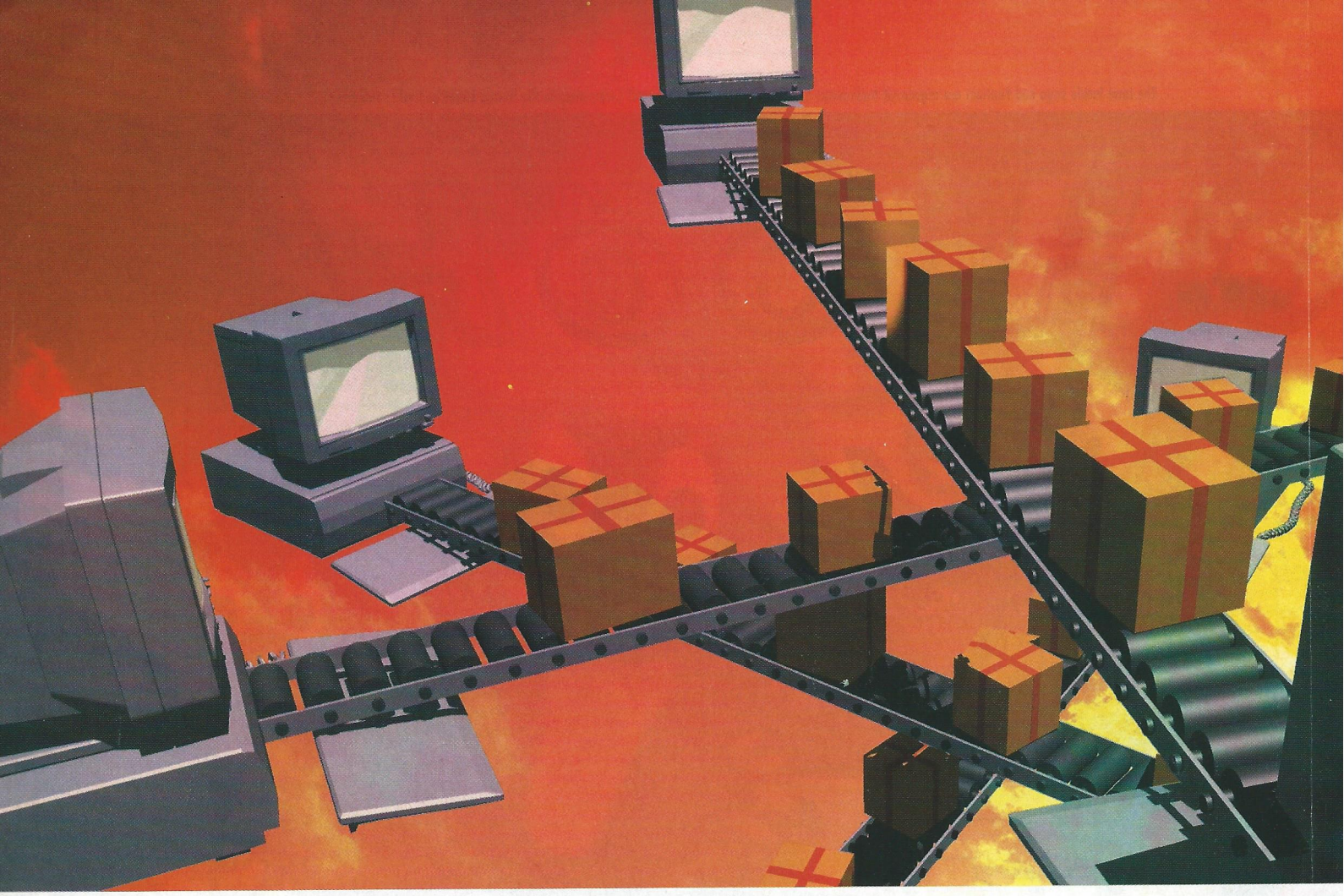


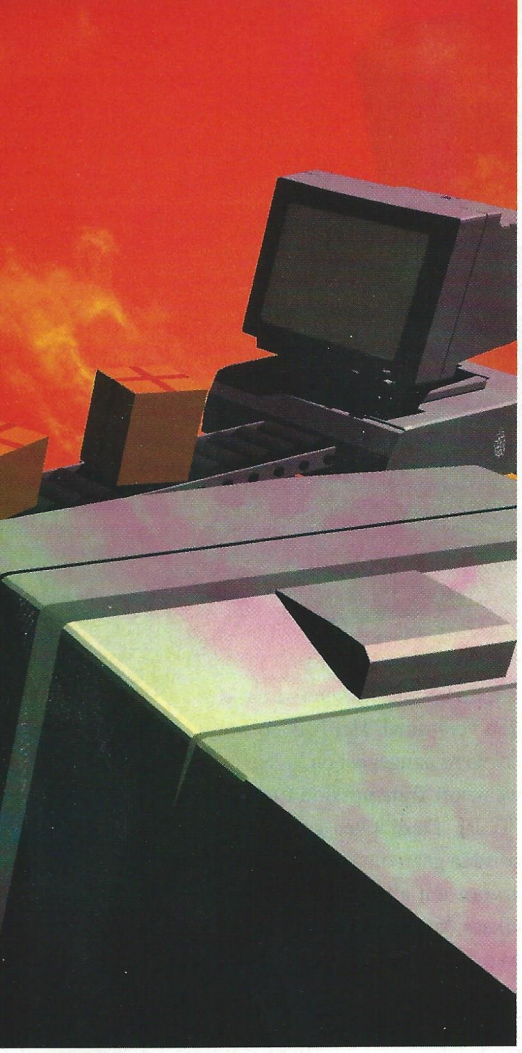
Delen zonder risico

Rinie Hooijer

Het is een nieuwe rage: met je eigen netwerk het Internet op gaan. En masse worden in Nederland allerlei servers geïnstalleerd om die éne Internet-aansluiting te kunnen delen met anderen. Alles lijkt goed te gaan. Maar op een dag blijken al u bestanden te zijn verdwenen, worden anderen de baas over uw computer en wordt uw bankrekening geplunderd. Eenmaal bekomen van de schrik blijft u achter met de vraag: "Wat deed ik fout?"

Duizenden mensen hebben in het verleden thuis een computernetwerkje aangelegd met als voornaamste reden toch nog iets nuttigs te kunnen doen met die 'oudere' computers. Dit netwerk stelt hen in staat om schijven, bestanden en modems te delen en natuurlijk tegen elkaar een fantastisch spel te spelen. Het aanleggen van zo'n netwerk dat niet is gekoppeld aan het Internet is een relatief eenvoudige klus, kost niet al te veel, en u hebt er bovenal niet veel computerkennis voor nodig. Door het toenemende Internet-gebruik zien we dat de reden om een netwerkje aan te leggen een totaal andere is. Men wil nu een Internet-aansluiting delen zodat de overige gezinsleden, vrienden of medestudenten ook via die éne aansluiting kunnen surfen, mailen of FTP kunnen gebruiken. Zeker onder de mensen die een permanente Internet-aansluiting hebben via de kabel is het opzetten van een dergelijk netwerk erg populair.

Maar hiervoor is kennis nodig. Kennis van proxyservers om gezamenlijk te kunnen surfen. Kennis van mailservers zodat iedereen kan e-mailen, kennis van FTP-servers zodat iedereen in staat is om bestanden te downloaden en bovenal kennis van beveili-



Met uw netwerk het Internet op

ging om indringers te weren. Is deze kennis niet aanwezig, dan kunnen de gevolgen wel eens erger zijn dan u denkt.

Want hoe zou u het vinden als de politie op de stoep staat met het verhaal dat u kinderporno in uw bezit hebt en achteraf blijkt dat een andere Internetter via uw proxyserver, dus onder uw naam, illegaal bezig is geweest? Of wanneer u een torenhoge rekening krijgt van uw provider omdat u ver over uw datalimiet heen bent en achteraf blijkt dat iemand 1500 MB aan bestanden op uw FTP-server heeft gezet? En ongetwijfeld hebt u ook al iets gehoord over de zogenaamde 'Trojan Horses', waarvan de bekendste Back Orifice, Netbus en Masters Paradise zijn. Met deze programmaatjes is het mogelijk om een computer op afstand te bedienen. Deze Trojan Horses bestaan namelijk uit twee verschillende gedeelten: een server en een client. Door de server op een andere computer te installeren, kunnen de twee afzonderlijke delen met elkaar communiceren. Uitermate handig zult u denken. Maar zal die gedachte niet veranderen wanneer uzelf ongemerkt het servergedeelte van zo'n programma installeert en al uw wachtwoorden, bankgegevens en creditcardnummers open staan voor heel de wereld?

Toch is, wat de Trojan Horses betreft, de soep niet zo heet als deze wordt opgediend. Alle horrorverhalen ten spijt zijn de gevaren van Trojan Horses eenvoudig te voorkomen door de juiste programma's te installeren of door simpelweg geen bestanden te activeren waarvan u niet zeker weet of ze veilig zijn.

We leggen hier expres de nadruk op activeren en niet op downloaden omdat dat vaak niet eens nodig is. Verderop in dit verhaal zullen we u laten zien dat we met gemak op de harde schijf van een aantal mensen kunnen komen en daarop simpelweg een bestand kunnen neerzetten of verwijderen. Als we kwaadwillend zijn, kunnen we hier met gemak een verklede Trojan Horse plaatsen die nadat de gebruiker deze heeft geactiveerd ervoor zorgt dat wij de baas worden over die computer en over hun netwerk. In dit specifieke geval heeft ons potentiële 'slachtoffer' blijkbaar geen idee van de gevaren waaraan hij zich blootstelt. En hij is echt niet de enige!

Het zijn gevaren die ook u kunnen overkomen als uw netwerk niet goed is geïnstalleerd. Natuurlijk is bijna ieder computernetwerk te kraken, maar sommige mensen maken het de andere Internetters wel heel erg eenvoudig om op hun computer te komen. Gelukkig zijn er onafhankelijk van ieder besturingssysteem tal van zaken die eenvoudig zijn te verbeteren. Maar inderdaad, je moet ze maar net even weten.

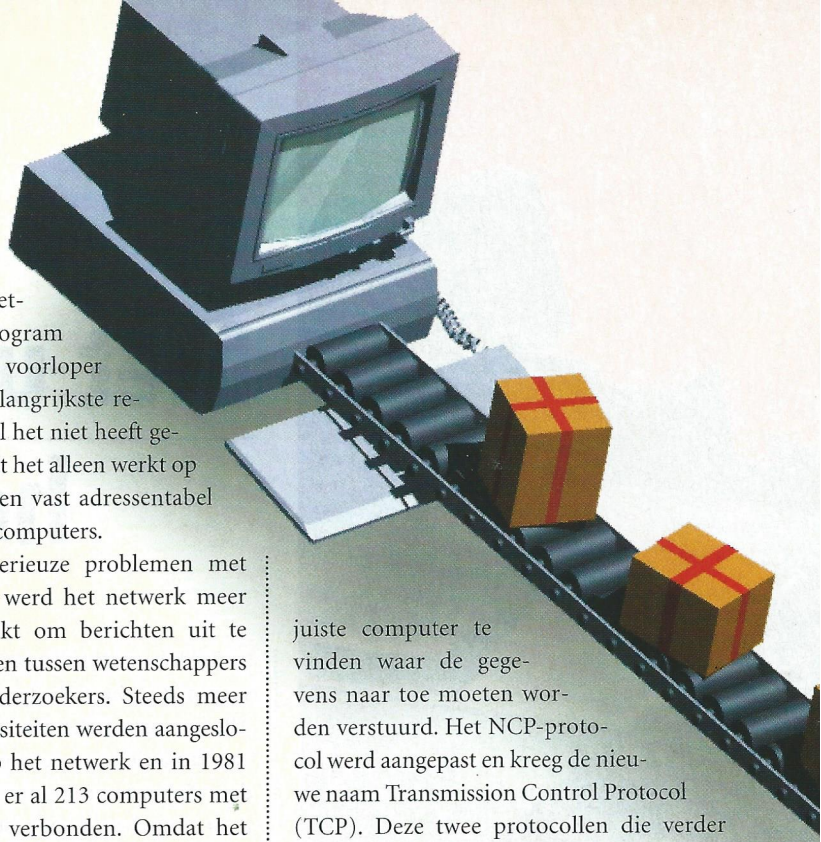
Daarom gaat Computer!Totaal de komende vijf maanden zeer veel aandacht besteden aan de vele netwerkaspecten waarmee u te maken krijgt als u met uw netwerk online gaat. We zullen gaan schrijven over de werking van proxy-, mail- en FTP-servers en we kijken ook naar wat de markt u op dit gebied te bieden heeft. Daarnaast natuurlijk veel aandacht voor de beveiliging van uw netwerk. Niet met de belofte dat uw systeem niet meer te kraken is, want dat is ieder systeem, maar wel met genoeg oplossingen zodat u rustig kunt gaan slapen zonder uw computer te hoeven uitzetten. Om dat te kunnen bereiken kijken we naar firewalls, utilities om het netwerk in de gaten te houden en de verschillende protocollen waardoor computers onderling kunnen communiceren. Als uitsmijter, nadat u uw beveiliging op orde hebt, zullen we nog eens in een apart verhaal aandacht besteden aan de verschillende programmaatjes, zoals de Trojan Horses, die een potentieel gevaar kunnen zijn voor u en uw mede Internetter.

De komende maanden staat u dus het een en ander te wachten. Zit u tijdens onze verhalenreeks met vragen of problemen dan kunt u deze altijd stellen. Speciaal daarvoor hebben we in het Forum een 'Netwerk'-onderdeel geopend. U kunt ons ook een e-mailtje sturen en wel naar netwerk@computertotaal.nl.

Protocollen

De eerste stap in het goed aanleggen van een netwerk waarmee u het Internet opgaat is een juiste instelling van de netwerkprotocollen. Deze instellingen kunt u opgeven bij het 'Netwerk'-icoontje in het configuratiescherm. Hoe u dat moet doen en waarop u moet letten vertellen we uitgebreid verderop. Allereerst gaan we kijken wat de belangrijkste protocollen zijn, waaruit ze bestaan en waarom ze zo belangrijk zijn voor de beveiliging van uw netwerk.

Een protocol is niets anders dan een aantal afspraken waaraan een computer zich moet houden als deze met een andere computer wil communiceren. In feite is protocol een duur woord voor gedragsregels waar iedereen dagelijks mee wordt geconfronteerd. Want waarom rijdt u altijd rechts op de weg en niet links? Simpelweg omdat daarover afspraken zijn gemaakt, oftewel er bestaat een



protocol waarin staat hoe u zich moet gedragen in het verkeer. Houdt u zich daar niet aan, dan hebt u grote kans dat de medeweggebruiker (lees andere computer) u niet begrijpt met alle gevolgen van dien. Net zoals we verschillende protocollen kennen in het dagelijkse leven geldt dat ook voor computers. Veel daarvan zult u als particulier zeker niet gebruiken. De twee protocollen waarmee u het meest te maken krijgt zijn NetBEUI en TCP/IP.

NetBEUI is een Microsoft protocol dat alleen bruikbaar is in Windows- en IBM-netwerken. Het zorgt ervoor dat als u op het icoontje 'Netwerkomgeving' op uw desktop klikt, u de andere aanwezige computers binnen het netwerk kunt ziet. De beperking van NetBEUI is dat het alleen werkt binnen één enkel netwerk: het is een 'non-routable protocol'. Dit wil zeggen dat het protocol niet in staat is om te communiceren met andere netwerken. NetBEUI is daarom niet geschikt voor het Internet.

Het meest gebruikte protocol ter wereld is TCP/IP. Dit protocol dat wel in staat is om te communiceren met andere netwerken vormt de basis van het Internet. Alle computernetwerken ter wereld kunnen ongeacht met welk besturingssysteem met dit protocol overweg. Reden genoeg om eens wat dieper in te gaan op de eigenschappen en geschiedenis van dit protocol.

TCP/IP

Op het hoogtepunt van de Koude Oorlog eind jaren zestig vroegen de Amerikanen zich af hoe zij moesten communiceren met elkaar en met bondgenoten ten tijde van een nucleaire aanval. Het antwoord werd gevonden in een netwerk van computers waar niemand de baas was. Het grote voordeel hiervan was dat als er een computer uitviel de overige computers gewoon met elkaar in contact konden blijven. Het Pentagon zag daar wel iets in en richtte in december 1969 de projectgroep 'Advanced Research Project Association' op. Het jonge netwerk kreeg de naam ARPANET, de naam van de belangrijkste geldschieter. Binnen drie jaar had men het voor elkaar dat er 37 computers met elkaar konden communiceren over een grote afstand. Deze computers waren alle voorzien van een uniek netwerkadres met een lengte van 8 bits. Het maximaal aantal computers dat dus kon worden aangesloten was 256. De computers binnen dit éne netwerk communiceerde met elkaar door middel van het Network Control Program (NCP) protocol, de voorloper van TCP/IP. De belangrijkste reden dat dit protocol het niet heeft gehaald, komt doordat het alleen werkt op een netwerk met een vast adressentabel van maximaal 256 computers.

Mede omdat serieuze problemen met Rusland uitbleven werd het netwerk meer gebruikt om berichten uit te wisselen tussen wetenschappers en onderzoekers. Steeds meer universiteiten werden aangesloten op het netwerk en in 1981 waren er al 213 computers met elkaar verbonden. Omdat het maximum van het netwerk bijna was bereikt en de beheersproblemen te groot werden, besloot de Amerikaanse overheid in 1983 het ARPANET te splitsen in het MILNET voor militaire organisaties en een nieuw ARPANET voor niet-militaire organisaties. Het was echter wel de bedoeling dat de twee nieuwe netwerken met elkaar verbonden bleven.

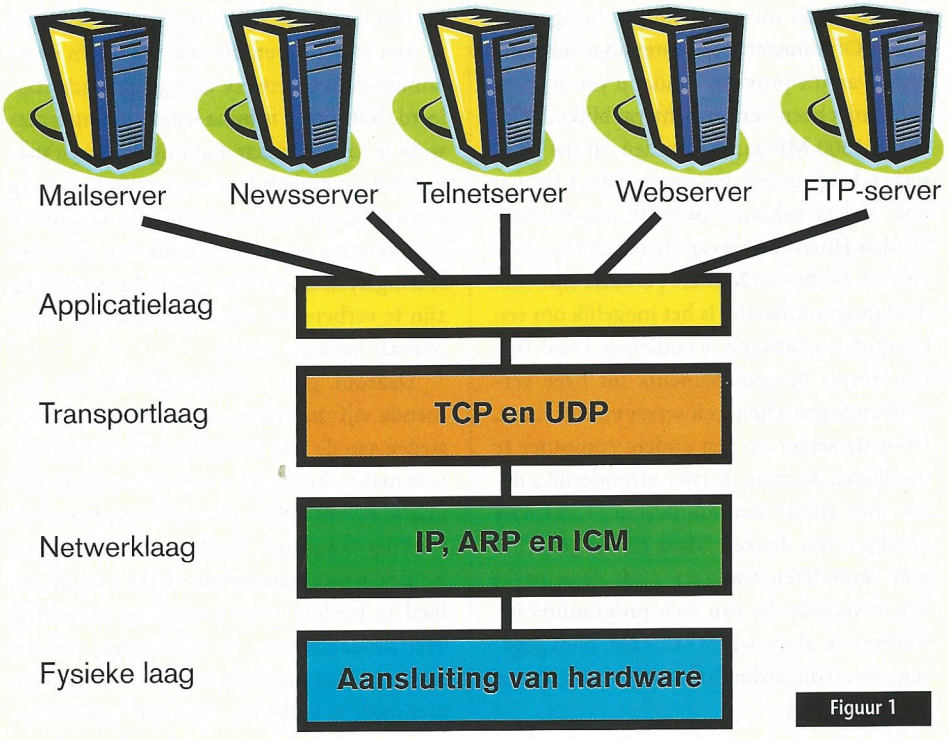
TCP/IP is het meest gebruikte protocol ter wereld

En dat is het moment waarop het Internet Protocol (IP) werd uitgevonden. Dit protocol is in staat om de route te bepalen en de juiste computer te vinden waar de gegevens naar toe moeten worden verstuurd. Het NCP-protocol werd aangepast en kreeg de nieuwe naam Transmission Control Protocol (TCP). Deze twee protocollen die verder zouden gaan onder de naam TCP/IP zorgden ervoor dat alle netwerken op de wereld met elkaar konden communiceren en daarmee was de geboorte van het Internet een feit.

TCP/IP-suite

Vaak zijn namen misleidend en dat is niet anders bij de protocolnaam TCP/IP. Na het ontstaan van dit protocol zijn er tal van onderdelen aan toegevoegd. Het is dan ook beter om te spreken van TCP/IP-suite; een bonte verzameling gedragsregels die al het ver-

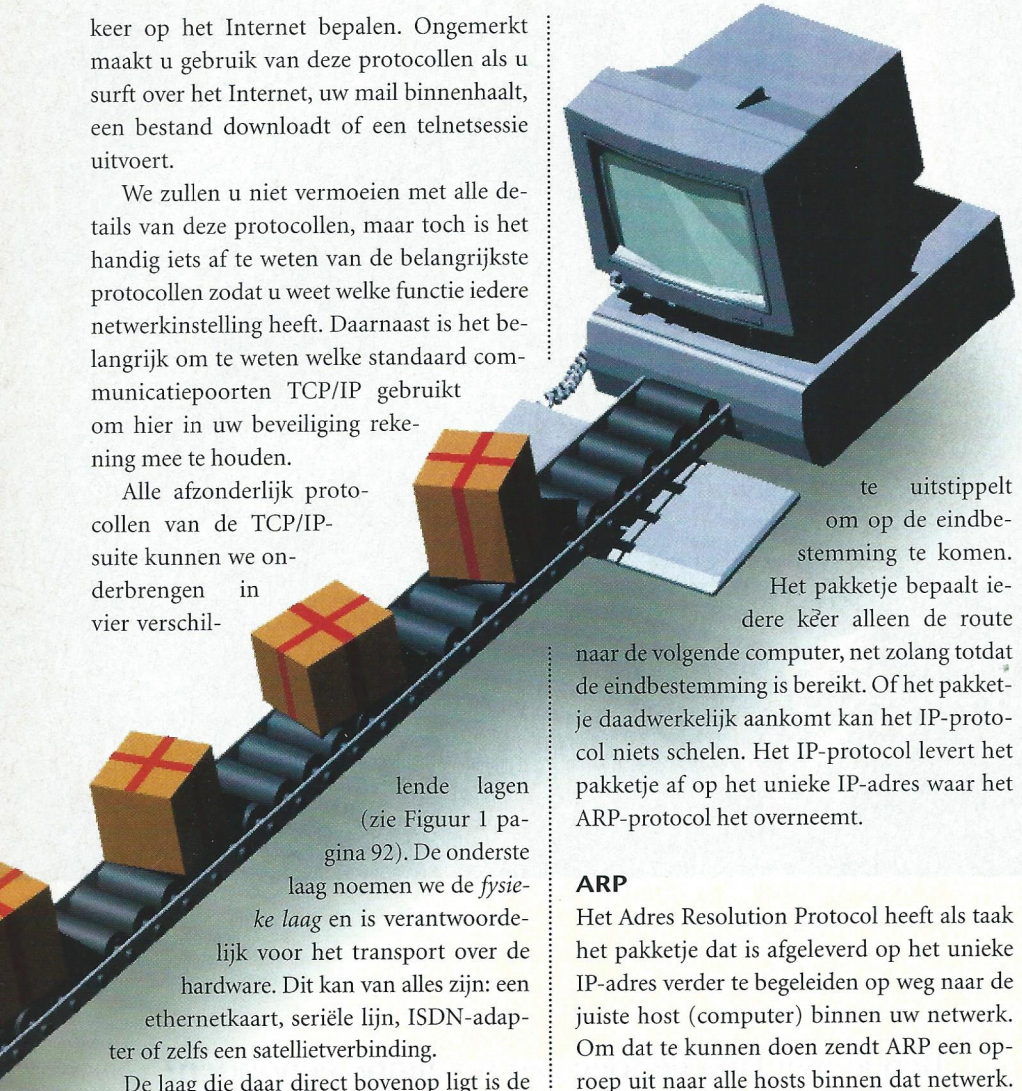
De TCP/IP-suite



Figuur 1

keer op het Internet bepalen. Ongemerkt maakt u gebruik van deze protocollen als u surft over het Internet, uw mail binnenhaalt, een bestand downloadt of een telnetsessie uitvoert.

We zullen u niet vermoeien met alle details van deze protocollen, maar toch is het handig iets af te weten van de belangrijkste protocollen zodat u weet welke functie iedere netwerkinstelling heeft. Daarnaast is het belangrijk om te weten welke standaard communicatiepoorten TCP/IP gebruikt om hier in uw beveiliging rekening mee te houden.



Alle afzonderlijk protocollen van de TCP/IP-suite kunnen we onderbrengen in vier verschillende lagen (zie Figuur 1 pagina 92). De onderste laag noemen we de *fysieke laag* en is verantwoordelijk voor het transport over de hardware. Dit kan van alles zijn: een ethernetkaart, seriële lijn, ISDN-adapter of zelfs een satellietverbinding.

De laag die daar direct bovenop ligt is de *Netwerklaag* en die zorgt ervoor dat uw computer contact kan leggen met een andere computer. De belangrijkste protocollen die in deze laag worden gebruikt zijn IP, ARP en ICMP.

IP

De belangrijkste taak van het Internet Protocol is het vinden van een route naar de eindbestemming. Het maakt hiervoor gebruik van IP-adressen die uniek zijn. (Zie kader Ipv6.) Het IP-protocol werkt niet met vaste netwerkverbindingen. Dit betekent dat ieder pakketje dat wordt verstuurd, zijn eigen route uitstippelt om op de eindbestemming te komen. Het pakketje bepaalt iedere keer alleen de route naar de volgende computer, net zolang totdat de eindbestemming is bereikt. Of het pakketje daadwerkelijk aankomt kan het IP-protocol niets schelen. Het IP-protocol levert het pakketje af op het unieke IP-adres waar het ARP-protocol het overneemt.

POORTNUMMERS

Server	Poortnummer	Transportprotocol
HTTP	80	TCP/UDP
FTP	21	TCP
SMTP	25	TCP
POP3	110	TCP
Telnet	23	TCP/UDP
DHCP	67/68	TCP/UDP
DNS	53	TCP/UDP

ARP

Het Adres Resolution Protocol heeft als taak het pakketje dat is afgeleverd op het unieke IP-adres verder te begeleiden op weg naar de juiste host (computer) binnen uw netwerk. Om dat te kunnen doen zendt ARP een oproep uit naar alle hosts binnen dat netwerk. Deze oproep gebeurt niet op basis van IP-adressen maar op basis van MAC-adressen. Iedere ethernetkaart in een computer bezit namelijk zo'n uniek Medium Access Control-adres dat door de fabrikant is ingesteld. Het MAC-adres dat zich aangesproken voelt door de oproep zal reageren, waarmee de 'echte eindbestemming' is bereikt.

ICMP

Het zal u vast wel eens zijn overkomen dat uw e-mailapplicatie de melding geeft dat de eindbestemming niet is gevonden omdat de 'destination host unreachable' is. Dit bericht wordt gegenereerd door het Internet Control Message Protocol (ICMP) dat fouten registreert en dat vervolgens aan u laat weten.

De derde laag heet *transportlaag* en zorgt voor de communicatie tussen applicaties, waardoor het mogelijk wordt dat een client met de juiste server kan communiceren. Om de juiste server te kunnen aanspreken gebruiken de transportprotocollen 'poortadressering'. Omdat de computer beschikt over tienduizenden poorten, zijn aan de belangrijkste servers vaste nummers toegekend. Zo kunt u bijvoorbeeld een proxyserver, die het HTTP-protocol gebruikt, benaderen met poortnummer 80. (zie kader Poortnummers.) De komende maanden zullen we u laten zien dat deze poortnummers een belangrijke rol spelen in de beveiliging van uw computer. Voor nu hoeft u alleen te weten dat ieder pakketje dat u verzendt over het Internet een poortnummer bevat. De transportprotocollen leveren dit pakketje vervolgens af aan de server met hetzelfde poortnummer. De twee belangrijkste transportprotocollen zijn TCP en UDP.

TCP

Het Transmission Control Protocol is zeer belangrijk. Het zorgt er namelijk voor dat uw data op een veilige manier en compleet aankomt op de eindbestemming. Het is hiertoe in staat omdat het alle foutcontroles uitvoert die er zijn. Komt er een pakketje niet aan met het IP-protocol, dan zorgt TCP ervoor dat dit pakketje opnieuw wordt verstuurd. Het TCP-protocol maakt gebruik van een vaste verbinding tussen client en server. Als de verbinding tot stand is gekomen wisselen de client en server gegevens uit met elkaar. Zo weten ze precies van elkaar hoeveel data er moet worden verstuurd en zijn ze in staat om elkaar af te remmen als de data te snel binnenkomt.

UDP

Uw applicaties kunnen ook gebruik maken van het User Datagram Protocol. Dit protocol is veel minder veilig dan het veel grotere TCP-protocol. UDP geeft u namelijk niet de garantie dat uw pakketjes compleet aankomen en het legt geen verbinding met de eindbestemming. UDP zendt een signaal uit naar alle computers binnen een netwerk en iedere computer met dezelfde server kan dit signaal opvangen.

De bovenste laag van de TCP/IP-suite is de *applicatielaag*. In deze laag bevinden zich de protocollen die direct communiceren met de applicaties die u als eindgebruiker gebruikt. U kunt dan denken aan een e-mailpakket, een browser of een FTP-programma. Is de communicatie geslaagd, dan geven de protocollen in de applicatielaag de gegevens door aan de transportprotocollen. Omdat er meer dan twintig verschillende protocollen zijn in deze laag, zullen we alleen de bekendste toelichten. Daarnaast zullen de komende maanden meerdere protocollen worden uitgediept.

HTTP

Het Hyper Text Transfer Protocol is verantwoordelijk voor de communicatie op het World Wide Web. HTTP verstuurt HTML-pagina's met tekst, beeld en geluid naar uw browser. Het protocol is alleen actief als een verbinding wordt gelegd met een server of wanneer een server reageert op een verzoek van een client.

FTP

Om bestanden te kunnen downloaden van het Internet wordt vaak gebruik gemaakt van het File Transfer Protocol. Dit protocol zorgt er bijvoorbeeld voor dat u uw website bij de provider op de server kunt zetten.

SMTP

Voor het versturen van een e-mail naar een andere computer is het Simple Mail Transfer Protocol verantwoordelijk. Dit protocol gaat er vanuit dat de postbus van de ontvanger altijd bereikbaar is. Natuurlijk is dat niet zo en daarom werd er een aanvullend protocol ontwikkeld: POP3.

POP3

Omdat het met SMTP niet mogelijk is om mail op te halen van een mailserver werd het Post Office Protocol, versie 3, ontwikkeld. Met dit protocol kunt u mail ophalen maar niet versturen. Vandaar dat u van uw provider zowel de naam van een SMTP-server als POP3-server krijgt.

Telnet

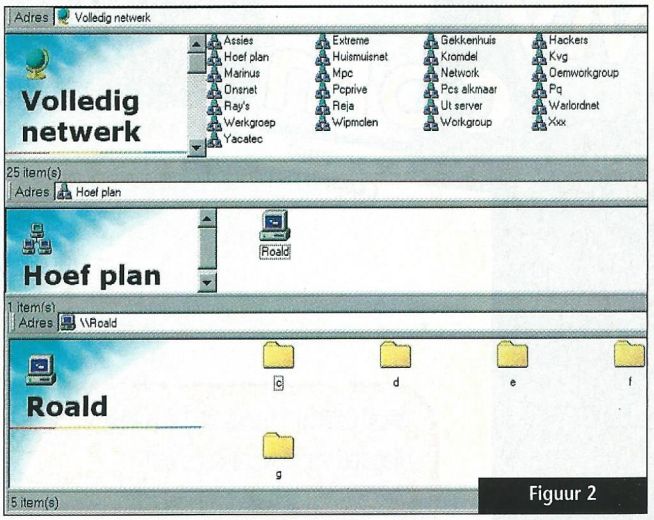
Het Telnet-protocol stelt u in staat om direct te kunnen werken op een andere computer. U kunt dan alles doen wat u ook kunt op uw eigen computer. U moet er alleen rekening mee houden dat u in een terminalvenster werkt en dus niet beschikt over grafische mogelijkheden.

DHCP

Niet iedereen in de wereld kan een vast IP-adres krijgen, simpelweg omdat er niet genoeg zijn. Dit is ook de reden waarom providers vaak extra geld vragen als een klant een vast IP-adres wil hebben. Om nu zo efficiënt mogelijk met IP-adressen te kunnen omgaan maakt een provider gebruik van een Dynamic Host Configuration Protocol server. Als gebruiker moet u op deze server inloggen en dan krijgt u een 'dynamisch' IP-adres toegewezen. Sluit u de verbinding af, dan wordt het IP-adres aan een andere gebruiker toegekend.

DNS

Het laatste protocol dat we hier zullen aanstippen is het Domain Name System protocol, dat verantwoordelijk is voor de vertaling van domeinnamen naar numerieke IP-adressen. Dit is zeer handig, anders zou u in plaats van domeinnamen (www.computertotaal.nl) IP-nummers moeten onthouden.



Waarschijnlijk had u nooit gedacht dat een protocol als TCP/IP voor zoveel zaken verantwoordelijk was. Bij het opzetten van een eigen netwerk met vaste verbinding naar het Internet en dat voorzien is van een aantal servers, krijgt u altijd te maken met het merendeel van de bovengenoemde protocollen. Draait u geen servers dan zullen de meeste instellingen voor u geen problemen opleveren omdat u hiervoor de gegevens krijgt van uw provider.

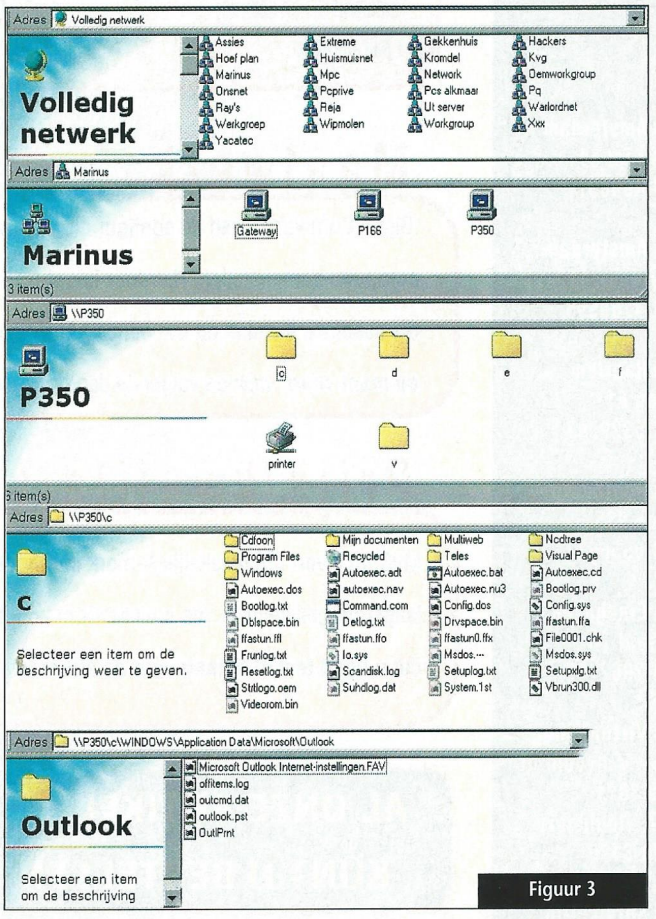
Wat wel problemen kan opleveren, ongeacht of u servers draait, zijn de instellingen van de netwerkprotocollen zoals NetBEUI en TCP/IP. Een verkeerde instelling van deze protocollen kan verstrekkende gevolgen hebben.

Zichtbaar voor iedereen

We hebben u verteld dat NetBEUI het standaard protocol is voor Windows- en IBM-netwerken. Is dit protocol eenmaal geïnstalleerd dan toont het alle computers binnen het netwerk die ook dit protocol hebben. U kunt dit controleren door op uw desktop op 'Netwerkomgeving' te klikken en vervolgens te kiezen voor 'Volledig netwerk'. Is het protocol op uw netwerk geïnstalleerd dan ziet u nu alle computers binnen uw eigen netwerk.

Het TCP/IP-protocol, waarmee u communiceert op het Internet, heeft ook een dergelijke functie. Standaard heeft dit protocol bindingen met het Microsoft-netwerk en is daardoor in staat gedeelde schijven of computers te tonen. En dat niet iedereen dit door heeft blijkt uit het volgende voorbeeld.

Op een dag klikten wij, na alle beveiligingen te hebben uitgezet, met onze muis op het welbekende netwerkicoontje op de desktop en daarna op 'Volledig netwerk'. We kregen 25 computers in beeld die allemaal aangesloten zijn op de kabel in Alkmaar. (Zie Figuur 2). Uiteraard zijn wij nieuwsgierig en we klikten willekeurig op de verschillende icoontjes voor onze neus. De eerste compu-



IPV6, INTERNET PROTOCOL THE NEXT GENERATION

Iedere computer op het TCP/IP-netwerk heeft een uniek adres. Deze wordt door IP (Internet Protocol) routers gebruikt om de pakketjes met gegevens naar de juiste plaats te versturen. Dit adres is 32 bits lang, oftewel 4 bytes. Door de manier van toewijzen van de adressen aan apparatuur en de onderverdeling in de A-, B- en C-klassen is het niet mogelijk om alle 4 miljard mogelijke adressen efficiënt te verdelen. Met de enorme groei van het Internet levert dit een groot probleem op: er zijn niet genoeg adressen. De introductie van het Common Interdomain Routing Protocol (CIRP) maakt het mogelijk om uit een aantal type C-adressen een soort mini klasse B-netwerk te maken, zodat de verdeling van de adressen iets efficiënter wordt.

Een ander probleem dat ontstaat is de grote van de routingtabellen. Een router bepaalt welke weg een pakketje over het netwerk moet gaan om op de plaats van bestemming te komen. Een router moet weten welke netwerken zijn aangesloten, en dit doet hij door middel van het bijhouden van tabellen. Doordat de IP-adressering slechts twee hiërarchische niveaus kent kunnen deze tabellen nogal groot worden. Ook hier weer biedt CIRP een voorlopige oplossing. Maar het blijft een lapmiddel. Hoelang we het nog volhouden met de huidige vierde versie van IP is niet bekend, maar dat er iets constructief moet gebeuren moge duidelijk zijn.

Om deze problemen tegen te gaan is in 1996 een opvolger van IPv4 bedacht: IP versie 6, ofwel IP next generation. Een van opmerkelijkste verschillen is wel de grote van het adres. Waar er bij IPv4 32 bits werden gebruikt, heeft IPng de beschikking over 128 (!) bits, ofwel 16 bytes. De notatie voor zo'n adres is x:x:x:x:x:x:x:x:x:x:x:x:x:x:x:x, waarbij een x de hexadecimale notatievorm van een byte is en de bytes worden gescheiden door een dubbele punt. Dit in tegenstelling tot de huidige notatievorm welke d.d.d.d is. Vier decimalen gescheiden door een punt.

Er zit meer vast aan IPv6. De volgende generatie IP-adressen zullen door de nieuwe hiërarchische structuur veel minder vast zitten aan één plaats. U kunt uw eigen IP-adres meenemen en op iedere plek in het netwerk gebruiken. Een andere nieuwe eigenschap van IPv6 is de Quality of Service (QoS). Hierdoor kunnen bepaalde applicaties stukjes bandbreedte reserveren, wat zeer handig is voor de nieuwe eisen van multimediadiensten. Voor diezelfde diensten zijn 'multicast' en 'anycast' een uitkomst. Deze technieken zorgen ervoor dat video- of audiostromen die naar meerdere computers worden verstuurd pas op het laatste moment worden gedistribueerd, waardoor onnodige bandbreedteverslibbing op het eerste gedeelte van het traject wordt voorkomen.

De introductie van al deze nieuwe voordelen van Ipv6 levert ook een probleem op dat te vergelijken is met de introductie van de Euro; alle apparatuur moet geschikt zijn voor IPv6. Aangezien het Internet zo enorm groot is kan onmogelijk alles stil worden gelegd om overal tegelijk Ipv6 te implementeren. Ipv6 zal dus langzaam moeten integreren met het bestaande IPv4. Gelukkig is het nieuwe protocol zo ontworpen dat het de oude adressering na kan doen, zodat het moeiteloos kan worden gebruikt op de oude apparatuur. Maar de bedoeling is natuurlijk dat Ipv6 zo snel mogelijk het oude protocol zal overnemen om zo de problemen van de toekomst voor te zijn.

Menno vd Leden

Meer informatie is te vinden op: **http://www.cs-ipv6.lancs.ac.uk/**

Klassen van IP-adressen

Klas	Waarde van de eerste groep	Netwerk ID/Host ID	Aantal netten	Maximum aantal computers per net
A	1-126	net.host.host.host	126	16.777.214
B	128-191	net.net.host.host	16.384	65.534
C	192-223	net.net.net.host	2.097.152	254

ter die we benaderen heet Hoef-plan. We zien dat de gebruiker, vermoedelijk met de naam Roald, één computer heeft en dat die computer uit minimaal vijf schijven bestaat. Helaas vangen we bij deze gebruiker bot, omdat hij wachtwoorden heeft toegekend aan zijn gedeelde schijven.

Anders is dat bij het netwerkje dat als werkgroepnaam 'Marinus' heeft. Als we hier op klikken zien we dat dit netwerkje uit minimaal drie computers bestaat. Een Gateway, een Pentium 166 en een Pentium 350. Bij twee van de drie computers gebeurt er niets. We zien geen gedeelde mappen of schijven. De gebruiker van de P350 is echter minder zorgvuldig geweest. Zoals u kunt zien in Figuur 3 heeft deze computer minimaal vijf schijven en tot onze grote verbazing zijn er geen wachtwoorden toegekend aan deze schijven. We kunnen daardoor bij alle mappen en bestanden die deze computer rijk is. Zoals u ziet konden we ook in de Outlook map komen en als we hadden gewild, konden we de mail van deze gebruiker lezen. Evengoed hadden we de cache van de browsers kunnen kopiëren om op ons gemak te kunnen zoeken naar de gegevens van een creditcard of de wachtwoorden kunnen achterhalen van het inbelaccount. Dat vonden we te erg dus we hebben alle schijven gewist

zodat niemand anders dit wel kon doen. U schrikt? U moet eens weten hoe vaak dit gebeurt en bovendien kunnen ze ons toch niet achterhalen!!

Natuurlijk hebben wij de schijven niet gewist. We hebben keurig een berichtje achtergelaten op de desktop en daarin vertelt hoe deze gebruiker zijn beveiliging kan aanpassen. Een dag later zagen we de computer niet meer terug in het volledige netwerk.

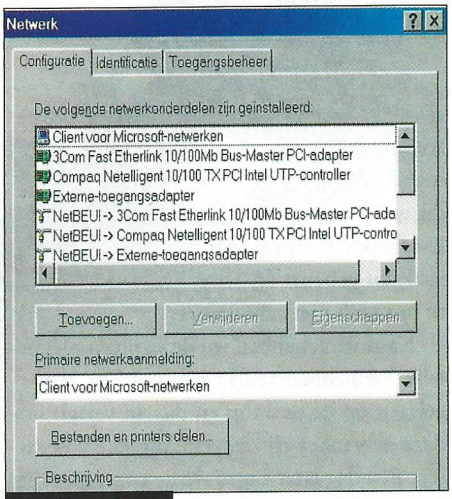
Netwerkprotocollen instellen

Om u te kunnen uitleggen welke instellingen noodzakelijk zijn om 'onzichtbaar' te blijven op het Internet gaan we uit van de volgende situatie die we ook in de artikelen de komende maanden zullen hanteren. We hebben drie computers in een lokaal netwerk. Computer 1 heet 'Server' en bevat twee netwerkkaarten. Een daarvan is bedoeld om lokaal te kunnen communiceren terwijl de ander de permanente aansluiting verzorgt met de kabel. Computer 2 heet 'Client2' en bezit één netwerkkaart. Computer 3 heet 'Client3' en bezit ook een netwerkkaart. Als eerste gaan we zometeen de instellingen goed zetten van het lokale netwerk om ons vervolgens bezig te houden met de connectie naar het Internet.

De reden waarom we uitgaan van een vaste verbinding met de kabel is tweeledig. De eerste reden is dat mensen die internetten via de kabel en dus een permanente verbinding hebben, eerder geneigd zijn een netwerk aan te leggen zodat iedereen er volop gebruik van kan maken. De tweede reden is dat mensen die inbellen met een modem of ISDN-adapter minder problemen ondervinden met verkeerde instellingen omdat zij direct inbellen met een computer van de provider. Deze provider heeft de boel zo afgeschermd dat andere computers nooit zichtbaar worden.

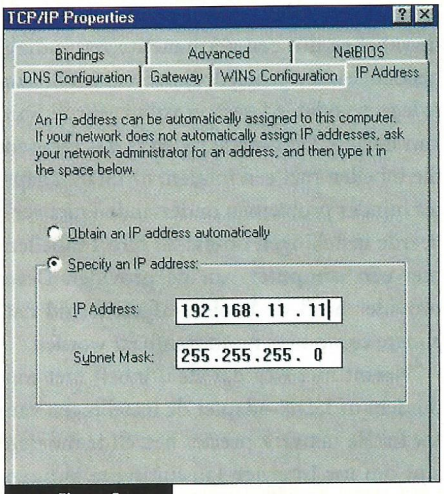
Neemt niet weg dat als u inbelt met een modem of ISDN-adapter de instellingen van uw lokale netwerk precies hetzelfde moeten zijn om uw Internet-aansluiting te kunnen delen.

- Dubbelklik in het configuratiescherm op het icoontje 'Netwerk'.
- In het scherm dat u nu ziet (Figuur 4) worden de geïnstalleerde netwerkkaarten of adapters getoond.



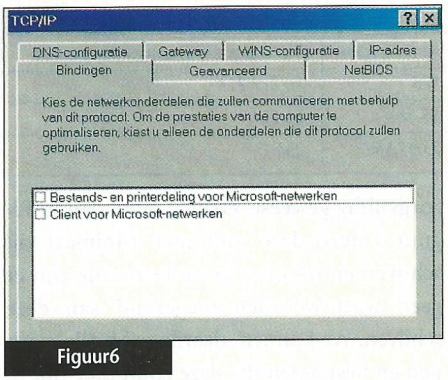
Figuur4

- Gaat u nu eerst naar Bestanden en printers delen en vink deze opties aan. Herstart de computer en ga weer terug naar uw netwerkinstellingen.
- U ziet dat aan iedere adapter een protocol is gekoppeld. Is dat niet het geval, dan kunt u deze alsnog installeren door op de knop toevoegen te klikken. U gaat dan naar de protocollen van Microsoft en installeert NetBEUI en TCP/IP.
- Het protocol IPX/SPX kunt u zonder meer verwijderen, tenzij u een Novell netwerk hebt draaien.
- In ons voorbeeld is de 3COM-kaart bedoeld voor het lokale netwerk. Selecteer nu de TCP/IP-instellingen van uw eigen adapter die het lokale verkeer moet regelen en klik op eigenschappen. (Figuur 5)



Figuur5

- Allereerst moet u nu een IP-adres toekennen aan deze kaart. Hiervoor hebt u drie mogelijkheden. U mag alle adressen gebruiken in de range 10.0.0.0 tot en met 10.255.255.255 of in de range van 172.16.0.0 tot en met 172.31.255.255 en in de range van 192.168.0.0 tot en met 192.168.255.255.
- Wij hebben voor de laatste range gekozen en kenden het IP-nummer 192.168.11.11 toe aan de 3COM-kaart. Als subnetmasker kunt u invullen 255.255.255.0. Het is belangrijk dat u deze nummers goed onthoudt, zodat u straks bij de overige computers de juiste instellingen kunt gebruiken.
- De overige tabbladen kunt u overslaan en als u op OK klikt komt u weer in het eerste scherm.
- Omdat de adapter die het uitgaande verkeer regelt alleen communiceert door middel van het TCP/IP-protocol kunnen we zonder gevolgen het NetBEUI-protocol dat eraan is gekoppeld verwijderen.
- Ga naar de TCP/IP-instellingen van de adapter die communiceert met het Internet.
- Vul hier alle gegevens in die u van uw provider hebt gekregen. Dus IP-nummer en subnetmasker, tenzij u gebruik maakt van een DHCP-server, DNS, en Gateway.
- Speciale aandacht verdient het tabblad Bindingen. Als u niet wilt worden gezien op het netwerk, schakelt u hier de bestands- en printerindeling alsook de client voor Microsoft-netwerken uit. (Figuur 6).



Figuur6

- Als u dit alles hebt gedaan staan de netwerkinstellingen van deze computer goed.
- Stel nu de TCP/IP-instellingen in van de overige computers en herhaal stap 1 t/m 4.
- Het enige dat u nu nog hoeft in te stellen op beide computers zijn de IP-adressen en de Subnetmaskers.
- Aan 'Client1' kent u het IP-adres 192.168.11.12 toe en als subnetmasker 255.255.255.0.
- Aan 'Client2' kent u het IP-adres 192.168.11.13 toe en als subnetmasker 255.255.255.0.

Uw instellingen staan nu goed. Alle lokale machines kunnen communiceren met elkaar door middel van het NetBEUI-protocol. Wel moet u ervoor zorgen dat u bij de Netwerkinstellingen bij het tabblad identificatie alle computers in dezelfde werkgroep indeelt. Let u er bij de naamgeving op dat u namen kiest die niet al te veel over uw systemen of over uzelf vertellen.

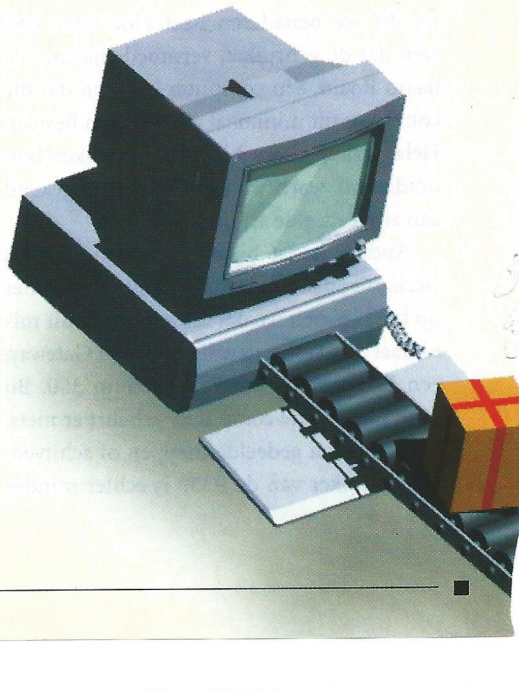
U kunt nu naar wens alle bestanden en schijven delen. Ken hier nog wel wachtwoorden aan toe, totdat u een proxyserver met een werkende firewall hebt geïnstalleerd. Hoe dat in z'n werk gaat vertellen we u volgende maand.

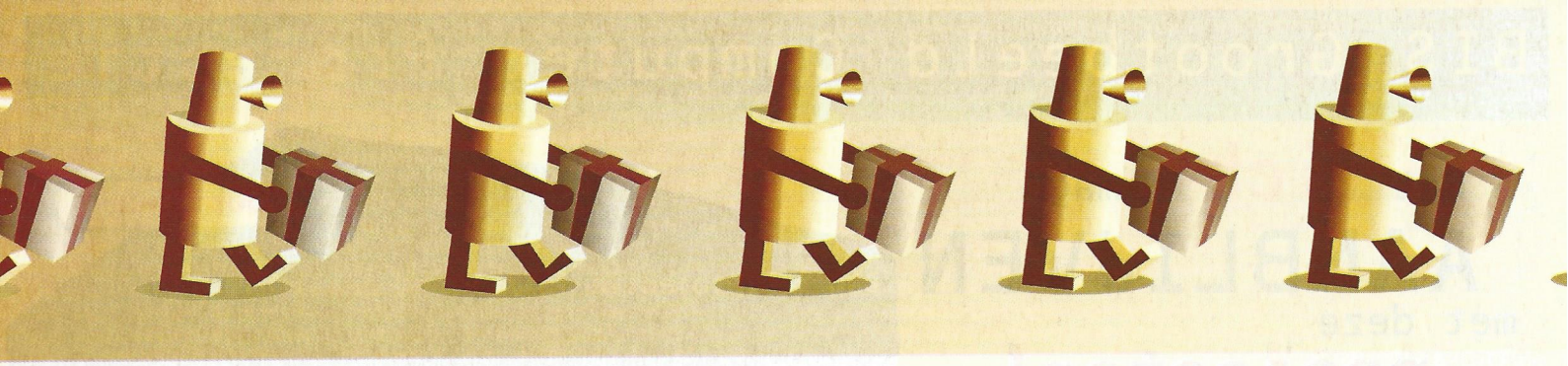
AAN TE RADEN NASLAGWERKEN

Washburn & Evans, Het onderhouden van een TCP/IP Netwerk, 1997, Addison Wesley Longman, ISBN 90-6789-841-4.
Vanheste, Het Internet handboek voor netwerkbeheerders, 1997, Addison Wesley Longman, ISBN 90-6789-919-4.
Stoltz, Windows 95 netwerk geheimen, 1997, Sybex, ISBN 90-4190-028-4.
Dulaney e.a, MCSE training guide TCP/IP, 1998, New Riders publishing, ISBN 1-56205-747-2.

OP ONZE SITE

Op **www.computertotaal.nl** in de rubriek Deze maand kunt u aanvullende informatie vinden over het aanleggen van netwerken en Ipv6.





Raak uw pakketjes niet

Met TCP/IP-utilities weet u alles over uw Internet-verbinding

WWW lijkt niet alleen voor World Wide Web te staan, maar kan ook als World Wide Wait worden opgevat. Internet lijkt vaak traag, ook met een relatief snelle Internet-verbinding kan het nog voorkomen dat u erg lang moet wachten. Om na te gaan hoe die verbinding nu precies verloopt zijn er utilities beschikbaar die wij eens nader voor u hebben bekeken.

Robbin Ooijevaar

De 'normale' consument thuis maakt contact met het Internet via een Internet Service Provider (ISP). Wanneer u een pagina op het Internet wilt bekijken, tikt u in de browser het adres van de server in waar de pagina staat. Na een druk op de entertoets stuurt de computer een 'request' voor die pagina naar de server. In de meeste gevallen komt deze ook daadwerkelijk aan en zal de desbetreffende server de pagina opsturen naar uw computer. Pas dan verschijnt de pagina in de browser. De route die deze pakketjes met de 'request' volgen is geen directe verbinding tussen uw computer en de opgegeven server. De pakketjes data die uw computer verstuurt komen langs vele tussenpunten, ook wel 'hops' genoemd. Hoe meer hops er worden gepasseerd, des te langer duurt het voordat de server kan reageren. De vertraging die de pakketjes oplopen wordt voornamelijk veroorzaakt door deze tussenpunten en is afhankelijk van de hoeveelheid verkeer op zo'n tussenpunt. De weg terug van de server naar uw computer hoeft niet per definitie dezelfde route te zijn als de heenweg.

TCP/IP-protocol

De computers die zijn aangesloten op het Internet worden hosts genoemd. Al deze hosts draaien vele verschillende besturingssystemen en ook de hardware en de wijze waarop de Internet-verbinding tot stand komt lopen erg uiteen. Communicatie tussen de verschillende besturingssystemen en hardwaretechnieken is alleen mogelijk wanneer iedereen dezelfde 'taal' spreekt. De meest gesproken taal op het Internet is die van het TCP/IP-protocol. De verschillende computernetwerken die op het Internet zijn aangesloten zijn door middel van TCP/IP-routers met elkaar verbonden.

Alle apparaten die zijn aangesloten op het Internet hebben een uniek adres: het IP-nummer. De data die over het Internet wordt verstuurd tussen verschillende hosts en routers wordt opgesplitst in pakketjes: IP-frames. De adressering en routering van deze pakketjes zijn vastgelegd in het IP-protocol. De betrouwbaarheid van de dataoverdracht wordt door het TCP-protocol geregeld.

De IP-adressen van computers die aan het Internet zijn gekoppeld worden toegekend door het Network Information Center (NIC). De thuisgebruiker die inbelt op het Internet krijgt van een Internet Service Provider (ISP) een IP-adres toegekend. Bijna alle ISP delen dynamische adressen uit. Dit houdt in dat de inbellende computer vrijwel altijd een ander IP-nummer krijgt. Wanneer de verbinding wordt verbroken wordt het IP-nummer weer vrijgegeven en kan de ISP deze weer aan een andere inbellende computer weggeven. Een van de voordelen hiervan is dat de ISP niet zoveel IP-nummers hoeft te kopen bij het NIC als dat ze abonnees heeft. Vaak is het wel mogelijk om tegen een meerprijs een vast IP-nummer aan te vragen bij uw ISP. Kabelmodemgebruikers krijgen vrijwel altijd een vast IP-nummer toegekend.

Maar waar is zo'n IP-nummer nu eigenlijk goed voor? Om kort te zijn: voor de adressering. Wanneer er een pagina wordt opgevraagd bij een server, weet de server wie de aanvrager is en waar hij de pagina dus naar toe moet sturen. Ook iedere server heeft een IP-num-

mer. Het wordt de surfende Internetter alleen wat gemakkelijker gemaakt door middel van dynamic name servers (DNS). Wanneer bijvoorbeeld http:// www.tucows.com in de browser wordt opgegeven, zal de DNS-server van uw ISP in een tabel

kwijt

opzoeken welk IP-nummer hiervoor is aangevraagd. Dit IP-nummer kan ook direct in de browser worden opgegeven om de homepage te bereiken.

Een IP-adres bestaat uit vier binaire bytes. De vier bytes worden gescheiden door een punt. Ondanks het feit dat IP-adressen binair zijn, worden ze vrijwel altijd decimaal aangeduid. Door IP te gebruiken zijn er verschillende metingen waaronder naar snelheid en bereikbaarheid te verrichten. Het eerste onderwerp waar we bij belanden is 'Packet Internet Groper', beter bekend als ping.

Ping

Ping heeft z'n naam te danken aan de sonartechniek. De sonarpuls wordt verzonden en keert terug met een 'ping'-geluid wanneer de puls wordt weerkaatst. De ping-utilitie wordt bij vrijwel alle Windows-versies geleverd en is te vinden in de Windows directory als ping.exe. Het doel van het programmaatje is simpel maar doeltreffend. Met ping is de bereikbaarheid van vrijwel alle apparaten die aan het Internet hangen te controleren. Dit doet ping door een pakketje naar de opgegeven server te sturen. Ping gebruikt hierbij de 'echo request' van het Internet Control Message Protocol (ICMP) en vraagt hiermee een pakketje terug te sturen naar de afzender.

Om met ping.exe te werken onder Windows kan het beste eerst een DOS-box worden gestart. Wanneer ping.exe vanuit het Startmenu / Opstarten wordt gestart, sluit het programma wanneer de pingsessie klaar is automatisch weer af en is het resultaat nauwelijks te volgen.

We gaan nu de server van de sharewaresite van Tucows pingen. Dit kan zowel door de domeinnaam www.tucows.com, maar ook door het IP-nummer van de server op te geven. Wanneer de domeinnaam wordt gepingd zien we gelijk het IP-nummer van de server. Tik in de DOS-box: PING www.tucows.com. Ping stuurt standaard vier pakketjes naar de Tucows-server. De resultaten van deze sessie worden één voor één terug ontvangen.

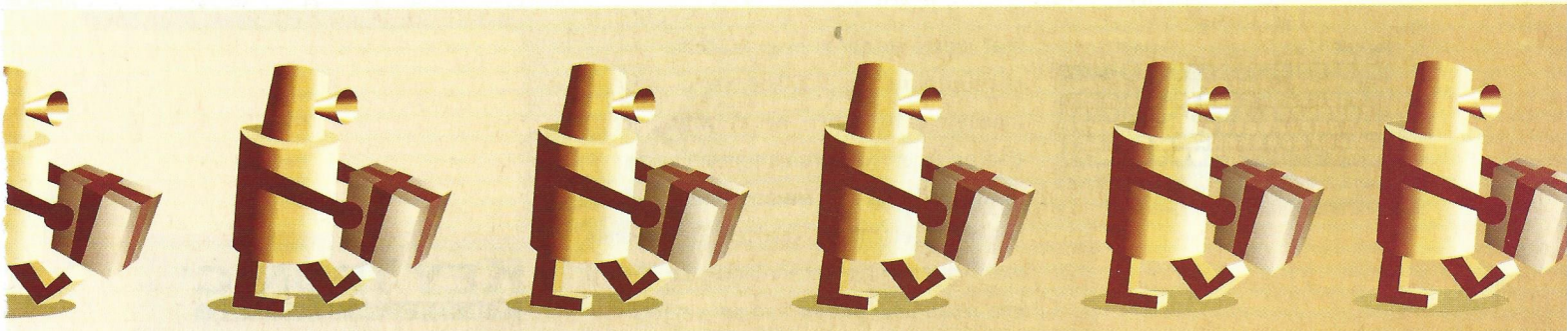
Standaard worden er vier pakketjes met een lengte van 32 bit verstuurd. Door de parameter -l omvang_pakketjes achter het pingcommando op te geven kan deze waarde worden gewijzigd. De tijd geeft in milliseconden aan hoelang het duurt voordat de Tucowsserver reageert op het verzoek om reactie. Deze tijd is slechts een momentopname ter indicatie en zal vrijwel nooit hetzelfde zijn. De snelste reactietijd tijdens deze pingsessie is 254 ms. Tijdens de weg die de pakketjes naar de server afleggen worden er verschillende tussenstations (hops) gepasseerd. Met de TTL (times to live) kan worden opgegeven hoeveel tussenstations (hops) er maximaal mogen worden gepasseerd totdat de opgegeven server is bereikt. TTL is in het TCP/IP-protocol ingebouwd zodat wanneer de server niet te bereiken is, de pakketjes niet over het Internet kunnen blijven dwalen. De standaard TTL-waarde is 32 hops. Deze kan met de parameter -i aantal_hops worden gewijzigd.

Ping kan ook worden gebruikt om de bereikbaarheid van een server te blijven controleren. Door de parameter -t op te geven wordt er een continue pingsessie gestart die pas ophoudt wanneer de gebruiker deze afbreekt met Ctrl-C. Dit kan handig zijn voor mensen die op het Internet inbellen met een modem. Tijdens een download is het mogelijk dat de voortgang van het downloadproces om de een of andere reden blijft hangen. Wanneer er verder geen Internet-verkeer plaatsvindt van of naar uw computer kan uw provider na een x aantal minuten de verbinding verbreken. Door een willekeurige server op het Internet continu te pingen met dusdanig kleine pakketjes zodat de download hier zo weinig mogelijk van merkt, blijft er verkeer van het Internet naar uw computer. Dit voorkomt dat de verbinding wordt verbroken. Een overzicht van alle pingparameters wordt verkregen door ping te starten met de parameter –h.

Trace route

Zoals vermeld passeren de datapakketjes verschillende tussenpunten (hops) voordat de opgegeven server wordt bereikt. Het programma tracert.exe laat precies zien welke weg een pakketje aflegt over het Internet voordat het bij de server aankomt. Net als ping maakt trace route gebruik van de ICMP echofunctie. De werking van trace route gaat als volgt: de eerste drie pakketjes die worden verzonden krijgen een 'time to live'-veld (TTL) van 1. Ieder tussenpunt verlaagt de TTL met 1. Dit houdt in dat na het passeren van het eerste tussenpunt de TTL nul is geworden en terug wordt gestuurd naar de afzender. Vervolgens worden er drie pakketjes met een TTL van 2 verzonden. Deze pakketjes zullen na het passeren van de tweede hop niet meer geldig zijn en worden ook teruggestuurd. Dit gaat net zolang door totdat de opgegeven server is bereikt of het maximaal opgegeven hops wordt overschreden. De maximale TTL staat standaard op 30. Dit kan net als bij ping worden aangepast door een extra parameter op te geven: -h maximum_hops.

Tracert.exe geeft een overzicht van de gepasseerde tussenstations en de tijd die voor een tussenstation nodig is om te reageren. Wanneer de 'trace' is voltooid weet u hoeveel en welke tussenpunten het pakketje is gepasseerd van uw computer naar de opgegeven tegenpartij. Het belangrijkste is echter dat u nu kunt zien waar de pakketjes de meeste vertraging oplopen. Ook tracert.exe moet in een



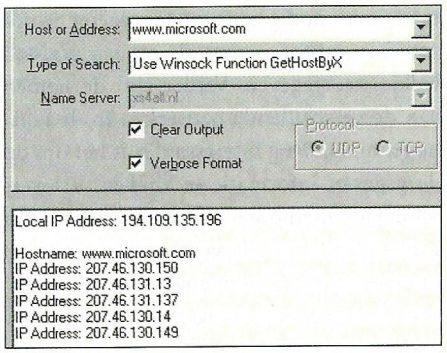
DOS-box worden gestart. Om de route naar www.tucows.com te traceren tikt u in achter de DOS-prompt: tracert www.tucows.com/.

Grafische utilities

Natuurlijk zijn er genoeg shareware-programmaatjes die dezelfde informatie kunnen verschaffen als de opdrachten ping en tracert, en die ook nog eens zijn voorzien van een leuke grafische interface. Ook zijn deze programma's in staat om u iets meer te vertellen over de computers, routers en andere apparaten die op het Internet zijn aangesloten.

CyberKit 2.4

CyberKit is een Internet utilitie suite waarin verschillende TCP/IP-functies zijn samengebracht. Naast ping, trace route en finger kan er een NS-look-up worden gedaan. Ook is het mogelijk om de klok van uw computer te synchroniseren met één van de Internet time servers. De ping- en trace route-functies



Met NS-look-up kunnen de IP-adressen die achter een domeinnaam schuilgaan worden opgezocht.

doen eigenlijk niet meer dan de bij Windows geleverde utilities. Wel is het door de grafische interface eenvoudiger om instellingen als de omvang van datapakketjes, in te stellen.

Met de finger-functie kan er worden gekeken of een bepaalde gebruiker online in een domein is ingelogd. Wanneer iemand een Internet-connectie heeft en de inlognaam is gelijk aan de naam die voor een e-mailadres wordt gebruikt, kunt u gemakkelijk kijken of één van uw kennissen online is. Om te zien of robertjan@bitnet.be online is geeft u bitnet.be op bij Host en robertjan bij Query.

Door iemand te fingeren kunt u onder andere zien of diegene nieuwe e-mail heeft, momenteel online is of wanneer hij voor het laatst online was. Tevens ziet u welke directories er voor deze persoon zijn bestemd op de server. Indien uw ISP een Unix-server gebruikt kunnen anderen waarschijnlijk ook deze informatie over u opvragen. In de meeste gevallen kunt u dit uit laten zetten bij uw provider. De finger-optie werkt overigens niet bij free-mail e-mailadressen. Servers die onder NT draaien ondersteunen standaard geen 'finger-look-up'. Met NS-look-up, oftewel NameServer look-up, kan een hostnaam worden vertaald naar een IP-adres en omgekeerd is ook mogelijk. Tevens worden alle aliassen van de server getoond.

De WhoIs-functie doet ongeveer hetzelfde als finger maar raadpleegt de database van het Network Information Center (NIC). In deze database is een grote hoeveelheid informatie opgenomen over computers, servers, gebruikers en andere apparatuur die is aangesloten op het Internet. De server look-up geeft de naam van de server, eventuele aliassen en IP-nummers van een server. CyberKit kan ook meerdere e-mail accounts controleren en eventueel een mail reader starten. Overigens moet u wel beschikken over een POP3-account omdat het programma geen IMAP servers ondersteunt. De beperking van het programma zit hem vooral in de user interface. Het is af en toe knap lastig om gegevens naar het clipbord te kopiëren.

CyberKit 2.4 build 307, http://www.ping.be/cyberkit

Genoeg shareware-programma's geven informatie over uw Internet-verbinding

Net Medic 1.2.2

Met Netmedic kunnen veel onderdelen van de computer en het Internet worden gemeten en bekeken. NetMedic start standaard met Windows en minimaliseert naar de system-tray waar het programma op de achtergrond blijft draaien en alles in de gaten houdt. Door op het icoontje te klikken wordt een dashboard-interface gestart met wat standaard indicatoren. Het dashboard kan eenvoudig worden geconfigureerd met de gewenste indicatoren zoals onder andere de tijd die u online bent, modemsnelheid, Intranet-snelheid en de snelheid van een server naar uw computer. Ook de drukte bij uw ISP en de belasting van de locale processor kan in de gaten worden gehouden. Wanneer een van de gemeten onderdelen te laag scoort geeft NetMedic dit direct aan. Als u zelf iets aan de opgetreden vertraging zou kunnen doen wordt hiervoor een suggestie gegeven.

NetMedic is eenvoudig te bedienen, heeft een mooie user interface en goede online documentatie. Erg handig is dat een monitor aan de toolbar van de webbrowser kan worden gehangen.

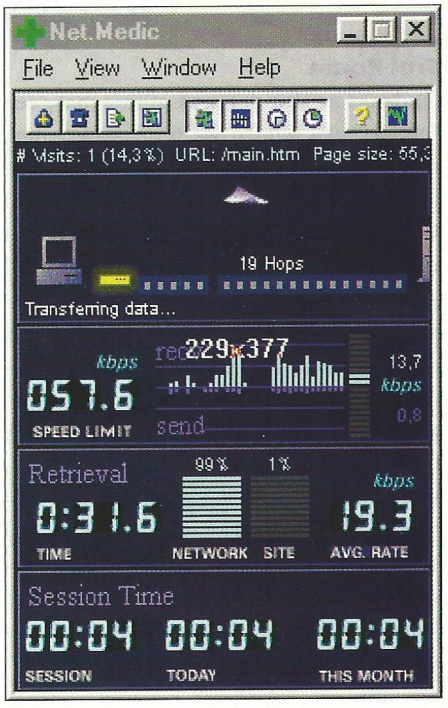
NetMedic is een goede utilitie om de gezondheid van een Internet-verbinding en vrijwel alles wat daar tussen ligt in de gaten te houden. Verder heeft het programma een uitgebreide logfunctie waarmee ook gegevens over uw Internet-gebruik kunnen worden opgeslagen.

Net Medic 1.2.2, http://www.vitalsigns.com

Sam Spade 1.10 Bèta

Na de installatie oogt Sam Spa een beetje speels. De mededelingen die bij 'tip of the day' verschijnen zijn vaak meer leuke citaten en weetjes dan echte tips die te maken hebben met het programma zelf. Het programma is echter een verzameling van zeer krachtige utilities die betrekking hebben tot IP.

De utilities worden op een gebruiksvriendelijke manier gepresenteerd. Het lijkt op het eerste gezicht wat sober, maar dit werkt in de praktijk bij dit soort utilities uitermate prettig. De opgespoorde gegevens worden in verschillende kleuren op het scherm getoond. Hierdoor staat er op het scherm niet een brei van getallen en letters en ziet u gemakkelijk welke gegevens bij elkaar horen. Erg handig is dat



NetMedic geeft een goede indicatie van de verbinding die uw machine met een server heeft.

bijna alle tekst (inclusief de tekst uit het informatieschermpje van 'about') naar het clipbord kan worden gekopieerd. De gebruikelijke ping- en trace route-functies kunnen eenvoudig naar uw wensen worden uitgevoerd.

Een andere traceermogelijkheid is het opsporen van de herkomst van (ongewenste) e-mail. In de helpfile wordt uitvoerig beschreven hoe de gegevens uit de e-mail header moeten worden geïnterpreteerd en hoe u ongewenste e-mailzenders (spammers) kunt traceren. De WhoIs-functie van Sam Spade is erg snel en niet beperkt tot het zoeken naar gegevens over een host of server in de database van het Network Information Center. In een lijst kunnen tal van andere informatie servers worden geselecteerd. De trace route-functie laat met een grafisch schuifbalkje in één oogopslag zien waar de knelpunten tussen uw computer en de opgegeven server zich bevinden.

Andere utilities die zijn opgenomen in het pakket zijn onder andere een finger client, DIG en een mogelijkheid om de locale computertijd te synchroniseren met een tijd-server op het Internet. In de helpfile is veel handige informatie over anti-spamming en het gebruik van trucjes met news groups te vinden.

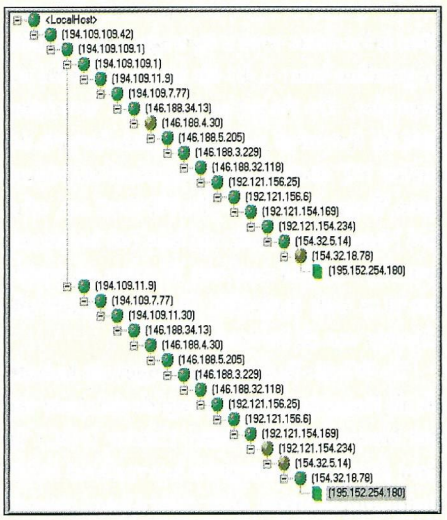
Sam Spade 1.10 Beta, http://www. blighty.com/ products/ spade

Visual Route is de ultieme trace utilitie

TreeRoute

Ondanks het feit dat deze utilitie maar één functie heeft wilden we u dit programma niet onthouden. TreeRoute kan maar één ding: een route over het Internet traceren. Het leuke is dat dit programma bewijst dat er 'meerdere wegen naar Rome leiden'. U kunt duidelijk zien dat de weg van uw computer naar een server op het Internet niet altijd hetzelfde is. De weg langs verschillende hops wordt in een boomstructuur weergegeven. De reactietijd van de gepasseerde tussenpunten wordt zowel beschreven als met een kleurcodering aangegeven. Wanneer er meerdere trace routes naar eenzelfde server worden gedaan, ziet u dat de verstuurde pakketjes af en toe een andere weg inslaan. Verder kan er een maximum time-out tijd worden ingesteld en het aantal time-outs.

TreeRoute, http://www.mindspring.com/~phantom 01/index.html



TreeRoute laat zien dat de reis van de pakketjes naar een bepaalde server niet altijd dezelfde weg hoeft te zijn.

4-Net v1.1

4-Net is een mini utilitie die toch veel in huis heeft. Het programma wordt bediend vanuit de system tray en kan pingen, een trace route uitvoeren en heeft een finger client. De 'anti-idle'-functie maakt het mogelijk om een Internet-connectie 'in leven te houden' door om een x aantal minuten een ping uit te voeren. Dit voorkomt dat uw ISP de verbinding verbreekt wanneer er geen Internet-verkeer meer plaatsvindt. Verder kan er een host en local host look-up worden gedaan waarvan de gegevens met één simpele knop naar het clipbord worden gekopieerd.

4-Net v1.1, http://www. cartoonlogic.com

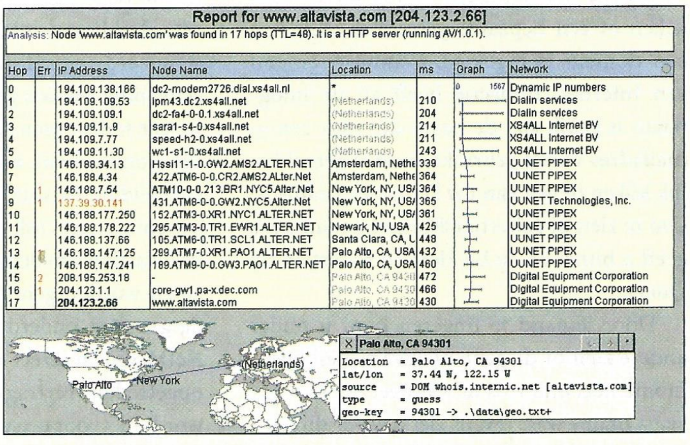
VisualRoute 4.01

De ultieme trace utilitie is wel VisualRoute. Dit programma heeft werkelijk alles in huis om een uitstekende trace route uit te voeren. Het combineert verschillende mogelijkheden om informatie over hosts, servers, routers en andere apparaten die aan het Internet hangen te verkrijgen. Na het invoeren van een IP-adres of hostnaam geeft VisualRoute een complete beschrijving van de afgelegde weg. Dit is nog niet alles. VisualRoute tekent op een wereldkaart de geografische weg die wordt afgelegd door de pakketjes. Zo kunt u precies zien waar de server zich op aarde bevindt. De route die door de pakketjes worden afgelegd is vaak allesbehalve rechtstreeks. Het is grappig om te zien dat sommige servers helemaal niet staan in het land waar de landcode achter het domein naar verwijst. Zo doet de landcode .se van http:// www.ericsson.se vermoeden dat het hier om een server in Zweden gaat. Natuurlijk is het een Zweedstalige pagina, maar deze server is in Nederland aan het Internet is gekoppeld.

VisualRoute geeft aan hoeveel tussenpunten er zijn gepasseerd en bij welke tussenpunten er een fout is opgetreden door een time-out. Naast de IP-adressen wordt ook de naam van de tussenpunten genoemd en de geografische locatie. De tijdsduur die een tussenpunt nodig heeft om te reageren wordt zowel in milliseconden als op een grafisch balkje weergegeven. Verder zijn de namen van de verschillende netwerken in de tabel opgenomen. Nog interessanter is het om op de gegeven informatie te klikken. Via verschillende methoden wordt er zonder dat u ingewikkelde instellingen en adressen hoeft op te geven informatie opgezocht. Alle gegevens kunnen eenvoudig naar het clipbord worden gekopieerd.

VisualRoute is een echte aanrader voor zowel de beginnende als gevorderde tracer. De informatie die kan worden verkregen is zeer uitgebreid door de integratie van verschillende IP-utilities als ping, trace route en WhoIs look-ups.

VisualRoute 4.01, http://www.visualroute.com



VisualRoute geeft naast uitgebreide technische informatie over de reis die pakketjes afleggen naar een bepaalde server ook de geografische route die wordt afgelegd.