gemaakt van het versturen van linklaagpakketten. Dit heeft als nadeel dat voor alle linklaagprotocollen een nieuwe versie van ARP moet worden ontwikkeld. In IPv6 wordt dit opgelost door gebruik te maken van *Neighbour Discovery*. Dit maakt gebruik van IP-multicasting om het linklaagadres te bepalen. Het gebruikt hiervoor een standaard multicast adres waarvan alle nodes op een link dit moeten kunnen ontvangen. Qua beveiliging is er weinig verschil tussen ARP en Neighbour Discovery.

Adresconfiguratie

De mogelijkheden voor een systeem om een IPv6-adres te krijgen zijn uitgebreider dan om een IPv4-adres te krijgen. In IPv4 is dit ofwel een handmatige configuratieactie ofwel er wordt gebruik gemaakt van een client-server protocol DHCP (Dynamic Host Configuration Protocol). Bij DHCP deelt een server IP-adressen uit aan de systemen binnen een netwerk. In IPv6 kunnen systemen hun eigen IP-adres genereren. Routers sturen hiervoor periodiek informatie uit op het multicast adres waar alle systemen op de link naar luisteren. Deze informatie bevat de prefix, de bijbehorende lengte en ook de default gateway (meestal de router zelf). De prefix bepaalt de eerste 64 bits van het adres, waarna het systeem zelf de overige 64 bits genereert. Het systeem moet vervolgens met Neighbour Discovery bepalen of het gegenereerde adres niet al in gebruik is; dit wordt Duplicate Address Detection (DAD) genoemd. Als dit het geval is, dan moet hij een ander adres generen en deze op dezelfde wijze toetsen. Is dit niet zo, dan is dat zijn IP-adres. Dit proces wordt *stateless autoconfiguration* genoemd. DHCP en handmatige configuratie worden overigens nog steeds ondersteund.

Een uitbreiding op stateless autoconfiguration is de *privacy extension*[RFC 3041]. Dit zorgt ervoor dat het moeilijker is te achterhalen welk systeem informatie ophaalt bij een server. Deze uitbreiding is voornamelijk bedoeld voor werkstations. Het principe is als volgt. Periodiek genereert een systeem een nieuw IP-adres. Dit nieuwe IP-adres wordt gebruikt bij het opzetten van nieuwe verbindingen. Reeds bestaande verbindingen worden nog steeds op basis van de oude IP-adressen in stand gehouden. Dit resulteert er dus in dat één systeem vele IP-adressen tegelijk heeft, die worden gebruikt voor communicatie. Er wordt er echter maar één gebruikt voor het opzetten van verbindingen. Het nadeel hiervan is dat het ook het monitoren van netwerken veel moeilijker maakt, vooral wanneer het een complex netwerk betreft en de MAC-adressen van de hosts niet bekend zijn op de plek waar monitoring plaatsvindt.

Het gebruik van stateless autoconfiguration kan verschillende beveiligingsproblemen opleveren, ten aanzien van de allocatie van adressen. Een aanvaller kan er namelijk voor zorgen dat een nieuwe gebruiker geen IP-adres kan krijgen, door voor elk adres dat de nieuwe gebruiker aanvraagt, te claimen dat hij deze reeds in gebruik heeft. Daarnaast kan de aanvaller zelf *router advertisements* gaan versturen, zodat de nieuwe gebruiker een niet werkbaar adres krijgt. Ook kan de aanvaller op deze manier al het verkeer in het netwerk naar zich toe trekken. Dit komt doordat de router advertisment ook het IP-adres van de default gateway bevat. Dit soort aanvallen kan worden gebruikt voor het afluisteren van netwerkverkeer en man-in-the-middle attacks. Om deze beveiligingsproblemen te voorkomen, is een uitbreiding in de vorm van *Secure Neighbour Discovery (SEND)* ontwikkeld. Hierbij wordt gebruik gemaakt van *Cryptographically Generated Addresses (CGA)*, waarbij een digitale handtekening wordt gekoppeld aan een IPv6-adres. Het host gedeelte wordt gegenereerd door het af te leiden van onder andere een publieke sleutel. De authenticiteit van dit IP-adres kan worden geverifieerd doordat het bericht digitaal is ondertekend met de private sleutel, behorende bij de publieke sleutel waarmee het adres is gegenereerd.

Network Address Translation overbodig

Het grotere aantal IP-adressen zorgt ervoor dat Network Address Translation (NAT) niet meer toegepast hoeft te worden, terwijl technisch gezien NAT nog wel te gebruiken is. Het niet toepassen van NAT heeft diverse grote voordelen. Een aantal belangrijke protocollen, onder andere SIP, FTP en RPC, hebben problemen om te kunnen functioneren wanneer NAT wordt gebruikt. Hiervoor zijn vaak gekunstelde oplossingen ontwikkeld, zodat deze protocollen toch met NAT kunnen werken.

Een nadeel van het niet toepassen van NAT is dat het vaak wordt ingezet als beveiligingscomponent; hoewel dit in principe niet de bedoeling is en ook geen sluitende beveiligingsoplossing biedt. In feite moet de beveiligingsfunctionaliteit geboden worden door bijvoorbeeld een firewall. Terwijl in IPv4 met NAT de hosts meestal niet vanaf de externe zijde zichtbaar en bereikbaar zijn zonder extra maatregelen, is in IPv6 waar NAT standaard niet wordt gebruikt, de host volledig bereikbaar vanaf het externe netwerk. Wanneer dit voor een onacceptabel risico zorgt, moet deze toegang door middel van firewall rules worden ingeperkt.

Netwerkscanning

Door de langere adressen is het heel moeilijk om een netwerkscan uit te voeren om te bepalen welke systemen op het netwerk aanwezig zijn, dit is een probleem en tegelijk een oplossing. Dit geldt zowel voor aanvallers als voor de beheerders van het netwerk. Aan de andere kant geldt dat aanvallers dit waarschijnlijk wel op een andere manier kunnen achterhalen, door bijvoorbeeld naar de DNS

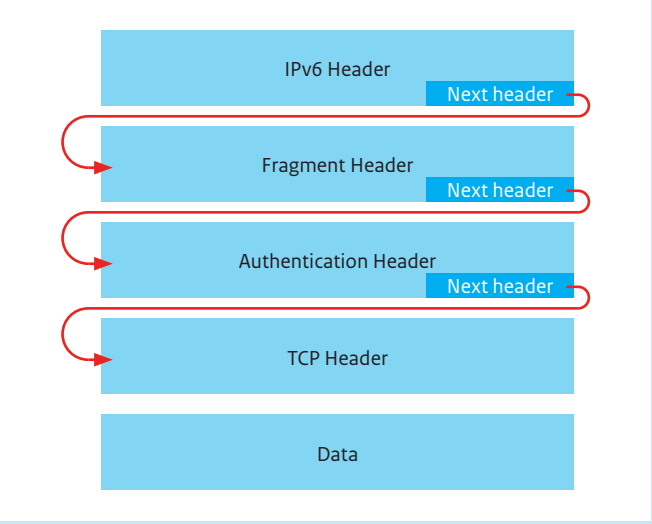
te kijken. Door het gebruik van harvesting methodes, waardoor er selectiever/gerichter gescand kan worden, en de toenemende beschikbare bandbreedte voor internetgebruikers zal het slechts een kwestie van tijd zijn voordat het uitvoeren van IPv6 netwerkscans praktisch uitvoerbaar is.

Multicast

Het veelvuldige gebruik van multicast voor verschillende toepassingen betekent wel dat aanvallers hiervan ook gebruik kunnen maken, bijvoorbeeld voor netwerkscanning toepassingen. Op de grenzen van het netwerk moet multicast verkeer dus voldoende gefilterd worden om dergelijke problemen te voorkomen. Dit in tegenstelling tot IPv4, waarvoor multicast zeer beperkt beschikbaar is op internet en voor de meeste vergelijkbare toepassingen broadcast wordt gebruikt, dat meestal op de netwerkgrenzen worden geblokkeerd.

Extension headers

Eveneens zijn er een aantal belangrijke andere wijzigingen aangebracht, die geen betrekking hebben op adressering. Een belangrijk aspect hiervan is het eenvoudig toestaan van uitbreidingen op IPv6, hiervoor zijn zogenaamde 'extension headers' ingevoerd. IPv4 beschikte over een beperkte mogelijkheid om opties mee te geven in de IP-header, zie figuur B-2 op pagina 23. Bij IPv6 is dit vervangen door een structurele oplossing waarbij de uitbreidingen als een ketting aan elkaar gekoppeld kunnen worden in de header.



Figuur B-5 Linking van headers in IPv6.

De functionaliteit die op deze manier toegevoegd is, is onder andere security in de vorm van IPsec ondersteuning voor roaming door Mobile IPv6. Daarnaast komen ook oude vertrouwde opties uit IPv4 terug, zoals *loose source routing*[23] en fragmentatie. De data (bijvoorbeeld TCP of UDP) van een IP-pakket worden in de laatste extension header aangegeven. Een gevolg van het gebruik van extension headers is dat de lengte van de IP-header constant is wat de verwerking in routers efficiënter maakt.

Er zijn momenteel zes typen extension headers gedefinieerd:
- Hop-by-hop options header. Deze wordt door alle systemen op het pad geëvalueerd;
- Destination options header. Deze wordt alleen door de bestemming geëvalueerd;
- Routing header. Deze wordt alleen door routers geëvalueerd;
- Fragment header. Wordt gebruikt om fragmentatie toe te passen;
- Authentication header. Is een onderdeel van IPsec dat authenticatie verzorgt;
- Encapsulated security payload. Is een onderdeel van IPsec dat authenticatie en vertrouwelijkheid verzorgt.

Pakketten opsplitsen

In IPv4 is het zo dat elk van de systemen tussen bron en doel van een IP pakket, het pakket mogen opsplitsen in meerdere pakketten (fragmenteren). Dit kan noodzakelijk zijn als het dragerprotocol slechts kleinere datapakketten kan verwerken. Bij IPv6 is dit veranderd door alleen de verzender fragmentatie te laten uitvoeren.

Deze beperking betekent wel dat, indien een dragerprotocol het aangeboden pakket niet kan verwerken, dit pakket weggegooid wordt. Om dit probleem op te lossen is een protocol ontwikkeld dat eerst de maximale grootte van een pakket over het hele pad bepaalt. Dit wordt *Path Maximum Transfer Unit (PMTU) discovery* genoemd. Hiervoor zijn een aantal standaardwaarden bepaald die dragerprotocollen moeten ondersteunen. Het PMTU discovery protocol probeert in eerste instantie het grootst mogelijke pakket te versturen en indien daar een foutmelding op terugkomt, verstuurt hij een pakket dat een stapje kleiner is en herhaalt dit proces totdat het pakket wel aankomt. In IPv6 is de minimale PMTU 1280 bytes (ter vergelijking, IPv4 vereist 576 bytes).
Het PMTU discovery protocol maakt voor de signalering gebruik van ICMPv6[24]. Paragraaf '*Gerelateerde protocollen*' op pagina 27 benoemt aandachtspunten bij ICMPv6.

De wijzigingen ten aanzien van de header en vooral de systematiek in de header zijn ook bedoeld om routers eenvoudiger en dus sneller IP-pakketten te laten verwerken.

De keerzijde van extension headers

Er zijn met extension headers veel mogelijkheden om IP-verkeer anders te interpreteren. Een firewall zal dan ook kennis moeten hebben van alle extension headers om een zinvolle beslissing te kunnen nemen. De extension headers maken daardoor de logica die in een firewall zit complexer. Daarnaast biedt het ook mogelijkheden om *denial of service* uit te voeren door een 'oneindige' reeks extension headers te creëren. Het feit dat de data in de laatste extension header worden gelinkt, betekend dat voor inspectie van de data – bijvoorbeeld om een TCP poortnummer te bepalen - het

23 Strict source routing uit IPv4 is niet meer aanwezig in IPv6.
24 Zie ook RFC1981 (http://www.facs.org/rfcs/rfc1981.html)

noodzakelijk is dat eerst alle extension headers worden doorlopen. Wanneer vercijfering gebruikt wordt met IPsec, is het niet mogelijk deze datavelden te analyseren. Een oplossing tegen misbruik van 'oneindig' linken van headers is bijvoorbeeld het tegenhouden van netwerkpakketten die meer dan een ingesteld aantal extension headers bevatten.

Jumbograms

Normaliter ondersteunen IPv4 en IPv6 een maximale pakketgrootte van 64 kilobyte, zij het dat dit meestal resulteert in fragmentatie. Voor de meeste toepassingen is deze omvang ruimschoots voldoende, maar vooral op het gebied van supercomputers kan het voordelig zijn om veel grotere pakketten te kunnen uitwisselen. Om dit mogelijk te maken is IPv6 uitgerust met een optie om Jumbograms te kunnen versturen. Hierdoor wordt het mogelijk om pakketten met een grootte van maximaal 4 megabyte te versturen. Dit is voornamelijk van belang in omgevingen waar zeer grote hoeveelheden data getransporteerd moeten worden. Voor veel reguliere toepassingen is deze vernieuwing minder relevant.

Quality of Service

Voor bepaalde toepassingen, zoals Voice over IP (VoIP) is het van belang dat er bandbreedte gereserveerd wordt of dat verkeer voorrang krijgt boven ander verkeer – dit wordt veelal ondergebracht in de term Quality of Service (QoS). QoS wordt in IPv6 ondersteund door middel van twee velden direct in de header, namelijk een *flow label* en een *traffic class*. De eerste wordt gebruikt om aan te geven dat een pakket bij een bepaalde datastroom (flow) hoort. Voor deze flow kan bandbreedte gereserveerd worden, door bijvoorbeeld gebruik te maken van het *Resource Reservation Protocol (RSVP)*; deze functionaliteit is niet direct aanwezig in IPv4. Het traffic class veld geeft aan welk type verkeer het betreft, aan de hand waarvan routers kunnen bepalen, welk pakket beter weggegooid kan worden. Ze doen dit natuurlijk alleen als dit noodzakelijk is. Dit kan bijvoorbeeld gebruikt worden als er te weinig bandbreedte beschikbaar is voor het aantal aangeboden pakketten om zo interactieve verkeerstromen de voorkeur te geven boven andere stromen. Dit wordt gebruikt door *Differentiated Services*. IPv4 ondersteunt dit ook onder de naam type of service.

Backporting

De meeste functionaliteit die in IPv6 is toegevoegd is inmiddels in IPv4 beschikbaar gemaakt, zij het vaak op een 'gehackte' manier die technisch niet altijd hetzelfde is. Dit betekent dat het geen standaard onderdeel van de IPv4 specificatie is en daardoor vaak slechts beperkt wordt ondersteund. IPsec is hier een voorbeeld van. Een ander voorbeeld is stateless autoconfiguration, dat in de vorm van ZeroConf aanwezig is in IPv4.

Gerelateerde protocollen

Naast het IP-protocol moeten ook andere protocollen worden aangepast voor IPv6. Dit betreft onder andere:

- ICMPv6. Dit protocol zorgt ervoor dat foutmeldingen en dergelijke worden teruggestuurd naar verzender.
- Routeringsprotocollen als OSPF en BGP. Deze zorgen ervoor dat bepaald kan worden hoe een pakket van bron naar bestemming kan gaan.
- DNS. Dit zorgt voor vertaling van namen naar IP-adressen en vice versa.
- TCP/UDP. De twee belangrijkste protocollen die gebruik maken van IP.
- DHCP. Dit is een protocol dat IP-adressen toewijst aan systemen.

ICMPv6 heeft een belangrijke functie in IPv6: Dit protocol wordt gebruikt voor de signalering van de PMTU. Het filteren/blokkeren van ICMP wordt binnen IPv4 beschouwd als een goede security oplossing, maar *rücksichtslos* al het ICMPv6 verkeer blokkeren, zal in dit geval kunnen leiden tot grote problemen.

Dit betekent automatisch ook dat wanneer bovengenoemde protocollen over de netwerkgrenzen worden gebruikt, ook de firewall rules moeten worden aangepast. Daarnaast heeft de relatie met andere protocollen ook gevolgen voor de methoden waarop een migratie naar IPv6 kan plaatsvinden. «

Bijlage C Afkortingen

Afkorting/Begrip	Omschrijving
AfriNIC	African Network Information Centre; registar voor Afrika
APNIC	Asia-Pacific Network Information Centre; registar voor Azië en de Pacific regio
ARIN	American Registry for Internet Numbers; registar voor Noord-Amerika en delen van de Caraïben.
ARP	Address Resolution Protocol
CGA	Cryptographically Generated Addresses
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
FTP	File Transfer Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPng	IP Next Generation
IPv4	Internet Protocol versie 4
IPv6	Internet Protocol versie 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
LACNIC	Latin American and Caribbean Internet Addresses Registry voor Latijns-Amerika en delen van de Caraïben.
MAC	Medium Access Control
NAT	Network Address Translation
NATPT	Network Address Translation and Protocol Translation
NLA	nextlevel aggregation
OS	Operating System
PMTU	Path Maximum Transfer Unit

QoS	Quality of Service
RFC	Request for Comments
RIPE NCC	RIPE Network Coordination Centre (RIPE NCC); registar voor Europa, het Midden-Oosten en Centraal-Azië
RPC	Remote Procedure Call
RSVP	Resource Reservation Protocol
SCTP	Stream Control Transmission Protocol
SEND	Secure Neighbor Discovery
SIP	Session Initiation Protocol
SLA	sitelevel aggregation
SSH	Secure Shell
SSL	Secure Socket Layer
ST-2	Stream Protocol 2
TCP	Transmission Control Protocol
TLA	toplevel aggregation
TLS	Transport Layer Security
UDP	User Datagram Protocol
VoIP	Voice over IP

Bijlage D Relevante RFC's

Afkorting/Begrip	Omschrijving
[RFC 1981]	McCann, J., et al; "Path MTU Discovery for IP version 6"; RFC 1981; augustus 1996.
[RFC 3587]	Hinden, R., et al.; "An IPv6 Global Unicast Address Format"; RFC 3587; augustus 2003.
[RFC 2460]	Deering, S. en Hinden, R.,; "Internet Protocol, Version 6 (IPv6) Specification"; RFC 2460; december 1998.
[RFC 2675]	Borman, D., et al.; "IPv6 Jumbograms"; RFC 2675; augustus 1999.
[RFC 4941]	Narten, T., en Draves; "Privacy Extensions for Stateless Address Autoconfiguration in IPv6"; RFC 4941; september 2007.
[RFC 3056]	Carpenter, B. en Moore, K.; "Connection of IPv6 Domains via IPv4 Clouds"; RFC 3056; februari 2001.
[RFC 3971]	Arkko, J (ed.); "Secure Neighbor Discovery (SEND)"; RFC 3971; maart 2005.
[RFC 3972]	Aura, T.; "Cryptographically Generated Addresses"; RFC 3972; maart 2005
[RFC 5214]	Templin, F.; "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)"; RFC 5214; maart 2008.
[RFC 4380]	Huitema, C. Teredo: "Tunneling IPv6 over UDP through Network Address Translations (NATs)"; RFC 4380; februari 2006.
[RFC 4779]	Asadullah, S.; "ISP IPv6 Deployment Scenarios in Broadband Access Networks"; RFC 4779; januari 2007.
[RFC 3542]	Stevens, W. and Thomas, M.; "Advanced Sockets API for IPv6"; RFC 3542; mei 2003.
[RFC 4301]	Kent, S., Atkinson, R.; "Security architecture for the Internet Protocol"; RFC 4301; december 2005.
[RFC 4302, 4305]	Kent, S., Atkinson, R.; "IP Authentication Header"; RFC 4302, december 2005.
[RFC 4303]	Kent, S., Atkinson, R.; "IP Encapsulating security payload (ESP)"; RFC 4303; december 2005.
[RFC 4861]	Narten, T. et al.; "Neighbor discovery for IP version 6"; RFC 4861; september 2007.
[RFC 4862]	Thomson, S and Narten, T.; "IPv6 stateless address autoconfiguration"; RFC 4862; september 2007.
[RFC 4443]	Conta, A. and Deering, S.; "Internet control message protocol (ICMPv6) for the Internet Protocol version 6"; RFC 4443; maart 2006.
[RFC 2464]	Crawford, M.; "Transmission of IPv6 Packets over Ethernet Networks"; RFC 2464; december 1998.
[RFC 3701]	Hinden, R et al; "IPv6 Testing Address Allocation"; RFC 3701; maart 2004.
[RFC 2473]	Conta, A and Deering, S.; "Generic Packet Tunneling in IPv6 Specification"; RFC 2473; december 1998.
[RFC 4033, 4034, 4035]	Eastlake, D.; "Domain name system security extensions"; RFC 4033, 4034, 4035; maart 2005.
[RFC 3986]	Hinden, R., et al.; "Format for Literal IPv6 Addresses in URL's"; RFC 3986; januari 2005.
[RFC 4291]	Hinden, R. and Deering, S.; "IP version 6 addressing architecture"; RFC 4291; februari 2006.

Bijlage E Referenties

Nr	Omschrijving
[1]	Whitepaper “IP versie 6”, GovCERT versie 1.2 van 10 maart 2011
[2]	Interne memo’s IPv6, Frans van Leuven – ATOS
[3]	Erika Hersaeus and Roland Svahn - Swedish Post and Telecom Agency; “Deployment IPv6 – practical guidance”; 21-02-2012
[4]	Presentatie “IPv6 Security”, Arjen Holzer – TNO, voor MSP-ISAC op 14 december 2012
[5]	Artikel “Niets doen is geen optie”, Computable 04-06-2012, Dennis Silva en Erwin Blekkenhorst – Schuberg Philis
[6]	Cheswick, W.R. et al.; “Firewalls and Internet Security: repelling the wily hacker”, 2nd ed., Addison-Wesley, 2003.
[7]	Davies, E., et al.; “IPv6 Transition/Co-existence Security Considerations”; Internet draft draft-ietf-v6ops-security-overview-06; October 2006
[8]	Eddy, W en Ishac, J.; “Comparison of IPv6 and IPv4 Features”; Internet draft draft-eddy-ipv6-ip4-comparison-00; mei 2006.
[9]	“Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks”; United States Government Accountability Office; mei 2005.

Dit whitepaper is tot stand gekomen in een publiek-private samenwerking mede door waardevolle inbreng van de volgende deskundigen:

Ben Elsinga (Capgemini)
Peter Westerveld (NCSC)
Lex Dunn (Capgemini)
Jaap van der Veen (Belastingdienst)
Theo Arts (RWS)
Rinus Braak (EL&I/Dictu)
André van Harn (Capgemini)
Marco van der Pal (Capgemini)
Rogier Spoor (SurfNET)
Erwin Heringa (SIDN)
Frans van Leuven (AtoS)
Erwin Blekkenhorst (Schuberg Philis)
Dennis Silva (Schuberg Philis)
Robert Bennis (SSC ICT-Den Haag (Min BZK))
Mark Prins (Min BZK)
Eelco Stofbergen (NCSC)

Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
T 070 751 55 55 | F 070 888 75 50
www.ncsc.nl | info@ncsc.nl

Oktober 2013