3.3.3.e Omnummering van IP-netwerken

1. Introductie

Een omnummering van een IP-netwerk omvat het omzetten van de IP-adressen van alle nodes in een TCP/IP-netwerk. Nodes zijn bijvoorbeeld servers, routers, desktop computers, notebooks, printers, enzovoort en daarmee eigenlijk alles waarmee over het netwerk berichten worden uitgewisseld. Met andere woorden: het nummerplan van het netwerk wordt veranderd. In dit artikel worden de belangrijkste achtergronden en mogelijkheden die een rol spelen in het omnummeren van een IP- netwerk beschreven. Verder worden een aantal instrumenten aangereikt om een migratie soepeler te laten verlopen.

1.1 Wanneer is migratie nodig?

Een computernetwerk is niet statisch. Door diverse oorzaken zit er verandering in. Deze verandering betreft vaak tientallen procenten per jaar. Voorbeelden hiervan zijn:

- Koppelen van verschillende IP-netwerken. Door een fusie of overname is het in het algemeen wenselijk dat de partijen hun netwerken integreren. Dat is in het algemeen een voorwaarde om de overige IT te integreren, waarmee de voordelen van de fusie samenhangen. Ook zonder een formeel samengaan van bedrijven is er vaak voordeel te halen uit het koppelen van de netwerken. We spreken dan veelal van een extranet. In veel organisaties zijn er bijkantoren die niet over een verbinding op IP-niveau beschikken. Door de voortschrijdende automatisering en dalende netwerktarieven, wordt het belang van het koppelen van deze kantoren steeds groter. 'Last but not least', het realiseren van een internetkoppeling is ook een voorbeeld. In al deze gevallen is het niet zeer waarschijnlijk dat de gehanteerde nummerplannen een eenvoudige koppeling toelaten.
- Netwerk groeit uit huidige nummerplan. Met tientallen procenten groei per jaar is het te verwachten dat op enig moment het aantal nodes in een netwerk de beschikbare ruimte in het nummerplan overschrijdt. Een klasse C netwerk bijvoorbeeld, biedt ruimte aan 254 IP-adressen. Als dat op is moet er een extra klasse C netwerk bij, of er moet worden overgegaan op een klasse B netwerk.
- Overgang van routed naar switched LAN. De laatste jaren is er een sterke opkomst van switching als pakketschakel technologie op LAN-niveau. Bij switching worden routeringsbeslissingen niet meer op basis van IP-adressen genomen (zoals bij klassieke routers), maar op basis van ethernet-adressen. Hierdoor speelt de topologie van een LAN een minder grote rol in het ontwerp van een nummerplan dan voorheen.

- Overgang van vaste IP-adressen naar dynamische IP-adressen, die worden uitgereikt met DHCP-beheer. DHCP (Dynamic Host Configuration Protocol, zie verder) maakt het mogelijk om beheer van IP-adressen vanuit een centrale server te regelen, in plaats van iedere machine apart te moeten configureren. Dit is vooral handig voor notebook-computers en andere client-machines en maakt het mogelijk om een ander, zuiniger, nummerplan op te zetten.

1.2 Waarom is het moeilijk?

Er zijn een aantal redenen waarom het een grote uitdaging kan zijn om een IP- omnummering uit te voeren:

- Door niet of gebrekkig gebruik van namen en vertaling van die namen naar IP-adressen via DNS (Domain Name Service), staan IP-adressen vaak vast ingeprogrammeerd in de configuraties of software van diverse nodes. Ook gebeurt het dat softwarelicenties afhangen van vaste IP-adressen. Het is niet eenvoudig om al deze gevallen op te sporen.
- De essentie van een nummerplanverandering is dat deze simultaan, of althans zeer gecoördineerd, op veel apparaten en locaties tegelijk uitgevoerd moet worden. Dat vergt veel planning en capaciteit.

2. Technische aspecten

2.1 IP-nummers

Een IP-adres is een getal van 32 bits dat, in principe, een wereldwijd unieke identificatie is van een netwerk-interface aan een netwerknode. Meestal wordt een IP- adres genoteerd als een viertal getallen, gescheiden door punten. Het grootste getal is dus 255.255.255.255. Deze nummers worden zowel in TCP, als in het onderliggende IP gebruikt om nodes te adresseren. Op de protocollagen daarboven worden meestal zogenaamde FQDNs (Fully Qualified Domain Names) gebruikt. Een voorbeeld van een FQDN is: *www.deloitte.nl*, het daarbij horende IP-adres is 194.73.19.82. Op de laag eronder zijn de adressen specifiek voor het soort verbinding: ethernet heeft een ander soort adressen dan ATM.
Om IP-adressen in netwerken te groeperen, wordt tegenwoordig het aantal bits aangegeven dat beschikbaar is voor een groep. Een voorbeeld hiervan is 192.168.128/10. Deze omvat de adressen van 192.168.128.0 tot en met 192.168.191.255.
Meer informatie over IP-adressen is te vinden in het artikel van Anton Holleman, *Netwerknummers en -namen*, elders in deze uitgave.

2.2 Nummerplannen

Een nummerplan is de toewijzing van bepaalde nummerreeksen aan bepaalde groepen nodes (veelal locaties). De twee belangrijkste functies van een nummerplan zijn routering en allocatie. Het num-

merplan dient om de allocatie van nummers aan machines overzichtelijk te maken en te kunnen decentraliseren naar bijvoorbeeld LAN-beheerders. Een nummerplan moet garanderen dat IP-adressen uniek zijn. Op basis van het nummerplan worden tabellen gemaakt, zodat verkeer tussen locaties onderling en met het internet kan worden gerouteerd.
Er worden op z'n minst geografische groepen onderscheiden, bijvoorbeeld kantoor Amsterdam en kantoor Zwolle. De reden voor een geografische scheiding is dat er dan op kantoorniveau kan worden gerouteerd.
Een voorbeeld van een geografisch nummerplan staat in de volgende tabel:

TABEL 1

Locatie	*IP-adresreeks*
Amsterdam	*192.168.128/10*
Zwolle	*192.168.192/8*
Jipsing-Boertange	*192.168.193/8*

Ook kunnen functionele groepen worden onderscheiden, zodat bijvoorbeeld servers en clients elk hun eigen reeksen krijgen. Dit is vooral handig om het beheer te uniformeren. Een voorbeeld van een dergelijk plan is de volgende tabel (hierbij wordt het laatste byte van het adres gebruikt als functieaanduiding):

TABEL 2

Functie	*Range*
Netwerknummer	*0*
Routers	*1-8*
Servers	*25-44*
Printers	*45-60*
Clients	*61-197*
Broadcast-adres	*255*

Als het aantal nodes meer dan een paar honderd wordt, verdient het aanbeveling om deze nummers te gaan beheren met een geïntegreerd hulpmiddel (tool). Het voert buiten het bestek van dit artikel om daar gedetailleerd op in te gaan. Kort samengevat wordt in een

dergelijk tool alles beheerd dat te maken heeft met namen, IP-nummers, eventueel MAC- (ethernet-) adressen en locaties van machines. Daarmee worden dan DHCP en DNS-servers gevoed, kunnen routeringstabellen worden beheerd, en kunnen firewall-instellingen worden gegenereerd. Idealiter kunnen deze gegevens dan ook nog ter beschikking staan van een netwerkmanagement-tool. Het voordeel van een dergelijk tool moet onder meer gezocht worden in het bewaken van de consistentie van de verschillende gegevens.

2.3 Private Ranges

De internetadressen raken op. De toekomstige oplossing daarvoor, is de volgende versie van het IP-protocol IPv6, waarin IP-adressen een lengte van 128 bits krijgen. In de tussentijd is er een andere oplossing. Door de netwerkautoriteiten zijn een drietal reeksen aangewezen als zogenaamde 'private ranges'. Deze reeksen zijn: 10/8, 172.16/12, en 192.168/16. Deze adressen mogen door iedereen vrijelijk worden gebruikt, als ze maar niet op het internet komen. Hiermee wordt het dus mogelijk voor organisaties die geen of niet genoeg publieke adressen kunnen of willen hebben, om toch een legaal IP-adres te gebruiken. Het wordt als een doodzonde beschouwd om een IP-adres te gebruiken dat aan een andere organisatie is toegekend. Bovendien is het een nachtmerrie voor de netwerkbeheerder. (Zie verder RFC 1918, *Address Allocation for Private Internets*). Deze private ranges mogen onder geen voorwaarde op het publieke internet zichtbaar worden. Om toch verbinding met het internet te hebben is het nodig om Network Address Translation te doen.

2.4 Network Address Translation

Het centrale idee van Network Address Translation (NAT) is dat tussen het eigen netwerk en het internet een machine staat waardoor de interne IP-adressen worden omgezet in een beperkt aantal externe IP-adressen. Deze taak ligt meestal bij een router of firewall. De twee belangrijkste redenen om dit te doen zijn: de structuur van het eigen netwerk mag niet zichtbaar zijn naar buiten of het aantal extern beschikbare IP-adressen is te beperkt.
Een manier om er naar te kijken is de volgende: Elke node is op het internet bekend met een adrestweetal: dat van de NAT-machine, plus het interne private range-adres. Als je een 16-bits private range hebt heb je daarmee dus 48-bits internetadressen gemaakt.
Als er sprake is van een organisatie met verschillende vestigingen die met elkaar communiceren via het publieke internet, dan is het zinvol om een nummerplan te maken voor het hele netwerk (inclusief alle vestigingen). De NAT-router, of een firewall, koppelt dan de netwerken via een 'tunnel'. Dit valt buiten het onderwerp van dit artikel.
Voor meer informatie zie verder: RFC 1631, The *IP-Network Address Translator (NAT)*.

2.5 DHCP

Het Dynamic Host Configuration Protocol (DHCP) geeft client-machines de mogelijkheid om zichzelf via het netwerk te configureren, inclusief netwerkadres (Even tussendoor: 'host' is het oude internetwoord voor een computer die toegang heeft tot het netwerk, in tegenstelling tot een router, die een functie heeft *in* het netwerk. Zowel clients als servers zijn dus hosts. De oude term voor router is 'gateway', deze term komt nog veel voor). Via een DHCP-server kunnen machines worden geconfigureerd met hun IP-adres, een subnet mask, een default-route, DNS-server, WINS-server, enzovoort. Als hiermee alle configuratiegegevens worden ingesteld die geraakt worden bij een omnummering, kan een omnummering voor deze machines dus volstaan met het aanpassen van de DHCP-server configuratie. DHCP kan ook gebruikt worden voor servers en printers, die veelal een vast IP-adres nodig hebben (in verband met hun DNS-entries). Veel DHCP-servers ondersteunen dit, doordat ze aan het MAC-adres een vast nummer kunnen toewijzen. Het kan erg handig zijn om zoveel mogelijk machines via DHCP te configureren. Deze DHCP-server wordt dan wel een vrij essentiëel netwerkcomponent: als die gestoord is kan er geen machine worden opgestart.

2.6 Dual-homed nodes

In een IP-netwerk heeft elke interface (bijvoorbeeld een ethernetkaart) van elk machine een eigen IP-adres. Een machine met twee interfaces heeft dus in principe twee IP-adressen. Het is echter ook mogelijk dat een interface meerdere IP-adressen heeft. Dit kan gebruikt worden in een migratie. Door de belangrijkste servers te voorzien van een IP-adres in het oude nummerplan *en* een IP-adres in het nieuwe nummerplan, kan de omnummering van de clients worden losgekoppeld van de omnummering van de servers. Er zijn dan als het ware twee netwerken gecreëerd die beide van dezelfde kabels gebruik maken. Servers zijn dan in beide netwerken aanwezig. Dit is mogelijk als de software van alle servers en routers dit toelaat, en als het oude en het nieuwe nummerplan niet overlapt.

2.7 VPNs en Firewalls

Virtual Private Networks (VPNs) leveren complicaties op. Er is immers een tunnel tussen het privénetwerk en een ander netwerk (client op een publiek netwerk, andere locatie, et cetera), waardoor het waarschijnlijk is dat interne IP-adressen elders bekend zijn. Die moeten dus mee gemigreerd worden. Firewalls zijn de dragers van NAT- en VPN-functionaliteit. Firewalls zullen dus adressen hebben die wel veranderen en adressen die niet veranderen (extern zichtbare adressen). Firewalls blokkeren verkeer, onder meer op basis van IP-adressen. Ook hebben veel firewalls een licentie waarin het IP-adres een sleutel is, na omnummeren werken ze dan niet meer. De firewall-beheerder heeft dus een belangrijke rol.

2.8 DNS (intern en extern)

De Domain Name Servers spelen een belangrijke rol in een omnummerproces. Omdat ze namen op IP-adressen afbeelden (en andersom), is dit de plaats waar de meeste aandacht nodig is. Organisaties met een firewall hebben meestal twee DNS-systemen: een waarin alle adressen voorkomen, voor intern gebruik, en een waarin alleen een aantal extern zichtbare adressen voorkomen, een zogenaamde split-DNS.
DNS werkt met expiration: aan de client wordt verteld hoe lang een bepaald gegeven geldig is. Deze periode staat meestal voor een paar dagen. Het is verstandig dit voor een migratie terug te brengen naar een uur. Oude gegevens zullen dan minder lang overleven, ten koste van een verwaarloosbaar hogere belasting op de DNS-servers.
Het is van essentieel belang dat het hele DNS-beheer van een organisatie op orde is, voordat aan een omnummering wordt begonnen. Zoals eerder is aangegeven is het verstandig dit beheer in overeenstemming te brengen met het beheer van machines en nummerplannen.
Meer informatie over de opzet en het beheer van DNS is te vinden in het artikel van Anton Holleman, *Netwerknummers en -namen*, elders in deze uitgave.

2.9 Tools

Tijdens een omnummering is het waarschijnlijk dat er fouten in de uitvoering optreden. Het is dan van belang om over een aantal diagnostische instrumenten te beschikken om de bron van deze fouten op te sporen. Het is ook handig om van tevoren met deze instrumenten te oefenen. Voorbeelden zijn:

- Ping. Is een machine met een bepaald adres bereikbaar?
- Traceroute. (Tracert onder Windows) Langs welke routers gaat een pakket? Handig om routeringslussen op te sporen.
- Route print. Welke routeringstabel heeft een machine gekregen?
- DNS-lookup. Wat zegt een bepaalde server over namen en adressen?
- Winipcfg. Welke configuratie heeft een Windowsmachine van de DHCP-server gekregen?

Voor de meeste van deze functies heeft Windows een aantal standaard DOS-tools. Daarnaast is er een reeks aan public domain-pakketten met grafische user-interfaces. Ook voor de andere platforms (Unix, Mainframe, enzovoort) zijn deze tools beschikbaar.

3 Migratie strategieën

Er is een aantal migratiestrategieën denkbaar. Een eerste stap in het omnummerproces is daarom om voldoende gegevens te verzamelen, zodat het mogelijk wordt om een weloverwogen keuze te maken.

3.1 D-day

De D-day-strategie bestaat eruit dat in een bepaalde periode achtereenvolgens alle nodes in het eigen netwerk worden omgenummerd.

Aangezien er gedurende deze periode feitelijk geen gebruikgemaakt kan worden van het netwerk zal dit waarschijnlijk op een avond of in een weekend moeten gebeuren. Het risico van deze methode is dat door tijdgebrek of onverwachte storingen de migratie niet afkomt en teruggedraaid moet worden. Het nachtmerriescenario is dan dat het terugdraaien niet lukt.
Als het aantal nodes beperkt is, is het voordeel van de strategie dat er geen dubbel werk gedaan wordt. Verder kunnen er technische redenen zijn waardoor dit de enige strategie is die in aanmerking komt.

3.2 Intern NAT

Voor het koppelen van eigen netwerken kan ook worden gekozen voor adrestranslatie tussen deze netwerken. Nu is NAT tussen een intern netwerk en het internet al gecompliceerd. NAT tussen twee interne netwerken maakt de nummerplannen nog onoverzichtelijker. Verder zal blijken dat deze aanpak slechts leidt tot uitstel van executie. Een nieuw nummerplan is nog steeds nodig.

3.3 Dual addresses

Zoals eerder is aangegeven is het veelal mogelijk om machines op hetzelfde netwerk meerdere adressen te geven. Dit kan gedaan worden om servers zowel een adres in het oude als in het nieuwe nummerplan te geven. Hiermee wordt het mogelijk om het omnummeren in kleine stapjes uit te voeren, en het netwerk door te laten werken tijdens de migratie. Uiteraard moeten de routers als eerste worden omgeconfigureerd.
Als het enigszins mogelijk is, is het aan te raden om deze strategie te volgen.

4 STAPPENPLAN

In deze sectie worden onder meer enkele formulieren en tabellen gepresenteerd voor de te verzamelen gegevens. Reken voor het totale project in de orde van een uur per node, dit is exclusief gebruikerstijd. Zie voor verdere inzichten ook de website van PIER - Procedures for Internet and Enterprise Renumbering: http://www.isi.edu/div7/pier.

4.1 Vaststellen doel migratie

Welk zakelijk nut wordt er nagestreefd met de migratie? De meest voorkomende redenen zijn: toegang tot applicaties op andere locaties, toegang tot internet, verbeteren elektronische communicatie. Zonder een expliciet doel van de migratie is aan management en gebruikers niet uit te leggen waar al die moeite en pijn goed voor is. Ook is dit doel de maatlat waarlangs de aanvaardbaarheid van tijdelijk functieverlies wordt afgemeten.
Op hoog niveau wordt nu de communicatie met een ‘opdrachtgever’ ingericht. Deze bewaakt voortgang en verdedigt het project-

team tegen de rest van de organisatie. Als een van de eerste stappen wordt contact gezocht met alle interne en externe partijen die door de omnummering worden geraakt.

4.2 Inventarisatie uitvoeren

Van alle relevante hardware en software moet worden gedocumenteerd waar en hoe er gebruik wordt gemaakt van IP-adressen. Een lijst van na te lopen punten is:

- Routers, switches, WAN-links, en LAN-links;
- Servers en firewalls. DNS-Zone files. NNTP, NTP, access control lists;
- Pc's, printers. Een truc is om een 'bekend' IP-adres te nemen (van een belangrijke server of zo) en daarop alle files en de registry van Windows te doorzoeken;
- Applicaties (licenties, hardcoded IP-adressen). Als er geen applicaties worden gevonden met harde IP-adressen, ga er dan maar vanuit dat er niet goed gezocht is;
- Externe partijen (denk onder meer aan VPN-koppelingen).

Het resultaat van deze stap is dus een lijst van aan te passen componenten, hun huidige nummer, locatie en verantwoordelijke beheerder.

Wellicht is dit een goed moment om een rigoureuze opschoonactie uit te voeren en eventueel over te stappen op modernere vormen van beheer.

4.3 Nummerplan maken

Een nummerplan definieert hoe blokken adressen worden toegekend aan locaties. Een locatie is een verzameling machines die in een LAN hangen. Locaties worden gekoppeld met WAN-technologie. Met moderne LAN-switching-technologie is het niet nodig om binnen een locatie een verdere onderverdeling te maken.
Het nieuwe nummerplan moet liefst een jaar of vijf meekunnen. Documenteer de aannames die de grondslag vormen voor deze inschattingen. Om hoeveel locaties zal het gaan? Hoeveel nodes hebben deze locaties gemiddeld, dan wel maximaal? Hoe wordt er omgegaan met groei binnen een locatie, groei van het aantal locaties? Probeer verder te vermijden dat er adressen zijn die zowel in het oude als in het nieuwe plan geldig zijn.
In de inleiding van dit artikel wordt een aantal aanleidingen voor een omnummering genoemd. Welke daarvan kunnen binnen vijf jaar opnieuw optreden? De 'boete' voor verkeerd inschatten is opnieuw omnummeren.

4.4 Routeringsplan maken

Veelal heeft een organisatie slechts behoefte aan een statisch routeplan, omdat er nooit twee verschillende routes tussen twee punten

zijn. Voor wat grotere organisaties is er veelal een backbone waarop redundantie aanwezig is, en geldt voor de meeste locaties dat ze alleen een route naar de backbone hoeven te kennen. Probeer routeringsinformatie te beperken tot zo weinig mogelijk machines. De overige kunnen dan volstaan met een default route. Complicaties zijn er vooral bij en rond de firewall en de eventuele ontkoppelingsnetwerken die dan vaak ontstaan.
Een aantal machines zal routeringsinformatie hebben. Bij voorkeur is dat een enkele machine per locatie, meestal de router waar de WAN-verbinding aan hangt. Van deze machines moet de routeringstabel zorgvuldig worden vastgesteld. Het volgende voorbeeld illustreert de structuur van deze tabel. Deze tabel komt overeen met de uitvoer van het programma 'route print' onder Windows. Onder andere operating systems zijn vergelijkbare programma's die een vergelijkbare presentatie geven.
De eerste kolom bevat het bestemmingsadres. De tweede kolom (mask) geeft aan hoe specifiek deze route is. Is het mask bijvoorbeeld 255.255.255.0 dan geldt deze route voor alle adressen die in de eerste 24 bits overeen komen met de 'destination'. Een dergelijke route leidt naar een router die het koppelpunt is met het volgende netwerk. Deze router kan bereikt worden via de interface waarvan het adres in de vierde kolom staat (in IP heeft immers elke interface een eigen adres, hier 192.168.2.2). De 'interface metric' geeft aan wat de 'kosten' zijn van een route. Routeren gebeurt altijd naar de meest specifieke route. De route 0.0.0.0 is dus de default route als er geen andere route is.
Tabel 3 ziet er ingewikkeld uit, maar zegt in feite alleen dat we hier op netwerk 192.168.2/8 zitten, en dat al het andere verkeer naar de default gateway 192.168.2.220 gaat.

TABEL 3

Destination NetworkAddress	*Networkmask*	*Gateway(router)*	*Address*	*Interface Metric*
0.0.0.0	*0.0.0.0*	*192.168.2.220*	*192.168.2.2*	*1*
127.0.0.0	*255.0.0.0*	*127.0.0.1*	*127.0.0.1*	*1*
192.168.2.0	*255.255.255.0*	*192.168.2.2*	*192.168.2.2*	*1*
192.168.2.2	*255.255.255.255*	*127.0.0.1*	*127.0.0.1*	*1*
192.168.2.255	*255.255.255.255*	*192.168.2.2*	*192.168.2.2*	*1*
224.0.0.0	*224.0.0.0*	*192.168.2.2*	*192.168.2.2*	*1*
255.255.255.255	*255.255.255.255*	*192.168.2.2*	*0.0.0.0*	*1*

Zorg dat zowel de oude als de nieuwe tabel op papier beschikbaar zijn.

4.5 Omnummerplan maken

Op basis van de inventarisatie van nodes en het nummerplan wordt er een omnummer plan gemaakt. Dit bestaat uit een aantal tabellen. Een voorbeeld van zo'n tabel is tabel 4.

Tabel 4

Locatie	*Amsterdam*			
Netwerkadres:	*192.168.128/10*			
Subnetmask:	*255.255.252.0*			
Default gateway:	*192.168.128.1*			
DNS:	*192.168.128.5*			
Machine	***Nieuw***	***Oud***	***NAT***	***Wie?***
Server 1	*192.168.128.10*	*10.1.1.1*	*194.73.19.82*	*Laurel*
Printer 1	*192.168.128.100*	*10.1.1.100*	*geen*	*Hardy*

De kolom NAT wordt ingevuld met het eventuele externe adres dat de machine heeft. Bij de laatste kolom wordt aangegeven wie verantwoordelijk is voor het omnummeren van deze machine.
Verder hoort bij dit omnummerplan de nieuwe configuraties van de DNS- en DHCP-servers, en van alle routers.

4.6 Draaiboek en testplan maken

Het draaiboek van de daadwerkelijke omnummering kan nu gemaakt worden, of dat nu een geleidelijke, of een D-day aanpak wordt. In hoofdlijnen zijn de stappen als volgt:

1 Controleer of alle documentatie en alle plannen gereed zijn;
2 Voorzie alle routers van een dubbel nummerplan;
3 Geef alle servers dubbele adressen;
4 Test, in verband met eventuele roll-back, alle belangrijke functionaliteit;
5 Herstart DNS in het nieuwe nummerplan;
6 Herstart DHCP in het nieuwe nummerplan;
7 Omnummeren van servers die maar één adres hebben;
8 Test de herstart en correcte werking van een DHCP-client;
9 Aanpassen firewall;
10 Testen;
11 Herstarten alle DHCP-clients;

12 Testen;
13 (Na enige tijd) opruimen van oude nummers op servers en routers.

Het migratiedraaiboek moet ook bij alle tests een 'fall back'-plan hebben, voor het geval de tests falen, en reparaties niet slagen. Essentieel is vast te stellen wie de bevoegdheid heeft om hier besluiten te nemen over bijvoorbeeld tijdelijk functieverlies.
Meerdere malen tijdens dit plan moet worden getest of alles nog werkt. Omdat het een netwerkomnummering betreft, die bovendien geen functionele impact hoeft te hebben, moet vooral naar de connectiviteit gekeken worden. De belangrijkste punten zijn:
- Kunnen clients bij alle relevante applicaties, ook over locatiegrenzen heen?
- Kan er e-mail uitgewisseld worden tussen locaties en met externen?
- Kan er ingebeld worden?
- Kan er geprint worden?

4.7 Communicatieplan maken

Beschrijf wie met welke frequentie waarover wordt geïnformeerd. Beschrijf hoe gebruikers hun problemen kunnen melden, en wat de escalatieprocedures zijn. Zorg dat van helpdesks van toeleveranciers (bijvoorbeeld firewall) de juiste contactgegevens beschikbaar zijn op papier, ook de noodnummers voor buiten kantooruren.

4.8 Gebruikersinstructie

Indien er iets aan de configuratie van gebruikersmachines moet wijzigen kan het nodig zijn om dit door de gebruikers zelf te laten doen. De hiervoor benodigde gebruikersinstructie moet in ieder geval de volgende elementen bevatten:
- Reden van de migratie;
- Planning van het tijdstip waarop een en ander kan gebeuren respectievelijk gebeurd moet zijn;
- Gedetailleerde instructies, met screenshots, van de uit te voeren handelingen;
- Aangeven van helpdesk-procedures. Het kan handig zijn om per functionele eenheid een 'power user' te benoemen die vragen kanaliseert.

Uiteraard dient een instructie als deze door een aantal personen uit de doelgroep getest te worden. Deze moeten er zonder additionele uitleg mee uit de voeten kunnen.

4.9 Completion party

Als alles gemigreerd is, en goed bevonden, is het tijd voor een completion party. Afhankelijk van de tijd van de dag kan hier gekozen worden voor taart of champagne. Een netwerkmigratie raakt ver en diep. Zorg dat iedereen die een bijdrage heeft geleverd daarvoor wordt bedankt.

Nawoord

Ik wil alle collega's die een bijdrage hebben geleverd aan dit artikel hartelijk bedanken.

Auteursgegevens

Peter van Eijk is consultant bij Deloitte en Touche Bakkenist. E-mail: pve@van-eyk.net.