IP versie 4 of IP versie 6……ZX ronde 6 januari 2019

Tijdens de migratie van mijn website van Joomla naar Wordpress gebeurde er iets vreemds. In principe een hele nieuwe website gebouwd en zijn alleen onderdelen van de oude website gemigreerd. Daar is niets vreemd aan maar na een aantal dagen dat de website in bedrijf was kreeg ik meldingen van bezoekers dat ze de website niet konden bereiken. Bij navraag bleken dit bezoekers te zijn van de XS4ALL internetprovider. En dat is vreemd, waarom is daar de URL niet te bereiken? (URL = Uniform Resource Locator)

Nu kan iedere internet gebruiker zelf controleren of een URL wel of niet bereikbaar is. Dit door de URL te pingen in MS DOS. (tab " Uitvoeren / CMD / ping domeinnaam website "

De opdracht ping stuurt een datapakketje naar de aangegeven website en retourneert het IP-adres.

Dit IP adres kan worden weergegeven als IPv4 of IPv6 .

IPv6 is de nieuwste versie van het internetprotocol dat voornamelijk gebouwd is omdat het aantal beschikbare IP-adressen van versie 4 al lange tijd opraken.

Of de URL te bereiken is kan afhangen van de DNS van de Internet Service Provider. Als dat niet zo is kan het probleem zijn dat de host van de webserver een migratie heeft uitgevoerd die niet voor alle URL`s werkt. (DNS = Domain Name System)

In mijn geval weet ik dat niet omdat na controle met een ping alleen het IPv4 adres werd doorgegeven.

De volgende actie was een berichtje naar de webhost met de vraag of de URL ook in IPv6 ondersteund wordt? Het antwoord was dat hun web server platform werkt met zowel IPv4 als IPv6. (Dual stacked)

Het advies was om de bezoekers de URL te laten pingen en als het goed is zullen ze als antwoord krijgen van het IPv4 adres of van het IPv6 adres. Krijgen ze wat anders, dan is er een probleem met de DNS van XS4All.

Het zou kunnen dat voor de XS4ALL bezoekers alleen IPv6 wordt ondersteund of dat er toch nog wat mis is aan de zijde van de webhost??

Nadat ik de Webhost de testresultaten heb te laten zien bleek dat het probleem in DNSSEC verwerking te zitten. Ik had deze uitgeschakeld toen de website uit de lucht was maar na het inschakelen is deze niet goed verwerkt in de servers van de webhost.

Wat is een DNSSEC?

Elke website heeft een IP-adres. Omdat een dergelijk nummer lastig te onthouden is, zijn de domeinnamen bedacht. Het domeinnaamsysteem (DNS) vertaalt het IP-adres naar een domeinnaam. Dat vertalen gebeurt in de *nameservers*. Helaas is het mogelijk die vertaling te dwarsbomen. Zo kunnen bezoekers van je site op een andere site terechtkomen. Of iemand anders kan jouw mails lezen.

De DNSSEC voegt een digitale handtekening toe aan de DNS-informatie. Daardoor weet je zeker dat, als mensen naar je site zoeken, ze ook bij je site uitkomen. En dat niemand je mails leest.

Niet alle providers werken met DNSSEC. Een website test uitvoeren kan bijvoorbeeld op internet.nl. Toets de domeinnaam in van je gekozen site en je krijgt de graad van beveiliging van deze site te zien.

Waarom IP versie 6??

Ooit zullen alle IPv4-adressen opraken. Wanneer dat gaat gebeuren, dat weet niemand echt precies. De IANA is de organisatie verantwoordelijk voor het toekennen van IP-adressen en eind 2011 werden de laatste IPv4-blokken toegekend aan de betreffende regio's en daarna verdeeld tussen de ISP's in die regio.

In 2011 dachten we dat het eind 2012 al gedaan zou zijn met de IP-adressen. Die voorspelling bleek niet te kloppen. Er is een aantal redenen waarom we nog niet allemaal overgestapt zijn op ipv6.

Internet Service Providers hebben geen reden om echt over te stappen, omdat hun netwerken stabiel zijn. Er gaan wat klanten weg, er komen wat klanten bij, dus je hergebruikt wat adressen en alles gaat zijn gangetje.

Daarnaast gaat de overstap erg moeizaam, omdat je pas echt van de voordelen kunt genieten als ook het allerlaatste netwerk over is op versie 6. Niet echt geweldig.

Laat staan dat iedereen dan IPv6 aan moet zetten: hardwarefabrikanten, contentproviders, internetproviders en meer, en niemand heeft echt reden om dat te doen.

De nieuwe IPv6-adressen zijn een stuk langer in vergelijking met versie 4. Daarom worden deze adressen met een nieuwe notatie opgeschreven. Ze worden in groepen van acht in hexadecimale notatie opgeschreven, gescheiden met dubbele punten tussen elke groep.

Er zijn een aantal privacyzorgen als gevolg van IPv6. Elk apparaat krijgt namelijk een uniek adres, waardoor **NAT** niet meer nodig is. Dat betekent dat als jij straks een website bezoekt, dan ziet deze niet langer je externe IP-adres, maar direct het adres van je eigen apparaat.

IPv4 compenseerde de schaarste al aan het begin van de jaren negentig door onderscheid te maken tussen privé- en openbare adresruimtes.

Op lokale netwerken (LAN's) worden apparaten met toegang tot het internet met een privé-IP-adres lokaal geadresseerd en door een gemeenschappelijk openbaar IP-adres met het internet verbonden.

De belangrijkste poort tussen een openbaar en privé-adresgedeelte is de router. Hier vindt de Network Address Translation – oftewel NAT – plaats.

Wat is NAT?

Network Address Translation is een adresvertaling tussen twee netwerken die meestal in de router plaatsvindt. Het doel van deze techniek is het verbinden van lokale netwerken met het internet.

Met versie IPv6 is NAT niet meer noodzakelijk omdat er simpelweg voldoende IP adressen beschikbaar zijn.

Het opvallendste voordeel van IPv6 is dus de grote adressering. Met de 128bit-adressen (16 bytes) van IPv6 is de kans klein dat de adressen ooit opraken, aangezien daarmee ruim 340 sextiljoen adressen mogelijk zijn (dat is een getal met 36 nullen), in tegenstelling tot de 32-bitadressen van IPv4.

Andere voordelen zijn kleinere routing-tabellen, een eenvoudiger protocol, betere veiligheid en dat altijd hetzelfde IPv6-adres behouden kan worden.

De zesde versie van het internetprotocol heeft ervoor gezorgd dat er wereldwijd veel meer IP-adressen beschikbaar zijn..

Met andere woorden: ieder koffiezetapparaat krijgt een uniek, wereldwijd traceerbaar IP-adres .

Privacy

Ip-adressen waren al persoonsgegevens, zo oordeelde het **CBP**. Met IPv6 wordt het erger: je IP-adres wordt afgeleid van het mac-adres van het apparaat dat je gebruikt. Het wordt een soort 'supercookie'. Dat betekent dat apparaten door netwerken gevolgd kunnen worden, want je krijgt dan steeds een grotendeels identiek IP-adres toegekend.

Met een paar eenvoudige stappen kun je van het IPv6-adres het mac-adres van een apparaat herleiden. Er is een oplossing: privacy addressing, dat het mac-adres verbergt met adressen die regelmatig veranderen.

Dat is echter niet zo handig voor netwerkbeheerders, omdat IP-adressen dan onvoorspelbaar worden, wat het opsporen van fouten en beheer lastig maakt.

Er is een nieuwe standaard: Semantically Opaque Interface Identifiers, die zorgen dat netwerkadressen uniek zijn per netwerk, zodat je op hetzelfde netwerk wel steeds hetzelfde adres hebt, maar het compleet verschilt op een ander adres.

Wordt vervolgd…..