LENTE

COMPACT

NETWERKBEHEER EN -BEVEILIGING

1995/1

KWARTAALBLAD EDP-AUDITING

Compact ®
Jaargang 22, nummer 1
Een uitgave van KPMG EDP Auditors NV en Samsom Bedrijfs-Informatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 4 x per jaar.
Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
J.C. Boer RE RA
Ir. J.A.M. Donkers
Drs. R.G.A. Fijneman RE RA
Mw. S.M. Keijl
Drs. P. Veltman RE RA
Adviesraad
Prof.dr. J.C. Arnbak
J.H. Buisman RA
Ir. J.C. le Clerq
Mr. P. van Dijken
Prof.mr. H. Franken
Dr. K.Y. Mollema RE RA
Prof. H.B. Moonen RE RA
Prof.dr.ir. R. Paans RE
Redactiesecretariaat
Mw. I. de Koning,
Samsom Bedrijfsinformatie,
Postbus 4,
2400 MA Alphen aan den Rijn
Tel.: 01720 - 66 746
Fax : 01720 - 66 569
Vormgeving
Bureau Karakter, Delft
Abonnementen
f 135,- per jaar incl. BTW. Losse nummers f 45,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.
Abonnementsadministratie
Samsom BedrijfsInformatie,
Postbus 4,
2400 MA Alphen aan den Rijn
Tel.: 01720 - 66 800
Fax : 01720 - 75 933
Adreswijzigingen - ook tijdelijke - moeten minstens 8 weken voor de verschijningsdatum bekend zijn.

Uitgever
Drs. Th.P.M. Brinkman

Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 - 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals: • beoordeling automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacy-wetgeving • computercriminaliteit en nieuwe regelgeving.

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor EDP-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG EDP Auditors NV.

Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is. Noch KPMG Klynveld, KPMG EDP Auditors NV, noch de redacteuren persoonlijk, noch uitgeverij Samsom BedrijfsInformatie BV, deel uitmakend van Wolters Kluwer NV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers. Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij het secretariaat verkrijgbaar is.

Onlangs is het wereldwijde Internet wederom slachtoffer geworden van een geslaagde inbraakpoging. Deze vond plaats door misbruik te maken van de beperkte beveiligingsmogelijkheden van IP, het internetprotocol op de netwerklaag van de TCP/IP-protocol-stack. Bij de aanval werd gebruik gemaakt van IP-pakketten met een vervalst herkomstadres ('IP spoofing'). Applicaties die authenticeren aan de hand van IP-herkomstadres en op basis hiervan autorisatie verlenen, werden erdoor misleid. Opmerkelijke bijzonderheid is dat de eerste computer waarop werd ingebroken die van een computerbeveiligingsexpert was. Bij de inbraak zijn vermoedelijk creditcardnummers bemachtigd, waardoor kaarthouders financieel gedupeerd kunnen raken.

In Compact 1994/3 is aandacht besteed aan de beveiligingsaspecten van TCP/IP en de maatregelen die kunnen worden getroffen ter beveiliging van een aansluiting op het op TCP/IP gebaseerde Internet, zoals een 'firewall'. De IP spoofing-aanval had kunnen worden voorkomen door gebruik te maken van router-firewalls die IP-pakketten vanuit het externe netwerk met een IP-herkomstadres binnen het interne netwerk niet doorlaten.
In voorliggende Compact staat het management van netwerken, in het bijzonder heterogene netwerken, centraal. Netwerken bestaan behalve uit eindstations en kabels (en/of ether) uit talloze andere componenten, die invulling geven aan één of meer van de lagen van het OSI-model. Zulke componenten zijn onder andere hubs, bridges, gateways en eerder genoemde routers.

Routers functioneren op de netwerklaag van het OSI-model. Op basis van logische adressen, zoals IP-adres en ethernet/token ring MAC-adres, verzorgen zij een logische verbinding tussen de knooppunten van het netwerk. Doordat routers weet hebben van logische adressen kunnen zij worden geprogrammeerd om berichten van of naar een bepaald adres niet of vertraagd door te laten. Een dergelijke filtering kan ook worden gebaseerd op andere criteria, bijvoorbeeld pakketlengte.
Routers worden onder meer gebruikt voor LAN/WAN-verbindingen. In opkomst zijn routers die fungeren als 'collapsed backbone', waarop meerdere LAN-segmenten zijn aangesloten. Een dergelijke configuratie heeft voordelen op het gebied van kosten en performance, maar maakt de organisatie kwetsbaarder voor storingen in de router.

Voor WAN-connectiviteit kan behalve van routers ook gebruik worden gemaakt van gateways. Deze bieden uitgebreidere functionaliteit en meer beveiligingsmogelijkheden, maar zijn daardoor ook complexer in het beheer.

Netwerkmanagement houdt het beheer in van alle componenten waaruit het netwerk bestaat. Beheer wordt hierbij meestal gedefinieerd in termen van de functionele deelgebieden die in het OSI management framework worden onderkend, zoals performance management en security management.
Naarmate de netwerkcomponenten heterogener zijn, dat wil zeggen verschillen in functionaliteit en 'taal', wordt het beheer complexer. Het beheer van gekoppelde, heterogene netwerken wordt wel aangeduid als 'internetworking'.

Bij client/server-verwerking wordt het netwerk gebruikt om componenten van een zelfde applicatie die verwerkt worden op verschillende systemen, met elkaar te laten communiceren. De applicatiecomponenten die hierbij gewoonlijk worden onderscheiden, zijn de presentatielogica, de functionele logica en de gegevensbeheerlogica. In navolging van de Gartner Group kunnen vijf vormen van client/server-verwerking worden onderscheiden, variërend van gedistribueerde presentatie tot gedistribueerd gegevensbeheer.
Het behoeft geen betoog dat adequaat netwerkmanagement van groot belang is om de betrouwbaarheid en continuïteit van de client/server-applicatie te waarborgen.

In deze uitgave van Compact geven verschillende auteurs hun visie op de problematiek en mogelijkheden van netwerkbeheer en -beveiliging, zowel in algemene zin als toegespitst op de cliënt/server-architectuur. Hierbij worden vooral de technische aspecten, met verschillende diepgang, belicht. Vanzelfsprekend wordt uitgebreid stilgestaan bij de de facto-standaard op het gebied van netwerkmanagement: het Simple Network Management Protocol.

Drs. P. Veltman RE RA

Internetworking; beheerproblematiek en security-risico's

H. Roos RA en
ir. M.T.H. Heesbeen

Daar het koppelen van netwerken problemen kan introduceren, moet deze koppeling alleen worden gerealiseerd als daar een functionele behoefte tegenover staat, en moet de wijze van koppelen zorgvuldig worden gekozen.
Voor het koppelen heeft in de meeste gevallen een gateway de voorkeur, daar deze de meeste security-risico's kan tegengaan. Door het complexe beheer brengt een gateway echter betrekkelijk hoge exploitatiekosten met zich mee.

INLEIDING

Zolang wij in een vrije economie opereren zal, ondanks of misschien zelfs wel dankzij vergaande standaardisatie, voor elke functionele behoefte meer dan één oplossing verkrijgbaar zijn. Dat betekent dat op het gebied van informatietechnologie er altijd meerdere hardware- en softwarelijnen naast elkaar zullen blijven bestaan. Dit heeft tot gevolg dat verschillende bedrijven of bedrijfsonderdelen kunnen kiezen voor verschillende oplossingen. Als nu als gevolg van een business reengineering-project, fusieplannen of wijzigingen in de besturingsfilosofie bedrijven of bedrijfsonderdelen moeten gaan samenwerken, zullen de netwerken van de beide organisaties aan elkaar worden gekoppeld. Omdat beide organisaties tot voor kort niet of nauwelijks iets met elkaar te maken hadden of soms zelfs van elkaars bestaan onkundig waren, hebben zij meestal ook voor andere automatiseringsinvullingen en netwerkstandaarden gekozen. De koppeling van deze ongelijksoortige netwerken geeft aanleiding tot een internetworking-situatie. Naast deze 'toevallige' mogelijkheid levert de koppeling van twee (buitenlandse) vestigingen of de koppeling aan Internet een min of meer geplande internetworking-situatie op. Deze internetworking-situatie, en dan met name de beheerproblematiek en de security-risico's, vormt het onderwerp van dit artikel.

In dit artikel zal de problematiek van het uitwisselen van bestanden of gegevens tussen verschillende netwerken worden belicht, waarbij de aandacht met name zal worden gericht op de beheerproblematiek en de security-risico's die worden geïntroduceerd als verschillende netwerken worden gekoppeld. Of deze netwerken zich op één locatie bevinden of dat een deel daarvan zich aan de andere zijde van de wereld bevindt is voor de hier beschreven problematiek niet zo relevant. Natuurlijk kennen beide situaties ieder hun eigen problemen, maar die zijn geen onderwerp van dit artikel.

Voordat dieper wordt ingaan op de internetworking-situatie, worden eerst enkele basisbegrippen uit de netwerktechnologie nader toegelicht.

ARCHITECTUREN

Ondanks de vergaande standaardisatie in de automatiseringswereld worden er nog steeds verschillende netwerksystemen aangetroffen. Alvorens dieper in te gaan op deze verschillende systemen zal eerst het OSI-referentiemodel voor netwerken worden toegelicht.

OSI-model

In 1984 is door de *International Organization for Standardization* (ISO) het *Open Systems Interconnection reference model* (OSI-model) uitgebracht. Dit model had tot doel de verschillende leveranciers van netwerksystemen een referentie-architectuur aan te reiken waarop zij hun (toekomstige) produkten konden richten. Het OSI-model deelt het communicatieprobleem op in zeven deelgebieden (figuur 1).

<table>
<tr><th>OSI-referentiemodel</th><th>TCP</th><th>NetWare</th><th>Vines</th></tr>
<tr><td>Application layer</td><td rowspan="3">ftp SMTP
RLOGIN
telnet</td><td rowspan="2">applications
NetBIOS emulator LU 6.2 support</td><td>streettalk</td></tr>
<tr><td>Presentation layer</td><td rowspan="2">RPC</td></tr>
<tr><td>Session layer</td></tr>
<tr><td>Transport layer</td><td>TCP ICMP</td><td>SPX</td><td>IPC SPP</td></tr>
<tr><td>Network layer</td><td>IP ARP</td><td>IPX</td><td>VIP</td></tr>
<tr><td>Datalink layer</td><td rowspan="2">Ethernet SLIP
Token ring
FDDI</td><td rowspan="2">Ethernet
Token ring
FDDI</td><td rowspan="2">Ethernet
Token ring
FDDI</td></tr>
<tr><td>Physical layer</td></tr>
</table>

Figuur 1. OSI-referentiemodel[1].

De verschillende lagen handelen ieder een afgebakend deel van de communicatie af. De opzet van het model is dat elke laag communiceert met haar evenknie aan de andere zijde van de communicatieverbinding. Om dit correct te kunnen doen en om elkaar te kunnen herkennen hanteert elke laag een adresmethodiek. De belangrijkste functies van de verschillende lagen zijn:

- *Physical layer:* verzorgt de toegang tot het fysieke medium, zoals: koperkabel, glasvezel, de ether.

- *Datalink layer:* verzorgt het betrouwbaar transport over een in beginsel onbetrouwbaar fysiek medium. Hieronder vallen de fysieke adressering, netwerktopologie, flow control, error detection. Voorbeelden: HDLC, Ethernet, Token ring, FDDI.

- *Network layer:* is in staat een logische verbinding tussen twee systemen op het netwerk op te bouwen en te onderhouden. De systemen zijn nu in staat over deze logische verbinding gegevens uit te wisselen. Hiervoor worden logische adressen gebruikt. Voorbeelden: X.25, Internet Protocol (IP).

- *Transport layer:* zorgt voor betrouwbaar transport over de door de onderliggende lagen opgebouwde logische verbinding. Hierbij horen zaken als: virtuele verbindingen, foutdetectie en -correctie. Voorbeelden: Transmission Control Protocol (TCP).

- *Session layer:* vormt een logisch communicatiepad tussen twee applicaties, waardoor beide applicaties in staat zijn een communicatiesessie op te bouwen. Deze laag zorgt ervoor dat de informatie die via het netwerk op een systeem binnenkomt naar de correcte applicatie wordt doorgegeven.

- *Presentation layer:* zorgt voor uniforme presentatie, waardoor communicatie mogelijk wordt tussen twee applicaties welke met een verschillende datapresentatie werken. Indien nodig wordt de data vertaald van de ene naar de andere presentatie. Bijvoorbeeld een translatie van ASCII naar EBCDIC.

- *Application layer:* verzorgt de feitelijke communicatie tussen de applicaties. In feite is dit de 'ingang' voor de gebruikers of applicaties.

De verschillende netwerkprotocollen beschrijven procedures voor communicatie tussen één of meer lagen van het OSI-model tussen twee verschillende systemen.

Netwerkbesturingssystemen

Om een netwerk te kunnen laten functioneren is een netwerkbesturingssysteem nodig. Dit systeem levert de invullingen van de verschillende lagen van het OSI-model. Afhankelijk van het gekozen systeem worden meer of minder lagen ingevuld. In figuur 1 zijn voor enkele netwerkbesturingssystemen de verschillende lagen ingevuld. In deze figuur is duidelijk te zien dat de verschillende systemen qua structuur afwijken van het OSI-referentiemodel. Sommige lagen worden samengepakt of er zijn meerdere invullingen voor een laag. Naast de verschillen in de structuur van de systemen wijken ook de onderlinge invullingen van de lagen principieel van elkaar af. Hierdoor zijn de verschillende systemen niet zonder meer op elkaar aan te sluiten. Dit is het internetworking-probleem.
Enkele bekende netwerkbesturingssystemen in de markt zijn:
- Novell Netware;
- Banyan Vines;
- OS/2 LanServer;
- Windows NT/ Windows for Workgroups;
- TCP/IP.

NETWERKCOMPONENTEN

Om grote netwerken te kunnen bouwen zijn naast het netwerkbesturingssysteem ook andere netwerkcomponenten nodig. Deze internetworkingcomponenten kunnen op basis van hun functionaliteit in relatie tot het OSI-model in vier verschillende typen worden ingedeeld.

1 *In de figuur zijn ter illustratie van het referentiemodel voor enkele veel toegepaste netwerkbesturingssystemen invullingen van de lagen gegeven. Omwille van de duidelijkheid zijn de genoemde invullingen niet volledig.*

Repeater

Repeaters verbinden netwerken op laag 1 van het OSI-model. Zij zorgen ervoor dat fysieke begrenzingen kunnen worden overschreden en verzorgen overgangen tussen verschillende soorten media, zoals van coaxkabel naar glasvezelkabel of van coaxkabel naar UTP-kabel (unshielded twisted pair).

Bridge

Bridges verbinden netwerken op laag 2 van het OSI-model. Op basis van fysieke adressen (dit zijn unieke adressen van de netwerkkaarten (MAC-adres)) worden berichten tussen de twee netwerken doorgegeven, waardoor een scheiding van verkeer ontstaat. Berichten voor het ene netwerk worden niet aan het andere netwerk doorgegeven. De bridge heeft een tabel waarin staat welk fysiek adres zich in welk netwerk bevindt.

Router

Routers verbinden netwerken op laag 3 van het OSI-model. Op basis van het logische adres (uniek per toepassing, een station kan meerdere logische adressen hebben op één netwerkkaart (=fysieke adres)) worden berichten aan het andere netwerk doorgegeven. Routers kunnen worden geprogrammeerd om bepaalde berichten wel en andere niet door te geven. Het onderscheid tussen deze berichten kan worden gemaakt op basis van een groot aantal criteria, zoals adres afzender, adres ontvanger en soort bericht. Hierdoor zijn routers in staat bijvoorbeeld de diverse 'broadcast'-berichten van de netwerkbesturingssystemen te onderscheiden van het overige netwerkverkeer en eventueel te onderdrukken.

Gateway

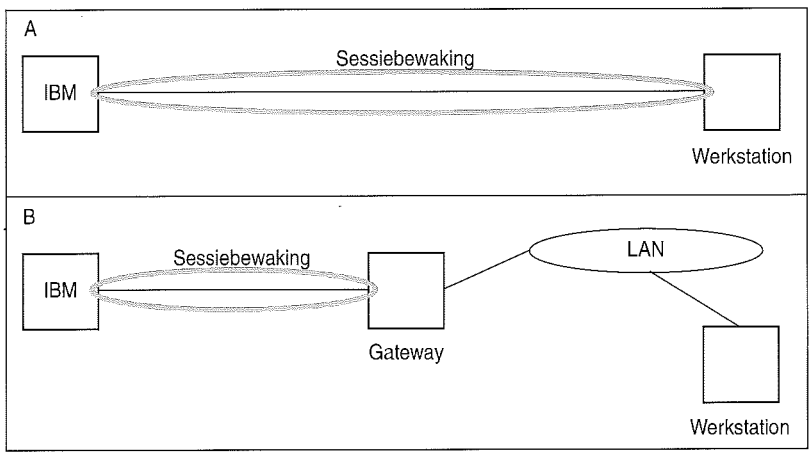
Gateways verbinden netwerken op alle lagen van het OSI-model. Ze worden vaak ingezet om geheel verschillende netwerken onderling te verbinden. De complexiteit van de gateways is sterk afhankelijk van de verschillen tussen de beide protocollen. Hoe meer lagen verschillend zijn in de beide te koppelen netwerken, hoe complexer een gateway moet zijn. Meestal wordt geprobeerd de gateway zoveel mogelijk conform het OSI-model op te bouwen. Maar omdat er nog steeds netwerken in omloop zijn die afwijken van het OSI-model, is dit niet altijd mogelijk. Vooral de mechanismen op datalink- en sessieniveau van de verschillende protocollen kunnen sterk uiteenlopen. In de programmatuur van een gateway zijn vaak allerlei listige technische trucs toegepast om deze verschillen op te lossen. Vaak echter zijn de verschillen tussen beide systemen zo groot dat een echte oplossing niet mogelijk is. Er ontstaat dan een situatie waarbij in negentig procent van de gevallen alles correct werkt, maar waarbij het in tien procent van de gevallen gewoon misgaat.

Een goed voorbeeld hiervan vormen de gateways welke de vertaling van LAN naar SNA verzorgen (Eicon gateway, Netware for SAA, etc.). In de normale situatie bewaakt de IBM-host de sessie tussen systeem en werkstation (zie figuur 2A). Bij toepassing van een gateway worden de signalen van het werkstation door de gateway nagebootst. De host denkt dat hij de gehele verbinding bewaakt, maar effectief wordt alleen de verbinding met de gateway afgedekt (zie figuur 2B). De gateway bewaakt via het LAN de sessie met de PC. Normaal werkt dit goed, maar de problemen ontstaan bij storingen. De gateway moet dan een vertaling maken van LAN-gebeurtenissen naar de host en andersom. Omdat de IBM-protocollen strakke timingschema's gebruiken, kan de gateway niet wachten op een ontvangstbevestiging via het LAN. De gateway is genoodzaakt om reeds een ontvangstbevestiging naar de host te sturen, voordat zeker is of het bericht ook daadwerkelijk bij het werkstation is aangekomen. Als dan achteraf aan de gateway duidelijk wordt dat er wel iets is misgegaan met de communicatie over het LAN, dan zit de gateway met het probleem dat hij reeds een ontvangstbevestiging aan de host heeft gezonden. In de meeste gevallen is een correct herstel dan eigenlijk niet meer goed mogelijk. Dit is de belangrijkste oorzaak van problemen met deze gateways.
Naast deze operationele problematiek, welke de beheerorganisatie steeds voor allerlei problemen met de gebruikers stelt, heeft deze situatie ook een security-risico in zich. Zoals reeds beschreven wordt in de normale situatie de sessie door de host bewaakt. Deze bewaking betreft niet alleen het foutloze datatransport, maar kan ook een veilig datatransport betreffen. Bij de toepassing van een gateway reikt de beveiliging van de host maar tot de gateway en moet het traject van de gateway naar het werkstation door het LAN worden beveiligd.

Fysieke invullingen

De hierboven beschreven internetworking-functies worden in de praktijk in een aantal verschillende fysieke verschijningsvormen aangetroffen. Na-

Figuur 2
A. Sessiebewaking met werkstation rechtstreeks aan IBM-host.
B. Sessiebewaking met gebruikmaking van een gateway.



tuurlijk bestaan er produkten die precies de hiervoor omschreven functies vervullen. Deze produkten voeren dan ook de namen van de hiervoor genoemde functies. Daarnaast zijn er produkten welke een combinatie van functies in zich hebben. De meest voorkomende zijn:

- *Hub:* wordt toegepast bij gestructureerde bekabelingssystemen (bijvoorbeeld AT&T Systimax, IBM Cabling System) om de bekabeling per gebruiker samen te voegen tot één netwerk. In feite vervult de hub de repeater-functie.

- *Intelligent hub:* hiermee wordt eigenlijk een netwerkprodukt bedoeld dat modulair met kaarten kan worden opgebouwd voor de benodigde functies. De kaarten zijn vaak beschikbaar met hubs, bridges en routers.

- *Brouter*: is een apparaat dat zowel kan bridgen als routeren.

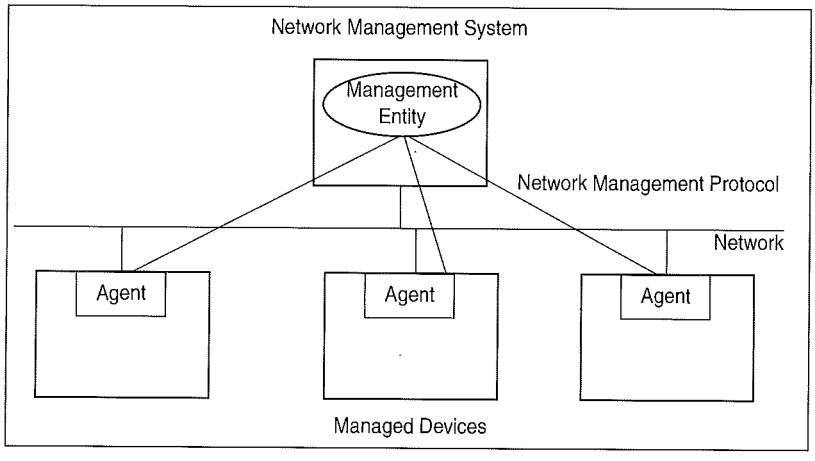
Alle hierboven genoemde produkten komen in verschillende formaten voor. Er zijn eenvoudige, goedkope oplossingen beschikbaar, soms als een softwarepakket op een PC. En ook dure, op specifieke hardware gebouwde oplossingen. Functioneel doen de verschillende formaten nauwelijks voor elkaar onder, de verschillen zitten voornamelijk in de verwerkingskracht. Afhankelijk van de behoefte moet de keuze plaatsvinden.

	Hub	Bridge	Router	Gate-way	Werk-station	Server	Netwerk-besturings-systeem
Configuration management	x	x	x	x	x	x	x
Performance management		x	x	x		x	x
Accounting management		x	x	x		x	x
Fault management	x	x	x	x	x	x	x
Security management	x	x	x	x	x	x	x

x = van toepassing
= geen onderwerp van dit artikel

Figuur 3. OSI-netwerkmanagementmodel.

Figuur 4. Netwerkmanagementarchitectuur.



NETWERKMANAGEMENT

Om de verschillende componenten zoals hierboven beschreven optimaal te laten functioneren, moeten de diverse parameters op de juiste wijze worden ingesteld en ingesteld blijven. Het optimaal houden van deze instellingen wordt netwerkmanagement genoemd. Netwerkmanagement of netwerkbeheer is onderverdeeld (OSI-model, figuur 3) in de volgende deelgebieden:

- *performance management:* houdt de netwerkperformance (responstijd, netwerkdoorvoer) binnen de afgesproken grenzen;
- *configuration management:* registreert en bewaakt de configuratie van de netwerkhardware en -software;
- *accounting management:* registreert het gebruik van het netwerk met het doel dit gebruik door te belasten;
- *fault management:* registreert en lost netwerkproblemen op;
- *security management:* bewaakt de toegang tot het netwerk.

Integraal netwerkmanagement doelt op het platformoverstijgend uitvoeren van deze functies voor zowel LAN als WAN. In principe vallen onder het netwerkmanagement alle componenten uit het netwerk, dus ook de servers, werkstations en het netwerkbesturingssysteem. Echter in dit artikel worden deze componenten buiten beschouwing gelaten.

In figuur 3 is aangegeven welke beheeraspecten wel en welke niet in dit artikel worden beschreven.

Om het managen van de netwerken adequaat te kunnen uitvoeren, zonder onmiddellijk voor heel veel extra netwerkverkeer te zorgen, werken de meeste netwerkmanagementsystemen met een architectuur zoals in figuur 4 is aangegeven.

In deze architectuur bezit elke te managen component een management-agent, welke lokaal de informatie verzamelt en alleen indien nodig of wanneer dat wordt gevraagd zijn gegevens doorgeeft aan het netwerkmanagementsysteem. Om optimaal gebruik te kunnen maken van alle mogelijkheden van de te managen netwerkcomponenten en van het netwerkmanagementsysteem, moeten de mogelijkheden van de agents goed aansluiten bij de mogelijkheden van de te managen componenten.

De huidige netwerkmanagementsystemen zijn gebaseerd op twee 'standaarden'. Dit zijn: het door OSI gedefinieerde CMIP (Common Management Information Protocol) en het vanuit de Internetsociety ontwikkelde SNMP (Simple Network Management Protocol). In tegenstelling tot SNMP wordt CMIP nog niet veel toegepast, omdat het aantal netwerken dat volgens de OSI-standaarden werkt nog niet zo groot is. Het grote verschil tussen SNMP en CMIP is de complexiteit: CMIP biedt veel meer functies, maar is ook veel complexer en duurder in ontwikkeling, implementatie en gebruik.

Naast Internet en OSI is nog een derde groep bezig met standaardisatie van integraal netwerkmanagement: de Open Software Foundation (OSF). Zij ontwikkelt de Distributed Management Environment (DME), die naar verwachting medio 1995 beschikbaar komt. DME maakt gebruik van SNMP en CMIP en biedt mogelijkheden om de produkten van vrijwel alle leveranciers integraal te beheren. DME is gebaseerd op object oriented-technologie, die de programmeurs in staat stelt een eenduidige applicatieschil aan te bieden aan de gebruiker, voor totaal verschillende onderliggende systemen.

Zoals hierboven reeds aangegeven zijn de meeste systemen gebaseerd op SNMP. Bijna elke leverancier levert zijn eigen netwerkmanagementsysteem. Om de mogelijkheden van de apparatuur goed te kunnen managen worden meestal uitbreidingen op het SNMP-protocol toegepast. De agents in de apparatuur zijn hierop aangepast. Hierdoor zijn de systemen optimaal geschikt gemaakt voor het managen van de eigen apparatuur. Produkten van derden kunnen wel worden gemanaged, maar alleen op de basis-SNMP-functionaliteit. Dit betekent dat de specifieke kenmerken van een bepaalde component, waardoor deze zich onderscheidt van de andere en die soms een belangrijke reden vormden voor de aanschaf, niet via het netwerkmanagementsysteem kunnen worden aangesproken.

Een internetworking-situatie is in de meeste gevallen niet een technisch geplande operatie, waarbij gelijksoortige netwerken worden gekoppeld. In de meeste gevallen moeten om organisatorische redenen netwerken die tot die tijd niets of nauwelijks iets met elkaar te maken hadden en om die reden ook nooit op basis van dezelfde standaardisatie zijn opgezet, aan elkaar worden gekoppeld. Hierdoor wordt men op het technische vlak vaak geconfronteerd met verschillende merken apparaten. Daarnaast is er op dit moment geen enkele leverancier die de gehele lijn van hub tot en met gateway goed kan invullen, waardoor de technisch optimale oplossing automatisch verschillende merken en leveranciers met zich meebrengt. Dit laatste is overigens één van de belangrijkste redenen waarom op dit moment zoveel grote leveranciers van netwerkapparatuur samenwerkingsverbanden aangaan.

Er is op dit moment geen enkele leverancier die de gehele lijn van hub tot en met gateway goed kan invullen.

De problematiek die ontstaat door het koppelen van de netwerken is de internetworking-problematiek. Totdat de standaardisatie op dit vlak haar werk heeft gedaan, blijft men zitten met de situatie waarin het beheer van een groot netwerk met verschillende netwerkapparaten een complexe situatie oplevert. In de praktijk treffen we diverse oplossingen aan:

– Er wordt een netwerkmanagementsysteem aangeschaft bij de leverancier waarvan men de meeste apparaten heeft staan. Gevolg is dat dit deel van de apparatuur goed kan worden beheerd, terwijl de overige apparatuur op het standaard-SNMP-niveau moet worden beheerd. In veel netwerken hebben bijvoorbeeld de hubs in aantal de overhand en vragen de hubs veel beheer bij het verhuizen van medewerkers. Daarom ligt vaak het accent op het beheer van de hubs. Het beheer van de veelal later aangeschafte bridges en routers komt daardoor op het tweede plan.

– Er worden meerdere netwerkmanagementsystemen aangeschaft. Dit heeft tot gevolg dat alle apparaten optimaal kunnen worden beheerd, maar beheer van de onderlinge relatie is niet mogelijk. Wijzigingen in het ene apparaat hebben vaak gevolgen voor de configuratie van het andere. Het oplossen van storingen wordt een zeer complex probleem, doordat niet één systeem kan aangeven waar de storing zit. Er moet steeds tussen de verschillende systemen worden geswitched om een fout goed te kunnen diagnostiseren. Doordat het managementsysteem uit meerdere losse deelsystemen bestaat, ontstaat een grote afhankelijkheid van de kennis en vaardigheden van de beheerders. Ook moet een goede documentatie over de onderlinge afhankelijkheden worden bijgehouden. In de praktijk wordt deze situatie vaak aangetroffen in een variant waarbij alle netwerkmanagementsystemen op één werkstation draaien. Hierdoor wordt een mate van integratie gesuggereerd die in het geheel niet aanwezig is. Weliswaar kunnen in de grafische user-interface meerdere vensters worden geopend, waarbij in elk venster één van de netwerk-

Voorbeeld 1. Ontstaan van internetworking-situatie.

Een bedrijf heeft twee autonome regionale vestigingen. Elk van deze vestigingen heeft in de loop der jaren een netwerk opgezet. Omdat er geen centrale sturing was voor de standaardisatie hebben beide vestigingen gekozen voor een verschillende invulling van hun netwerk. Als gevolg van wijzigingen in de besturingsfilosofie van het bedrijf worden de beide vestigingen onder één leiding gebracht. De nieuwe directeur wenst graag maandelijks de geconsolideerde resultaten van de beide vestigingen te zien. Mede hierdoor ontstaat er steeds meer behoefte aan het uitwisselen van bestanden tussen de beide vestigingen. De beide netwerken worden gekoppeld met een router en nu kunnen de bestanden tussen de beide vestigingen worden uitgewisseld.

managementsystemen draait. Maar van echte integratie, dus onderlinge uitwisseling van gegevens, is geen sprake.

– Er wordt een netwerkmanagementsysteem aangeschaft bij een derde, omdat dat alle aanwezige apparatuur goed kan beheren. Vaak komt het beheer van de verschillende componenten niet tot het optimale niveau. Toch geeft deze oplossing de beste integratiemogelijkheden. Als later de standaardisatie geheel is afgerond, kunnen de vruchten hiervan het snelst worden geplukt.

In de internetworking-situatie, waarbij minimaal twee netwerken zijn gekoppeld, is met name het beheer van de routers van groot belang om de internetworking-koppeling te laten werken. Omdat de router de verbindende component is tussen de beide netwerken, speelt hij een grote rol in het functioneren van het totale netwerk. Belangrijkste aspecten zijn daarbij performance en security management. Het is van groot belang om het routerbeheer op de juiste wijze te laten uitvoeren en op de juiste plaats in de organisatie in te bedden.

Voorbeeld 2. Organisatorische inbedding router-beheer.

Omdat naast de routers vaak ook de beide (of meerdere) gekoppelde netwerken moeten worden beheerd, ligt het voor de hand om de beide beheerorganisaties te integreren en het router-beheer ook in deze organisatie onder te brengen. In de praktijk stuit dit vaak op weerstand en wordt om allerlei organisatorische redenen vaak gekozen voor een (voorlopig) gescheiden houden van de beide beheerorganisaties. Het router-beheer wordt dan vaak bij één van de beheerorganisaties, meestal de grootste, ondergebracht. Vanwege de verschillende achtergronden van de beide organisaties is er een onderlinge scepsis en die wordt alleen maar groter als de onderlinge verbinding (de router) door de grootste organisatie mag worden beheerd. Er ontstaat dan snel het gevoel dat de 'groten' de 'kleinen' toegang verlenen en dit expres maar heel beperkt doen. Dit is een verkeerde uitgangspositie voor een volledige integratie van de netwerken. Hieraan moet bij het onderbrengen van het beheer de nodige aandacht worden geschonken.

SECURITY-RISICO'S

Koppelen van verschillende netwerken introduceert een aantal security-risico's. Deze kunnen verschillende oorzaken hebben:

– Doordat het netwerk door de koppeling groter wordt, wordt de 'sociale' controle onder de gebruikers minder. Vaak kennen de beheerders de gebruikers niet meer persoonlijk. De afgenomen sociale controle heeft tot gevolg dat gebruikers meer gaan proberen op het netwerk. Ze gaan op ontdekkingsreis door het netwerk.

– Doordat het netwerk door de koppeling groter wordt, is het moeilijker te overzien voor de beheerders. Als gebruikers wijzigingen, hardware- of softwarematig, aan hun werkstation aanbrengen, dan is de kans op ontdekking gering.

– Doordat met de toename van de omvang van het netwerk de betrokkenheid en solidariteit onder de gebruikers afneemt, houden gebruikers geen of minder rekening met of hebben in het geheel geen weet van de gevolgen van hun handelen voor anderen in het netwerk. Zonder nadenken worden grote bestanden over het netwerk getransporteerd; de daaruit mogelijkerwijs voortvloeiende congestie in het netwerk vormt een bedrijfsrisico. Zeker nu bedrijven steeds afhankelijker worden van hun netwerken.

Voorbeeld 3. Gevolgen van onoordeelkundig netwerkgebruik.

E-mail-applicaties vormen bij onoordeelkundig gebruik een bedrijfsrisico, doordat ze het gehele netwerk kunnen laten vastlopen. Indien een medewerker grote bestanden (mega- of gigabytes) als attachment aan een mail meestuurt over het netwerk kan het gehele netwerk verstopt raken. Met name bridges, routers en gateways kunnen geheel verstopt raken door zo'n groot verkeersaanbod. Het complete netwerk kan komen stil te liggen. Een ander risico wordt gevormd door het zenden van berichten met attachment naar veel geadres-seerden. In sommige mail-systemen wordt de aangehechte file voor elke geadresseerde opnieuw opgeslagen. Hierdoor kan de gehele mailserver vastlopen met alle gevolgen van dien.

– De omwille van de schaal noodzakelijk te nemen beveiligingsmaatregelen worden als lastig en hinderlijk ervaren; gebruikers vinden allerlei wegen om deze te omzeilen.

– Grote netwerken herbergen meestal ook meerdere host-systemen. Veel grote organisaties gaan uit oogpunt van gebruikersvriendelijkheid over tot 'single-logon'-systematiek. Dit is een methode waarbij een gebruiker maar op één systeem hoeft in te loggen en vandaar (schijnbaar) zonder controle naar andere systemen kan overschakelen. Als echter een user-id/wachtwoord-combinatie in handen van een derde belandt, dan heeft deze de mogelijkheid om toegang te krijgen tot alle systemen waarvoor de rechtmatige eigenaar van de

In een grote organisatie werd onlangs bij toeval ontdekt, dat groepen gebruikers uit gemakzucht collectief een zelfde wachtwoord gebruikten. Omdat er lijsten met user-id's op de afdelingen beschikbaar waren, konden op deze manier collega's eenvoudig in elkaars bestanden kijken. Systemen bieden geen hulpmiddelen om dit soort risico's te onderscheppen.

Voorbeeld 4. Omzeiling van als hinderlijk ervaren beveiligingsmaatregelen.

user-id/wachtwoord-combinatie toegangsrechten heeft. In de praktijk wordt in een 'single-logon'-situatie vaak een extra zwaar authenticatiemechanisme gehanteerd.

– Een aantal van de netwerkbesturingssystemen (Banyan Vines, OS/2 LanServer, Novell Netware 4.x) is reeds aangegeven of gaat op korte termijn over op de 'domain'-benadering. Deze domain-benadering komt erop neer dat een gebruiker niet meer hoeft in te loggen op de servers van het netwerk, maar dat hij inlogt op het netwerk zelf. Daarna kunnen alle servers waarvoor de gebruiker gerechtigd is, worden benaderd. Deze methode is een vorm van 'single-logon', en heeft dus dezelfde risico's in zich.

– Alle netwerkbesturingssystemen hebben een security-mechanisme. Reeds eerder is aangegeven dat de verschillende netwerkbesturingssystemen alle op een verschillende wijze invulling aan het OSI-model hebben gegeven. Omdat voor de security-mechanismen geen referentiemodel bestaat, zijn de invullingen voor elk netwerksysteem anders. De meeste van deze mechanismen zijn erop gebaseerd dat de bevoegdheden tot het starten en stoppen van processen worden gelimiteerd. De autorisatie hiervoor wordt echter op verschillende wijzen vastgelegd. Om in een internetworking-situatie de security-mechanismen goed te laten werken is het van groot belang dat deze autorisaties goed worden overgedragen tussen de netwerksystemen. Als dat niet zo is, kan het gevolg zijn dat geautoriseerde personen op het andere netwerk geen processen kunnen starten of stoppen, maar het kan ook dat ongeautoriseerde personen nu ineens wel processen kunnen starten en stoppen, met alle security-risico's van dien. De problemen die worden geïntroduceerd, lijken veel op de problematiek van de gateways die eerder in dit artikel is toegelicht.

Om deze risico's afdoende te kunnen beheersen, moeten de toegepaste netwerkcomponenten voldoende hulpmiddelen bieden. In de huidige routers is het niveau van de geboden faciliteiten op dit gebied onvoldoende. Dat is ook niet de oorspronkelijke opzet van een router geweest. De toepassing van de veel complexere en dus ook duurdere gateways kan veel meer van deze risico's efficiënt beheersen. Gateways bezitten namelijk de intelligentie om niet alleen het soort boodschap te bewaken, maar kunnen ook de gehele inhoud van de boodschap bewaken. Indien nodig kunnen ze zelfs gedurende de sessie ingrijpen. Vanzelfsprekend staat tegenover dit voordeel ook weer een nadeel: het beheer van een gateway is zeer complex, zeker van die modellen welke de inhoud van de boodschappen bewaken.

Een voorbeeld van zo'n gateway zijn de zogenaamde proxies. Een proxy is een softwarepakket op een Unix-systeem dat wordt gebruikt voor de beveiliging van een koppeling aan Internet (deze vorm van beveiliging wordt ook wel firewall genoemd). Een ftp-proxy kan bijvoorbeeld het kopiëren van bestanden naar Internet niet toestaan, terwijl het laden van bestanden vanaf Internet wel wordt toegestaan. Een router kan file transfer niet beveiligen, doordat hij de berichten alleen tot en met laag 3 inziet. Ftp is echter een protocol van de hogere lagen. In deze situatie is dus een gateway de enige oplossing.

CONCLUSIE

Zoals hiervoor aangegeven kan het koppelen van netwerken een aantal problemen introduceren. Daarom moeten deze koppelingen alleen worden gerealiseerd als daar een functionele behoefte tegenover staat.

De wijze van koppelen moet zorgvuldig worden gekozen. Het is van belang vooraf goed de te verwachten veiligheidsrisico's te inventariseren en die af te zetten tegen de benodigde investeringen in hardware en beheergereedschappen en de benodigde beheerinspanning. Pas na een goede weging van deze facetten kan een gefundeerde keuze worden gemaakt.

Hoewel moeilijk te beheren, heeft de inzet van de gateway in veel gevallen de voorkeur. De relatief hoge exploitatielasten, als gevolg van de complexe beheerproblematiek, moeten goed worden afgewogen tegen de afname van de security-risico's.

H. Roos RA
Is directeur bij KPMG Management Consulting. Geeft leiding aan een groep adviseurs op het gebied van telecommunicatie en netwerken, software engineering, DIS, cryptografie, informatie security en risico-analyse. Actief op de gebieden risicomanagement van grote IT-projecten, architectuur en beheer van corporate communicatiesystemen, IT-gerelateerde organisatieverandering en information security in elektronische betaalsystemen, netwerken en EDI-toepassingen.

Ir. M.T.H. Heesbeen
Is senior organisatie-adviseur bij KPMG Management Consulting. Heeft jarenlange ervaring in het ontwerpen van telematica-infrastructuren. Hij heeft zich gespecialiseerd in de ontwerp- en architectuuraspecten van telecommunicatie en netwerken.

Geïntegreerd netwerkbeheer

Ing. W.A.A. Zoon

SNMP-managementplatformen zijn goed inzetbaar voor operationeel beheer in multi-vendor bedrijfsnetwerken. Bij het opzetten van een geïntegreerd managementsysteem voor een organisatie zijn geen standaardoplossingen beschikbaar. Maatwerk is hier noodzakelijk daar iedere netwerkomgeving verschillend is en andere eisen stelt ten aanzien van operationeel, tactisch en strategisch beheer.

INLEIDING

In dit artikel wordt een beschouwing gegeven van de voornaamste beheersystemen (managementsystemen) die momenteel gebruikt worden voor het beheren van grotere multi-vendor LAN- en WAN-omgevingen. Tevens wordt de inzetbaarheid van deze beheersystemen aangegeven in grotere netwerken, die niet alleen lokaal zijn, maar tevens geografisch verspreid zijn. Het aantal componenten dat kan worden beheerd met een beheersysteem is de afgelopen jaren aanzienlijk toegenomen door de introductie van een standaard-beheerprotocol (het Simple Network Management Protocol). Voorheen waren meerdere beheersystemen noodzakelijk die ieder een eigen beheerprotocol ondersteunden.

Naast LAN-componenten, waarmee het fysieke lokale netwerk (infrastructuur) wordt opgebouwd, zoals hubs, zijn er vele componenten die op het LAN worden aangesloten. Huidige netwerken zijn veelal verspreid over meerdere locaties, zodat een Wide Area Network (WAN) ontstaat. In dit WAN zijn veelal koppelvlakken (gateways) gedefinieerd naar grote centrale systemen (databases) of externe netwerken, zoals Internet.
Voor het beheren van grotere bedrijfsbrede netwerken is een beheerorganisatie noodzakelijk die onder andere verantwoordelijk is voor het goed functioneren en onderhouden van het netwerk. Momenteel wordt operationeel beheer van bedrijfsbrede netwerken steeds vaker uitbesteed (outsourcing). Tevens zien we dat automatiseringsafdelingen inclusief netwerkbeheer binnen de overheid worden geprivatiseerd.
De beheerorganisatie werkt het meest efficiënt met een centraal beheersysteem dat een overzicht kan geven van alle aanwezige netwerkcomponenten binnen het bedrijfsbrede netwerk. Alle netwerkproblemen kunnen centraal verzameld (gemeld) worden in een database, waarbij correlatie en verwerking van de gegevens mogelijk is. Oplossen van problemen is hierdoor eenvoudig, daar op één plaats in het netwerk bekend is, welke componenten goed functioneren (alle componenten zijn immers met elkaar verbonden en vormen samen 'het netwerk'). Voor het uiteindelijk gedetailleerd oplossen van problemen kunnen specialistische deelsystemen worden gebruikt.

Er wordt een onderscheid gemaakt tussen een beheersysteem, een beheerplatform en een beheerapplicatie. Een beheersysteem is één fysiek beheersysteem. Een beheerplatform is een gespecificeerd raamwerk, dat in principe uit meerdere fysieke systemen kan bestaan, waarop meerdere beheerapplicaties van verschillende leveranciers (als de specificaties open zijn) ondersteund kunnen worden. Een beheerapplicatie is een applicatie die als onderdeel van een beheerplatform, veelal via grafische beelden, netwerk- of systeemcomponenten beheert.

Dit artikel begint met een kort historisch overzicht van netwerkbeheersystemen, waarna de behoeften voor het geïntegreerd beheren van netwerken op een rij worden gezet. Vervolgens wordt de hiërarchie binnen netwerkbeheersystemen besproken.

Uiteindelijk komen de SNMP-managementplatformen aan bod, waarbij het artikel ingaat op de mogelijke inzetbaarheid van dergelijke centraal, breed toepasbare beheersystemen in bedrijfsbrede netwerken. Leveranciers geven aan dat hun beheersystemen breed toepasbaar zijn voor grote bedrijfsnetwerken. Er wordt getracht een indruk te geven van deze praktische toepasbaarheid.

GESCHIEDENIS NETWERKBEHEER

Tot voor kort werden bedrijfsbrede netwerken, telecommunicatienetwerken in het bijzonder, beheerd op basis van specifieke gesloten oplossingen. Netwerkbeheersystemen waren toegespitst op het beheren van slechts een specifiek deelgebied, hetgeen tevens sterk leverancier-afhankelijk was. Iedere leverancier bracht zijn LAN- of WAN-produkten op de markt met een eigen beheersysteem dat alleen op eigen specifieke produkten van toepassing was.

In grotere LAN/WAN-omgevingen ontstaan dus meerdere beheersystemen, met ieder een eigen operating-systeem (vaak ook eigen hardware) en gebruikers-interface. Uiteindelijk resulteerde dit in een overmaat aan beheersystemen, welke beperkt waren in hun mogelijkheden en problemen gaven rondom onderlinge samenwerking. De effectiviteit rondom het beheren en automatiseren van het beheren van netwerken neemt hierdoor sterk af. Het antwoord op de behoefte aan geïntegreerd beheer is uiteindelijk de ontwikkeling van diverse netwerkbeheer-standaarden geweest.

Een beheersysteem is één fysiek beheersysteem. Een beheerplatform is een gespecificeerd raamwerk, dat in principe uit meerdere fysieke systemen kan bestaan, waarop meerdere beheerapplicaties van verschillende leveranciers (als de specificaties open zijn) ondersteund kunnen worden.

De belangrijkste standaarden voor netwerkbeheer zijn:

- De *'OSI suite of protocols'*, gesponsord door computergebruiker DOD (Amerikaanse Ministerie van Defensie) ISO/ITU-S [ISO7498-4] (International Standardization Organization/International Telecommunications Union - Standards Sector (voorheen CCITT)), met als protocol het Common Management Information Protocol of CMIP.

- De *'Internet suite of protocols'*, de Internet comité standaard [RFC (Request for Comments) 1155, RFC1157], met als managementprotocol het Simple Network Management Protocol of SNMP.

Jammer genoeg is er bij het opzetten van beide standaardisatie-activiteiten vrijwel geen coördinatie tussen de comités onderling geweest. Hoewel zij als resultaat momenteel een gelijkwaardig beheermodel hanteren, wijken de gebruikte beheerprotocollen van elkaar af. Hetzelfde geldt voor de Structure of Management Information (SMI), die de structuur vastlegt van hoe de beheerinformatie wordt opgeslagen. Het succes van SNMP is voornamelijk te danken aan de eenvoud van het protocol en de snelle beschikbaarheid (mede door eenvoud) en dus mogelijke implementatie. Het standaard-communicatieprotocol binnen de 'Internet suite of protocols' is TCP/IP (Transmission Control Protocol/Internet Protocol).

TCP/IP is momenteel het enige beschikbare gestandaardiseerde multi-vendor communicatieprotocol. SNMP is aan deze TCP/IP-protocolfamilie toegevoegd, met als gevolg dat vrijwel alle op TCP/IP gebaseerde produkten nu tevens SNMP ondersteunen en dus op een standaardmanier beheerbaar zijn geworden. Door de brede ondersteuning van SNMP in de markt, die vooral uit LAN-produkten maar nu ook WAN-produkten bestaat, is het theoretisch mogelijk één (logisch) beheersysteem of beheerplatform te gebruiken. Een beheerplatform of managementplatform vormt een basisraamwerk voor het aansturen van een netwerkomgeving. Het is theoretisch mogelijk meerdere fysieke systemen te integreren tot één logisch beheersysteem. De eisen en wensen aan deze beheersystemen en de mogelijkheden en verschillen van de huidige beheersystemen worden in onderstaande alinea's uitgewerkt.

NETWERKMANAGEMENT-BEHOEFTEN

Huidige netwerken bestaan uit vele systemen en netwerkcomponenten, waarvan hieronder een mogelijke samenhang wordt gegeven. PC's, terminals en printers zijn via een LAN inpandig gekoppeld met servers en systemen. Het LAN (datanetwerk) is via routers gekoppeld aan bandbreedtemanagement-apparatuur, waaraan tevens het telefonienetwerk en het mogelijke mobiele of video-bewakingsnetwerk gekoppeld zijn. Bandbreedtemanagement-apparatuur (van leveranciers als Stratacom en Newbridge) wordt ingezet op het LAN/WAN-koppelvlak en biedt standaardaansluitingen voor data, spraak, mobiele communicatie en video. Hierdoor wordt een dure WAN-verbinding optimaal gebruikt. De bandbreedtemanagement-apparatuur wordt dus direct gekoppeld op het WAN. In het WAN bevinden zich meerdere locaties met als knooppunt weer een bandbreedtemanager of switch. De nieuwe technologie voor bandbreedtemanagers is ATM (Asynchronous Transfer Mode). Al deze componenten dienen op een zo efficiënt mogelijke wijze binnen een organisatie beheerd te worden.

Iedere omgeving gebruikt veelal 'eigen' tools voor operationeel management. Deze tools bestaan uit een veelvoud aan componenten van verschillende leveranciers met 'eigen' managementoplossingen. Uiteindelijk resulteert dit in vele management-consoles, die ieder een eigen grafische of karaktergeoriënteerde gebruikers-interface hanteren, waarvan de opzet en aansturing verschillend zijn. Er is geen correlatie tussen systemen onderling, zodat het zoeken en oplossen van problemen tijdrovend en complex is. Dit geldt met name in grotere netwerkomgevingen waar LAN-beheer een radertje is ten opzichte van het beheer van het totale netwerk.

Managers zijn de actieve componenten die een groep passieve agents aansturen (vragen om informatie). De agents verzamelen de operationele informatie en zijn de harde werkers in de beheeromgeving.

Complexiteit

Er bestaat geen beheersysteem dat simpelweg ingezet kan worden voor het beheren van het totale netwerk. De complexiteit van het beheer van het netwerk is grotendeels afhankelijk van de volgende factoren:

- het aantal en soort te beheren componenten. Een groot aantal te beheren componenten vraagt bijvoorbeeld veel aandacht voor het opzetten van een netwerkadresseringsplan. Complex te beheren componenten met vele beheerparameters vragen veel kennis van de beheerder;
- de heterogeniteit van de systemen en componenten (protocollen, interfaces, systeemsoftware);
- de verspreiding van de te beheren componenten;
- aantal betrokken beheerorganisaties en de onderlinge verantwoordelijkheden;
- de manier waarop services geïntegreerd zijn en subnetwerken verbonden zijn;
- het aantal te ondersteunen gedistribueerde applicaties en netwerkdiensten.

Tabel 1. Overzicht van te beheren componenten in een netwerkomgeving.

Systeemomgeving	WAN-omgeving	LAN-omgeving
Mainframes	Routers/bridges	Hubs
Mini's	Multiplexers/switches/bandbreedte-managers	Bridges/routers/switches
		Virtuele netwerken
LAN-fileservers	PABX'en/CODECS (video)/Mobiel	Inbel-voorzieningen
Randapparatuur	Terminal adapters/modems	Bekabeling
PC's/werkstations/portables	Gateways/protocol translators	Terminal servers

Te beheren componenten

Voor de managementomgeving kunnen we voor de te beheren componenten globaal een opsplitsing maken in een systeemomgeving, een WAN-omgeving en een LAN-omgeving.

Zoals in tabel 1 is aangegeven, kan een netwerkomgeving vele componenten omvatten, waarbij het scheidingsvlak LAN/WAN niet duidelijk meer is aan te geven, daar vele functies zowel binnen de LAN- als binnen de WAN-omgeving overlappend zijn. Voornamelijk door het succes van SNMP is het mogelijk zowel systemen, WAN-componenten als LAN-componenten vanuit een enkele protocolomgeving te beheren. Om deze mogelijkheid optimaal te benutten is integratie binnen één managementplatform noodzakelijk.

Een gemeenschappelijke database voor alle netwerkcomponenten, waaruit alle andere managementapplicaties hun data putten, is momenteel nog niet mogelijk maar zeker gewenst. Wel kunnen verschillende SNMP-managementapplicaties geïntegreerd worden op één SNMP-managementplatform, maar iedere applicatie gebruikt een eigen database met gegevens voor de desbetreffende applicatie. Indien de database-omgeving gelijk is voor meerdere applicaties, kunnen gemeenschappelijke database-tools gebruikt worden.

Een beheerapplicatie is een applicatie die als onderdeel van een beheerplatform, veelal via grafische beelden, netwerk- of systeemcomponenten kan beheren.

Multi-vendor netwerken

Het betrekken van componenten van meerdere leveranciers in een netwerk kan op verschillende niveaus plaatsvinden. Applicatiekeuze is in vele gevallen nog steeds leverancier- of hardware-afhankelijk. De positie van het netwerk is belangrijker geworden daar alle systemen primair via het netwerk bereikbaar zijn. De gebruiker ziet het netwerk als 'de computer'. Indien het netwerk problemen heeft kan de gebruiker geen systemen meer bereiken. Het netwerk is de snelweg waar vele leveranciers samen komen richting eindgebruiker, waarbij de gebruikers-interface veelal grafisch is (PC met Windows, Macintosh, Unix-werkstation).

Aanschaffen van één leverancier-specifiek beheersysteem voor iedere omgeving is duur, moeilijk te beheren (geen integratie, kennis per platform nodig), tijdrovend en inflexibel. Tevens is voor elke specifieke tool specialisatie noodzakelijk, waarvoor extra mankracht dient te worden ingezet.

Oplossingen voor deze problemen moeten worden gezocht in:

- meer flexibiliteit binnen één beheerplatform;

- integratie van leverancier-specifieke applicaties op een platform;
- standaardisatie (noodzakelijk).

Uiteindelijk resulteert dit in kostenbesparing. De managementomgeving dient tevens gedistribueerd te kunnen worden gebruikt indien er sprake is van meerdere locaties of disciplines.

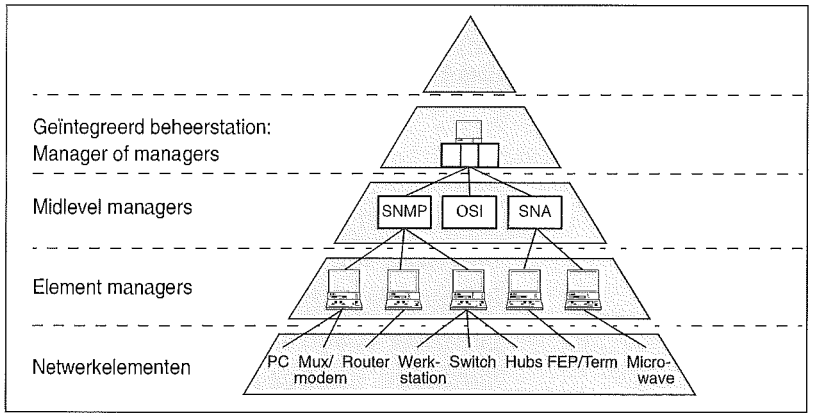
Agents initiëren alleen contact (traps) met managers bij serieuze of voorgedefinieerde gebeurtenissen. Managers zenden commando's, agents voeren de commando's uit.

Aandachtsgebieden multi-vendor beheersystemen
Hieronder wordt een aantal belangrijke aandachtsgebieden opgesomd:

- gebruik van gemeenschappelijke tools. Tools voor beheerplatformen dienen geïntegreerd te kunnen worden gebruikt voor het gehele beheerplatform;
- integreren van meerdere beheerapplicaties van verschillende leveranciers;
- gemeenschappelijk gebruik van verzamelde data van een beheerapplicatie;
- alarmcorrelatie of gemeenschappelijk gebruik van binnenkomende events door meerdere beheerapplicaties;
- gedistribueerd beheer;
- end-to-end-beheer. Tussen twee eindsystemen in een netwerk zijn veelal vele netwerkcomponenten aaneengeschakeld. Netwerkbeheersystemen dienen te begrijpen hoe het netwerk er 'end-to-end' uitziet en dit aan te geven als één van de componenten van de schakel uitvalt;
- top/bottom-beheer. Grote netwerken in subnetwerken grafisch weergegeven op een beheerscherm, dienen tot in detail beheerbaar te zijn;
- security;
- configuratie en probleemherkenning;
- kunnen beheren van multiprotocol-omgevingen.

NETWERKMANAGER-MODELLEN

Om te begrijpen wat de sterke en zwakke kanten zijn van de vandaag de dag beschikbare SNMP-netwerkbeheersystemen, is het belangrijk om te weten waar deze produkten precies passen binnen het enterprise netwerkmanagement-model. Dit is een hiërarchisch model, dat weergegeven is in piramidevorm. Dit model lijkt veel op het UNMA (Unified Network Management Model), ontwikkeld door AT&T eind tachtiger jaren. De gemodificeerde versie omvat als extra laag de zogenaamde midlevel manager (MLM) laag, die het totale model op een vierlaags configuratie brengt (zie figuur 1).



Figuur 1. De netwerkmanagement-piramide.

Managementhiërarchie

Hieronder worden de verschillende niveaus in de weergegeven managementpiramide nader uiteengezet.

Netwerkelementen
Het laagste niveau van figuur 1 wordt gevormd door de netwerkelementen, die uit fysiek en logisch te beheren componenten bestaan. Fysieke componenten zijn bijvoorbeeld hubs, routers, switches, multiplexers, modems en systemen. Logische componenten zijn bijvoorbeeld services, sessies en routetabellen.

Element managers (EMS'en)
Het tweede niveau van de piramide wordt gevormd door element managers of Element Management Systemen (EMS'en). De element-managementsystemen handelen slechts specifieke subsets aan netwerkcomponenten af. Element-managementsystemen zijn leverancier-specifieke beheersystemen, waarmee alleen netwerkcomponenten van de leverancier zelf beheerd kunnen worden. Voorbeelden van EMS'en zijn specifieke managementsystemen voor modems, multiplexers, LAN-hubs, routers en bandbreedtemanagers (netwerkknooppunten).

SNMP-platformen als SunNet Manager, HP OpenView en NetView/6000 functioneren primair als Midlevel Manager (MLM).

Midlevel managers (MLM's)
Huidige SNMP-managers als HP OpenView, SunNet Manager en NetView for AIX passen het best binnen de MLM-laag. De MLM's zijn uitstekend in staat op SNMP gebaseerde apparatuur te

beheren. Om het management-integratieniveau (MOM) te kunnen behalen zijn er krachtiger mechanismen noodzakelijk om niet-SNMP-componenten en -systemen te kunnen beheren.

Platformen vormen de basis voor mogelijke integratie van netwerkbeheer. De platformen van de eerste generatie boden slechts integratie van hardware, huidige platformen wisselen in beperkte mate informatie uit. Oplossingen voor werkelijke integratie zijn nog niet in zicht.

Midlevel Managers (MLM's) vullen het derde niveau in van het hiërarchische model.
MLM's zijn in staat alarmsignalen te monitoren van een groep netwerkelementen waaronder tevens EMS'en kunnen vallen, waarbij niet alle systemen van dezelfde leverancier hoeven te zijn. Agents van managementcomponenten en EMS'en rapporteren managementinformatie aan MLM's.

Een tweede karakteristiek van MLM's is dat deze managementplatformen voorzien in Application Program Interfaces (API's), die gebruikt kunnen worden door de EMS'en en netwerkmanagement-applicaties, zoals probleemmanagement- en configuratiemanagement-applicaties. De API's maken het mogelijk deze applicaties enigszins te integreren op het grafische gebruikers-interface (GUI) niveau. Algemeen geldt dat MLM's in staat zijn managementinformatie van agents te integreren die binnen dezelfde protocolfamilie vallen.

IBM's NetView/390 vervult feitelijk dezelfde taak als een SNMP MLM maar dan voor SNA-agents. MLM's die voor OSI CMIP-agents deze functie vervullen, beginnen beschikbaar te komen.

Manager of managers (MOM)
Bovenaan in het hiërarchische model staat het management-integratieplatform (MOM) centraal, dat informatie verzamelt van EMS'en en MLM-systemen en een universele database creëert van alle te beheren data. Vanuit dit platform is een totaal overzicht, monitoring en controle mogelijk van het gehele netwerk. In een multiprotocol enterprise netwerkomgeving moet een MOM via een gateway (verzorgt translatie van protocol naar native gateway protocol) of rechtstreeks (native-mode) aansluiten bij alle managementprotocollen (SNMP, SNA/APPN, CMIP). Native-mode interfaces werken efficiënter dan gateways of vertalers. Hoewel de midlevel managers de potentie hebben om enterprise manager te worden en gateways ondersteunen naar andere protocollen, is geen van de MLM-managers oorspronkelijk opgebouwd als multiprotocol management-integratieplatform.

Om te kunnen spreken van een geïntegreerde managementomgeving dienen eerst deze basis-ontwerpcriteria te worden aangepast.

Zwakke punten huidige MLM's

Hieronder worden de MLM's geëvalueerd op basis van een aantal belangrijke managementbehoeften. Per punt zal de ondersteuning voor huidige SNMP MLM's worden aangegeven.

Multiprotocol-ondersteuning
Bekende midlevel managers zoals HP OpenView, SunNet Manager en NetView for AIX zijn gebouwd op basis van één protocol, in dit geval SNMP. De interne software-architectuur, grafische interface, API's en alarmanalyse-architectuur, zijn op maat gemaakt voor dat ene protocol. Andere protocollen kunnen via gateways worden aangestuurd, maar behalen niet dezelfde functionaliteit als die van native aangestuurde protocollen, ofwel SNMP-managers beheren SNMP-componenten beter dan TCP/IP-componenten.

Geïntegreerd zicht op het netwerk (één MAP)
Niet één van de drie platformen voorziet in een geïntegreerd beeld van een multiprotocol-netwerk. Ieder protocol wordt binnen een aparte map gevisualiseerd. Een geïntegreerd beeld van alle netwerkcomponenten en protocollen van het gehele netwerk is een primaire behoefte voor een enterprise-managementsysteem.

Schaalbaarheid
Ondanks wat leveranciers beweren zijn de MLM's niet geschikt voor het beheren van enterprise-netwerken met meer dan een paar duizend eindnodes. Bij het bouwen van grote managementomgevingen ontstaat er een dimensioneringsprobleem, daar het gebruik van X-Window clients, meerdere managementconfiguratie-applicaties, trouble ticketing-applicaties en cable management-applicaties alle vanuit één platform gestuurd dient te worden. Voor het dimensioneren van het beheersysteem geeft de leverancier alleen regels voor zijn eigen beheerapplicatie. In een grote beheeromgeving waarin beheerapplicaties van meerdere leveranciers geïntegreerd dienen te worden, is dimensioneren moeilijker. In deze situatie kan een system integrator uitkomst bieden.

Alarmcorrelatie
Hoewel SNMP-managers andere protocollen kunnen beheren via gateways, wordt elk protocol via gescheiden systemen beheerd, zodat gescheiden databases ontstaan. Huidige MLM's zijn niet in staat alarmmeldingen te correleren tussen verschillende protocollen, zodat gebruikers zelf moeten uitzoeken hoe en waar het probleem ligt wanneer problemen in een deel van het netwerk relateren tot een ander deel van het netwerk. Huidige SNMP-beheersystemen hebben zelfs moeite om alarmsignalen van SNMP-componenten te correleren.

Gedistribueerd management
Het lijkt alsof iedereen gedistribueerd management op de markt aanbiedt, maar bij huidige MLM's ontbreekt iedere manager-to-manager-faciliteit, waarbij een decentrale manager kan communiceren met een andere manager over bijvoorbeeld probleemescalatie. De SNMP-managementplatformen leveren geen standaardfunctionaliteit om gedistribueerd te kunnen werken met een database. Binnen de nieuwe versie van het SNMP-protocol (SNMP-versie 2) is informatie-uitwisseling tussen SNMP-beheersystemen mogelijk. Dit protocol is een stuk complexer en wordt nog niet ondersteund door huidige MLM's.

Applicatie-integratie
Geen van de momenteel beschikbare MLM's ondersteunt geïntegreerde managementapplicaties voor probleemoplossing, configuratiebeheer, accounting, security, of performance management. Configureren dient met verschillende applicaties te gebeuren, waarbij iedere applicatie eigen commando's hanteert. Integreren is niet mogelijk zonder een platformarchitectuur die gedistribueerd werken toestaat, zodat belasting verdeeld kan worden en databases gedistribueerd kunnen worden.

Configuratie en probleemherkenning
Om te werken met op Unix gebaseerde SNMP-beheersystemen is het noodzakelijk uitgebreide kennis te hebben van zowel het Unix-operating-systeem als het SNMP-beheerprotocol. Management Information Bases (MIB's) van verschillende leveranciers dienen op het Unix-beheerplatform geladen te worden. Configureren met het SNMP-protocol is complex, daar vanuit een lijst met beheerparameters van de desbetreffende component (vendor-MIB) geconfigureerd moet worden. Een groot nadeel van SNMP-configuratiebeheer is dat het SNMP-protocol geen beveiliging kent. Netwerkproblemen worden door netwerkcomponenten via een SNMP-'trap'-melding bekend gemaakt. De 'trap'-meldingen zijn niet altijd even duidelijk en dienen geïnterpreteerd te kunnen worden. De netwerkbeheerorganisatie dient kennis te hebben van zowel de Unix-omgeving, het SNMP-protocol als de netwerkcomponenten.

Interoperability
Plannen voor het bouwen van gedistribueerde netwerkbeheersystemen hangen volledig af van de mogelijkheid of verschillende platformen onderling kunnen samenwerken. Momenteel kunnen HP OpenView, SunNet Manager en NetView for AIX onderling geen beheerdata uitwisselen, zodat het niet mogelijk is enterprise-applicaties te ontwikkelen. Iedere leverancier ziet zijn beheerplatform bij voorkeur als MOM-platform. Het lijkt wel of leveranciers het extra moeilijk maken om tussen beheerplatformen onderling te kunnen communiceren. Het is zelfs niet mogelijk tussen twee HP OpenView platformen, of tussen twee NetView for AIX platformen optimaal te communiceren. De nieuwe versie van SNMP - bekend als SNMP 2 - voegt opties toe voor manager-tot-manager-communicatie, waarvan er momenteel nog geen implementaties zijn.

Backward compatability
Eén van de moeilijker op te lossen problemen is het ondersteunen van oudere reeds bestaande protocolomgevingen (legacy protocols), waarbij element managers (EMS'en) niet in staat zijn te communiceren met een MLM. De MLM is gebaseerd op het standaard-SNMP-protocol en is niet in staat oudere protocollen te beheren. De enige mogelijkheid is om de netwerkcomponenten op te waarderen naar een te beheren niveau, hetgeen een dure conversie kan zijn. Een gateway-oplossing is mogelijk, maar dient veelal zelf te worden ontwikkeld. In veel gevallen is opwaarderen van componenten naar een te beheren niveau via een nieuwe softwareversie mogelijk.

Security
Huidige MLM's zijn gebaseerd op SNMP-versie 1, die geen beveiligingsmechanismen kent. Gebruikers in het bezit van een netwerkmonitor zijn in staat vanuit SNMP-verkeersstromen alle SNMP-componenten te herconfigureren. Dit is de reden dat in WAN-omgevingen SNMP-configuratiebeheer niet gebruikt wordt. Per te beheren component kan bepaald worden of er geconfigureerd mag worden met SNMP. WAN-componenten worden veelal via het TCP/IP remote login 'telnet'-protocol geconfigureerd.

SNMP

Eind tachtiger jaren is het Simple Network Management Protocol (SNMP) een industriestandaard geworden voor het beheren van enterprise (bedrijfsbrede) netwerken. Deze standaard is mede ontwikkeld door de groep IETF (Internet Engineering Task Force), die zich bekommert om het wereldwijde Internet. Internet is een verzameling van netwerken die onderling wereldwijd verbonden zijn en is het grootste netwerk ter wereld. Het aantal aangesloten gebruikers neemt momenteel bijna exponentieel toe. Voor dit multi-vendor netwerk was dringend behoefte aan goed beheergereedschap.

Rol van standaarden:
Standaarden beheren momenteel geen netwerken, hoewel we toch spreken over SNMP-management en CMIP-management.

SNMP is een geaccepteerd protocol en wordt door vrijwel alle LAN/WAN-leveranciers ondersteund. SNMP is het enige beschikbare protocol dat momenteel in grote bedrijfsbrede multi-vendor netwerken gebruikt kan worden voor het beheer. SNMP is zoals de naam al zegt een simpele taal (protocol), die gesproken wordt tussen het beheerstation (manager) en het te beheren object (client).

Binnen het protocol is tevens vastgelegd hoe de te beheren informatie wordt opgeslagen (SMI = Structure of Management Information) en wat voor soort informatie kan worden opgeslagen (MIB = Management Information Base), zodat het voor iedere leverancier mogelijk is produkten te bouwen. De te beheren informatie of MIB is voor ieder te beheren produkt verschillend. Er is sprake van een standaard-MIB (MIBII) en een MIB-extensie (Private of vendor MIB), die door de leverancier aan het produkt toegevoegd kan worden. Op een SNMP-beheersysteem kan deze MIB geladen worden zodat de hier te beheren componenten bekend zijn.

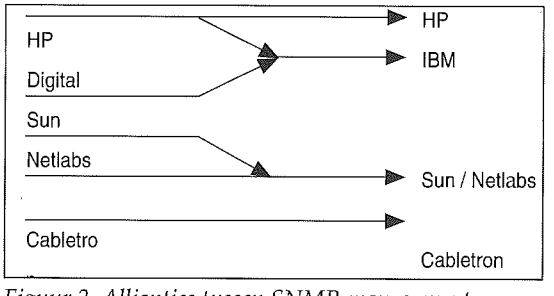
Sinds de ontwikkeling van SNMP is het aantal organisaties dat Management Information Bases (MIB's) ontwikkelt en implementeert boven verwachting gestegen. Het voornaamste communicatieprotocol binnen multi-vendor bedrijfsbrede netwerken is het Transmission Control Protocol (TCP/IP). Binnen TCP/IP-netwerken wordt SNMP als beheerprotocol gebruikt. SNMP-ondersteuning binnen niet-IP-omgevingen wordt tevens geboden, boven op andere transportprotocollen of via conversie.

Het is nu een aantal jaren geleden dat SNMP-beheersystemen voor de doorbraak zouden moeten zorgen voor het beheren van bedrijfsbrede netwerken. Dit zou bedrijfsbreed netwerkbeheer (over alle componenten in het netwerk) in de praktijk mogelijk moeten maken. Het zou slechts een kwestie van tijd zijn voordat SNMP-beheersystemen mainframe-gebaseerde netwerkbeheersystemen voor netwerkbeheer zouden kunnen vervangen. Mainframe-georiënteerde beheersystemen zijn leverancier-afhankelijk en zullen alleen binnen de eigen netwerkomgeving, maar met name de systeemomgeving, toegepast blijven worden. Momenteel presenteren LAN/WAN-leveranciers hun netwerkbeheerprodukten nog steeds als bedrijfsbrede totaaloplossingen, terwijl netwerkmanagers nog steeds wachten op leveranciers die hun beloften nakomen.

SNMP is de dominante netwerk-management-standaard voor het beheren van multi-vendor netwerken, maar SNMP-beheersystemen zijn nog in een constante ontwikkelingsfase.

De SNMP-platformen

Een beheerplatform of managementplatform vormt de basis voor het aansturen van een netwerkomgeving. Een managementplatform biedt naast standaarddiensten (automatisch in kaart brengen van alle netwerkcomponenten) voor beheerapplicaties tevens een 'open' interface naar beheerapplicaties. Momenteel zijn de voornaamste SNMP-managementplatformen OpenView Network Node Manager van Hewlett-Packard Co. en SunNet Manager van Sunsoft Inc. IBM kocht de licentie van HP OpenView twee jaar geleden en verkoopt zijn gemodificeerde versie als NetView/6000 (momenteel NetView for AIX versie 3). Deze drie vooraanstaande managementplatformen zijn wereldwijd goed voor meer dan zestig procent marktaandeel in de op Unix gebaseerde netwerkmanagement-markt van 1993 (International Data Corp.). De concurrentie tussen de marktleiders is groot. IBM probeert zich te differentiëren van HP OpenView door de code te herschrijven en unieke functionaliteit toe te voegen. Ondertussen verschijnen er nieuwe versies van HP OpenView op de markt, die veel meer functionaliteit bieden dan de oorspronkelijke Node Manager. Sunsoft, die historisch afhankelijk is van andere leveranciers die extra functionaliteit aan het Sun-produkt toevoegen, reageert door middel van het uitbrengen van nieuwe softwareversies en nieuwe strategieën.



Figuur 2. Allianties tussen SNMP-management-leveranciers.

In figuur 2 is de huidige status zichtbaar van de leveranciers en samenwerking tussen leveranciers van vooraanstaande SNMP-beheersystemen. Bovengenoemde systemen hebben een vooraanstaande positie verworven betreffende operationeel management in Local Area Network (LAN) omgevingen, voor het afhandelen van onder meer alarmmeldingen en trouble tickets (probleemrapporten). In figuur 2 is te zien dat IBM voor de ontwikkeling van zijn SNMP-management-produkt heeft samengewerkt met HP en dat Digital met IBM is gaan samenwerken. SNMP-beheersystemen worden ingezet voor het beheren van LAN-omgevingen zoals hubs, routers, bridges, switches en adapters. Deze SNMP-beheersystemen zijn uitontwikkeld tot geïntegreerde beheerplatformen, die naast LAN-componenten tevens WAN-componenten kunnen beheren. Ondanks belangrijke vooruitgang in de afgelopen twee jaar ontbreken er binnen de huidige SNMP-platformen voorname elementen (zie zwakke punten huidige MLM's) voor het beheren van bedrijfsbrede netwerken.

SNMP-applicaties

Genoemde toonaangevende SNMP-management-platform-leveranciers bieden alle een produkt op basis van Unix dat voorziet in basisfunctionaliteit voor het beheren van SNMP-componenten in een netwerk. Het SNMP-managementsysteem wordt

aangesloten op het LAN en kan vervolgens de aanwezige componenten op het LAN die SNMP of TCP/IP ondersteunen, zelf ontdekken. Indien de te beheren netwerkcomponenten niet van de leverancier van het SNMP-beheerplatform zijn, kan via basis-SNMP-functionaliteit (MIBII) een aantal gegevens worden opgevraagd. MIBII voorziet voornamelijk in primaire TCP/IP-communicatiefunctionaliteit, zodat door een SNMP-managementplatform gesignaleerd kan worden of de netwerkcomponent nog kan communiceren. Natuurlijk is het gewenst dat alle parameters van de netwerkcomponenten worden beheerd; hiertoe dienen de extra te beheren specifieke componentparameters eveneens bij het netwerkbeheersysteem bekend te worden gemaakt. Door de vendor MIB te laden in het beheersysteem is beheer via SNMP-variabelen mogelijk.

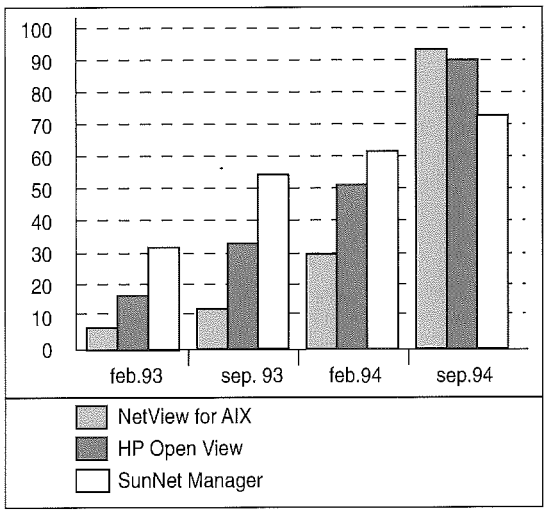
Een voorbeeld van een vendor MIB is de 'Toaster MIB'. De broodrooster wordt aangesloten op het netwerk en voorzien van een zogenaamde 'Toaster agent', zodat communicatie-uitwisseling en dus remote monitoring en besturing mogelijk is. Via het beheerplatform kan de status van de broodrooster ('Hoeveel minuten nog voordat het brood klaar is?') worden opgevraagd. Bij problemen kan de 'Toaster agent' een 'trap' versturen (brood zit vast, verwarming defect). Het beheerplatform weet initieel niets van broodroosters en krijgt gegevens over de broodrooster aangereikt via de Toaster MIB. De beheerder krijgt op het scherm van het beheersysteem een lijst parameters waarmee hij de broodrooster kan beheren. Om de opwarmtijd van de broodrooster in te stellen dient wel de juiste parameter te worden ingesteld.

De beheerder dient gegronde kennis te hebben van SNMP en zijn parameters om dit in de praktijk uit te kunnen voeren. Via een 'Toaster applicatie' kan de status van de broodrooster grafisch op het scherm worden weergegeven (de applicatie vertaalt grafisch de vendor MIB). De beheerder zou door met zijn muis op de broodrooster te klikken de configuratie kunnen wijzigen. Beheren wordt op deze manier een stuk eenvoudiger. Dit is de reden dat leveranciers bij hun produkten tevens een applicatie meeleveren, die als proces geïntegreerd kan worden binnen het SNMP-managementplatform. Het woord integreren is hier een groot woord omdat de verschillende applicaties nauwelijks samenwerken. De applicaties benutten de grafische gebruikers-interface van het beheerstation en verschijnen in de reeds aanwezige menustructuur.

Managementapplicaties

Geen van de genoemde netwerkbeheersystemen voorziet in een breed geïntegreerd systeem dat alle netwerkmanagement-functionaliteit biedt zonder toevoeging van third party-produkten (produkten toegevoegd door derden).

Het aantal beschikbare third party-managementapplicaties bepaalt mede het succes van SNMP-managementplatformen, daar additionele applicaties de totale functionaliteit van het SNMP-managementplatform vergroten. In figuur 3 is per managementplatform een indicatie aangegeven van het aantal beschikbare third party-managementapplicaties. In de figuur komt duidelijk de brede ondersteuning vanuit leveranciers voor Sun tot uitdrukking. Er is tevens een inhaalrace gaande van ondersteunende third party-produkten voor HP en IBM. Het IBM-platform scoort samen met het HP-platform strategisch het beste, daar hiervoor de meeste applicaties ontwikkeld zullen worden.



Figuur 3. Vergelijkbare groei van third party-applicaties per managementplatform (source: Interop Atlanta 1994).

SNMP-ondersteuning

Huidige middelgrote tot grote netwerken bestaan uit een reeks bestaande componenten, die niet alle SNMP ondersteunen. SNMP-ondersteuning is het sterkst vertegenwoordigd in de LAN-omgeving. Vrijwel alle hub- en router-leveranciers leveren SNMP-applicaties en MIB's mee met hun netwerkcomponenten. Door het vrijgeven van private MIB's is het mogelijk apparatuur van andere leveranciers te beheren op basis van SNMP.

Beheren van werkstations en PC-platformen vergt meer aandacht dan alleen SNMP, daar op deze platformen veelal meerdere protocollen actief zijn. Naast protocollen zijn hier tevens applicaties en hardware (onder andere CPU, insteekkaarten, diskdrives) actief. Met name de Desktop Management Task Force (DMTF) tracht standaardisatie binnen systeemmanagement op te zetten en zal een interface uitbrengen op basis van SNMP. De DMTF houdt zich bezig met het standaardiseren van de hardwaregegevens in systemen, zodat bij het plaatsen van hardware in een netwerk, informatie over deze hardware beschikbaar komt (bijvoorbeeld via SNMP).
Momenteel wordt het beheer van PC-platformen ondersteund via de meest gangbare TCP/IP-softwarepakketten (via een SNMP-agent), maar die bieden slechts ondersteuning voor het TCP/IP-gedeelte en niet voor de PC en de applicaties zelf. Hetzelfde geldt voor Netwerk Operating Systemen (NOS) op fileservers, waarbij SNMP wel te implementeren is maar niet meer voorstelt dan een monitorfunctie.

Op het vlak van de Wide Area Network (WAN) communicatie zien we een sterk commitment van WAN-leveranciers in de richting van SNMP. Voorbeelden hiervan zijn de PABX-leveranciers en bandbreedtemanagement-leveranciers. De nieuwe WAN-produkten op het gebied van Asynchronous Transfer Mode (ATM) als nieuwe technologie voor de integratie van voice, data en video komen tevens op basis van SNMP op de markt beschikbaar. De huidige WAN-bandbreedtemanagement-apparatuur gebruikt proprietary protocollen voor het beheren van netwerken en levert veelal per type een eigen managementplatform. Binnen de high-end WAN-omgevingen is SNMP minder populair, aangezien het grote aantal te beheren nodes, het sterk gedistribueerde karakter en de noodzaak tot beveiliging een grote rol spelen (zie zwakke punten huidige MLM's).

SNMP wordt ondersteund voor: PC's, Macintoshes, bridges, routers, switches, hubs, fileservers en host-systemen.
SNMP is momenteel het primaire protocol voor het beheren van multi-vendor netwerken.

De belangrijkste reden voor de populariteit van SNMP-managementplatformen is te danken aan de enorme ondersteuning voor SNMP (agents) zelf. SNMP-agents worden routinematig meegeleverd met vrijwel alle IP- en LAN-produkten inclusief TCP/IP-host-systemen, multiprotocol-routers, bridges en hubs.

Verschillen tussen SNMP-beheersystemen

In tabel 2 zijn de drie vooraanstaande SNMP-managementplatformen aangegeven, waarbij per platform de mate van ondersteuning voor gespecificeerde beheertaken is aangegeven. Naast de standaard aanwezige eigenschappen van de beschreven SNMP-beheersystemen is additionele functionaliteit vrijwel altijd gewenst. Het beheren van TCP/IP-netwerken door middel van SNMP klinkt eenvoudig, maar er is specialistische kennis voor nodig om alle objecten van een Management Information Base (MIB) te kunnen interpreteren. Een beheerapplicatie die grafisch de te beheren componenten weergeeft is voor iedereen eenvoudig te bedienen en levert enorme tijdbesparing op. Voor specifieke netwerkcomponenten als geïntegreerde hubs, routers, terminal servers of switches worden door de specifieke produktleveranciers de beste managementapplicaties gebouwd. Zij kennen immers hun produkten het beste en leveren veelal hun beheerapplicaties op HP OpenView, SunNet Manager en NetView for AIX. Wel zien we een verschil in beschikbaarheid van genoemde produkten, hetgeen afhankelijk is van de managementstrategie van de leverancier.

Handeling	HP	IBM	SUN
Installatie en administratie	G+	U-	G+
On-line help	R	U-	R-
On-line documentatie	R-	R+	G-
Plug and play	U-	G-	G-
Autodiscovery	G+	U	G-
Topologie TCP/IP	G+	U-	R
Topologie multiprotocol	R	G+	R-
Bewegen binnen topologie MAP	G	G-	R+
Grafische User Interface (GUI)	U-	U-	G+
Objectgeoriënteerde GUI	R-	U	R-
Eenvoud gebruik Unix en niet MIB-specialisten	R-	R	R-
Alarm monitoring	G-	R	R+
Alarm filtering/automation	R	G	R-
Correlatie tussen alarmsignalen	R-	R+	R-
Identificeren falende componenten	U-	R	U-
Eenvoud vaststellen probleem	G	U-	G-
Eenvoud werken met MIB	R-	G	R-
Expertsysteem-eigenschappen	I	R-	I
Verzamelen/grafieken van data	R	I	R+
Monitoren managementapplicaties	G+	R	G
Extra applicaties te leveren door leverancier	G-	U-	R-
Aantal third party-applicaties	G+	G	U-
Kwaliteit van applicatie-integratie	B-	G	G-
Open API's	I	I	I
Data sharing tussen applicaties	R-	R-	R-
Gemeenschappelijke opslag voor netwerkdata	I	I	I
Ondersteuning objectgeoriënteerde databases	I	I	I
Ondersteuning meerdere databases	I	I	I
Gedistribueerde architectuur	I	I	I
Manager-naar-manager-interface	I	I	I
Mogelijkheid als enterprise MOM	R-	R-	R-
Schaalbaarheid	R-	R-	R-
Gemiddelde beoordeling			
Voor kleine tot middelgrote TCP/IP-netwerken	U	U	U-
Voor grote TCP/IP-netwerken	G	G	G
Voor grote multiprotocolnetwerken	R	R	R

Beoordeling van de voornaamste SNMP-platformen.
U = Uitstekend R = Redelijk
G = Goed I = Incompleet

Tabel 2. Verschillen tussen SNMP-managementplatformen.

Hoewel alle drie managementplatformen zowel sterke als zwakke eigenschappen bezitten, zijn de platformen even geschikt (als ongeschikt) voor het beheren van verschillende typen netwerken. De platformen zijn uitstekend geschikt voor het beheren van kleine tot grote op TCP/IP gebaseerde netwerken. Voor grote multiprotocol-netwerken laten deze beheersystemen nog veel te wensen over.

Hoewel de genoemde SNMP-beheersystemen van verschillende leveranciers komen, hebben de platformen een aantal belangrijke gemeenschappelijke eigenschappen. Voor IBM en HP is dit zeker geen verrassing, daar IBM HP OpenView-technologie in licentie heeft genomen om als basis te dienen voor NetView for AIX. Voorbeelden hiervan zijn het gemeenschappelijke Unix-operating-systeem en TCP/IP, die voor alle drie platformen de core van het managementsysteem vormen. Alle maken gebruik van Unix-deamons, die als achtergrondprocessen continu aanwezig zijn en dynamisch veranderingen in netwerktopologie en SNMP-'trap'-meldingen van agents bijwerken in de database.
De belangrijkste gemeenschappelijke features van de drie platformen zijn:
- krachtige grafische gebruikers-interface voor controle- en monitorfuncties;
- automatische opbouw van de netwerktopologie;
- alarmmechanisme op icon-basis (en berichtenverkeer);
- beheerders kunnen extra informatie over alarmsignalen opvragen en diagnose stellen;
- statistische informatie kan grafisch worden weergegeven;
- leveranciers en gebruikers kunnen zelf applicaties toevoegen en integreren;
- specifieke beheerapplicaties kunnen gemonitoord worden.

SNMP-netwerkmonitoring

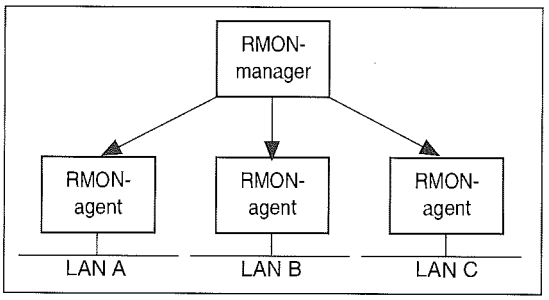
Netwerkmonitors worden met name toegepast indien op protocolniveau netwerkanalyse noodzakelijk is. Voorheen was dat een eenvoudige taak, daar netwerken uit één of enkele segmenten bestonden. Hedendaagse netwerken bestaan uit een veelvoud aan netwerksegmenten, die opgebouwd zijn rondom een collapsed backbone. Nieuwe netwerken zullen opgebouwd gaan worden rondom de gedistribueerde collapsed backbone, waarbij tevens gedistribueerd segmentatie zal gaan plaatsvinden. Behoefte aan extra bandbreedte is de belangrijkste reden voor het toepassen van vergaande segmentatie. Een andere belangrijke reden voor segmentatie is het dynamisch kunnen aanpassen van het netwerk aan de organisatie.

Virtuele netwerken zijn eenvoudig te reorganiseren indien de zakelijke behoeften veranderen. Virtuele netwerken passen zich aan de organisatiestructuur aan.

Momenteel staat routing-technologie voor het toepassen van segmentatie ter discussie. Virtuele netwerkarchitecturen zullen met name binnen LAN's de belangrijkste vorm van segmentatie gaan vormen. Switching-technologie gecombineerd met gecentraliseerde routing-functies staat fysiek in het hart van deze nieuwe virtuele netwerken. Binnen werkgroepen van tweehonderd gebruikers zullen al snel zo'n tien fysieke segmenten in geswitchte vorm geïmplementeerd worden.

Door deze verandering binnen netwerkinfrastructuren en backbone-ontwerpen ontstaan tevens nieuwe behoeften voor het monitoren van netwerken. Gebruikers die voorheen binnen een segment communiceerden, zitten nu in een virtuele werkgroep. Binnen een virtuele werkgroep kunnen vele segmenten aanwezig zijn. Om deze nieuwe behoeften te adresseren moet aandacht worden besteed aan de volgende aspecten:
- plaatsing netwerkmonitor;
- verkeeranalyse per virtuele werkgroep;
- meer intelligentie met automatische suggesties;
- samenwerking tussen netwerkmonitors onderling.

De introductie van nieuwe Management Information Bases (MIB's) maakt het mogelijk binnen SNMP gedistribueerde remote monitoring toe te passen gecontroleerd vanuit een centraal netwerkmanagement-platform. In de hub, router of switch kan decentraal monitoring van netwerksegmenten plaatsvinden, waarbij naast logging van de systemen die de hoogste netwerkbelasting genereren, tevens traces op netwerk-pakketniveau gemaakt kunnen worden.



Figuur 4. Model van gedistribueerde monitoring. De RMON-manager kan een applicatie zijn op een SNMP-managementplatform. De agent kan een hardware- of softwaremodule zijn in bijvoorbeeld een hub of switch.

RMON
RMON is gestandaardiseerd en vastgelegd binnen RFC 1271 (Request for Comment) door de Internet Engineering Task Force (IETF), die zich bekommert om alle documenten omtrent TCP/IP. Met RMON wordt tevens de agent-applicatie of het produkt (netwerkmonitor) aangeduid, waarbij in de agent RFC- 1271 ondersteund wordt. RMON is een belangrijke applicatie geworden binnen LAN- en WAN-omgevingen. RMON is gestandaardiseerd voor token ring- en ethernet-netwerken en maakt 'off-line operation' mogelijk, zodat geen constante connectie met de centrale netwerkmonitor (RMON-manager) noodzakelijk is. RMON ondersteunt gelijktijdig meerdere SNMP-managers. RMON is praktisch gezien een software- of hardwaremodule, die in een hub, router, switch of bijvoorbeeld supervisor (netwerkbeheer-module van een hub) ondergebracht kan worden.

De functionaliteit van RMON wordt opgedeeld in negen groepen. Voor ethernet specificeren twee groepen statistieken en historische informatie, en voorzien zeven groepen in algemene monitoring-functies. Voor token ring specificeren vier groepen de MAC (fysieke laag) en datalink (control laag), en monitoren vijf groepen specifieke token ring-functies. Binnen de standaard is niet opgenomen dat alle groepen van RMON ondersteund dienen te worden. Zo zijn er probes op de markt die slechts twee groepen ondersteunen met het RMON-label. Huidige RMON-implementaties worden steeds uitgebreider ondersteund. Hieronder worden de beschreven RMON-groepen weergegeven, waarbij iedere groep staat voor een geboden functionaliteit.

'Distributed monitoring' maakt centralisatie mogelijk en bespaart tijd voor netwerkbeheerders. Correlatie en gedetailleerde analyse van gedistribueerd netwerkverkeer is mogelijk vanuit één beheerstation.

Ethernet

Statistieken en historische informatie:

1. *Statistics:* tellers geven hoeveelheid verkeer aan en netwerkfouten als runts (te klein pakket), jabbers (te groot pakket), CRC errors, pakketlengte.

2. *History:* periodiek verzamelen van informatie (sample interval= 30 sec. tot 30 min. default). Meerdere gelijktijdige informatietabellen mogelijk.

Algemene monitoring-functies:

1. *Alarms:* plaatsen van tresholds op alle MIB (integer) variabelen. Absolute of deltawaarden zijn instelbaar. Overtreden van treshold levert een event op.

2. *Host:* host discovery en statistieken per station (pakkettellers, fouttellers).

3. *Host Top N:* N te monitoren systemen op basis van te selecteren host-parameter. Systemen worden gesorteerd op basis van statistieken. (N = 10 = default.)

4. *Matrix:* verkeersmatrix tussen paren communicerende stations.

5. *Filter:* instellen van criteria voor filteringdoeleinden.

6. *Packet capture:* gefilterde verzamelde pakketten, pakketten worden gebufferd.

7. *Event:* gegenereerd door alarms. Event-groep houdt de logging van events bij.

Specifieke uitbreiding voor token ring (RFC 1513):

Vier groepen specificeren MAC- en datalink-informatie:

1. *MAC-layer statistics group:* informatie betreffende fysieke fouten en tellers.

2. *Promiscuous statistics group:* isolating en non-isolating errors, Beacon, claim-token.

3. *MAC-layer history group:* MAC-layer tellers, vooraf gedefinieerde tijdsintervallen.

4. *Promiscuous history group:* promiscuous = 'pakket luister' mode (neemt niet deel in ring).

Vijf groepen monitoren specifieke token ring-informatie:

1. *Ring station control group:* welke actieve stations zitten er in de ring, ringstatus.

2. *Ring station group:* station status en softerror status.

3. *Ring station order group:* volgorde zoals stations in de ring zitten.

4. *Ring station configuration group:* informatie over configuratie van actieve stations.

5. *Source routing statistics group:* source route (token ring), bridging, ringnummer, tellers, routes, hops.

Remote beheer van netwerken, waarbij gedistribueerd verzamelen van data aan de orde is, wordt steeds belangrijker. De omvang van netwerken wordt groter, het aantal gekoppelde locaties en het aantal netwerksegmenten nemen toe. Vrijwel alle grote netwerkleveranciers leveren intelligente agents in de hub met RMON-functionaliteit. Tevens zijn er gespecialiseerde leveranciers die reeds jarenlange ervaring hebben met netwerkmonitoring, zoals Network General, die momenteel een complete RMON-implementatie (ondersteunt alle negen RMON-groepen) op HP OpenView levert.

CONCLUSIE

Communicatiesystemen zijn van infrastructureel belang voor een organisatie. Zij worden gebruikt voor het uitwisselen van informatie tussen mensen en processen van gedistribueerde netwerkapplicaties. Het functioneren van het netwerk en dus ook het netwerkmanagement spelen een belangrijke rol in de uiteindelijke 'quality of service' van de totale organisatie (intern en extern).

SNMP-managementplatformen zijn geschikt voor het beheren van multi-vendor bedrijfsnetwerken en zijn beschikbaar via verschillende leveranciers. SNMP-managementplatformen zijn uniek in de manier waarop zij meerdere beheerapplicaties ondersteunen. Op één SNMP-platform worden gelijktijdig applicaties van verschillende leveranciers ondersteund. De SNMP-managementplatformen

gebaseerd op HP OpenView, zoals Netview for AIX, ondersteunen dezelfde applicatie-interface voor het bouwen van netwerkbeheerapplicaties. Wel dient de applicatiecode 'open' te zijn zodat hij opnieuw gecompileerd kan worden op een ander operating-systeem.

Deze SNMP-managementplatformen zijn in een aantal opzichten nog niet volwassen. SNMP-managementplatformen ondersteunen geen MOM-functionaliteit, maar bieden basisintegratie op systeemniveau (netwerk interface, user interface). Op managementapplicatie-integratieniveau valt nog een hoop te verbeteren. Applicaties die correlaties kunnen leggen tussen verschillende gebeurtenissen in het netwerk of tussen specifieke databaseinformatie komen langzamerhand beschikbaar. Grotere organisaties kunnen zich veroorloven applicaties op maat te maken en de benodigde integratie te realiseren. Deze applicaties vergen veel ondersteuning in onderhoud en beheer.

SNMP-managementplatformen zijn goed inzetbaar voor operationeel beheer in multi-vendor bedrijfsnetwerken. Bij het opzetten van een geïntegreerd managementsysteem voor een organisatie zijn geen standaardoplossingen beschikbaar. Maatwerk is hier noodzakelijk daar iedere netwerkomgeving verschillend is en andere eisen stelt ten aanzien van operationeel, tactisch en strategisch beheer. Een belangrijk voordeel van SNMP-managementplatformen is dat de leverancier van netwerkcomponenten tevens de netwerkapplicatie ontwikkelt (voor het SNMP-managementplatform). Router-leverancier Cisco Systems inc. levert bijvoorbeeld optioneel een bijbehorende router-applicatie voor SunNet Manager, HP OpenView of NetView for AIX. Bij verandering van softwareversies van de Cisco-router komt tevens een nieuwe versie van de managementapplicatie beschikbaar. Terugvallen op de leverancier is dus mogelijk.

Naast 'open' SNMP-managementplatformen zijn er leveranciers die Midlevel Management Systemen of zelfs Manager of Manager (MOM) systemen leveren met eigen applicatie-interface. De leverancier van het managementplatform ontwikkelt zelf de benodigde applicaties voor integratie van het beheer van netwerkcomponenten (router-applicatie, hub-applicatie), of sluit hiervoor overeenkomsten met de desbetreffende netwerkcomponenten-leveranciers. Deze applicaties lopen altijd achter indien softwareversies van netwerkcomponenten (de router) veranderen. Leveranciers van netwerkcomponenten hebben de strategische SNMP-platformen boven aan hun ontwikkellijst staan.

Uit ervaring blijkt dat bij het ontwerpen van grote bedrijfsnetwerken de beheeromgeving een steeds belangrijkere rol gaat spelen. Voor het ontwerpen van een geïntegreerde beheeromgeving is kennis noodzakelijk van alle te integreren componenten. Tevens is kennis noodzakelijk voor specificatie van het managementplatform (hardware en software, licenties, aantal netwerkbeheerders) binnen de beheerorganisatie. Hiervoor dient veelal extra kennis tijdelijk te worden ingezet tijdens het opzetten van de beheerorganisatie, zoals helpdesk, eerste lijn support, keuze van het type onderhoudscontract, procedures voor het voorzien in reserve-onderdelen.
Grote system integrators hebben kennis en ervaring in alle te integreren netwerkcomponenten, managementplatformen en systemen binnen bedrijfsbrede netwerken. Nauw overleg tussen de system integrator en de desbetreffende organisatie is van wezenlijk belang. Veelal wordt een beheerorganisatie gefaseerd opgebouwd, daar het een levend geheel is dat met de organisatie mee verandert.

LITERATUUR

[Hege94] H. Hegering en S. Abeck, *Integrated Network and System Management*, Addison-Wesley publishing company, 1994.

[McCo94] J. McConnell, *Building Workable Management Solutions*, Interop Atlanta 1994.

Ing. W.A.A. Zoon
Heeft acht jaar ervaring op het gebied van datacommunicatie en netwerken opgebouwd binnen de Getronics organisatie. Momenteel is hij werkzaam als Principal Consultant bij Getronics Networks. Deze projectorganisatie is verantwoordelijk voor ontwerp en implementatie van grote en complexe data- en telecommunicatieprojecten.

Client/server geconcretiseerd

J.C. van Praat RE RA

**Wat is client/server nu eigenlijk?
Welke begrippen en produkten zijn kenmerkend voor een client/server-omgeving?
In dit artikel wordt een state-of-the-art overzicht gegeven van dit sterk in de belangstelling staande fenomeen.**

INLEIDING

Het client/server-concept staat momenteel sterk in de belangstelling. In de automatiseringsliteratuur wordt bijna wekelijks aandacht besteed aan de diverse aspecten van het fenomeen client/server. Ondanks deze grote belangstelling bestaat er nog altijd veel onduidelijkheid over het client/server-concept. Blijkbaar is er nog geen literatuur voorhanden die ingaat op alle aspecten van client/server. Dit artikel heeft als doelstelling een volledig concreet overzicht te geven van het client/server-concept.
In dit artikel zal aandacht worden besteed aan een aantal typische componenten van een client/server-omgeving. Het betreft de volgende componenten:

- gebruikers-interface;
- besturingssystemen;
- transportfuncties;
- netwerkbesturingssystemen;
- gedistribueerd client/server-management;
- database-servers;
- groupware.

Afsluitend zullen we ook nog kort aandacht besteden aan het Information Warehouse concept van IBM.
Voordat we echter ingaan op deze componenten zal in de volgende paragraaf eerst een overzicht worden gegeven van een client/server-omgeving. Hierdoor ontstaat meteen enige duidelijkheid over de relatie tussen die hiervoor genoemde componenten.

DE CLIENT/SERVER-OMGEVING

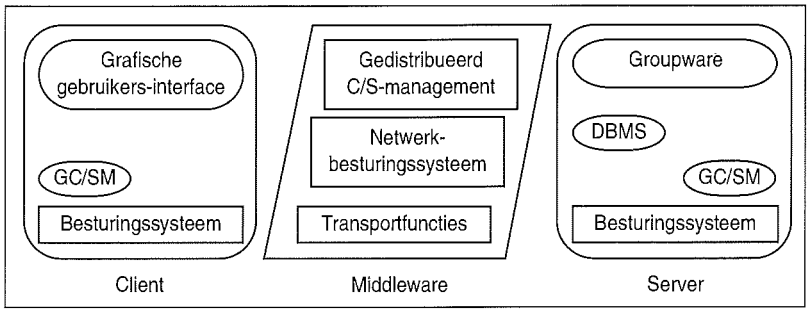
In figuur 1 is een schematisch overzicht gegeven van de componenten van een client/server-omgeving. Hierbij valt meteen een driedeling op waaruit blijkt dat er sprake is van een client, een server en daartussen de middleware.
In de eerste plaats onderscheiden we de client. In de praktijk betreft dit meestal een gewone personal computer waarop een aantal softwarecomponenten draait. Deze softwarecomponenten zijn in ieder geval de grafische gebruikers-interface en het lokale besturingssysteem dat nodig is om de eigen centrale verwerkingseenheid te besturen. Hierna zullen we nog wat uitgebreider stilstaan bij de grafische gebruikers-interface, terwijl het besturingssysteem slechts kort aan de orde zal komen.

Aan de andere kant van het model bevindt zich de server. Net als bij de client geldt ook hier dat we het meestal hebben over een volledig computersysteem waarop diverse softwarecomponenten draaien. Deze server kan zijn een mainframe of een minicomputer, maar ook een krachtige PC kan de functie van server vervullen. Op een dergelijk systeem functioneert uiteraard ook het lokale besturingssysteem. Verder zal op de server gebruik worden gemaakt van een database-managementsysteem, in een client/server-omgeving ook wel aangeduid als de database-server. Op deze database-server zullen we hierna nog uitgebreid teruggekomen. Ten slotte speelt op de server ook nog de groupware een rol. Ook op dit fenomeen gaan we hierna kort in.

Tussen de client en de server bevindt zich ten slotte het meest kenmerkende onderdeel van een client/server-omgeving: de middleware. In dit artikel ga ik uit van een vrij ruime definitie van middleware. Het betreft hier alle programmatuur die het mogelijk maakt om een client en een server met elkaar te laten communiceren. Op het laagste niveau vinden we de transportprotocollen die het technisch mogelijk maken dat informatie uitgewisseld wordt tussen de beide systemen.

Hierboven bevindt zich het zogenaamde netwerkbesturingssysteem. Dit netwerkbesturingssysteem vervult een aantal meer applicatiegerichte functies die het op applicatieniveau mogelijk maken dat toepassingen met elkaar samenwerken.

Een derde onderdeel dat aan de orde komt speelt eigenlijk een rol in zowel het client- als het serversysteem, terwijl de middleware ervoor zorgt dat een en ander gecoördineerd wordt. Het betreft hier het gedistribueerde client/server-management (GC/SM). Het client/server-concept heeft onder meer gezorgd voor het ontwikkelen van programmatuur en protocollen ten behoeve van het management van een client/server-omgeving. Kreten als Simple Network Management Protocol, Common Management Information Protocol, NetView en OpenView spelen hierbij een rol.



Figuur 1. Client/server-architectuur.

GRAFISCHE GEBRUIKERS-INTERFACE

Kenmerkend voor de moderne grafische gebruikers-interfaces (ook wel afgekort als GUI, afkomstig van het Engelse begrip Graphical User Interface) is dat ze gebruik maken van rechthoekige kaders, ook wel windows genoemd. Deze windows kunnen elkaar overlappen. De gebruikers kunnen binnen een window diverse activiteiten uitvoeren zoals het veranderen van de omvang en het verplaatsen van de window. Een window bevat objecten die een gebruiker kan selecteren met behulp van een muis. Met de muis wordt een icoon aangewezen, waarna door een 'dubbel-klik' met de muis het desbetreffende object geactiveerd wordt.
Opvallend is dat in deze situaties de gebruiker geen commando's meer hoeft in te toetsen. Het gebruik van dergelijke interfaces heeft de nodige consequenties voor de programmeur. Kernpunt hierbij is dat de gebruiker te allen tijde de programmatuur moet kunnen gebruiken zoals hij dat wenst. In de meer traditionele vorm van programmeren werd achtereenvolgens een onderscheid gemaakt tussen invoersecties, verwerkingssecties en uitvoersecties. Bij het gebruik van grafische gebruikers-interfaces moet het mogelijk zijn dat willekeurige gebeurtenissen op elk moment voor kunnen komen. Een applicatie moet hier uiteraard wel voor zijn ingericht.

Kenmerken grafische gebruikers-interface

In de vorige paragraaf is al aangegeven dat een grafische gebruikers-interface gekenmerkt kan worden door de gebeurtenissen die met een GUI gerealiseerd kunnen worden. Deze gebeurtenissen leiden vervolgens tot bepaalde vormen van uitvoer. Beide onderdelen, gebeurtenissen en uitvoer, komen hierna aan de orde.

Gebeurtenissen
Hoewel er verschillen zijn tussen de diverse GUI's kunnen er toch gebeurtenissen worden onderscheiden die in vrijwel elke GUI voorkomen. Deze zijn:

– *Muisacties.* Deze acties komen voor als een gebruiker de muis bewogen heeft naar een bepaald

object gevolgd door een 'dubbele-' of 'enkele' klik met de muis.

– *Toetsenbordacties.* Door het indrukken van een toets op het toetsenbord wordt een reactie verwacht van de GUI.

– *Menu-acties.* Een gebruiker kan ook een keuze maken uit een door de GUI gepresenteerd menu.

– *Window-activering.* Als een bepaalde icoon of een window beschadigd is zal deze hersteld moeten worden. Ook hiervoor worden activiteiten van de GUI verwacht.

– *Veranderen omvang.* Het is te allen tijde mogelijk de omvang van een window te wijzigen naar de behoefte van de gebruiker.

– *Activeren en deactiveren.* Het is altijd mogelijk een window al of niet te activeren door deze aan te wijzen. De tot dat moment actieve window krijgt dan de status inactief.

– *Initialisering en afsluiting.* Het is altijd mogelijk nieuwe windows aan te maken c.q. te verwijderen indien ze niet meer nodig zijn.

Kenmerkend voor de moderne grafische gebruikers-interfaces is dat ze gebruik maken van rechthoekige kaders, ook wel windows genoemd.

Uitvoer van een GUI
Met name uit de uitvoer van een GUI blijken de verschillen tussen de diverse toepassingen. Het gaat hierbij om het gebruik van
- coördinaten;
- tekenalgoritmen;
- kleuren;
- lettertypen.

Door gebruik te maken van coördinaten is het voor de GUI mogelijk de individuele pixels op het scherm te adresseren. Hierbij wordt gebruik gemaakt van een startpunt. Vanuit dit startpunt wordt vervolgens tweedimensionaal een bepaalde richting opgegaan.
Dat er ten aanzien van de kleuren en de lettertypen verschillen zijn behoeft verder geen toelichting. Wel wordt nog opgemerkt dat de GUI's verschillende faciliteiten kunnen bieden om wijzigingen in de gebruikte kleuren en lettertypen aan te brengen. Sommige zijn erg flexibel, terwijl andere dat niet zijn.

Produkten

Momenteel zijn er verschillende grafische gebruikers-interfaces op de markt beschikbaar. Het is binnen het bestek van dit artikel niet mogelijk om de werking van al deze produkten te beschrijven. Daarom wordt hier volstaan met een opsomming van de meest bekende GUI's. Wil iemand weten hoe ze precies werken, dan wordt aanbevolen om er in de praktijk eens mee aan de slag te gaan.
De bekendste produkten zijn:
- MS/Windows (Microsoft);
- Presentation Manager (OS/2 van IBM);
- Open Look (Sun);
- X Windows (MIT, Unix);
- Motif (Open Software Foundation);
- Macintosh (Apple).

Het ontwikkelen van een GUI voor een toepassing

De interface van de Macintosh was één van de eerste GUI's en heeft dan ook als basis gediend voor de andere GUI's die in de vorige paragraaf zijn genoemd. Deze MAC-interface behoorde tot de eerste implementaties van objectgerichte systeemontwikkeling.
De ideeën voor deze interface zijn in het begin van de zestiger jaren ontstaan bij Xerox. Deze ideeën hebben geleid tot het ontstaan van iconen, pull down menu's en windows. Deze objecten zijn destijds ontwikkeld met behulp van de taal SmallTalk.

Overigens moet men er zich van bewust zijn dat het icoon zelf niet het object is, het is uitsluitend de grafische weergave van een object. Het feitelijke object zelf is een verzameling van gegevens waarin vastgelegd zijn:
- gegevens over de structuur (bijvoorbeeld de coördinaten, de kleur en het gebruikte lettertype);
- de status van het object;
- de procedures die met het object uitgevoerd kunnen worden (bijvoorbeeld hoe wordt een bestand geopend en gesloten, hoe wordt het afgedrukt);
- de activiteiten waarvoor het object gebruikt kan worden.

Het ontwikkelen van programmatuur waarbij gebruik wordt gemaakt van een grafische gebruikers-interface vraagt andere technieken dan bij de conventionele ontwikkeltechnieken. Kenmerkend voor deze technieken is het gebruik maken van een sequentiële benadering. Dit betekent voor de gebruiker dat men meestal via een hiërarchie van menu's geleid wordt naar de functionaliteit die men wilde gebruiken, een andere mogelijkheid was niet aanwezig. Nu moet bij het schrijven van programmatuur rekening worden gehouden met het feit dat een gebruiker op elk willekeurig moment een bepaalde actie wil uitvoeren. We spreken in dit geval van het ontwikkelen op basis van events, ofwel gebeurtenissen. Deze gebeurtenissen zijn hiervoor reeds aan de orde gekomen.

Bij MS/Windows leidt elke gebeurtenis tot een zogenaamde 'message'. De GUI plaatst vervolgens

deze messages in een rij die behoort bij de toepassing waarop deze message betrekking heeft. Deze rijen worden vervolgens op basis van fifo (first in first out) uitgelezen door de desbetreffende applicatie. Dit uitlezen geschiedt met het commando *GetMessage*. Als er geen messages zijn, wordt er gewacht op een bericht. Tijdens dit wachten wordt de besturing overgegeven aan het besturingssysteem, zodat andere toepassingen gebruik kunnen maken van het systeem.

Als er wel messages zijn dan wordt de inhoud van de eerste message in de rij gelezen en wordt de gevraagde functie aangeroepen. Dit geschiedt op basis van de functie *DispatchMessage*. De functie DispatchMessage is een voorbeeld van een API (Application Programming Interface). Een API is een hulpmiddel dat de relatie legt tussen de verschillende vormen van software, in dit geval de relatie tussen de GUI en de applicatie die op een bepaalde manier aangeroepen kan worden door de GUI.
Elke GUI heeft een eigen set van API's, die meer of minder uitgebreid kan zijn. Voor MS/Windows kan een programmeur bijvoorbeeld kiezen uit zeshonderd functies.

Ontwikkelhulpmiddelen

Naast de 'standaard GUI's' die kant en klaar geleverd worden door leveranciers, moet ook voor zelf ontwikkelde applicaties, bijvoorbeeld een financieel systeem, gebruik gemaakt worden van een grafische gebruikers-interface. Voor het ontwikkelen van deze interfaces is een veelheid aan ontwikkelhulpmiddelen beschikbaar. Het gaat hierbij om honderden produkten die alle in meerdere of mindere mate de ontwikkelaar ondersteunen bij het ontwikkelen van een 'standaard'-gebruikers-interface voor die specifieke toepassing. Vaak wordt gekozen voor een interface die geldt voor alle applicaties die in een organisatie worden ontwikkeld.

Hierna volgt een opsomming van een aantal veel gebruikte ontwikkelhulpmiddelen. Deze lijst geeft geen indicatie over de kwaliteit van het desbetreffende hulpmiddel. Deze hulpmiddelen zijn:
- EDA/SQL (Information Builder);
- Visual Basic (Microsoft);
- Powerbuilder (Powersoft);
- SQL Windows (Gupta);
- Paradox SQL Link (Borland);
- New Era (Informix);
- Uniface.

BESTURINGSSYSTEMEN

In deze paragraaf komen uitsluitend de besturingssystemen aan de orde die draaien op de client- en server-hardware. Achtereenvolgens wordt kort ingegaan op de functies van besturingssystemen, terwijl ook de bekendste besturingssystemen aan de orde zullen komen.
Omdat de meeste lezers redelijk bekend zullen zijn met de standaardfunctionaliteiten van een besturingssysteem wordt hierna volstaan met een korte opsomming. Het betreft de volgende functies:
- beschikbaarheid van request/reply-mechanismen;
- filetransfer-faciliteiten;
- multi-tasking;
- mogelijkheid van prioriteiten;
- interproces-communicatie (IPC);
- achtergrondverwerking;
- grafische gebruikers-interface.

De bekendste besturingssystemen zijn:
- MS/DOS, al dan niet in combinatie met MS/Windows;
- Windows New Technology (Windows NT);
- OS/2;
- Windows Advanced Server;
- NetWare;
- Unix.

Aan de client-kant speelt DOS nog steeds een zeer belangrijke rol. Wereldwijd zijn er meer dan 120.000.000 exemplaren verkocht. DOS zal zeker op de korte termijn een belangrijke rol blijven spelen, temeer omdat Windows 3.1 altijd gebruik maakt van DOS als onderliggend besturingssysteem.

Vaak wordt gekozen voor een interface die geldt voor alle applicaties die in een organisatie worden ontwikkeld.

In het succes van DOS kan echter snel verandering optreden. Een belangrijke ontwikkeling op dit terrein betreft de aankondiging van versie 4 van Windows, ook wel bekend onder de naam Chicago of Windows95. Dit wordt een volledig zelfstandig besturingssysteem.
Verder wordt nog opgemerkt dat DOS op een server niet toepasbaar is. Dit komt door het beperkte geheugenbereik en de beperkte multi-tasking mogelijkheden.

Ook OS/2 wordt steeds meer een concurrent van DOS. Met name de recente introductie van OS/2 Warp is een belangrijke impuls voor de acceptatie van OS/2 als besturingssysteem op het client-systeem. Een probleem van OS/2 is de beperkte beschikbaarheid van standaardtoepassingen voor OS/2. Leveranciers van deze produkten durven het nog niet echt aan om hun toepassingen geschikt te maken voor gebruik op OS/2.
Het voordeel van OS/2 is wel dat het ook gebruikt kan worden op server-systemen. OS/2 is een 32-bits besturingssysteem met voldoende multi-tasking mogelijkheden. Het is echter niet mogelijk gebruik te maken van server-systemen die voorzien zijn van meerdere processoren, ook wel bekend onder de naam SMP, Symmetric Multi-processing.

Een veelbelovende ontwikkeling betreft Windows New Technology. Dit is een produkt dat met name op server-systemen vele mogelijkheden heeft. Windows NT ondersteunt wel SMP. Maximaal kunnen zestien CPU's aangestuurd worden. Verder draait het niet alleen op Intel-processoren, maar ook op de Alpha-processor van DEC. Hierdoor zijn er uiteraard meer gebruiksmogelijkheden.
Ook voor client-systemen kan goed gebruik worden gemaakt van Windows NT. Het is een 32-bits besturingssysteem en de meeste DOS- en windows-pakketten draaien ook onder Windows NT. Het nadeel is echter wel dat minimaal 16 MB intern geheugen nodig is.

De overige drie produkten zijn speciaal bestemd voor de server-systemen. Overigens spelen Windows Advanced Server en NetWare ook een belangrijke rol als netwerkbesturingssysteem. Hierop komen we bij de behandeling van de middleware nog terug.

Unix is voor client/server-omgevingen de marktleider als server-platform.

Last, maar zeker not least moet Unix nog worden genoemd. Unix is zeker voor client/server-omgevingen de marktleider als server-platform. Er is een groot aantal Unix-varianten te onderscheiden met elk hun eigen voor- en nadelen. Het ligt in de lijn der verwachting dat in de toekomst Unix samen met Windows NT het besturingssysteem zal worden voor server-systemen.

Verder moet in dit kader nog worden gewezen op de proprietary besturingssystemen die draaien op mini- en mainframe-computers (zoals MVS, VMS). Ook deze platformen gaan een steeds belangrijkere rol spelen in de wereld van client/server. In de pers wordt momenteel veel aandacht besteed aan de ontwikkelingen met betrekking tot deze besturingssystemen.

TRANSPORTFUNCTIES

Het doel van de transportfuncties is het voorzien in een transparante communicatie tussen de diverse componenten die een rol spelen in een technische infrastructuur. Het betreft de middelste lagen van het bekende OSI-referentiemodel.

De onderste lagen worden over het algemeen ingevuld door de zogenaamde netwerkadapters ofwel netwerkkaarten. We spreken in dit geval ook wel over de zogenaamde device-drivers. De bekendste hiervan zijn token ring en ethernet. Echter ook SDLC en ISDN vervullen dezelfde functie.

Boven deze onderste lagen onderscheiden we de netwerklaag tot en met de presentatielaag. Deze lagen worden ingevuld door de transportfuncties die hier aan de orde zijn.
Op het niveau van de transport- en de netwerklaag betreft het de volgende protocollen:
- NetBEUI (NetBIOS Extended User Interface);
- SPX/IPX (Sequenced Packet Exchange/ Internet Packet Exchange);
- APPC/SNA (Advanced Program to Program Communication/Systems Network Architecture);
- TCP/IP (Transmission Control Protocol/ Internet Protocol).

Hiermee correspondeert een aantal protocollen op de sessielaag. Dit betreft achtereenvolgens:
- NetBIOS (Network Basic Input/Output System);
- TLI (Transport Layer Interface);
- CPI-C (Common Programming Interface for Communications);
- Sockets.

Hierna worden deze transportprotocollen kort toegelicht.

NetBIOS en NetBEUI

NetBIOS vormt een programmeer-interface op de sessielaag van het OSI-model. De programmeer-interface en de specificaties van sommige implementaties zijn gedefinieerd door IBM, waarbij de implementatiedetails overgelaten zijn aan de afzonderlijke leveranciers. Momenteel ondersteunen alle belangrijke LAN-leveranciers NetBIOS op DOS-, Windows-, OS/2- en Unix-systemen.

Applicaties communiceren met NetBIOS via een datastructuur die Network Control Block (NCB) genoemd wordt. Een applicatie moet waarden specificeren voor het commandoveld in de NCB-datastructuur, afhankelijk van het NCB-commando. Uiteindelijk stuurt de applicatie een NCB naar het NetBIOS. De precieze interface hangt af van het besturingssysteem. In alle gevallen retourneert het onderliggende NetBIOS-programma een bericht dat aangeeft of de opdracht succesvol is uitgevoerd door het Return Code-veld van de NCB te beschrijven.

NetBIOS vormt in de praktijk een solide communicatiemethode, die de de facto-standaard bij PC-netwerken is geworden. Het zorgt voor een efficiënt en snel transport van gegevens van knooppunt tot knooppunt of van client naar server.

SPX/IPX en TLI

Deze protocollen zijn door Novell geïntroduceerd in de NetWare-produkten, veruit het meest gebruikte netwerkbesturingssysteem. Het IPX-protocol wordt door Novell aanbevolen als de commu-

nicatiemethode voor client/server-applicaties. Het IPX-protocol is een implementatie van het Internetwork Datagram Packet (IDP)-protocol van Xerox. In principe is het een faciliteit waarmee datagrammen verzonden kunnen worden. Aan de andere kant geeft het SPX-protocol de garantie dat de gegevens correct worden afgeleverd. Het IPX-protocol biedt zo een interface voor de netwerklaag en een programmeer-interface voor de sessielaag. Het is een snelle en efficiënte communicatie-interface, omdat per pakket slechts weinig overhead nodig is.

APPC/SNA en CPI-C

APPC maakt communicatie mogelijk tussen twee verschillende knooppunten in een SNA-omgeving. Het is de basis voor de samenwerking tussen gedistribueerde processen die ondersteund wordt door IBM.

De kracht van APPC ligt in het feit dat twee willekeurige knooppunten die LU 6.2 ondersteunen, met elkaar kunnen communiceren, onafhankelijk van hun locatie in het netwerk, het besturingssysteem en het hardwareplatform. Zo kan een DOS-werkstation met een IBM-mainframe communiceren, als ze tenminste beide APPC ondersteunen, zowel in de hardware als in de software. Natuurlijk kunnen ook twee DOS-machines met elkaar communiceren via een APPC-interface.

APPC kan gebruikt worden als een bouwsteen van een client/server-systeem. De server kan een mainframe zijn, maar ook een minicomputer of een PC-server die APPC-ondersteunende software draait. Vanwege de geheugenbeperkingen van een DOS-machine levert dit echter in de praktijk nogal eens problemen op.

Het client/server-systeem dat op APPC is gebaseerd, is in de praktijk alleen zinvol voor organisaties die reeds beschikken over een SNA-omgeving en die hun applicaties willen omzetten naar PC-servers of die gegevens op mainframes rechtstreeks toegankelijk willen maken voor PC-clients.

TCP/IP en Sockets

TCP/IP is de de facto-standaard in Unix-omgevingen. Binnen TCP/IP zijn sockets de bouwstenen om de communicatie op te zetten (interface) tussen de toepassing en het besturingssysteem. Aan elke socket zijn één of meer processen verbonden. Het type van de socket bepaalt de methode van gegevensoverdracht in de socket. Een socket bestaat uit een Internet Address en een Port Address. Het Internet Address verwijst naar een unieke TCP/IP-netwerk-interface (netwerkkaart), terwijl het Port Address verwijst naar een toepassing die draait op het systeem waarin de netwerkkaart is opgenomen.

FUNCTIES VAN NETWERKBESTURINGS-SYSTEMEN

In deze paragraaf gaat het over de functies van het netwerkbesturingssysteem. Het netwerkbesturingssysteem moet zorgen voor een transparante werking van het transportmechanisme.
Van het netwerkbesturingssysteem wordt in principe het volgende verwacht:

- Het uitbreiden van de functies van het lokale besturingssysteem om het bereik van deze lokale besturingssystemen uit te breiden naar hulpbronnen die voor het gehele netwerk beschikbaar zijn, zoals printers, directories en modems.

- Het bieden van gedistribueerde faciliteiten en wel op een zodanige wijze dat er voor de gebruiker één enkel systeem ontstaat zonder dat hij of zij zich druk hoeft te maken over de fysieke plaats van de benodigde hulpbronnen.

- Het ondersteunen van de samenwerking tussen diverse onderdelen van applicaties die verdeeld kunnen zijn over diverse client- en serverplatformen.

Om deze functies op een gecoördineerde manier in te kunnen vullen is enkele jaren geleden de Open Software Foundation opgericht. Deze samenwerking heeft geleid tot de ontwikkeling van de zogenaamde Distributed Computing Environment (DCE). Hierop komen we hierna uitgebreid terug. Na een algemene inleiding op DCE wordt vervolgens meer specifiek aandacht besteed aan de beveiligingsfaciliteiten en de zogenaamde Remote Procedure Calls.

Transparantie

Reeds eerder werd al gezegd dat de netwerkbesturingssystemen moeten zorgen voor een transparante communicatie tussen client en server. Over het algemeen spreken we van een transparant systeem als voldaan wordt aan de volgende aspecten van transparantie:

- *Locatie:* Als gebruiker hoeft men zich niet druk te maken over de plaats van een benodigd hulpmiddel. Een gebruiker moet kiezen uit namen, het systeem zorgt er vervolgens voor dat het gevraagde hulpmiddel beschikbaar komt.

- *Naamgeving*: De naamgeving is zodanig ingericht dat de gebruiker ondersteund wordt bij het zoeken naar een bepaald hulpmiddel. Om dit te kunnen doen moet gebruik worden gemaakt van naamgevingsconventies.

- *Logon:* De gebruiker behoeft zich slechts eenmaal te identificeren en krijgt vervolgens alle hulpbronnen ter beschikking waarvan hij gebruik mag maken.

- *Replicatie:* Een gebruiker hoeft zich niet druk te maken over het aantal kopieën dat beschikbaar

moet zijn voor een adequate werking van de infrastructuur. Het netwerkbesturingssysteem moet zorgen voor synchronisatie van de inhoud van de diverse kopieën.

– *Distributie:* In principe moet een gebruiker vanaf elke willekeurige plaats gebruik kunnen maken van de hulpbronnen waarvan hij ook daadwerkelijk gebruik mag maken.

– *Tijd:* Ten slotte moet, zeker bij wereldwijde toepassingen, de gebruiker zich niet druk hoeven te maken over tijdsverschillen. Het netwerkbesturingssysteem moet de klokken van de servers synchroniseren.

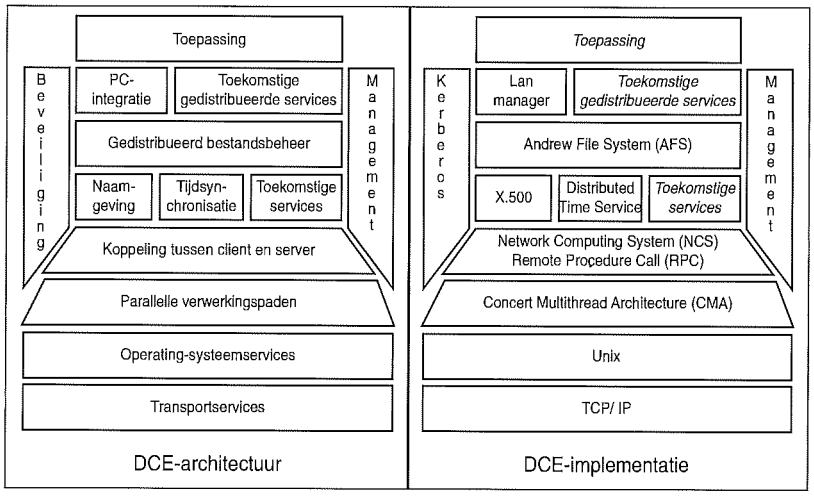
Distributed Computing Environment (DCE)

De distributie van de software over de diverse componenten maakt het nodig dat de samenwerking tussen deze componenten gecoördineerd wordt. De informatietechnologie heeft voor deze coördinatie oplossingen bedacht. Met name de samenwerking tussen verschillende computerleveranciers (bijvoorbeeld IBM, DEC, Siemens-Nixdorf, Olivetti) in de Open Software Foundation (OSF) heeft hiertoe bijgedragen. Het doel van de Open Software Foundation is om produkten op de markt te brengen die voldoen aan de standaard voor open systemen.

Het model dat de OSF hiervoor ontwikkeld heeft, staat bekend als 'Distributed Computing Environment Architecture' (DCE). In figuur 2 is deze architectuur aan de linkerkant getekend. Rechts van de architectuur is een aantal momenteel in de markt verkrijgbare produkten genoemd.

Hierna gaan we kort in op de belangrijkste in figuur 2 genoemde componenten. Verder zullen we wat uitgebreider stilstaan bij twee componenten, te weten de beveiliging en het gebruik van de Remote Procedure Calls (RPC).

Figuur 2. Distributed Computer Environment.



De onder in de figuur genoemde componenten transportservices en operating-systeemservices zijn hiervoor al aan de orde geweest. Hierboven zijn de parallelle verwerkingspaden (threads) opgenomen. Hiermee is het mogelijk dat meerdere processen tegelijk worden uitgevoerd. De Thread-service zorgt voor het beheer en de controle op de goede uitvoering van al deze processen.
De component tijdsychronisatie zorgt ervoor dat de klokken van de diverse systemen gesynchroniseerd worden. Zeker wanneer we denken aan de concurrency-problematiek bij het gebruik van database-servers is tijdsynchronisatie van groot belang. Naamgeving maakt het mogelijk alle namen van de bronnen waarmee gewerkt wordt op te slaan.
De component PC-integratie maakt het mogelijk dat ook schijfloze werkstations kunnen functioneren in een client/server-omgeving. Het is dan mogelijk systemen op te starten vanaf het server-systeem.
Gedistribueerd bestandsbeheer (distributed file services) maakt het mogelijk op een lokaal systeem bestanden te benaderen die op de schijf van een ander systeem opgeslagen zijn. In DFS zitten allerlei functies die het netwerk zoveel mogelijk ontlasten, zoals het repliceren van bestanden.

Beveiliging

Ook de beveiliging heeft in DCE de nodige aandacht gekregen. Het Massachusetts Institute of Technology (MIT) heeft samen met IBM en DEC het authenticatieprotocol Kerberos ontwikkeld.

DCE stelt de gebruiker in staat de beveiliging zodanig in te richten dat na één enkele login alle systemen ter beschikking staan, mits men daartoe geautoriseerd is. Hiervoor worden de beveiligingsgegevens vastgelegd in een afzonderlijke security-database, die bij voorkeur opgeslagen wordt op een afzonderlijke security-server. In principe kunnen in deze security-database alle relevante componenten worden opgenomen, dus niet alleen bestanden, maar ook directories, printers, toepassingen en besturingssystemen.
Naast deze security-database wordt ook gebruik gemaakt van een ticket granting server (TGS). Deze server zorgt ervoor dat men toegang krijgt tot de verschillende objecten die door een gebruiker benaderd kunnen worden. In feite werkt het net zo als de toegang voor bijvoorbeeld een pretpark of een theater. Men krijgt bij binnenkomst een kaartje, ofwel een ticket dat recht geeft op toegang tot het pretpark of het theater.

Binnen Kerberos worden drie stappen onderscheiden. Na het intoetsen van identificatie- en authenticatiegegevens worden de identificatiegegevens doorgegeven aan de security-server. Deze stelt vast of de desbetreffende gebruiker bekend is. Na identificatie is het mogelijk om de ticket granting server te benaderen waarmee toegang kan worden verkregen tot een bepaald object. Dit gebeurt in de tweede stap, de gebruiker krijgt een ticket voor het gevraagde object.
In de derde stap wordt dit ticket naar het gevraagde object gestuurd. Dit object komt vervolgens

voor de gebruiker beschikbaar na verificatie van de identiteit van de gebruiker.
Het grootste voordeel van Kerberos is dus dat de gebruiker zich slechts eenmaal hoeft te identificeren en authenticeren. Hierna verkrijgt men op transparante wijze toegang tot alle objecten waartoe men gerechtigd is. Verder is Kerberos relatief eenvoudig te implementeren, het mechanisme is meestal een geïntegreerd onderdeel van het besturingssysteem.
Een derde voordeel van Kerberos is dat voorzien wordt in vercijfering. Berichten gaan vercijferd over de lijn zodat het voor een hacker onmogelijk is in te breken. Ten slotte is een belangrijk voordeel van Kerberos dat het een openbaar protocol is, iedereen kan het in principe toepassen in zijn eigen produkten.
Kerberos heeft echter ook nadelen. Zo is de geldigheidsduur van een ticket beperkt. De beheerder is in principe vrij deze tijdsduur zelf in te stellen. Als deze te lang is kan een gebruiker die resterende tijd misbruiken, terwijl bij een te korte tijdsduur het wachtwoord opnieuw moet worden ingevoerd. Een tweede belangrijk nadeel dat nog genoemd moet worden, betreft het feit dat voor bepaalde objecten nog nadere autorisatie nodig is. Men verkrijgt toegang tot een bepaald object, bijvoorbeeld een toepassing. Vaak zal binnen deze toepassing een nadere toegangsbeveiliging geregeld moeten worden.

Remote Procedure Calls

Om twee programma-onderdelen met elkaar te laten samenwerken wordt gebruik gemaakt van zogenaamde *Remote Procedure Calls* (RPC). Deze zijn vergelijkbaar met het aanroepen van procedures, zoals dat gebruikelijk is in een 'normaal' toepassingsprogramma. Vaak worden bij het aanroepen van deze procedures parameters meegegeven die de aangeroepen procedure als invoer gebruikt. Al deze procedures zijn in een afzonderlijke bibliotheek opgeslagen en zijn als zodanig beschikbaar voor het eigenlijke programma. In dit geval spreken we echter van *Local Procedure Calls* (LPC): ze zijn namelijk opgeslagen op hetzelfde systeem als het aanroepende programma zelf.

In een client/server-omgeving werkt het precies hetzelfde. Het enige verschil is dat de procedures 'extern' opgeslagen zijn op een server, zodat we nu daadwerkelijk kunnen spreken van *Remote* Procedure Calls. Momenteel komt er steeds meer afzonderlijke programmatuur beschikbaar die zelfstandig zorgt voor deze koppeling. Dit heeft tot gevolg dat de systeemontwikkelaar gebruik kan maken van de RPC's alsof het gewone lokale procedures zijn.

GEDISTRIBUEERD CLIENT/SERVER-MANAGEMENT

De ontwikkelingen met betrekking tot client/server hebben tevens geleid tot hulpmiddelen ten behoeve van het management van client/server-infrastructuren. Aan de hand van het Management Framework zoals dat door OSI is ontwikkeld, wordt in deze paragraaf ingegaan op deze hulpmiddelen. Na een korte behandeling van het OSI Management Framework worden vervolgens de componenten behandeld waaruit een Open gedistribueerd client/server-platform bestaat. Daarna komt een drietal managementprotocollen aan de orde, te weten SNMP, SNMP 2 en CMIP. Deze paragraaf wordt afgesloten met enige opmerkingen over de ontwikkelingen met betrekking tot X/Open.

OSI Management Framework

OSI onderscheidt met betrekking tot het management van netwerken een vijftal aandachtsgebieden die als volgt kunnen worden gedefinieerd:

Fault management
Het proces dat netwerkfouten ontdekt, lokaliseert en oplost. Fault management bestaat uit:
- het identificeren van het optreden van een fout in het netwerk;
- het bepalen van de oorzaak van de fout;
- het oplossen van de fout (uiteraard als dit mogelijk is).

Configuration management
Het proces dat het mogelijk maakt om de netwerkconfiguratie te beheersen. Het bestaat uit:
- het verkrijgen van informatie over de huidige configuratie;
- het gebruiken van de informatie om de configuratie aan te passen aan veranderende omstandigheden;
- het opslaan van gegevens over de configuratie, gericht op het bijhouden van een actuele registratie, leidend tot rapportages die gebaseerd zijn op deze gegevens.

Security management
Betreft het beschermen van de opgeslagen gegevens door de toegang tot de componenten waarin de informatie opgeslagen is, te beschermen. Security management bestaat uit:
- het identificeren van de te beschermen informatie;
- het vastleggen van de 'toegangspoorten' tot de componenten;
- het beveiligen van deze toegangspoorten;
- het onderhouden van de beveiliging van de toegangspoorten.

Performance management
Dit proces is gericht op het efficiënte gebruik van het netwerk, dat wil zeggen dat het netwerk voortdurend toegankelijk is voor de gebruikers zonder dat er sprake is van een overbelast gebruik. Performance management bestaat uit:
- het verzamelen van gegevens over het huidige gebruik van de netwerkcomponenten en de verbindingen daartussen;

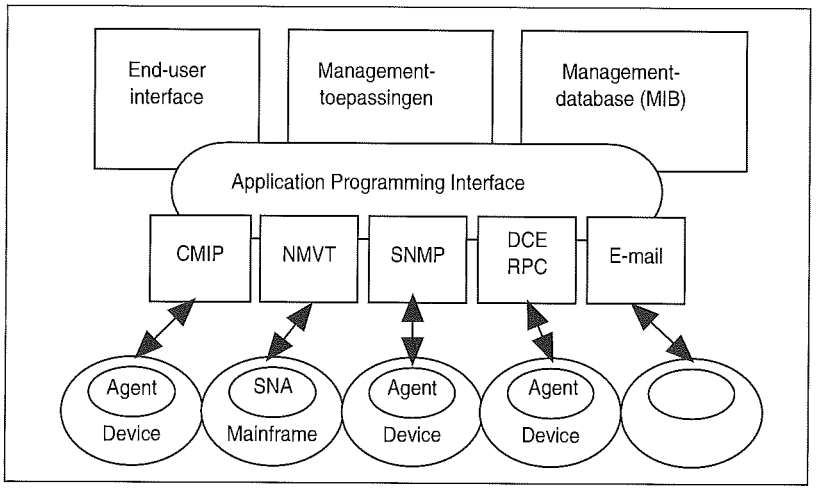
- het analyseren van de beschikbare gegevens gericht op het verkrijgen van inzicht in ontwikkelingen die in het netwerk optreden;
- het implementeren van grenzen in het netwerk;
- het gebruiken van simulatietechnieken om te kunnen bepalen waar aanpassingen in de toekomst nodig zijn om de performance van het netwerk te optimaliseren.

Accounting management
Is gericht op het meten van het gebruik van de netwerkcomponenten waardoor het mogelijk is inzicht te verkrijgen in de kosten van het netwerk en deze kosten vervolgens door te berekenen aan de gebruikers. Accounting management bestaat uit:
- het verzamelen van gegevens met betrekking tot het gebruik van de netwerkcomponenten;
- het implementeren van meetpunten in het netwerk;
- het doorbelasten van de kosten met betrekking tot het netwerkgebruik.

Om een andere invulling te geven aan het Management Framework heeft OSI ook richtlijnen gegeven over de manier waarop dit framework nader ingericht zou kunnen worden. Het gaat hierbij achtereenvolgens om:
- ISO 10165-1 Management Information Model (MIM);
- ISO 10165-2 Definition of Management Information (DMI);
- ISO 10165-4 Guidelines for the Definition of Managed Objects (GDMO);
- ISO 10165-5 Generic Management Information (GMI).

Uit deze richtlijnen blijkt dat met name het Managed Object een centrale rol speelt. In feite gaat het hier om elke component waarover gegevens vastgelegd moeten worden in het kader van het netwerkbeheer, dat wil zeggen gegevens over elk knooppunt in het netwerk en elke verbinding die tussen de knooppunten bestaat.

Figuur 3. Componenten Open GC/SM-platform.



Deze gegevens maken het mogelijk inzicht te verkrijgen in het gedrag van het desbetreffende object. Zij kunnen worden verdeeld in vier groepen, te weten attributen, acties, operations en notificaties. Uit dit onderscheid blijkt dat het ook hier gaat om een objectgeoriënteerde benadering. Vervolgens zorgt het managementprotocol ervoor dat deze gegevens op centraal niveau beschikbaar komen. Dit geschiedt op basis van commando's. Hiermee kunnen door het centrale beheersknooppunt operaties worden uitgevoerd die weer leiden tot antwoorden van het object. Verder is het uiteraard mogelijk dat een object op eigen initiatief gegevens naar het centrale knooppunt stuurt, de zogenaamde notifications. Hoe een en ander werkt komt hierna nog uitgebreid aan de orde.

Componenten Open GC/SM-platform

Om de infrastructuur te kunnen beheersen beschikt de netwerkbeheerder tegenwoordig over een groot aantal hulpmiddelen die bestaan uit een aantal onderdelen. Deze onderdelen zijn (zie ook figuur 3):

Een end-user interface
Gezien al het voorgaande zal het duidelijk zijn dat het hier meestal een grafische interface betreft die het de beheerder mogelijk maakt om op een zeer gebruikersvriendelijke manier te voorzien in zijn informatiebehoeften.

Programmatuur ten behoeve van het management-framework
In de vorige paragraaf is een groot aantal activiteiten genoemd die behoren tot het management-framework. Om deze activiteiten uit te kunnen voeren moet men beschikken over programmatuur die deze activiteiten ondersteunt. Deze programmatuur moet gegevens kunnen vastleggen, verzamelen en veredelen ten behoeve van het voorzien in de informatiebehoeften van de beheerder.

De management-database
In deze database (ook wel de Management Information Base, ofwel MIB genoemd) kunnen de nodige gegevens worden vastgelegd over de diverse componenten die onderdeel zijn van het netwerk. Het is erg belangrijk dat vooraf duidelijk is welke gegevens vastgelegd moeten worden om te kunnen voorzien in de informatiebehoeften van de beheerder. Men moet er zich van bewust zijn dat alles wat vastgelegd wordt, leidt tot vertragingen in het functioneren van het systeem. Juist vanwege deze vertragingen bestaat nogal eens de neiging om het gehele management maar te vergeten. Door vooraf goed na te denken over de vast te leggen gegevens is het mogelijk een zodanig selectieve vastlegging van gegevens te verkrijgen dat de vertraging die hiervan het gevolg is beperkt kan blijven en daardoor ook acceptabel is voor de gebruikers van het netwerk.

De Application Programming Interfaces
Deze interfaces maken het mogelijk te communiceren met diverse soorten agents die elk op basis van eigen protocollen gegevens hebben vastgelegd over een bepaalde component.

Managementprotocollen
Ten slotte zijn er de managementprotocollen die ervoor zorgen dat voor elke specifieke component gegevens worden vastgelegd. Afhankelijk van het platform kan er gebruik worden gemaakt van verschillende systemen. Enkele van deze protocollen komen hierna nog aan de orde. Protocollen die niet aan de orde komen, doch ook belangrijk zijn, zijn bijvoorbeeld:
- NMVT (Network Management Vector Transport) voor SNA-platformen;
- Remote procedure Calls voor DCE-platformen;
- E-mail, waarmee uiteraard ook gegevens ten behoeve van het management opgehaald en vastgelegd kunnen worden.

De bekendste managementprotocollen zijn SNMP, SNMP 2 en CMIP. Deze drie protocollen komen hierna kort aan de orde.

Het *Simple Network Management Protocol* (SNMP) is momenteel veruit het meest gebruikte protocol ten behoeve van het netwerkmanagement. Het wordt ondersteund door een nog steeds toenemend aantal netwerkcomponenten. SNMP doet precies wat de naam doet vermoeden: het voorziet in relatief eenvoudige voorzieningen ten behoeve van het beheer van de componenten. Het protocol wordt gebruikt om MIB-gegevens zo nodig aan te kunnen passen c.q. op te kunnen vragen.

SNMP is een protocol dat voorziet in de volgende opdrachten:

- *Get:* Dit is een opdracht die het mogelijk maakt de waarde van een managed object op te vragen. Het is een atomaire operatie, dat wil zeggen dat alle waarden worden doorgegeven of er worden geen waarden doorgegeven.

- *Get-Next:* Deze opdracht zorgt ervoor dat de waarden van het volgende managed object uit de MIB-hiërarchie worden uitgelezen.

- *Set:* Met deze opdracht is het mogelijk de waarde van het managed object aan te passen. Omdat SNMP slechts zeer beperkte beveiligingsmogelijkheden biedt om het wijzigen van deze waarden te kunnen beheersen, wordt aanbevolen om deze opdracht zo weinig mogelijk te gebruiken.

- *Trap:* Deze opdracht wordt gegenereerd op eigen initiatief van het managed object. Deze notificaties worden afgegeven naar aanleiding van bepaalde, meestal ongewenste feiten (bijvoorbeeld een koude start of het constateren van een te lage performance).

De grootste nadelen van SNMP zijn de beperkte beveiliging en de onmogelijkheid om grote massa's gegevens op te vragen. Ten aanzien van de beveiliging geldt dat het voor een hacker relatief eenvoudig is om in te breken in het systeem. Verder is het gebruik van het Set-commando niet zonder gevaren. Een ander beveiligingsprobleem betreft de matige kwaliteit van het UDP-protocol dat door SNMP als basisprotocol wordt gebruikt. Er wordt in dit geval geen gebruik gemaakt van het Acknowledge-mechanisme, zodat een agent er niet zeker van is dat verzonden berichten ook daadwerkelijk aangekomen zijn.

De grootste nadelen van SNMP zijn de beperkte beveiliging en de onmogelijkheid om grote massa's gegevens op te vragen.

Om aan de bezwaren van SNMP tegemoet te komen is in maart 1993 de tweede versie van SNMP geïntroduceerd, beter bekend als *SNMP 2*. In deze versie wordt voorzien in:
- een nieuw veiliger protocol (niet alleen UDP, maar ook IPX en AppleTalk);
- de mogelijkheid om al of niet gebruik te maken van encryptie;
- de mogelijkheid dat ook managers met elkaar communiceren;
- het transport van massale hoeveelheden van gegevens;
- meerdere MIB-objecten;
- de mogelijkheid om tabelrijen toe te voegen of te verwijderen.

Ook is er een aantal nieuwe opdrachten. Deze zijn:

- *Get-Bulk:* Hiermee wordt een pakket (vaste lengte) volledig gevuld met gegevens over het managed object. Dit in tegenstelling tot de hiervoor genoemde Get-opdracht, waarbij in elk pakket slechts één enkele waarde opgenomen wordt. Pas als het pakket vol is wordt het totale bericht getransporteerd.

- *Inform:* Hiermee kunnen managers met elkaar communiceren.

Het *Common Management Information Protocol* (CMIP) van OSI is een veel uitgebreider protocol dan SNMP en SNMP 2. Het heeft alleen veel tijd gekost om een en ander te ontwikkelen, waardoor er nu sprake is van een bepaalde achterstand. Vanwege de betere kwaliteiten mag verwacht worden dat op de lange(re) termijn, zeker voor de grotere client/server-omgevingen, gebruik gemaakt zal gaan worden van CMIP.

Voor elk managed object kunnen gegevens vastgelegd worden waarbij gebruik gemaakt kan worden van de door OSI gepubliceerde 'Guidelines for the definition of Managed Objects'.

Ook CMIP kent een aantal opdrachten die veel lijken op de SNMP-opdrachten. Het betreft de opdrachten Get, Event-Report, Action, Create en M-delete. Binnen CMIP heeft men de keuze de berichten al of niet te laten bevestigen.

X/Open Management Standards

Bull en Hewlett Packard hebben een interface ontwikkeld die als basis heeft gediend voor de X/Open Management API (XMP). Deze API kan gebruikt worden als een overkoepelende interface waarmee verschillende soorten managementprotocollen gekoppeld kunnen worden, met name SNMP en CMIP.

Verder voorziet XMP in een X/Open Object Manager (XOM) waarmee is mogelijk is meerdere gegevensstructuren te benaderen. Hierbij wordt gebruik gemaakt van XOM API-calls.

DATABASE-SERVERS

In deze paragraaf besteden we aandacht aan database-managementsystemen in het perspectief van een client/server-omgeving. Leveranciers van DBMS'en die op dit terrein belangrijk zijn, zijn Oracle, Sybase, Informix, Ingres en Gupta. Hun DBMS'en werken echter op een verschillende manier. Deze verschillen komen hierna aan de orde. Ze hebben echter ook gemeenschappelijke kenmerken. Dit betreft in de eerste plaats de relationele structuur en in de tweede plaats de mogelijkheid om gebruik te maken van Structured Query Language. Op SQL gaan we hierna eerst in. Na de behandeling van de verschillende architecturen besteden we daarna nog aandacht aan het gebruik van stored procedures, triggers en rules, waarna deze paragraaf wordt afgesloten met een behandeling van SQL Middleware.

Structured Query Language

SQL wordt gebruikt om complexe operaties met betrekking tot de in de database opgeslagen data mogelijk te maken. Hierbij wordt gebruik gemaakt van relatief eenvoudige commando's.
Met deze commando's kunnen in principe de volgende activiteiten worden uitgevoerd:
- het interactief opvragen van gegevens ten behoeve van de invulling van ad hoc-informatiebehoeften;
- het maken van programma's voor het benaderen van de database;
- het definiëren en het beheren van gegevens(defmities);
- het benaderen van alle relationele databasemanagementsystemen met een algemene taal.

Er zijn door de jaren heen verschillende versies van SQL verschenen. De eerste versie staat bekend als ANSI SQL en werd in 1989 geïntroduceerd. In 1992 verscheen een nieuwe versie, beter bekend als SQL2. In 1995 wordt SQL3 verwacht. De meeste DBMS'en ondersteunen vrijwel alle faciliteiten van SQL2, terwijl sommige al enige faciliteiten van SQL3 aankunnen.
Hieronder volgt een kort overzicht van de faciliteiten van de drie SQL-versies.

SQL-89
- SQL Intersection
- Embedded SQL
- Referentiële integriteit

SQL-92
- Connections
- Binary Large Objects (BLOB)
- Join Operators
- Catalogs
- Dynamic SQL
- Domein-integriteit

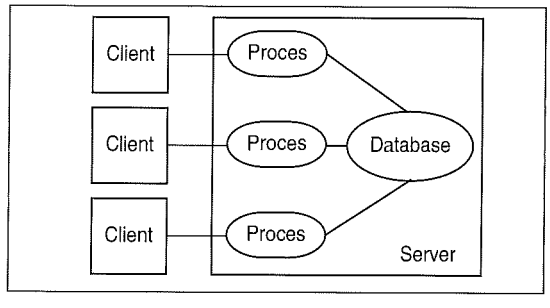
SQL-95
- Object SQL
- Stored Procedures
- Triggers
- Sensitive cursors
- Multimedia.

SQL Database Server Architecturen

Database-managementsystemen kunnen in principe op drie manieren verzoeken van clients afhandelen, namelijk proces-per-client, multi-threaded en hybride. Hierna wordt kort ingegaan op deze drie vormen.

Proces-per-client architectuur
Bij deze vorm (zie figuur 4) krijgt elk verzoek van een client een eigen adresruimte ter beschikking, ofwel een eigen proces. Het grote voordeel hiervan is dat de clients volkomen van elkaar gescheiden worden terwijl ook het DBMS zelf wordt beschermd tegen de gebruikers. Deze architectuur vraagt wel de nodige multi-tasking faciliteiten van het lokale (server-)besturingssysteem.
Het nadeel van deze architectuur is het grote geheugenbeslag, terwijl het DBMS ook vaak langzaam zal functioneren vanwege de relatief grote overhead ten behoeve van de interproces-communicatie.

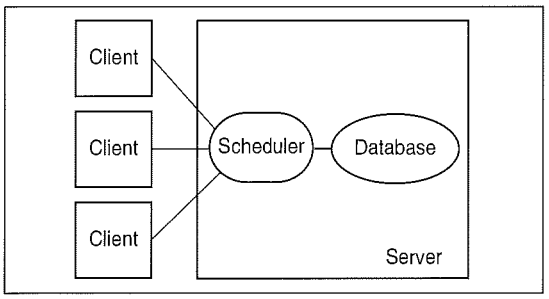
Figuur 4. Proces-per-client architectuur.



Voorbeelden van DBMS'en die volgens deze architectuur werken zijn DB2/2, Informix en Oracle6.

Multi-threaded architectuur
Bij deze architectuur draaien de toepassingen en de database zelf in één enkele adresruimte. Er wordt gebruik gemaakt van een eigen interne 'scheduler' en er wordt dus in mindere mate gesteund op de multi-tasking faciliteiten van het lokale besturingssysteem. Deze benadering heeft het grote voordeel dat men minder afhankelijk is van het besturingssysteem zodat het desbetreffende DBMS breder toe te passen is. Ook wordt er bespaard op geheugenruimte en wordt er minder een beroep gedaan op de centrale verwerkingseenheid.

Het nadeel is wel dat bij onjuiste verzoeken van clients het gehele systeem plat kan gaan. De bekendste voorbeelden van deze architectuur zijn Sybase en SQL Server.



Figuur 5. Multi-threaded architectuur.

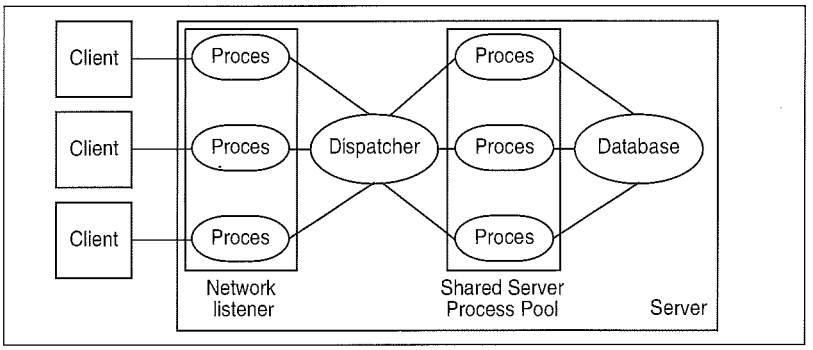
Hybride architectuur
Bij deze architectuur worden in principe drie componenten onderscheiden:

– *Multi-threaded network listener.* De taak van deze component is om het verzoek van de client toe te wijzen aan de dispatcher.

– *Dispatcher.* Deze zorgt ervoor dat de berichten in een rij worden gezet om ze later af te kunnen handelen.

– *Shared Server Process Pool.* Deze haalt de opdrachten op uit de rij, voert het verzoek uit en plaatst het resultaat in een uitvoerrij.

Het voordeel van deze architectuur is dat zij voorziet in een beschermde omgeving, terwijl de verzoeken niet steeds aan hetzelfde proces gekoppeld worden. Het nadeel van de benadering is de performance-problematiek. Het is nog de vraag of de performance bij gebruik van een TP-monitor niet beter zal zijn. Het bekendste voorbeeld van deze architectuur is versie 7 van Oracle.
Samenvattend kan gesteld worden dat de proces-per-client architectuur de voorkeur heeft vanwege de beste bescherming. Het nadeel is de slechte performance bij veel gebruikers. De multi-threaded architectuur kan beter overweg met grote aantallen gebruikers. Over de hybride architectuur is op dit moment nog niet zoveel te zeggen.



Figuur 6. Hybride architectuur.

Stored procedures, triggers, rules
De meeste moderne DBMS'en voorzien tegenwoordig in ingebouwde uitbreidingen waarmee het mogelijk is de toepassingen te ontlasten van bepaalde standaardprocedures. Het gaat hier met name om de begrippen stored procedures, triggers en rules.

Een *stored procedure* is te beschouwen als een soort Remote Procedure Call, maar dan gericht op databases. Een stored procedure is een verzameling SQL-statements, die gecompileerd zijn tot een geheel en rechtstreeks gekoppeld zijn aan de database zelf. Deze procedures accepteren parameters zodat ze een taak op een bepaalde manier kunnen uitvoeren.

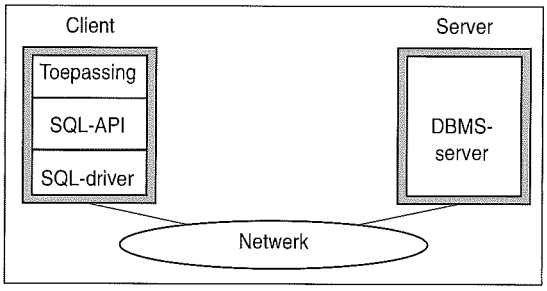
Naast de stored procedures onderscheiden we ook nog triggers en rules. In feite is zowel een *trigger* als een *rule* ook een stored procedure, ze worden echter niet geactiveerd naar aanleiding van een client-toepassing, maar worden geïnitieerd door gebeurtenissen die plaatsvinden binnen het DBMS zelf, de zogenaamde events. Hierbij richt een rule zich op een specifiek gegeven zelf (bijvoorbeeld een geprogrammeerde controle op het maximumsalaris), terwijl een trigger geactiveerd zal worden naar aanleiding van een gebeurtenis met betrekking tot een gegeven (bijvoorbeeld het melden dat de minimumvoorraad is bereikt).

SQL Middleware
SQL Middleware wordt gebruikt om het mogelijk te maken gegevens te benaderen die opgeslagen kunnen zijn in databases van verschillende leveranciers, met andere woorden, het is een mechanisme dat het benaderen van een database transparant maakt voor de gebruiker.

De problematiek is het eenvoudigst wanneer er gebruik wordt gemaakt van één enkele database. In dit geval moet men beschikken over een SQL-driver die geleverd wordt door de leverancier van de database zelf.

Als er sprake is van databases van verschillende leveranciers (multi vendor-omgeving) dan moet men in principe beschikken over verschillende drivers voor het benaderen van elke specifieke data-

base. Verder moet men beschikken over een SQL-API die ervoor zorgt dat de desbetreffende driver aangesproken wordt. De werking hiervan blijkt uit figuur 7.



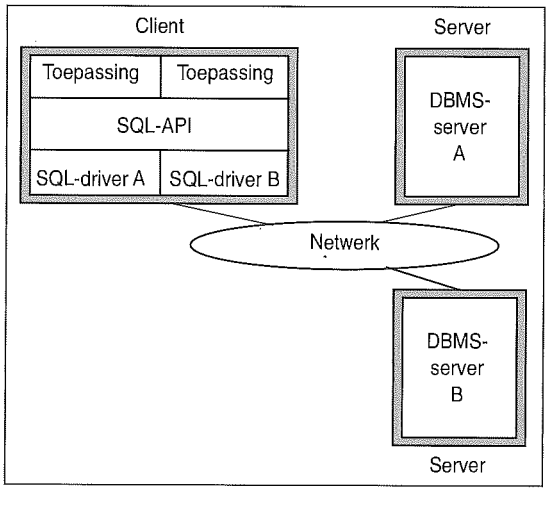
Figuur 7. De werking van de SQL-driver.

Om het nu toch mogelijk te maken dat de verschillende databases transparant benaderd kunnen worden, zijn er in principe meerdere oplossingen mogelijk.

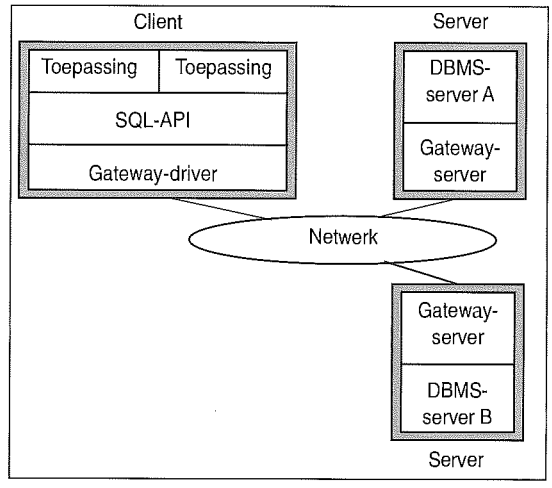
De eerste oplossing richt zich op het gebruik van één standaard-SQL-interface (zie figuur 8). Deze interface wordt dan aangeroepen door alle toepassingen waarna de interface zelf bepaalt welke database benaderd moet worden om aan het verzoek van de toepassing te kunnen voldoen. Voorbeelden van deze oplossing zijn Embedded SQL en de Common SQL Interface (CLI). Deze laatste interface is van toepassing voor:
- Open Database Connectivity (ODBC);
- Oracle Glue;
- Integrated Database Application Programming Interface (IDAPI).

Het nadeel van deze oplossing is dat er nog steeds meerdere database-drivers nodig zijn.

Figuur 8. Het gebruik van één standaard-SQL-interface.



Om het probleem van de verschillende database-drivers op te lossen kan ook gebruik worden gemaakt van een open SQL-gateway (zie figuur 9). Deze gateway vangt alle berichten op en vertaalt deze naar de lokale SQL-interface van de desbetreffende database-server.
Deze oplossing wordt momenteel toegepast door:
- Enterprise Data Access (EDA/SQL) van Information Builders Incorporated;
- Distributed Relational Database Architecture (DRDA) van IBM.



Figuur 9. Het gebruik van een open SQL-Gateway.

GROUPWARE

De opkomst van client/server-technologie heeft ook geleid tot de opkomst van het fenomeen groupware.
Groupware is een verzameling van technologieën die het mogelijk maken om complexe processen die plaatsvinden tussen een groep samenwerkende functionarissen te ondersteunen. Groupware is gebaseerd op de volgende vijf technologieën:
- multimedia document management;
- workflow management;
- electronic mail;
- scheduling;
- conferencing.

Bij *multimedia document management* staat het begrip document centraal. Een dergelijk document heeft een zeer flexibele structuur. Het is bijvoorbeeld mogelijk verschillende objecten te benaderen en te gebruiken. Voorbeelden hiervan zijn tekst, plaatjes, grafieken, spraak en video.

Groupware beschikt ook over voorzieningen ten behoeve van *workflow management*. Bij workflow management staan de drie R's centraal, te weten routes, regels en rollen.

Een *route* definieert het pad waarlangs een object zich kan verplaatsen. Hierbij behoren tevens de definities van de objecten die getransporteerd moeten

worden. De *regels* geven aan welke informatie getransporteerd moet worden en waar deze informatie naar toe moet gaan. Ook wordt aangegeven aan welke voorwaarden moet worden voldaan wil transport mogelijk zijn en er wordt aangegeven hoe problemen afgehandeld moeten worden.
Ten slotte geven de *rollen* aan de functies die met het object kunnen worden uitgevoerd.

In het kader van workflow management moet groupware het mogelijk maken om zowel standaardprocessen als ad hoc-processen af te handelen.

Electronic mail maakt het mogelijk berichten over het netwerk te transporteren. Hierbij wordt gebruik gemaakt van het store-and-forward-principe. Is een gebruiker op een bepaald moment niet aanwezig dan wordt het bericht opgeslagen en op het moment dat een gebruiker wel aanwezig is, alsnog doorgegeven aan de desbetreffende gebruiker.

Scheduling was één van de eerste faciliteiten van groupware. Hiermee is een adequaat agendabeheer mogelijk. Ook zijn er voorzieningen om 'to do'-lijsten aan te maken en tevens kan ook de afloop van bepaalde handelingen worden bewaakt en vastgelegd.

De laatste mogelijkheid, *conferencing*, is één van de recentste faciliteiten. Hiermee is het mogelijk 'elektronische vergaderingen' te organiseren. Het gaat hierbij zowel om realtime conferencing als anytime conferencing. Bij deze laatste vorm heeft een deelnemer zelf de mogelijkheid om mee te doen aan de discussie wanneer hij dat wil.

Bekende groupware-produkten zijn:
- Lotus notes;
- Flowmark/2;
- ImagePlus/2.

INFORMATION WAREHOUSE

De ontwikkelingen met betrekking tot client/server hebben IBM gebracht tot de introductie van het Information Warehouse. Dit raamwerk is in september 1991 door IBM geannonceerd. Vervolgens is in oktober 1993 een groot aantal op OS/2 gebaseerde produkten geïntroduceerd.
Het warehouse bestaat uit een afzonderlijke database ten behoeve van de besluitvorming (decision support). Het betreft een verzameling van gegevens die verzameld worden om te kunnen distribueren door de gehele organisatie; dit ten behoeve van de besluitvorming op alle niveaus in de organisatie.
Het Information Warehouse bestaat uit vier componenten:
- een informationele database;
- open SQL-access;
- automatisch copy-management;
- een informatie-catalog.

De *informationele database* bevat gegevens van verschillende afkomst die nodig zijn ten behoeve van de informatievoorziening van alle gebruikers in de organisatie.

Open SQL-access maakt het mogelijk alle databases, van welke soort dan ook (relationeel en niet-relationeel), te benaderen.

Het *automatisch copy-management* is nodig om de gegevens daadwerkelijk ter beschikking te stellen aan de gebruikers. Het gaat hierbij om distributie van gegevens, waarbij deze functionaliteit voorziet in verschillende faciliteiten ten behoeve van het in stand houden van de integriteit van de opgeslagen gegevens.

Groupware is een verzameling van technologieën die het mogelijk maken om complexe processen die plaatsvinden tussen een groep samenwerkende functionarissen te ondersteunen.

Ten slotte is er de *information catalog*. Hierin wordt vastgelegd welke gegevens in de informationele database zijn opgenomen, hoe ze eruit zien en hoe ze benaderd kunnen worden.

TOT SLOT

In dit artikel is een groot aantal componenten aan de orde gekomen die alle met elkaar samen moeten werken om een beheerste gegevensverwerking te kunnen realiseren. Deze adequate gegevensverwerking is weer nodig om een goede informatievoorziening te kunnen waarborgen.
Om aan deze doelstelling te kunnen voldoen wordt veel gevraagd van de middleware. In deze middleware biedt met name het gedistribueerde client/server-management samen met de Distributed Computer Environment van de Open Software Foundation een groot aantal aanknopingspunten voor een beheerste gegevensverwerking.

Er ligt voor de EDP-auditor een belangrijke taak om een adequaat gebruik van deze hulpmiddelen zoveel mogelijk te bevorderen.

J.C. van Praat RE RA
Is als EDP-auditor werkzaam bij BDO CampsObers en houdt zich fulltime bezig met EDP-auditing. Hierbij richt zijn aandacht zich op de beoordeling van de automatisering in zowel kleine als grote organisaties.
Daarnaast is hij als docent betrokken bij zowel AMBI (module HS.5) als bij de postdoctorale EDP-auditopleiding aan de Erasmus Universiteit te Rotterdam.

LITERATUUR

[Albe93] A. Alberts en J.P.G. Frints, *Beheersing van client/server omgevingen*, Handboek EDP-auditing, aflevering 7, Kluwer Bedrijfswetenschappen, Deventer 1993.

[Boch94] B. Bochenski, *Implementing Production-Quality Client/Server Systems*, John Wiley & Sons Inc., New York 1994.

[Hasp93] T. van den Haspel, *Client/server management*, Academic Service, Schoonhoven 1993.

[Matt90] R.L. Matthijssen en J.H.J.M. Truijens, *Computers, Datacommunicatie en Netwerken*, Academic Service, Schoonhoven 1990.

[Nieu94] S. Nieuwenhuyzen Kruzeman, W.Y. Keller en J.B. Crompvoets, *Applicatieontwikkeling voor client/server*, Tutein Nolthenius, 's-Hertogenbosch 1994.

[Praa92] J.C. van Praat en J.M. Suerink, *Inleiding EDP-auditing, Kwaliteitscontrole en beveiliging van informatiesystemen*, Kluwer Bedrijfswetenschappen, Deventer 1992.

[Ross93] G. Rossen, *Het client/server-concept bij gebruik van databasesystemen*, Management en Organisatie van Automatiseringsmiddelen, nummer 4, oktober 1993.

[Zant94] D. Zantinge en P.W. Adriaans, *Client/server en gedistribueerde databases*, Lansa Publishing BV, 1994.

Radio-LAN's in de praktijk

Ir. B.J. Busropan, ir. G.J. de GHroot, ir. W. Hollemans, ir. E.C. den Toom en ir. A. Verschoor

Mobiele communicatie is één van de snelst groeiende vormen van telecommunicatie. De systemen op dit gebied, zoals autotelefonie en Greenpoint, voorzien dan ook in een enorme gebruikersbehoefte: voldoende bewegingsvrijheid hebben en toch met anderen contact kunnen onderhouden. Maar niet alleen buiten, ook binnen bedrijven is 'mobiel' aan haar opmars begonnen. Recente ontwikkelingen op het gebied van radio Local Area Networks (radio-LAN's) brengen de voordelen van een vergrote mobiliteit en flexibiliteit nu eveneens onder handbereik van gebruikers van lokale datanetwerken. De introductie van radio-LAN's zou daarmee wel eens tot belangrijke verschuivingen op de markt voor LAN's kunnen leiden.

INLEIDING

In de loop van 1995 zal PTT Telecom starten met de levering van radio-LAN's. Gekozen is in eerste instantie voor WaveLAN, een radio-LAN dat dankzij zijn gemakkelijke, decentrale opzet in hoge mate tegemoet komt aan de marktwens naar meer flexibiliteit en mobiliteit.
Radio-LAN's kunnen het vaak moeizame en tijdrovende aanleggen van een LAN-bekabeling gedeeltelijk overbodig maken. Ook voor mobiele teams, bijvoorbeeld accountantsgroepen, is een radio-LAN een aantrekkelijke optie. Ongeacht het bedrijf waarbinnen zij aan het werk zijn, kunnen de teamleden namelijk gemakkelijk data met elkaar uitwisselen. Een derde toepassingsgebied is de moderne bedrijfsomgeving waarin nieuwe stations (laptops, PC's, etc.) snel bijgeplaatst moeten worden of waarin verhuizingen of reorganisaties gemakkelijk op te vangen moeten zijn. Kortom, de toepassingsmogelijkheden van radio-LAN's zijn onbeperkt en deze opsomming is dan ook zeker niet compleet.

De ontwikkelingen op het gebied van radio-LAN's zijn het gevolg van twee algemene trends. De eerste daarvan is de toenemende verbreiding van portable personal computers (laptops, notebooks en notepads). De tweede trend is het koppelen van personal computers, servers en randapparaten in lokale netwerken (LAN's), teneinde programmatuur, gegevensbestanden en dure randapparatuur gemeenschappelijk en daardoor efficiënter te kunnen gebruiken. Radio-LAN's bieden de mogelijkheid om beide trends op een flexibele wijze te combineren.

Over de marktomvang voor radio-LAN's lopen de verwachtingen nogal uiteen. Volgens sommigen zal de toepassing van radio-LAN's tot zeer specifieke applicaties beperkt blijven. Anderen voorspellen dat radio-LAN's in de totale markt voor LAN's uiteindelijk een belangrijke plaats gaan krijgen. Deze uiteenlopende verwachtingen zijn terug te voeren op een onvolledig beeld van enerzijds de eigenschappen van huidige radio-LAN's en anderzijds de ontwikkelingen die op dit gebied binnenkort zullen plaatsvinden.
Door de eigenschappen van radio-LAN's voor nu en de nabije toekomst te schetsen, zal in dit artikel[1] het beeld verduidelijkt worden. Om te beginnen wordt een overzicht gegeven van de werking en algemene eigenschappen van radio-LAN's; voor- en nadelen komen aan de orde, kenmerkende toepassingen worden genoemd. Ontwikkelingen op het gebied van standaarden voor radio-LAN's en de daarvan afgeleide produkten komen daarna aan bod. Uitgebreide aandacht is er vervolgens voor twee zaken die belangrijk zijn wanneer een radio-LAN geïnstalleerd moet worden: de planning van het netwerk en het vermijden van storing.

1 *Dit artikel is een bewerking van een in januari 1994 verschenen artikel in PTT Telecom Studieblad.*

maatregelen kunnen berichten in radio-LAN's dan ook gemakkelijk door onbevoegden worden afgeluisterd. Overigens kunnen met gespecialiseerde apparatuur ook bepaalde typen kabel-LAN's afgeluisterd worden. Data-encryptie is een goede en relatief goedkope methode om afluisteren tegen te gaan. Zij kan op applicatieniveau worden toegepast. Sommige radio-LAN's bieden echter ook data-encryptie op een lagere OSI-laag.

Uitzending van elektromagnetische straling
De laatste tijd is er bij gebruikers van radio-apparatuur toenemende bezorgdheid over eventuele gezondheidsrisico's van elektromagnetische straling. Hoewel dergelijke risico's nooit zijn aangetoond, kan de bezorgdheid erover leiden tot weerstand bij de gebruikers van radio-LAN's.

Risico voor storing van elektronische apparatuur
In sommige omgevingen, zoals in ziekenhuizen en de procesindustrie, wordt met uiterst gevoelige elektronische apparatuur gewerkt. Eventuele storing van deze apparatuur door radiosignalen zou tot gevaarlijke situaties kunnen leiden. Voor installatie van radio-LAN's in een dergelijke omgeving moet de onderlinge verdraagzaamheid van die elektronische apparatuur en het radio-LAN grondig worden bekeken. Zo nodig moeten maatregelen worden getroffen om gevoelige apparatuur af te schermen voor radiostraling.

Samenvattend kan worden gesteld dat de lagere capaciteit het belangrijkste nadeel is ten opzichte van kabel-LAN's. De overige hier genoemde nadelen kunnen door een goede produktkeuze en een juiste installatie vermeden worden.

Toepassingsgebieden van radio-LAN's

Er zijn vele toepassingen te noemen waarin de voordelen van radio-LAN's bijzonder tot hun recht komen en de nadelen geen belemmering vormen. Drie kenmerkende voorbeelden van dergelijke toepassingen worden hier besproken.

Magazijnbeheer
Voor het beheer van de aanwezige voorraad in magazijnen wordt over het algemeen gebruik gemaakt van een database-systeem. Voor het afhandelen van de bestelling van een artikel wordt aan het database-systeem gevraagd of en zo ja, hoeveel er nog van het gevraagde artikel in voorraad is en waar deze voorraad zich bevindt. Deze gegevens moeten vervolgens worden overgedragen aan de medewerker die de bestelling van het artikel gaat afwerken. De procedure kan efficiënter worden gemaakt door magazijnmedewerkers uit te rusten met notebook-PC's die via een radio-LAN aan het database-systeem gekoppeld zijn. De medewerkers kunnen dan in het magazijn op hun notebook instructies ontvangen over de afhandeling van bestellingen of via hun notebook de voorraad-database raadplegen en de gegevens daarin actualiseren.

Tijdelijke netwerken
In sommige branches zoals de accountancy worden teams van medewerkers soms voor korte tijd uitgezonden naar wisselende bedrijven/bedrijfsvestigingen. Om gemeenschappelijk gebruik te kunnen maken van programmatuur en gegevensbestanden, zonder afhankelijk te zijn van de ter plaatse aanwezige voorzieningen, zullen zij vaak een eigen netwerk meebrengen. Wanneer dit LAN bestaat uit PC's die zijn voorzien van radio-LAN-apparatuur, kan men direct aan het werk zonder eerst een netwerk aan te leggen. Ook op beurzen en conferenties kan dit een uitkomst zijn.

Gevaarlijke omgevingen
In bepaalde bedrijfssituaties, bijvoorbeeld in de zware industrie, kan de aanwezigheid van bekabeling tot riskante situaties voor de bedrijfsvoering leiden. Zo kan de omgeving door hoge temperaturen of het risico van mechanische beschadiging bijzonder onvriendelijk zijn voor de aangebrachte bekabeling. In dergelijke omstandigheden biedt een radio-LAN een goed en vooral veilig alternatief.

STANDAARDEN EN PRODUKTEN

De eerste radio-LAN-produkten verschenen begin jaren negentig op de Amerikaanse markt. In Europa werden deze radio-LAN's echter niet toegelaten voordat specifiek Europese frequentiebanden aan deze produkten waren toegewezen. Europese richtlijnen (standaarden) dienden geformuleerd te worden waaraan deze produkten moeten voldoen. Produkten die voldoen aan deze Europese standaarden hebben het voordeel dat men geen aparte zendmachtiging hoeft aan te vragen voor gebruik van deze produkten in de EU.

Spread-spectrum radio-LAN's

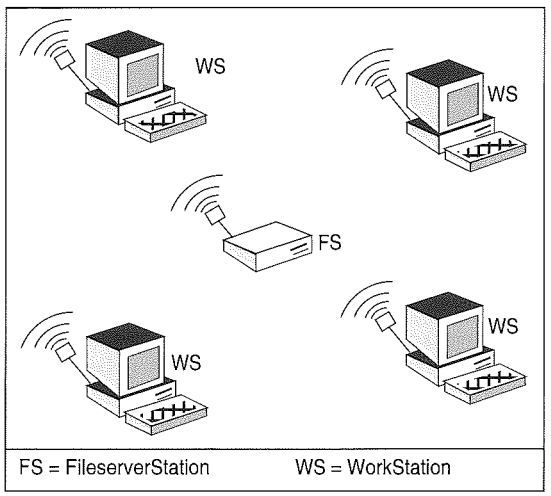
In 1991 startte de Europese standaardisatie-organisatie ETSI met de ontwikkeling van standaarden voor radio-LAN's. Eén hiervan is de standaard voor spread-spectrum LAN's die gebruik maken van de 2,4 GHz frequentieband. Deze band is ook bekend als de ISM-frequentieband. Deze frequentieband kan zonder licentie worden gebruikt voor allerlei medische, industriële en wetenschappelijke apparatuur. De magnetronoven is een bekend voorbeeld van deze categorie.

De standaard
De spread-spectrum radio-LAN standaard stelt alleen eisen aan maximaal zendvermogen en bandbreedte, verschillende produkten hoeven echter niet onderling compatibel te zijn. Deze standaard is in 1994 gepubliceerd (ISM).
De term spread-spectrum is afkomstig van de modulatiemethode die de radio-LAN's in deze frequentieband moeten gebruiken. Door middel van deze modulatiemethode wordt bereikt dat andere ISM-apparatuur (zoals magnetronovens en verhittingsapparatuur) de communicatie van deze radio-

LAN's minder gemakkelijk kan storen. Bovendien worden zo andere communicatiesystemen binnen de ISM-band ook minder gestoord door het radio-LAN.

Produkten
Er is een groot aantal produkten dat gebruikt maakt van de spread-spectrum technologie, voornamelijk gericht op de Amerikaanse markt. WaveLAN, van AT&T, voldoet echter ook aan de Europese spread-spectrum radio-LAN-standaard. WaveLAN is een draadloos LAN dat sinds eind 1993 in Europa verkrijgbaar is. Elk station in het radio-LAN is uitgerust met een PC-insteekkaart en een antenne. In 1995 komen ook PCMCIA-modules beschikbaar voor gebruik in laptop-computers. Naast deze hardware is ook software nodig voor de koppeling met het LAN Operating System in het werkstation.

De stations binnen WaveLAN communiceren autonoom met elkaar via de radioweg; hier wordt dus een decentraal toegangsprotocol toegepast. Een voorbeeld van een configuratie wordt gegeven in figuur 3. WaveLAN kan gemakkelijk met een bekabeld netwerk gekoppeld worden. Een mogelijkheid is het gebruik van een speciale bridge, WavePoint genaamd.



Figuur 3. Voorbeeld van een WaveLAN-configuratie.

De netwerkcapaciteit van WaveLAN is weergegeven in figuur 2, samen met de netwerkcapaciteit van andere typen LAN's. In deze figuur is de netwerkcapaciteit uitgezet tegen het aantal werkstations dat tegelijkertijd met een fileserver communiceert. De netwerkcapaciteit zal steeds over de actieve stations worden verdeeld. Als gevolg van het toegepaste toegangsprotocol in WaveLAN krijgt elk station evenveel capaciteit. In figuur 2 zien we bijvoorbeeld dat de netwerkcapaciteit bij drie stations circa 1,5 Mbit/s is; dat betekent dat elk station 500 kbit/s beschikbaar heeft voor zijn datacommunicatie.

HIPERLAN

Momenteel wordt gewerkt aan een standaard voor radio-LAN's die gebruik zullen maken van de 5 GHz, 17 GHz en 61 GHz frequentiebanden. Deze standaard staat bekend als de HIgh PErformance Radio LAN standaard, ook wel HIPERLAN-standaard (HLAN) genoemd. Alle produkten die aan deze standaard voldoen, zullen onderling compatibel zijn; het is dan mogelijk een netwerk met produkten van verschillende fabrikanten op te bouwen.

De standaard
HIPERLAN wordt nu nog in ETSI-verband gestandaardiseerd. De HIPERLAN-standaard wordt zodanig flexibel opgezet dat het mogelijk moet zijn meerdere diensten (data, spraak, video) in één netwerk te integreren. Produkten volgens deze standaard zullen een transmissiesnelheid in de orde van 20 Mbit/s bieden. Dit ligt hoger dan de 10 Mbit/s transmissiesnelheid die op huidige ethernet kabel-LAN's beschikbaar is. Eén van de nadelen van de huidige radio-LAN's, de lage datasnelheid ten opzichte van kabel-LAN's, zal voor HIPERLAN's verleden tijd zijn.

Produkten
De HIPERLAN-standaard zal op zijn vroegst half 1995 gereed zijn, produkten volgens deze standaard worden dan ook pas omstreeks 1997 verwacht. De verwachting is dat meerdere fabrikanten produkten volgens deze standaard zullen ontwikkelen.

DECT

Voor een compleet overzicht van de Europese standaarden op het gebied van radio-LAN's dient ten slotte nog de DECT-standaard te worden vermeld. DECT is een standaard voor draadloze communicatiesystemen ten behoeve van zowel spraak- als datacommunicatie (DECT). Sinds de DECT-standaard in 1993 van kracht geworden is, mogen produkten die aan deze standaard voldoen zonder licentie worden gebruikt.

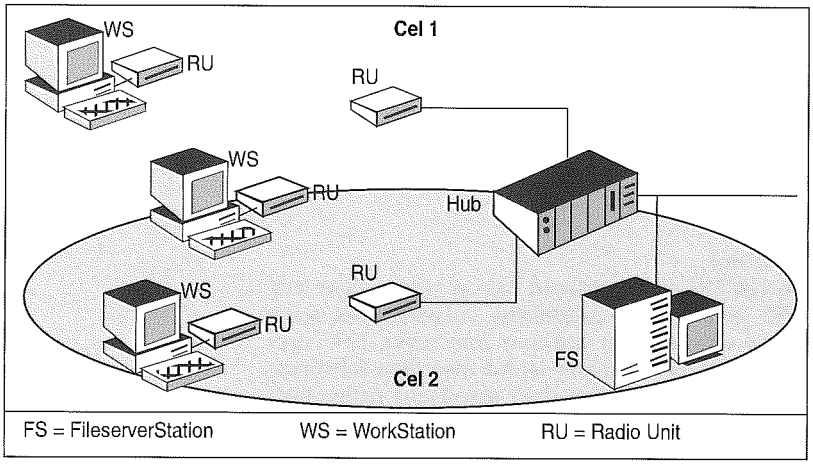
De standaard
Voor DECT is in Europa de frequentieband 1880 tot 1900 MHz gereserveerd. In deze band zijn tien kanalen met elk een nettocapaciteit van 576 kbit/s beschikbaar. Met deze standaard is het in principe mogelijk spraak- en datacommunicatie in één netwerk te integreren, hoewel de produkten die nu op de markt zijn een dergelijke integratie nog niet ondersteunen.

Produkten
Produkten volgens de DECT-standaard zijn medio 1993 op de markt gebracht. Olivetti heeft tot nog toe als enige een radio-LAN (Net cubic of Net^3) volgens deze standaard ontwikkeld. De werkstations binnen Olivetti Net^3 communiceren over de radioweg via een hub. Hierbij wordt een centraal

toegangsprotocol gebruikt. Een hub werkt hier als een basisstation, zoals dat bijvoorbeeld ook gebeurt bij autotelefonie. Het radio-LAN kan via de hub ook worden gekoppeld aan een kabel-LAN (ethernet of token ring).

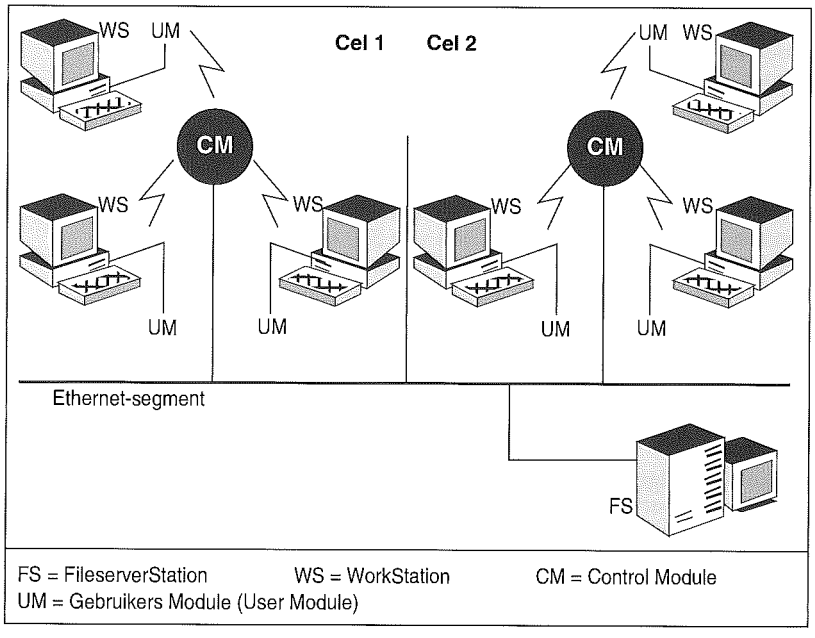
De hub wordt uitgerust met een radio-unit en speciale software. De overige werkstations in het LAN hebben een half-size PC-insteekkaart met radio-unit en software nodig. Een illustratie wordt gegeven in figuur 4.

In figuur 2 is te zien dat de netwerkcapaciteit van Net^3 laag is ten opzichte van de andere LAN's. Dat wordt voornamelijk veroorzaakt doordat de communicatievorm bij DECT afwijkt van de gangbare vorm bij LAN's (zoals ethernet). In LAN's vindt communicatie tussen de stations in de regel pakketgeoriënteerd plaats. Bij het circuitgeschakelde DECT wordt voor de communicatie steeds een verbinding opgezet, waarna alle pakketten kunnen worden verstuurd. De DECT-standaard is dan ook hoofdzakelijk gericht op spraakcommunicatie, waarvoor circuitschakeling gebruikelijk is. De capaciteit van de hub naar een kabel-LAN is 10 Mbit/s.



Figuur 4. Voorbeeld van een Net^3-configuratie.

Figuur 5. Voorbeeld van een (in Nederland niet toegelaten) Motorola Altair-configuratie.



Overige produkten

Behalve de produkten die aan de hierboven genoemde standaarden voldoen, is er (met name voor de Noordamerikaanse markt) een aantal andere produkten ontwikkeld. Veel van deze produkten maken gebruik van de 900 MHz band, een frequentieband die in Europa echter voor mobiele telefonie in gebruik is.
Een bekend produkt is Altair van Motorola. Altair werkt in een frequentieband (18 GHz) die in Europa al voor andere doeleinden (straalverbindingen) is gereserveerd. Om deze reden is Altair in Nederland niet toegelaten. In sommige andere Europese landen worden soms wel zendmachtigingen voor dit systeem verstrekt.

Het Altair-systeem kent twee soorten modules, te weten een Control Module (CM) en een Gebruikers Module (User Module, UM). Communicatie tussen werkstations, die via een standaard-ethernetkaart zijn aangesloten op een UM, verloopt via een radioverbinding met een CM die de communicatie verder afhandelt. Altair werkt dus met een centraal toegangsprotocol. De functie van de CM is te vergelijken met een basisstation van het autotelefoonnet. In de praktijk zal een CM, of zullen meerdere CM's, via een kabel-LAN gekoppeld worden aan een mainframe of fileserver (zie figuur 5).

De netwerkcapaciteit van het Altair-systeem is afhankelijk van het aantal CM's in het netwerk. De totale capaciteit die een CM kan bieden, is in figuur 2 weergegeven als functie van het aantal werkstations dat tegelijkertijd via de CM communiceert. Bij een aantal van vier werkstations is de maximale capaciteit van de CM bereikt (3,3 Mbit/s), bij een toenemend aantal gebruikers zal de capaciteit per gebruiker evenredig afnemen. Door extra CM's en een evenredige verdeling van het aantal gebruikers over de CM's kan de netwerkcapaciteit geoptimaliseerd worden.

Enkele eigenschappen van de in deze paragraaf besproken produkten zijn in tabel 1 op een rijtje gezet.

	WaveLAN	HIPERLAN-produkten	Olivetti Net^3	Motorola Altair
Frequentie	2,4 GHz (ISM-band)	5,2 GHz	1,9 GHz (DECT-band)	18 GHz
Zendvermogen	100 mW	100 mW	maximaal 250 mW	25 mW
Toegangsprotocol	Decentraal, pakket-georiënteerd, compatibel met ethernet via WavePoint	Decentraal, pakket-geschakeld	Centraal, circuit-geschakeld, compatibel met ethernet en token ring via hub	Centraal, pakket-georiënteerd, compatibel met ethernet
Uitvoering	Insteekkaart in PC met antenne	Half-size insteek-kaart in PC met radiomodule	Half-size insteek-kaart in PC met radiomodule. Aparte hub-hardware	Externe Control Modules en User Modules aan ethernetkaart in PC
Software-compatibiliteit	Novell, TCP/IP, LanManager, LanServer		Novell, LanManager	Netwerk operating software die wordt ondersteund door ethernet

Tabel 1. Enige kenmerken van WaveLAN, toekomstige HIPERLAN-produkten, Olivetti Net^3 en Motorola Altair.

PLANNING VAN RADIO-LAN'S

Het is algemeen bekend dat de sterkte van een radiogolf afneemt met het toenemen van de afstand tot de zender. Bevindt men zich op een te grote afstand, dan zal het signaal uiteindelijk zo zwak worden dat de ontvangst wegvalt. Een voorbeeld hiervan is de ontvangst van Nederlandse radiozenders in het buitenland.

Overigens is de demping van een radiogolf buiten veel geringer dan binnen. Binnenshuis ondervindt de radiogolf op haar weg een sterke demping door de vele muren, deuren, kasten, etc. die zij moet passeren. De mate van demping is daarbij sterk afhankelijk van het soort materiaal en de materiaaldikte. Uit diverse onderzoeken is bijvoorbeeld bekend dat een gipsen wand een veel geringere demping veroorzaakt dan een stenen wand. De maximale afstand tussen zender en ontvanger, het bereik, is dus sterk afhankelijk van de binnenhuisomgeving waarin het systeem wordt geplaatst. Afhankelijk van het type radio-LAN zal het bereik in een kantoorgebouw tussen vijftien en dertig meter liggen. In produktiehallen kan het bereik oplopen tot honderd meter. In tabel 2 wordt voor een aantal produkten aangegeven hoe groot het bereik minimaal is.

Tabel 2. Typisch bereik van een radio-LAN.

Omgeving	WaveLAN	Net^3	Altair
Open ruimte	100 meter	100 meter	6 meter
Gesloten kantoor	20 meter	30 meter	13 meter

Signaalvertragingen die ontstaan door het optreden van meerwegpropagatie kunnen het bereik in open ruimten nog verder verkleinen. Meerwegpropagatie heeft namelijk tot gevolg dat verschillende signalen, die ieder een verschillende fysieke route van zender naar ontvanger afleggen, met een onderling tijdverschil bij de ontvanger arriveren. Als dit tijdverschil te groot wordt en de signalen ongeveer dezelfde sterkte hebben, gaan de opeenvolgende bits in het signaal elkaar overlappen, waardoor het zonder speciale maatregelen onmogelijk wordt het oorspronkelijke signaal te reconstrueren.

Opdeling in cellen

Het kan natuurlijk voorkomen dat de afstand tussen twee werkstations in een radio-LAN zo groot is dat geen betrouwbare onderlinge communicatie meer mogelijk is. In dat geval zal het radio-LAN opgedeeld worden in meerdere segmenten, ook wel cellen genoemd. Binnen iedere cel moet de afstand tussen twee willekeurige werkstations klein genoeg zijn om een betrouwbare communicatie mogelijk te maken. De grootte van een cel is dan ook afhankelijk van het systeem dat gebruikt wordt.
Verschillende cellen kunnen onderling worden verbonden door een traditioneel bekabeld LAN, zoals ethernet. Hiervoor zijn meestal speciale modules beschikbaar, zoals WavePoint voor het WaveLAN-systeem en de hub voor Net^3.

Bij tijdelijke installaties zullen de gebruikers zich meestal binnen een straal van vijftien meter bevinden en kan met één cel worden volstaan. Denk hierbij aan het al eerder genoemde accountantsteam dat zijn werk bij de klant verricht. Voor deze toepassing van een radio-LAN zal planning in de meeste gevallen overbodig zijn. Het is eenvoudig een kwestie van uitpakken, aanzetten en werken.
Bij de installatie van een permanent radio-LAN

zullen net als in een cellulair netwerk (autotelefoon, draadloze bedrijfstelecommunicatiecentrale) meestal meerdere cellen nodig zijn om het gebouw volledig af te dekken. In deze gevallen zal vooraf het netwerk zorgvuldig moeten worden gepland.

Benodigd aantal cellen

Het aantal cellen dat nodig is om een gebouw af te dekken is afhankelijk van het bereik van een systeem en dus ook sterk afhankelijk van het type gebouw. Om de kosten voor een netwerk te minimaliseren moet het aantal cellen zo klein mogelijk worden gehouden. Daarentegen mogen de cellen ook weer niet zo groot worden dat de afstand tussen twee werkstations te groot wordt en er geen betrouwbare verbinding kan worden opgezet.
Het is echter zeer moeilijk de grootte van een cel exact te voorspellen door de vele factoren die de voortplanting van radiogolven beïnvloeden. Zolang er geen goede modellen voor het voorspellen van het bereik van een cel zijn, moeten metingen ter plekke uitgevoerd worden voor de bepaling van het aantal benodigde cellen om het gebouw af te dekken.

Het is zeer moeilijk de grootte van een cel exact te voorspellen door de vele factoren die de voortplanting van radiogolven beïnvloeden.

Onderlinge beïnvloeding van cellen

Wanneer (tijdelijk of permanent) meerdere cellen of verschillende radio-LAN's in een gebouw gebruikt worden, moet er rekening mee worden gehouden dat de capaciteit per gebruiker (het aantal bits per seconde) terug kan lopen. In WaveLAN werken alle cellen op dezelfde frequentie. De kans is bovendien vrij groot dat in twee naast elkaar liggende cellen gelijktijdig berichten worden verstuurd. Hoewel de stations te ver uit elkaar liggen om tot dezelfde cel te behoren, kunnen de signalen elkaar vanzelfsprekend nog wel storen. De transmissiecapaciteit van beide cellen zal daardoor tot maximaal de helft kunnen dalen. Hieruit blijkt wel het belang om de planning zodanig uit te voeren dat de onderlinge beïnvloeding tussen cellen minimaal is.

Daarentegen bezitten Motorola Altair en Olivetti Net^3 de mogelijkheid om in de aangrenzende cellen verschillende frequenties te gebruiken. In diverse cellen gelijktijdig verzonden berichten kunnen elkaar dan ook niet of nauwelijks storen. Dit betekent dat de totale capaciteit in het gebouw nagenoeg gelijk is aan het produkt van de capaciteit van één geïsoleerde cel, en het totale aantal cellen.

Mobiliteit

Mobiliteit is het vermogen zich in een radio-LAN te verplaatsen zonder het contact met het netwerk te verliezen. Vooral voor gebruikers van bijvoorbeeld notebook-computers is dit van belang. De huidige radio-LAN-produkten zijn qua mobiliteit nog niet geheel vergelijkbaar met cellulaire netten zoals de netwerken voor autotelefonie. In een cellulair net kan een gebruiker vanuit iedere cel een verbinding opzetten. Nog niet alle radio-LAN's bezitten deze functionaliteit. Elke cel is dan een afzonderlijk systeem. Apparatuur van de ene cel kan daardoor niet zonder meer in andere cellen worden gebruikt. De mobiliteit van de gebruiker blijft beperkt tot de cel waartoe hij behoort.
Van de in dit artikel genoemde produkten biedt alleen Net^3 gebruikersmobiliteit over verschillende cellen. Voor de opvolger van WaveLAN zal deze functionaliteit ook beschikbaar zijn.

BEHEER EN BEVEILIGING

Het gebruik van de radioweg als transmissiemedium stelt enkele specifieke eisen aan een radio-LAN op het gebied van beheer en beveiliging. In deze paragraaf wordt daar nader op ingegaan.

Beheer

Door het geheel of gedeeltelijk ontbreken van bekabeling kan het beheer van de fysieke infrastructuur van een radio-LAN aanzienlijk eenvoudiger zijn dan het beheer van een bekabeld netwerk. Het is niet langer nodig een omvangrijke database bij te houden waarmee overzicht gehouden wordt op de bekabeling in een gebouw. Daartegenover staan enkele typische aspecten die bij het beheer van een radio-LAN een rol spelen. Instelling van radiokanalen, monitoring van de kwaliteit van een radiolink en beheer van toegangscodes zijn enkele voorbeelden daarvan.
Alle radio-LAN-produkten leveren software waarmee deze beheerfuncties lokaal uitgevoerd kunnen worden. Daarnaast ondersteunen de in dit artikel besproken produkten netwerkmanagementsystemen die gebaseerd zijn op het Simple Network Management Protocol (SNMP) en de standaard Management Information Base (MIB). Bovendien worden bij de verschillende produkten speciale MIB's geleverd, waarmee het mogelijk is voor het radio-LAN specifieke parameters te monitoren. Hierdoor kan het beheer van het radio-LAN, dat onderdeel is van een groter netwerk, volledig geïntegreerd worden in het beheer van het gehele netwerk.

Beveiliging

Het risico van afluisteren is bij het gebruik van radio groter dan bij het gebruik van kabels, omdat een radiosignaal in principe niet beperkt blijft tot één ruimte. Daarbij moet echter wel opgemerkt worden dat als gevolg van de lage zendvermogens

en hoge frequenties de signalen van de in dit artikel genoemde radio-LAN's nauwelijks buiten het gebouw te ontvangen zullen zijn.

Er zijn twee vormen van beveiliging van belang: beveiliging tegen afluisteren en toegangsbeveiliging. Afhankelijk van de gebruikerswensen kunnen verschillende vormen van afluisterbeveiliging worden toegepast. Net zoals in kabel-LAN's kan in radio-LAN's additionele data-encryptie op applicatieniveau worden uitgevoerd. Radio-LAN's bieden hiermee een beveiliging die equivalent is aan die van kabel-LAN's.

Daarnaast bieden diverse leveranciers van radio-LAN's hardware-encryptie op een lager niveau, waarbij ook de routeringsinformatie versleuteld wordt. Deze vorm van encryptie biedt naast beveiliging tegen afluisteren ook toegangsbeveiliging.

INVLOED VAN STORING

Zowel bekabelde LAN's als radio-LAN's zijn gevoelig voor stoorsignalen. Kabel-LAN's zijn vooral gevoelig voor allerlei pulsvormige stoorsignalen, afkomstig van bijvoorbeeld TL-verlichting of bliksem. Deze signalen kunnen via de lichtnetbekabeling overspreken op de LAN-bekabeling. De communicatie over radio-LAN's kan gemakkelijk gestoord worden door radiosignalen. Allerlei elektronische apparatuur zendt onbedoeld radiosignalen uit, die het de radio-LAN-ontvanger moeilijk maken het gewenste signaal foutloos te ontvangen. Een voorbeeld hiervan is het kloksignaal van de computer, waarvan de harmonischen vaak storing veroorzaken in de FM-omroepband rond 100 MHz. Ook radiozendapparatuur kan buiten de eigen frequentieband radiosignalen uitzenden die andere radiosystemen verstoren.

Er zijn wettelijke eisen die beperkingen stellen aan de uitstraling van radiosignalen door elektronische apparatuur. Dit zijn zogenaamde EMC-eisen, waarbij EMC staat voor Elektromagnetische Compatibiliteit, het vermogen van apparatuur om zonder storingen in elkaars omgeving te kunnen functioneren. Deze wettelijke eisen gelden echter in het frequentiegebied beneden 1 GHz, terwijl de meeste radio-LAN's hogere frequentiebanden gebruiken. Voor radiozendapparatuur gelden aparte normen. De limieten die in deze normen genoemd zijn, zijn veel strenger dan de normale EMC-normen.

De aard van de stoorsignalen verschilt per gebruikte frequentieband.

– In de 18 GHz band, waar het Motorola Altair-systeem gebruik van maakt, en de 5 GHz band van HIPERLAN, komen weinig stoorsignalen voor. Signalen met zulke hoge frequenties komen zelden of nooit voor in potentiële stoorbronnen.

– Op de DECT-standaard gebaseerde radio-LAN's, zoals Olivetti Net^3, functioneren in een band rond 1900 MHz. Hier komen veel meer stoorsignalen voor. Het is bekend dat bijvoorbeeld ontstekingsmechanismen van auto's binnen deze frequenties storing kunnen genereren. De verwachting is dat computers, wanneer onvoldoende rekening wordt gehouden met de elektromagnetische compatibiliteit van het produkt, ook storingen in deze band kunnen gaan veroorzaken door de steeds hoger wordende kloksnelheden.

– De zogenaamde spread-spectrum radio-LAN's, bijvoorbeeld WaveLAN, werken in de ISM-band. Dit is een band tussen 2400 en 2500 MHz die bedoeld is voor apparatuur die elektromagnetische energie gebruikt voor andere doeleinden dan communicatie. Dit is voornamelijk verhittingsapparatuur, meestal aangeduid met de term Industrial, Scientific and Medical apparatus. Omdat de toegepaste vermogens vaak erg groot zijn, heeft het geen zin eisen te stellen aan de maximale uitstraling van apparatuur. Het gevolg hiervan is dat radiocommunicatiesystemen die ook in deze band werken, zeer gemakkelijk gestoord kunnen worden. Het is dus verstandig een spread-spectrum radio-LAN niet toe te passen in omgevingen waar veel magnetrons gebruikt worden of in ziekenhuizen waar medische verhittingsapparatuur wordt gebruikt.

SLOTOPMERKINGEN

In de jaren tachtig hebben we een explosieve groei in het gebruik van personal computers kunnen meemaken. Met het toenemend gebruik van deze overigens niet-draagbare computers groeide ook de behoefte aan onderlinge communicatie of gezamenlijk gebruik van schaarse middelen (printers, software, enz.), wat tot de introductie van LAN's leidde.

Momenteel zien we een groeiend gebruik van draagbare computers. Als een logisch gevolg van dit toenemende gebruik van draagbare computerapparatuur zal ook een groeiende behoefte aan mobiele datacommunicatie ontstaan. Eerst waarschijnlijk vooral in de communicatie van buiten naar het bedrijf toe. Zo is in de mobiele wereld datacommunicatie duidelijk in opkomst via bijvoorbeeld het Europese autotelefoonsysteem GSM en de Inmarsat-satellieten. Bovendien zijn datacommunicatiemogelijkheden via Greenpoint beschikbaar. Al deze toepassingen zijn echter voor intensief dataverkeer niet geschikt.

De tot nu toe lage toepassingsgraad van radio-LAN's wordt waarschijnlijk veroorzaakt door de nog betrekkelijk lage penetratie van draagbare computers binnen de bedrijfsmuren, de relatieve onbekendheid met de hiervoor besproken plannings- of storingsaspecten, de huidige datasnelheid van radio-LAN's en het feit dat de kosten per radio-LAN-aansluiting voor veel toepassingen nu nog boven die van een gewone kabelaansluiting liggen.

Voor allerlei specialistische toepassingen, waarin de flexibiliteit en mobiliteit die draadloze netwerken bieden ten volle uitgebuit kunnen worden, zijn

Ir. B.J. Busropan, ir. G.J. de Groot, ir. W. Hollemans, ir. E.C. den Toom en ir. A. Verschoor Zijn allen werkzaam bij KPN Research, een onderdeel van Koninklijke PTT Nederland NV. De auteurs werken in het onderzoeksgebied radiocommunicatiesystemen. In opdracht van de business unit Zakelijke Markt van PTT Telecom hebben zij onderzoek verricht aan radio-LAN's. Aan de hand van dit onderzoek heeft PTT Telecom gekozen voor opname van het WaveLAN radio-LAN-produkt in het assortiment.

radioLAN's nu al een goed alternatief voor bekabelde netwerken.

Verwacht wordt dat de ontwikkeling van nieuwe radio-LAN-standaarden, zoals de hoge capaciteit HIPERLAN-standaard, én de frequentiereservering hiervoor, het gebruik van radio-LAN's voor een veel bredere groep gebruikers aantrekkelijk zullen maken. Radio-LAN's zullen dan ook een steeds belangrijker deel gaan uitmaken van de totale LAN-markt.

LITERATUUR

[ETSI92] European Telecommunications Standards Institute, *Digital European Cordless Communications (DECT) Common Interface*, ETS 300 175, October 1992.

[ETSI93] European Telecommunications Standards Institute, *Wide band transmission systems. Technical characteristics and test conditions for data transmission equipment operating in the 2.4 GHz ISM band and using spread spectrum modulation techniques*, ETS 300 328, May 1993.

[ETSI94] European Telecommunications Standards Institute. *High Performance European Radio-LAN (HIPERLAN) System overview*, October 1994.

3DAS-kenmerk, een uniek middel voor identificatie en authenticatie

Ir. W.H.M. Sipman RI

Wat is het 3DAS-kenmerk en hoe kan 3DAS gebruikt worden als sleutel, als identificatiemiddel en voor authenticatie? Dit artikel geeft een beschrijving van het 3DAS-systeem en mogelijkheden voor toepassing ervan.

INLEIDING

Om personen, voorwerpen of sleutels te kunnen identificeren, dienen zij over een uniek kenmerk te beschikken. Dit kenmerk moet voldoende onderscheidend zijn en gemakkelijk te herkennen. Bovendien mag men het kenmerk niet eenvoudig kunnen namaken of falsificeren. 3DAS is zo'n kenmerk, dat aan de strengste beveiligingseisen kan voldoen. Dit artikel gaat in op de problematiek van identificatie en authenticatie en hoe 3DAS hierbij een unieke rol kan spelen.

Eén van de problemen bij beveiliging is in staat te zijn mensen of voorwerpen uniek te identificeren. Een slot mag pas open wanneer de sleutel, die er uniek voor gemaakt wordt, erin past. Elke andere sleutel dient geweigerd te worden. Geld wordt pas ten laste van een rekening uitgekeerd, wanneer dat ene unieke pasje zich meldt.
Echter, unieke identificatie is niet zo gemakkelijk. Bij een gekozen sleuteltype is er slechts een zeer beperkt aantal verschillende sleutels mogelijk, bijvoorbeeld tien voor binnenhuissloten of koffersloten tot enige tienduizenden voor geavanceerde toepassingen. En het unieke bankpasje blijkt nog niet beveiligd te zijn tegen kopiëren. Veel unieker zijn biologische kenmerken, zoals de stem, het netvlies, een vingerafdruk, enz. Maar het herkennen van deze kenmerken gaat niet geheel probleemloos. Iedere keer dat een opname gemaakt wordt, is deze net weer iets anders dan de vorige. Is het dus wel de juiste of is het hem niet?

Het 3DAS-systeem heeft de voordelen van de uniciteit, de grote variatie in kenmerken, en een hoge mate van reproduceerbaarheid. Hierdoor kan het uitstekend toegepast worden voor identificatie van mensen en voorwerpen, als sleutel en als authenticiteitskenmerk voor documenten en voorwerpen. De lage kostprijs van 3DAS maakt het geschikt voor sleutelinformatie met een eenmalig of kortdurend karakter, zonder dat aan de betrouwbaarheid van de identificatie of authenticatie op enigerlei wijze afbreuk wordt gedaan.

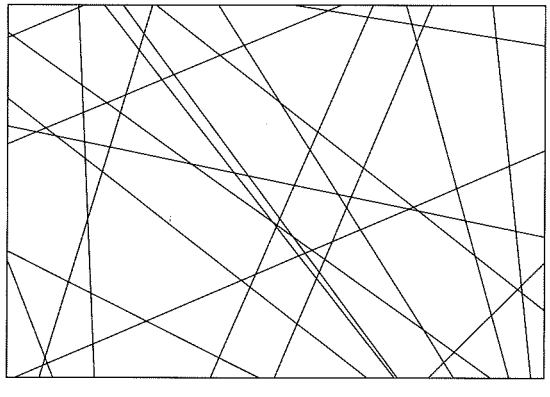
Identificatie

Om personen of voorwerpen te identificeren, dient men deze te herkennen aan een kenmerk dat uniek is voor die persoon of dat voorwerp. Meestal zijn er meerdere van dergelijke kenmerken. Personen kan men herkennen aan hun stem, hun vingerafdruk, hun netvlies, hun DNA, de geometrie van hun hand, hun geschiedenis en dergelijke. Voorwerpen kan men herkennen aan specifieke afwijkingen zoals krasjes, aan een aangebracht nummer, of aan de structuur van het materiaal. Een probleem bij veel van deze kenmerken is dat ze niet stabiel zijn of moeilijk meetbaar. Hierdoor krijgt men bij verificatie van een dergelijk kenmerk een niet eenduidig resultaat: bijvoorbeeld het waargenomen kenmerk stemt voor 99 procent overeen met het geregistreerde kenmerk. Het 3DAS-kenmerk heeft deze bezwaren niet. Het kenmerk vertoont geen slijtage en levert bij meting reproduceerbare resultaten. Dit maakt het 3DAS-kenmerk zo uniek. Bovendien is het door zijn driedimensionale karakter niet of nauwelijks na te maken of te simuleren.

HET 3DAS-KENMERK

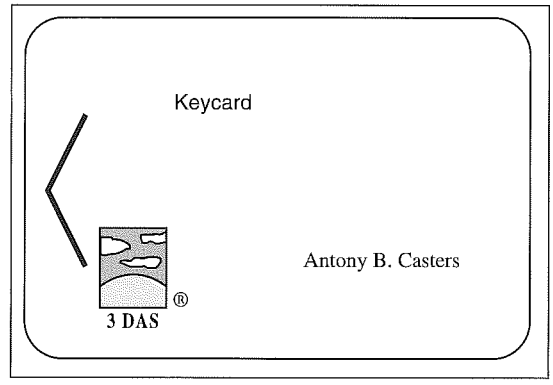
Het 3DAS-kenmerk vormt het hart van het 3DAS-systeem. Het kenmerk bestaat uit een vezelstructuur, die zich gemakkelijk laat hechten aan andere materialen. Deze vezelstructuur is opgebouwd uit filamenten van polyester met een dikte van slechts 38 µm. Tijdens het produktieproces worden de filamenten op een random wijze samengevoegd tot een soort doek. De structuur wordt niet door weven of breien gefixeerd, maar door onderlinge versmelting van de vezels. Hierdoor veranderen de patronen die door de ligging van de vezels ontstaan, niet of nauwelijks. Het random karakter van de ontstane patronen is dusdanig dat een monster van nog geen 3 × 3 mm ruim voldoende is voor een unieke identificatie. De vezelstructuur die gebruikt wordt, heeft een dikte van 280 µm. Dit is voldoende om de driedimensionale eigenschappen van het kenmerk tot hun recht te laten komen. Om de optische uitleesbaarheid van de vezelstructuur te verbeteren is deze voorzien van een metaalcoating.

Figuur 1. 3DAS-vezelstructuur.



De 3DAS-kaart

De 3DAS-kaart is het eerste produkt waarop het 3DAS-systeem toegepast wordt. De kaart is een gewone plastic kaart, vergelijkbaar met een bankpasje, die voldoet aan de norm voor plastic kaarten ISO 7810. In deze kaart is een 3DAS-kenmerk aangebracht op een dusdanige locatie dat deze combinatie met magneetstrip en/of chip niet verhindert. In een combinatiekaart (3DAS met chip) kan het 3DAS-kenmerk de chipkaart beter beschermen tegen kopiëren of namaak. Naar believen kan het kenmerk zichtbaar of onzichtbaar in de kaart worden aangebracht.



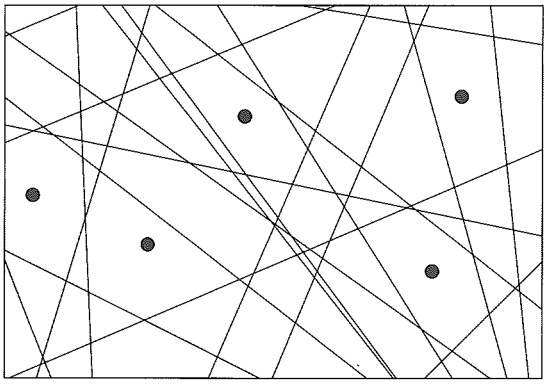
Figuur 2. 3DAS-kaart.

De 3DAS-lezer

De 3DAS-lezer is het apparaat waarmee het 3DAS-kenmerk gelezen wordt, en vertaald naar een unieke, goed reproduceerbare identificatiecode. Een infrarood lichtbron maakt een afbeelding van het kenmerk op een foto-elektrische cel. Op deze cel ziet men dan verlichte plekken (waar geen filamenten afgebeeld zijn) en donkere plekken (waar wel filamenten afgebeeld zijn). Van de grootste verlichte oppervlakken worden de zwaartepunten en de oppervlakte bepaald. Uit deze gegevens wordt een getallenreeks afgeleid, die de 'waarde' van het 3DAS-kenmerk representeert. Het stabiele karakter van het 3DAS-kenmerk maakt dat deze waarde goed reproduceerbaar is. De waarde is zowel onafhankelijk van de toegestane variaties in de positionering van de 3DAS-kaart in de lezer als van de toegestane variaties in de afmetingen van het kenmerk ten gevolge van buiging of temperatuur. Het driedimensionale karakter van het 3DAS-kenmerk komt tot zijn recht doordat het niet vanuit de normaal, doch vanuit twee verschillende hoeken belicht wordt. Door de beide afbeeldingsresultaten te vergelijken ontstaat een parallaxwaarde. Deze geeft aan of het kenmerk een echt 3DAS-kenmerk is, dan wel een falsificaat.

Het 3DAS-algoritme

Het algoritme is bepalend voor de bruikbaarheid van een kenmerk zoals het 3DAS-kenmerk, om personen of objecten te identificeren. Het 3DAS-al-



Figuur 3. Zwaartepunten van de vijf grootste vlakken met hun marges.

goritme vertaalt de afbeelding van het 3DAS-kenmerk naar een reproduceerbare code. Deze code bestaat uit de coördinaten van de zwaartepunten en de oppervlakten van de tien grootste door filamenten omsloten vlakken. Hierbij worden toleranties van vijf eenheden in de coördinaten van de zwaartepunten of honderd in de bepaling van de oppervlakten toegestaan om het kenmerk toch nog juist te identificeren, met een nauwkeurigheid van 1 op 10^{23}. In de praktijk zijn de waargenomen toleranties echter aanzienlijk kleiner, waardoor de identificatie van het kenmerk volledig gegarandeerd is. Het algoritme wordt uitgevoerd in de lezer, de identificatie in het achterliggende systeem.

Het 3DAS-logo

3DAS-kaarten worden voorzien van een 3DAS-logo, om kenbaar te maken dat deze kaarten voorzien zijn van een 3DAS-kenmerk. Door dit logo weet de gebruiker dat het om een 3DAS-kaart gaat, die in een 3DAS-lezer uitgelezen moet worden.

VERANTWOORDING VAN DE CLAIMS

De bruikbaarheid van het 3DAS-kenmerk als uniek identificatiemiddel is onderzocht door TNO-TPD (TNO Technisch Physische Dienst). Aan de hand van standaard-vezelmateriaal heeft deze dienst bekeken hoe groot het onderscheidend vermogen is van het 3DAS-systeem en hoe het driedimensionale karakter vastgesteld kan worden.
Voor de berekeningen is het volgende model gebruikt:
Van een 3DAS-kenmerk werd een schaduwafbeelding gemaakt op een standaard CCD-chip, zoals deze gebruikt wordt in videocamera's. Uitgaande van een beeldoppervlak van 4,6 × 6,1 mm met 512 × 582 pixels werd de projectie bewerkt. In plaats van alle pixels te gebruiken, nam men slechts de helft, waardoor een nuttig oppervlak van 256 × 256 pixels ontstond. Binnen een dergelijk oppervlak worden gemiddeld dertig à vijftig objecten (witte vlakken) afgebeeld. Wanneer men de coördinaten van de zwaartepunten met een nauwkeurigheid van ten minste 10 bij 10 pixels kan bepalen, dan is de kans op een 'false accept' (een tweede sample, dat ten onrechte als identiek wordt beschouwd) $2{,}5 \times 10^{-22}$. Nemen we ook de volgorde van de verschillende elementen mee, bijvoorbeeld gerangschikt naar grootte van het object, dan neemt de kans af tot $6{,}8 \times 10^{-29}$. In de praktijk kunnen de zwaartepunten nauwkeuriger bepaald worden, zeker met een factor 4. Dit verlaagt de kans op een 'false accept' tot 10^{-36}. Anders gezegd: met deze methode kan men 10^{36} verschillende samples eenduidig identificeren.

Voor het vaststellen van de ruimtelijkheid maakt men gebruik van een tweede lichtbron. Beide lichtbronnen staan 20° uit de normaal, dus met een onderling hoekverschil van 40°. Bij een materiaaldikte van 280 µm ontstaat dan een totaal-parallax van gemiddeld 8400 pixels. De totaal-parallax wordt bepaald door het oppervlak in zestien gelijke vlakken te verdelen, van elk vlak het aantal verschoven pixels te tellen, en het totaal te sommeren. Bij de nul-test (materiaaldikte = 0) is dit verschil 0 pixels, zowel per deelvlak als voor het totaal. Een samengeperst sample, met een restdikte van 70 µm, levert altijd nog een parallax op van gemiddeld 2000 pixels. Hiermee is aangetoond dat het meten van de parallax een goede indicatie is van de ruimtelijkheid van het monster. De waarde van de parallax kan gebruikt worden om de echtheid van het 3DAS-merk te verifiëren: hebben we met een echt kenmerk te doen of met een afbeelding.
TNO heeft ook aan de hand van proefkaarten getest in hoeverre het 3DAS-kenmerk beïnvloed wordt door de kwaliteit van de kaart, met name onder invloed van buiging, torsie en temperatuur. Deze tests hebben geen merkbare veranderingen in het 3DAS-kenmerk uitgewezen. Het 3DAS-kenmerk blijkt dus goed reproduceerbare metingen te leveren. Deze theoretische tests zijn inmiddels geverifieerd door echte praktijktests, waarbij kaarten meermalen door verschillende lezers werden gelezen. Ook hier werden geen problemen met de reproduceerbaarheid geconstateerd die verband kunnen houden met instabiliteiten in het 3DAS-kenmerk.

TOEPASSINGEN

Het unieke van het 3DAS-kenmerk maakt de 3DAS-kaart geschikt voor twee soorten toepassingen: identificatie en authenticatie.

Identificatie

Bij identificatie geeft de 3DAS-kaart de drager toegang tot aan de kaart verbonden rechten. Dit kan fysieke toegang tot een gebouw of ruimte zijn, maar ook de logische toegang tot gegevens. Het presenteren van de kaart kan ook dienen om aan te geven dat de drager een zekere handeling verricht heeft, zoals een voorgeschreven controle tijdens een produktieproces (validatie). De identificatie vindt plaats doordat de lezer het 3DAS-kenmerk meet en de meetwaarden (de zwaartepunten, ge-

wichten en verificatiewaarde) doorgeeft aan de database. In deze database wordt de string meetgegevens vergeleken met die van de geldige kaarten. Bij overeenstemming wordt de kaart geaccepteerd. Overeenstemming wordt geacht bereikt te zijn wanneer gemeten en geregistreerde waarde binnen de voorgeschreven toleranties gelijk zijn. Bij de standaardtoleranties (zie de paragraaf over verantwoording) is de kans op een 'false accept' kleiner dan 10^{-36}. Desgewenst kunnen de toleranties ruimer ingesteld worden, door bijvoorbeeld minder elementen in de bepaling mee te nemen.

Het unieke van het 3DAS-kenmerk maakt de 3DAS-kaart geschikt voor twee soorten toepassingen: identificatie en authenticatie.

Authenticatie

Het 3DAS-kenmerk kan ook gebruikt worden om informatie op de kaart te authenticeren. Bij een magneetpas, die relatief eenvoudig gekopieerd of gewijzigd kan worden, kan het 3DAS-kenmerk gebruikt worden om de echtheid van de kaart aan te tonen. Hiertoe worden de 3DAS-meetwaarden en de inhoud van de magneetpas cryptografisch aan elkaar gekoppeld, bijvoorbeeld door het vercijferde resultaat van de 3DAS-meetwaarden op de strip vast te leggen. Een duplicaat van de kaart valt dan onmiddellijk door de mand als een vervalsing. Ook de smartcard kan op deze wijze beveiligd worden tegen simulatie met behulp van een valse kaart of een computer.
Een praktische uitvoering van het authenticatieproces zou de volgende kunnen zijn: de 3DAS-meetwaarden worden gecomprimeerd tot een reproduceerbare code van 512 bits. Deze code wordt met behulp van het RSA-algoritme vercijferd met een geheime sleutel. Dit is dan de verificatiecode. Bij het aanbieden van een pas kan de authenticiteit eenvoudig worden gecontroleerd door de 3DAS-code te vergelijken met de met de publieke sleutel vercijferde verificatiecode. Bij deze methode kan alleen de originele kaartuitgever correcte verificatiecodes maken, daar alleen hij beschikt over de juiste geheime sleutel. Overal echter kan de kaartauthenticiteit geverifieerd worden met behulp van de publieke verificatiesleutel.

VOORBEELDEN

Waar kan men de 3DAS-kaart nu in de praktijk toepassen? De technologie is nog dermate nieuw dat er geen referentie naar gerealiseerde projecten gemaakt kan worden. Daarom volgen hier enige theoretische voorbeelden.

Validatie
Produktieprocessen, bijvoorbeeld in de farmaceutische industrie, zijn aan strenge controle gebonden. Validatie speelt derhalve een grote rol. Op diverse punten in het proces moeten bepaalde controles verricht worden om het goede verloop van het proces te garanderen. Om achteraf te kunnen nagaan of een bepaalde controle daadwerkelijk is uitgevoerd, kan de 3DAS-kaart gebruikt worden om bij wijze van elektronische handtekening aan te geven dat de controle door een bepaalde persoon is verricht. Een dergelijke methode van validatie is onder andere geaccepteerd door de Amerikaanse FDA.

Sleutel
De traditionele mechanische sloten kennen slechts een beperkt aantal sleutelmogelijkheden. Dit maakt een uitgebreid en complex sleutelbeheer noodzakelijk, waarbij er steeds op toegezien moet worden dat een sleutel na gebruik weer ingeleverd wordt. Met behulp van de 3DAS-kaart kan dit veel eenvoudiger. Door de haast oneindige variatie aan mogelijke sleutels kan men de kaart voor eenmalig gebruik uitgeven. Na gebruik wordt het slot omgeprogrammeerd, en behoeft de kaart niet geretourneerd te worden. Deze oplossing kan zowel bij enkele sloten, zoals van een huisdeur, toegepast worden, als bij uitgebreide systemen, zoals van hotelkamers. De 3DAS-kaart onderscheidt zich van de nu in hotels vaak gebruikte ponskaarten, doordat deze niet kopieerbaar is, en er dus uitsluitend een origineel bestaat.

Toegangscontrole
Bij toegangscontrole wordt niet slechts een sleutel verstrekt, doch kan de toegang tevens door andere parameters geconditioneerd worden. Afdelingen kunnen tijdelijk gesloten worden voor bepaalde groepen (sleutel)kaarthouders. De voordelen van de 3DAS-kaart in deze toepassing zijn weer de gegarandeerde uniciteit, de onmogelijkheid tot kopiëren, en de relatief lage kostprijs.

Tagging
Het 3DAS-kenmerk kan men ook gebruiken om objecten te identificeren en volgen. Hiertoe voorziet men die objecten van een label, dat het 3DAS-kenmerk bevat (tagging). Het label maakt door de uniciteit van het 3DAS-kenmerk dat men het betrokken object overal eenduidig kan identificeren en onderscheiden van andere gelijksoortige objecten. Dit is van groot belang bij kwaliteitscontrole, waar men het gedrag van individuele objecten wil kunnen volgen.

Verzegelen
Wordt de tag onlosmakelijk met het object verbonden als een zegel, dan kan deze de echtheid (authenticiteit) van het betrokken object garanderen. Op deze wijze kan men voorwerpen van waarde eenduidig identificeren. Voorbeelden van dergelijke voorwerpen kunnen zijn: geldtransportkoffers, zakjes bloedserum, kunstvoorwerpen, sieraden.

Echtheidsgarantie
Van veel documenten is het wenselijk de echtheid te kunnen vaststellen. Men kan hierbij denken aan bankpasjes, paspoorten, rijbewijzen en dergelijke. Een oplossing is het document van een 3DAS-kenmerk te voorzien. Aan het document voegt men een controlegetal toe dat via een asymmetrisch cryptografisch algoritme gekoppeld is aan het 3DAS-kenmerk. Met behulp van de publieke sleutel die bij het algoritme hoort, kan men nu overal de authenticiteit van het document vaststellen, zonder in staat te zijn zelf een correct controlegetal te genereren. Een methode hiertoe staat beschreven in de subparagraaf 'Authenticatie'.

Evenementen
Grote evenementen worden vaak geplaagd door het in omloop brengen van valse toegangskaarten. Dit probleem kan organisatorisch aangepakt worden door de toegangskaarten slechts kort tevoren in omloop te brengen. Bij nationale en zeker bij internationale evenementen is dit nogal bezwaarlijk. De tijd om de kaarten te distribueren wordt onaanvaardbaar kort. Gebruikt men echter 3DAS-kaarten, dan wordt vervalsen uitgesloten, aangezien het systeem alleen de echte, uitgegeven kaarten kent. Namaakkaarten vallen onmiddellijk door de mand en geven de houder geen toegang tot het evenement.

Gebruiksrecht van software
Software, zoals programmatuur, videobanden en CD's, is niet of nauwelijks effectief te beschermen tegen kopiëren. Het is echter wel goed mogelijk illegaal gebruik tegen te gaan. Een veel toegepaste methode is het installeren van een dongle, die het gebruiksrecht limiteert. Een dongle is een soort stekker met een chip erin, die aangesloten wordt op de printerpoort van een PC. Nadeel van de dongle is het onpraktische gebruik, vooral wanneer men meerdere beschermde programma's tegelijkertijd wil gebruiken. Bovendien verstoort de dongle vaak andere elementen van het systeem. Een alternatief kan de 3DAS-kaart bieden. De software start nu pas op nadat een correcte 3DAS-kaart gepresenteerd en geverifieerd is.

Waarom 3DAS?

In principe kunnen in deze toepassingen ook andere technologieën dan 3DAS gebruikt worden, zoals chip of magneetstrip. In de gegeven voorbeelden springt 3DAS er door zijn unieke kenmerken uit. 3DAS onderscheidt zich door zijn fraudebestendigheid. Het is niet mogelijk een 3DAS-kenmerk te kopiëren of te wijzigen, zodat het voor een ander, geldig kenmerk, zou kunnen doorgaan. Verder is 3DAS ongevoelig voor omgevingsinvloeden, zoals statische elektriciteit, magnetische velden en straling. Bovendien kan 3DAS voldoende goedkoop aangeboden worden voor massagebruik of eenmalige toepassing.

3DAS is
ongevoelig voor omgevingsinvloeden,
zoals statische elektriciteit,
magnetische invloeden en straling.

TOEKOMSTIGE ONTWIKKELINGEN

Naar verwachting zullen in de toekomst andere technologieën worden ontwikkeld voor het verkrijgen van een betere beschrijving van het 3DAS-kenmerk. Ook zijn nieuwe algoritmen te verwachten en de toepassing van 3DAS op andere dragers.

3DAS-kaartlezer

De huidige kaartlezer is gebaseerd op het maken van een schaduwafbeelding van het 3DAS-kenmerk op een CCD-chip door middel van infrarood LED's. Het grootste voordeel van deze techniek is het feit dat er geen bewegende elementen in de lezer nodig zijn en er geen ingewikkelde optische constructies gemaakt hoeven te worden. De belangrijkste nadelen zijn de beperkte resolutie en de gevoeligheid voor lichtreflecties en buigingsverschijnselen. In vervolgontwikkelingen zal onder meer gezocht worden naar andere technologieën om een betere en betrouwbare beschrijving van het 3DAS-kenmerk te krijgen.

Algoritme

Het huidige algoritme gaat uit van zekere toleranties in de meetwaarden. Desondanks levert dit nog een onderscheidend vermogen op van 10^{36}. Dit is ruimschoots voldoende voor de hier beschreven toepassingen. Voor veel toepassingen is een dergelijk onderscheidend vermogen niet vereist. Daarom zullen er nieuwe algoritmen ontwikkeld worden, die meer toegespitst zullen zijn op de werkelijke gebruiksomgeving. Bijvoorbeeld algoritmen die de tolerantie compenseren, en een 3DAS-code leveren die direct geschikt is voor RSA-encryptie. Voor chip-authenticatie is een dergelijk algoritme wellicht handiger dan de nu voorgestelde methode.

Ir. W.H.M. Sipman RI
Is management consultant bij Digital Equipment B.V. te Utrecht. Tot zijn taakgebieden behoort expertkennis op het terrein van kaarten, kaartsystemen en beveiliging. Als zodanig is hij actief in diverse normalisatiecommissies en werkgroepen. Hij is (mede-) auteur van diverse boeken en artikelen over kaarten en beveiliging.

3DAS op andere dragers

Momenteel wordt 3DAS uitsluitend toegepast in kaartsystemen: de 3DAS-kaart. Dit is geen principiële, doch slechts een praktische keuze. De eerste situaties waarin 3DAS toegepast gaat worden, zijn kaartomgevingen. In de toekomst zal 3DAS ook elders toegepast kunnen worden. In de voorbeelden werd tagging genoemd. In plaats van 3DAS in een tag te plaatsen, kan men het ook integreren in het basismateriaal zelf of in de emballage. Een voorbeeld zou kunnen zijn de zakjes voor bloedplasma. Logischer dan 3DAS-tags aan de zakjes te bevestigen is het om 3DAS meteen te integreren in het materiaal waarvan het zakje gemaakt is.
Met behulp van 3DAS kunnen ook documenten voorzien worden van een echtheidskenmerk. Het 3DAS-kenmerk kan rechtstreeks in de omslag van het paspoort of in de drager van het rijbewijs worden opgenomen.
Bepaalde waardevolle voorwerpen kunnen vaak rechtstreeks of via de verpakking van een 3DAS-kenmerk voorzien worden. Onderzoek is hier momenteel nog nauwelijks verricht. In de toekomst behoren ook deze toepassingen tot de mogelijkheden.

CONCLUSIE

Het 3DAS-kenmerk vormt de basis van een nieuwe en unieke methode om personen en objecten te identificeren en authenticeren met een ongekende graad van nauwkeurigheid. De bijzondere eigenschappen van het 3DAS-kenmerk zijn:
- *fraudebestendigheid:* het kenmerk is nagenoeg niet na te maken, te kopiëren of te simuleren;
- *onderscheidend vermogen:* het kenmerk is dermate uniek, dat gegeven het algoritme en de uitleestoleranties meer dan 10^{36} kenmerken onderscheiden kunnen worden;
- *economie:* het 3DAS-kenmerk kan op zeer goedkope wijze vervaardigd en uitgelezen worden in vergelijking tot andere methoden. Daarom kan het 3DAS-kenmerk ruim toegepast worden, ook in 'wegwerp'-situaties.

Laboratoriumonderzoek en de eerste praktijktests hebben deze claims reeds ruimschoots bewezen.
De unieke eigenschappen van het 3DAS-kenmerk maken dat het zich leent voor een uitgebreide reeks van toepassingen, zoals sleutels, identificatielabels en -passen, en echtheidskenmerken voor documenten.

LITERATUUR

[TNO92] TNO, *TNO-TPD-HOI-RPT-92-279*, 1992.

[TNO94] TNO, *TNO-TPD-HOI-RPT-94-131*, 1994.

[Mole92] C. Molenaar e.a., *Plastic Cards, betaalmiddel of marketinginstrument*, 1992.

CUMULATIEF

Overzicht van eerder verschenen artikelen in Compact
Een compilatie van artikelen over informatica en recht die in eerdere Compacts zijn verschenen, is, aangevuld met actuele bijdragen over dit onderwerp, opgenomen in *Twintig over Informatietechnologie en recht*. Twintig auteurs behandelen een breed spectrum van aspecten van de raakvlakken van informatietechnologie en recht op voor EDP-auditor, manager, adviseur, jurist en accountant toegankelijke wijze.
Het boek is verkrijgbaar via de boekhandel onder nummer: ISBN 90 14 04634 0.

3 19e jaargang 92/3 herfst 1992

De EDI-infrastructuur bij de Kas-Associatie
P. van Berge

Beheersbaarheid van het EDI-verkeer in de praktijk
G.J. Endenburg RI

EDI bij de Rijksdienst voor het Wegverkeer
J.W.J. Laan

EDI, een strategisch perspectief voor het bankwezen
Drs. M.A. Bongers RE en mw.drs. M. Steeman

Beheersing van inzet en gebruik IT: van kopzorg tot hoofdzaak
Drs. G.C.M. Mol en drs. J.F.H. Vrins

4 19e jaargang 92/4 winter 1992

De veiligheid van betaalautomaten
E.R. Fekkes

S.W.I.F.T. and Security
This article was produced by S.W.I.F.T. s.c. Marketing and the Chief Inspector's Office

Het binnenlandse traject van SWIFT-posten; het SWIFT-8007-circuit
Drs. F.G. Knaack

Betrouwbaarheid van het FA-systeem
Drs. R. Oudega

Een Nederlandse standaard voor de elektronische handtekening
Mw.drs. M.C. van Lith

De beveiliging van elektronisch bankieren
Mw.drs. M.C. van Lith

Secure Cash Management; a case study
H. Roos RA and H. Veenman MBT

Beveiligingsaspecten en juridische aspecten als communicerende vaten
Ir. G.J. Schuringa en mr. R.E. van Esch

1 20e jaargang 93/1 lente 1993

Netwerkmanagement, de organisatorische opzet en financiële beheersing
Ir. E.J. Evelo

Akzo en telecommunicatie, de organisatorische ontwikkeling
H. Reijn

SURFnet, beveiliging in een open netwerk
E. Zegwaart

Beveiliging van digitale kieslijnen
Drs.ing. D. Brouwer

Secure Cash Management; an audit perspective
M. Kennett BA

Nieuwe ontwikkelingen in de cryptografie: Kerberos en Digital Signature Standard
Drs. T.P. de Vries

Beveiligingsperikelen rondom Novell NetWare
J.L. Ramos Najera

2 20e jaargang 93/2 zomer 1993

Informatietechnologie duur? I/T Assessment: een beproefde methode voor het beoordelen van effectiviteit en efficiëntie van de informatieverzorging
Drs. B.T. Janssen, ing. W.J.D. Koot en ir. E.J. Mutsaers

Prioriteitenstelling met Decision
Dr. P.J. van Meel RI

De audit van een IT-investeringsaanvraag
Drs.ing. S.R.M. van den Biggelaar en drs. P.P.M.G.G. Brouwers

Verzekerbaarheid van automatiseringsrisico's
Mw.mr.drs. A.W. Duthler

Beveiligingsstandaard voor informatiesystemen
Prof.dr.ir. R. Paans RE

Global electronic mail: integratie van elektronische post met X.400
Ir. A. van Kooij

3 20e jaargang 93/3 herfst 1993

De toegevoegde waarde van EDP-auditing bij systeemontwikkeling
Ir. J.A. Verstelle

Normenstelsels voor systeemontwikkeling: hoe bruikbaar zijn deze?
Mw.drs. C.D.M. van der Veen

Projectbeheersing en -audit: contingency-benadering vereist
Ir. B.A.W.M. Bruns

De toegevoegde waarde van inspectietechnieken tijdens het ontwikkeltraject
B. Rooth

Invoering van informatiesystemen
Drs. Th.H. van Hesteren

Twintig vuistregels voor 'foutloos' onderhoud
E. Bergler

4 20e jaargang 93/4 winter 1993

Ontwikkelingen in de accountantscontrole in een geautomatiseerde omgeving
Drs. R.G.A. Fijneman RE RA

Aandacht voor interne controle tijdens systeemontwikkeling
Drs. J.J. van Beek RE RA

Audit automation
Drs. L.H. Dam RA en drs. P. Veltman RE RA

Operational auditing en EDP-auditing; is hier sprake van een begripsverwarring?
J.C. Boer RE RA

Accountant, EDP-auditor en jurist: een multidisciplinaire samenwerking
Mw.mr.drs. A.W. Duthler

Automatiseringsrisico's, verzekeringen en de rol van de accountant
Drs. G.J.W.C. Vankan

Geautomatiseerde betalingen
Drs. R. Oudega en drs. P. Veltman RE RA

1 21e jaargang 94/1 lente 1994

De invloed van informatietechnologie op de beheersing van organisaties
Prof. A.W. Neisingh RE RA

Rekencentra: normen voor menskracht
Prof.dr.ir. R. Paans RE

Accountant en de kosten- en batenbeheersing van informatietechnologie
Prof. H.B. Moonen RE RA

Informatiebeveiliging: de tijd is rijp
Drs. H.G.Th. van Gils RE RA

Het beoordelen van het testen van systemen
P. van Berge

2 21e jaargang 94/2 zomer 1994

Audit van een SNA-netwerk
M.M. Buijs RI en E.J.M. Ridderbeekx RE RI

Beveiliging van analoge kieslijnen
Drs.ing. D. Brouwer RE

Beveiliging van UNIX
Mw.drs. M.C. van Lith RE

Typologie van workflow-managementsystemen
Drs. D.J.P.Witte

3 21e jaargang 94/3 herfst 1994

Inleiding tot op TCP/IP gebaseerde netwerken
Ir. P. Kornelisse

Internet? Maar dan wel met een firewall!
H. van Hulst

Netwerkverbindingen in een OpenVMS-omgeving
Ir. J.H. Lie-Tjauw

Enige juridische wegwijzers voor de elektronische snelweg
Mw. mr. G.P. van Duijvenvoorde

Betrouwbaarheid en beveiliging van een CICS-omgeving
Ing. G.H.M. Meijer RE en mw. J.A.M. Holla

4 21e jaargang 94/4 winter 1994

Geautomatiseerde gegevensbewerking en jaarrekeningcontrole
R.A. Jonker RA

De invloed van informatietechnologie op de interne-controleprincipes
J.C. Boer RE RA

Audit van een logistiek systeem
Drs. J.A.C. van Geel, ing. A.P.J. Mouwen en drs. E.P.R. van Vroenhoven RE RA

Informatiebeveiliging van theorie naar praktijk
Drs. P. Veltman RE RA

Informatie(beveiligings)beleid in concernverband
Prof. A.W. Neisingh RE RA