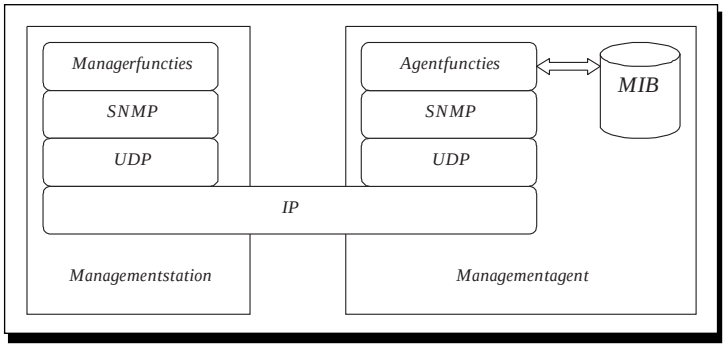
4.5.2 Netwerk Monitoring

SAMENVATTING

Meten is weten. Bij de eerste versie van het internet, het ARPANET, volstond een eenvoudige 'ping' om de bron van netwerkcongestie op te sporen. Maar het huidige internet met vele, complexe verbindingen vereist betere middelen voor netwerkbeheersing. Deze eis heeft aan het eind van de jaren tachtig geleid tot de ontwikkeling van het Simple Network Management Protocol (SNMP). Met behulp van dit protocol kan een managementstation (de manager) informatie die zich bevindt in de Management Information Base (MIB) van het te beheren systeem (de agent), ophalen en wijzigen (zie figuur 1).



FIGUUR 1
VERHOUDING TUSSEN SNMP EN MIB

1 INLEIDING

Door informatie te verzamelen van alle op het netwerk aangesloten systemen is het voor de netwerkbeheerder in principe mogelijk een compleet beeld te verkrijgen van al het verkeer dat door het netwerk stroomt. Het zal echter duidelijk zijn dat het ophalen van informatie uit alle op het netwerk aangesloten systemen veel tijd kost; voordat het laatste systeem is ondervraagd kan de informatie in het eerste systeem al weer veranderd zijn en het is in grotere netwerken dan ook nauwelijks mogelijk op deze wijze een goed beeld te krijgen van de toestand in het netwerk.

2 MEETMETHODEN

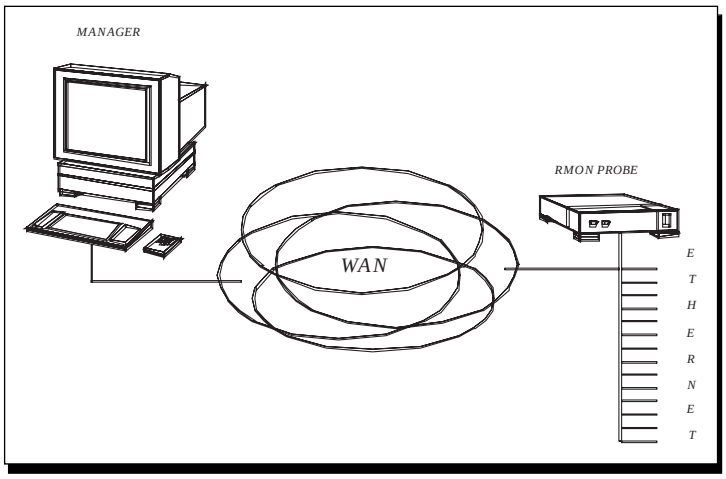
Een betere methode om de verkeersstromen door het netwerk te meten, is gebruik te maken van speciale meetsystemen. Een voorbeeld van een dergelijk meetsysteem is een 'sniffer'. Een sniffer is een apparaat dat op iedere verbinding in het netwerk kan worden aangesloten, waarna het al het verkeer dat over die verbinding gaat kan analyseren. Sniffers zijn vooral populair voor het meten aan traditionele Ethernet LAN's, omdat één enkel apparaat volstaat voor het analyseren van alle pakketten die over het broadcast medium worden verstuurd. Naast een groot aantal commerciële snif-

ferimplementaties, zijn er ook open source implementaties. De bekendste en meest geavanceerde open source snifferimplementatie is Ethereal (http://www.ethereal.com/). Net als bij de meeste andere sniffers draait bij Ethereal de meet- en user interface-software op hetzelfde systeem; vaak een aangepaste laptop. Alhoewel een dergelijke integratie handig is als er op ad hoc basis snel potentiële problemen opgespoord moeten worden, is het voor het structureel meten van verkeersstromen beter de user interface te scheiden van het meetsysteem (de probe). De software voor de user interface kan dan op een centrale machine worden geïnstalleerd; vanaf die centrale machine kan de netwerkbeheerder alle decentrale probes ondervragen en vervolgens een compleet beeld opbouwen van alle verkeersstromen. Bij commerciële producten is de communicatie tussen het meetsysteem en de centrale machine vaak op proprietary-protocollen gebaseerd, zoals bij Netflow van Cisco en LFAP van Enterasys. Er zijn echter ook producten die voor de communicatie tussen de probes en het centrale systeem gebruikmaken van open protocollen, zoals bijvoorbeeld HTTP en HTML. Een goed voorbeeld hiervan is Ntop (http://www.ntop.org/), een open source implementatie van een monitoring-systeem, die reeds in deel 3 van dit handboek in hoofdstuk 4.5.1 is beschreven.
Weer een stap verder gaan systemen waarvan de probe op afstand geconfigureerd kan worden. Door de probe op de juiste wijze te configureren, wordt het mogelijk zelfs op snelle Gbit-lijnen complexe metingen te verrichten. Voor het configureren, maar ook voor het uitlezen van de meetresultaten, wordt vaak gebruikgemaakt van SNMP en MIBs. Binnen de Internet Engineering Task Force (IETF), de organisatie die verantwoordelijk is voor de definitie van internetnormen, wordt gewerkt aan een tweetal MIB's.
De eerste MIB is de zogeheten 'meter' MIB (RFC 2720). Deze MIB is ontwikkeld door de Real-time Traffic Flow Measurement (RTFM)-groep en wordt vooral gebruikt ten behoeve van accounting. Het idee achter de meter MIB is dat de netwerkbeheerder een aantal 'rules' definieert. Een rule kan gezien worden als een combinatie van vijf velden: <source IP address, source port number, destination IP address, destination port number, type of service field>. Voor ieder (deel)veld kiest de netwerkbeheerder een bepaalde waarde; deze waarde mag ook een wildcard zijn. De vijf velden worden op een logische wijze (AND, OR) met elkaar verbonden, waardoor er een soort conditie ontstaat. Iedere keer als een pakket wordt ontvangen, doorloopt het meetsysteem de complete rule-set om te onderzoeken of er aan een of meerdere condities wordt voldaan. Indien dit het geval is, hoogt het meetsysteem de bij de conditie behorende teller op. Op deze manier krijgt de netwerkbeheerder een precies beeld van alle flows die door het netwerk stromen, en kan de gebruiker een rekening worden gepresenteerd voor de daadwerkelijke hoeveelheid verstuurd en ontvangen verkeer.

Ook voor de meter MIB bestaat er een open source-implementatie. Deze implementatie is ontwikkeld door de University of Auckland, en staat bekend onder de naam NeTraMet<ND TYPE="SP">1. De software draait op Linux- en Unix-systemen, en kan op een standaard Pentium-platform verkeer monitoren met een snelheid van vele honderden Mbit/s.
De tweede MIB is de 'Remote MONitoring' (RMON) MIB. Vanwege de bekendheid en goede toepasbaarheid zal de rest van dit hoofdstuk verder ingaan op deze MIB.

3 De RMON MIB

De oorspronkelijke versie van RMON, RMON Version 1 (RFC 2819), werkt op het niveau van de datalinklaag van het OSI-referentiemodel. Dit betekent dat een RMON1 probe (ook agent of monitor genoemd) alleen informatie kan verzamelen en verwerken over de LAN-segmenten waarop het is aangesloten (een probe kan op meerdere segmenten worden aangesloten). Vanwege de beperking tot de datalinklaag, kan een probe geen hogere laag informatie, zoals bijvoorbeeld het bron-IP-adres, bepalen.
Omdat de communicatie tussen manager en agent gebruikmaakt van SNMP, is het mogelijk het managersysteem en de probe op verschillende locaties op het netwerk aan te sluiten. Het is hierdoor voor een bedrijf met een afgelegen vestiging bijvoorbeeld mogelijk het verkeer binnen die vestiging op afstand te monitoren (zie figuur 2).

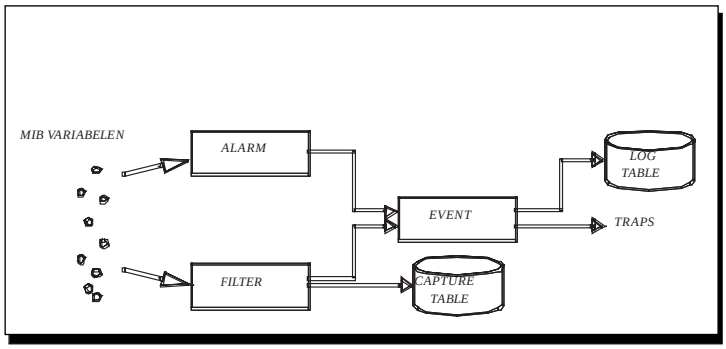


Figuur 2
Op afstand monitoren met RMON

De informatie die door de probe wordt verzameld, kan worden onderverdeeld in negen groepen: statistics, history, host, hostTopN, matrix, alarm, filter, capture en event. Daarnaast is er een tiende groep, de tokenRing-groep, gedefinieerd in een apart document (RFC 1513).

– De statistics-groep houdt actuele gegevens bij over het aantal verzonden pakketten, het aantal bytes alsmede mogelijke fouten op datalinkniveau.
  - De history-groep slaat periodiek gegevens uit de statistics-groep op in een circulaire buffer. De bemonsteringsfrequentie kan, net als de grootte van de buffer, door de netwerkbeheerder worden bepaald. Door bijvoorbeeld ieder halfuur een monster te nemen en een minimale buffergrootte van 48 cellen te kiezen, kunnen de gegevens van een hele dag worden bewaard. Om te voorkomen dat de gegevens na een dag worden overschreven, moet de netwerkbeheerder de circulaire buffer periodiek uitlezen.
  - De host-groep verzamelt voor ieder systeem dat op het LAN is aangesloten hoeveel verkeer er is verstuurd en ontvangen. Ook fouten worden bijgehouden.
  - De hostTopN-groep verzamelt dezelfde informatie als de host-groep, maar presenteert deze informatie gesorteerd op basis van een bepaald criterium (bijvoorbeeld de tien hosts die de meeste foute pakketten versturen).
  - De matrix-groep wordt gebruikt voor het bijhouden van het verkeer tussen alle host-paren in een sub-netwerk.
  - De alarm-groep definieert een verzameling grenswaarden voor bepaalde netwerkprestatieparameters en genereert events als een grens wordt overschreden. De parameters en grenswaarden zijn opgeslagen als MIB-variabelen (zie figuur 3).

FIGUUR 3
RELATIE TUSSEN ALARM-, FILTER- EN EVENT-GROEP



  - De filter-groep onderzoekt ieder pakket dat door de probe wordt ontvangen op de aanwezigheid van bepaalde bitpatronen. Voordat de filter-groep geactiveerd kan worden, moet de manager bepaalde variabelen in de RMON MIB configureren zodat de probe weet op welke bitpatronen gelet moeten worden. Indien er een match optreedt, kan een event worden gegenereerd. Ook kan het gehele pakket waarin het bitpatroon is aangetroffen worden opgeslagen.

- De capture-groep wordt gebruikt voor de buffering van pakketten die worden afgevangen in de filtergroep.
- De event-groep bepaalt wat er moet gebeuren nadat een alarm is opgetreden of een bepaald bitpatroon door de filtergroep is gedetecteerd. Mogelijke acties zijn het versturen van een SNMP trap bericht of het vastleggen van de gebeurtenis in een logtabel.
- De tokenRing-groep omvat vier subgroepen die specifiek bedoeld zijn voor het monitoren van token ring sub-netwerken.

3 RMON2

In de meest recente versie, RMON Version 2 (RFC 2021), kunnen probes ook informatie van hogere dan de datalinklaag monitoren. Dit betekent dat een RMON2 probe informatie kan analyseren die niet behoord bij het LAN-segment waaraan de probe gekoppeld is (bijvoorbeeld het bron-IP-adres van een pakket dat via een router binnenkomt). Ook kan de probe het verkeer behorende bij een bepaalde applicatie observeren. Een andere toevoeging is de 'tijdfilterindex', waardoor het mogelijk wordt dat de manager alleen informatie uit de probe haalt die na een bepaald tijdstip is veranderd. De RMON2 MIB is uitgebreid met negen groepen ten opzichte van RMON1 MIB: protocolDir, protocolDist, addressMap, nlHost, nlMatrix, alHost, alMatrix, usrHistory, en probeConfig.

– De protocol directory-groep (protocolDir) geeft aan welke protocollen de probe ondersteunt.
  - De protocol distribution-groep (protocolDist) bevat het aantal bytes en pakketten verzonden voor ieder van de ondersteunde protocollen.
  - De address map-groep (addressMap) beeldt de netwerkadressen af op datalink (MAC) adressen.
  - De network layer host-groep (nlHost) maakt het mogelijk pakketten te analyseren op basis van hun network layer-adressen.
  - De network layer matrix-groep (nlMatrix) maakt het mogelijk het verkeer tussen twee hosts te analyseren op basis van hun network layer-adressen.
  - De application layer host-groep (alHost) maakt het mogelijk pakketten te analyseren op basis van hun applicatieadressen.
  - De application layer matrix-groep (alMatrix) maakt het mogelijk het verkeer tussen twee hosts te analyseren op basis van hun applicatieadressen.
  - De user history collection-groep (usrHistory) neemt regelmatig monsters van variabelen op basis van de door de gebruiker aangegeven parameters.
  - De probe configuration-groep (probeConfig) beschrijft alle configuratieparameters van de probe. Omdat de parameters in de MIB-definitie precies zijn vastgelegd, is het gemengd

gebruik van probes van verschillende leveranciers geen probleem.

4 GEBRUIK VAN RMON

Nadat in het vorige hoofdstuk is beschreven welke informatie door RMON verzameld kan worden, beschrijft dit hoofdstuk een aantal voorbeelden hoe de netwerkbeheerder deze informatie kan gebruiken.

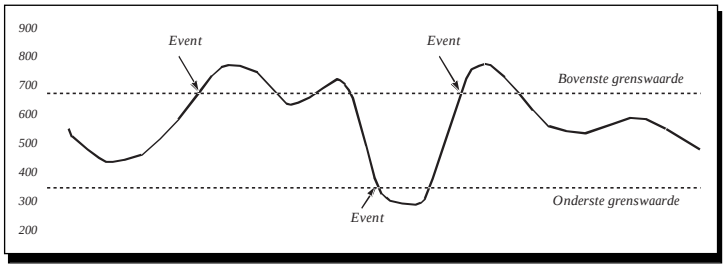
4.1 Oplossen van problemen

De real-time informatie die RMON probes verzamelen kan bijzonder nuttig zijn bij het opsporen van netwerkproblemen. Dit is tegenwoordig des te belangrijker, omdat netwerkbeheerders geen volledige controle meer hebben over alle applicaties die van het netwerk gebruikmaken; medewerkers kunnen immers ook zelf vaak programma's van het internet halen en ze op hun werkstations installeren en draaien. Met RMON kan een beheerder de gebruikers identificeren die de problemen op het netwerk veroorzaken om daarna passende actie te ondernemen. Zo kunnen bijvoorbeeld de aan een specifieke medewerker toegekende resources worden vergroot, of het gebruik van een applicatie worden verboden.
Laten we als voorbeeld aannemen dat uit de statistics-groep van de RMON MIB blijkt dat er veel pakketten worden verstuurd met een te korte lengte. Dergelijke informatie duidt in het algemeen op een hardwarefout. Dankzij RMON is het eenvoudig de bron van de te korte pakketten op te sporen; voor dit doel kan de host alsmede de hostTopN-groep van RMON MIB worden gebruikt. De host-groep wordt continu bijgehouden door de RMON probe en kan doorzocht worden op systemen die veel fouten veroorzaken. Nog comfortabeler gaat het zoeken door gebruik te maken van de hostTopN-groep van RMON MIB: de netwerkbeheerder kiest als sorteerparameter het aantal fouten, waarna de probe een tabel opbouwt met daarin de systemen die de meeste fouten genereren bovenaan.
Ook bij overbelasting van het netwerk kunnen de host- en hostTopN-groep goede diensten bewijzen. In dit geval moet als sorteerparameter van de hostTopN-groep het aantal verstuurde bytes worden gekozen. Een aardig voorbeeld deed zich voor tijdens de World Cup-wedstrijden die in 1998 in Frankrijk werden gehouden. Het netwerkmanagementteam werd plotseling geconfronteerd met een overbelasting van het netwerk. Door gebruik te maken van RMON, kon de veroorzaker van het probleem snel opgespoord worden: een gebruiker was bezig grote CAD-bestanden over het LAN te versturen en creëerde zo een flessenhals.

4.2 Voorkomen van problemen

Als proactief beheerinstrument kan RMON de netwerkbeheerder in een vroeg stadium waarschuwen voor mogelijke problemen.

Voor dit doel kan de manager de alarm- en event-groepen van de RMON MIB gebruiken.
Beschouw als voorbeeldprobleem de overbelasting van een bepaald LAN-segment. Overbelasting treedt op als het aantal per tijdseenheid verstuurde pakketten een bepaalde grenswaarde overschrijdt. Een variabele die het totaal aantal verstuurde pakketten telt, wordt bijgehouden door de statistics-groep van de RMON MIB. De manager kan de actuele belasting bepalen door deze variabele periodiek uit te lezen en het verschil te bepalen sinds de vorige meting. Voor het periodiek uitlezen kan de manager gebruikmaken van SNMP (deze methode wordt ook wel 'pollen' genoemd); de berekeningen kunnen dan door het managementsysteem worden uitgevoerd. Aan deze methode kleven echter wat nadelen: pollen genereert extra netwerkverkeer en het managementstation wordt extra belast. Het is daarom beter een andere methode te kiezen en gebruik te maken van de alarm-groep van de RMON MIB. Hiertoe vult de manager in een tabel van de alarm-groep de *object identifier* in van de variabele die bewaakt moet worden; in dit geval de variabele van de statistics-groep die het aantal verstuurde pakketten telt. Daarnaast vult de manager in de tabel de grenswaarde in, alsmede hoe frequent de variabele van de statistics-groep bemonsterd moet worden (de bemonsteringsfrequentie). Ook geeft de manager aan dat hij niet geïnteresseerd is in de absolute waarde van de variabele, maar in de verandering (delta) sinds het vorige monster. Nadat de RMON MIB op deze wijze is geconfigureerd, zal de RMON probe zelfstandig de netwerkbelasting bewaken en een gebeurtenis (event) opwekken als de grenswaarde wordt overschreden.



FIGUUR 4
EEN EVENT TREEDT OP ALS DE GRENSWAARDE WORDT OVERSCHREDEN

Indien de manager geïnformeerd wil worden over het optreden van de gebeurtenis, moet hij ook de event-groep configureren. In de event-tabel wordt hiertoe aangegeven om welk event het gaat, en dat de manager door middel van een speciaal bericht, een zogeheten trap, geïnformeerd wil worden. In de event-tabel kan daarnaast worden aangegeven dat de gebeurtenis in een logtabel moet worden opgeslagen.
De alarm-groep kan in principe iedere variabele binnen de RMON MIB, dus in principe alle informatie die in de probe is opgeslagen,

monitoren. Ook is het mogelijk meerdere variabelen gelijktijdig te monitoren. Hierdoor kan de manager ook worden geïnformeerd indien andere gebeurtenissen optreden, zoals bijvoorbeeld een te groot aantal fouten of bijvoorbeeld een te lage netwerkbelasting. Voor iedere gebeurtenis moet apart worden bepaald of er een trap moet worden verstuurd en of de gebeurtenis moet worden gelogd. RMON staat echter niet toe meerdere gebeurtenissen te combineren tot een enkele gebeurtenis; iedere gebeurtenis staat op zichzelf en genereert een eigen trap-bericht en / of entry in de logtabel.

4.3 Prestatiebeheer

Als reactief beheerinstrument kan RMON gedurende een bepaalde periode worden ingezet voor het verzamelen van informatie omtrent de netwerkbelasting. De netwerkbeheerder kan op basis van deze informatie bijvoorbeeld besluiten het netwerk te herconfigureren in een poging de belasting gelijkmatiger te verdelen. Ook kan de manager besluiten de capaciteit van het netwerk te vergroten. Beschouw als voorbeeld een bedrijf dat op een LAN een aantal servers en eindsystemen heeft aangesloten. Het bedrijf groeit en op een gegeven moment moet een aantal extra eindsystemen worden gekocht. Om de belasting laag te houden wordt besloten deze nieuwe systemen op een apart segment aan te sluiten dat via een bridge aan het oorspronkelijke LAN wordt gekoppeld. Alhoewel initieel alles naar wens verloopt, blijkt na verloop van tijd dat een aantal gebruikers klagen over slechte responsetijden van de servers. De netwerkbeheerder kan nu RMON inzetten om de bezettingsgraad van ieder LAN-segment te bepalen. Hiertoe kan bijvoorbeeld de history-groep worden gebruikt; de netwerkbeheerder vertelt de probe welke LAN-segmenten moeten worden bewaakt, hoe hoog de bemonsteringsfrequentie is, hoeveel samples moeten worden opgeslagen enzovoort. Na enige tijd zal de probe zo veel informatie hebben verzameld dat de netwerkbeheerder zich een goed beeld kan vormen betreffende de netwerkbelasting van ieder segment. Indien blijkt dat een bepaald segment wordt overbelast, dan kan de netwerkbeheerder besluiten een aantal systemen te verplaatsen naar een nieuw te creëren segment. Ook dat segment kan weer via een bridge op de rest van het netwerk worden aangesloten. Het is echter ook mogelijk dat uit de gegevens van de history-groep blijkt dat geen enkel LAN-segment wordt overbelast. In dat geval kan de netwerkbeheerder verder gaan met het analyseren van gegevens die door de matrix-groep zijn verzameld. De gegevens uit deze groep kunnen worden gebruikt om te bepalen welke eindsystemen het meest gebruikmaken van welke servers. Als de eindsystemen die het meest gebruikmaken van een server die server moeten bereiken via een bridge, kan het zijn dat de bridge verantwoordelijk is voor de slechte responsetijden. De netwerkbeheerder kan nu besluiten de eindsystemen die het meest gebruikmaken van een be-

paalde server op hetzelfde segment aan te sluiten als die server. Hiertoe kan het nodig zijn eindsystemen of servers te verplaatsen.

4.4 Accounting

In veel organisaties wil men de kosten van het netwerkgebruik doorberekenen aan individuele medewerkers of afdelingen. Ook de hiervoor benodigde informatie kan door RMON worden verzameld.

In de meest eenvoudige vorm krijgt iedere medewerker een rekening voor de hoeveelheid verkeer die is verstuurd dan wel ontvangen. Om te bepalen hoeveel iemand heeft verstuurd dan wel ontvangen, kunnen de gegevens uit de host-groep worden gebruikt.

In het geval van RMON2 zijn er wat meer mogelijkheden. Ten eerste kunnen in plaats van de gegevens uit de host-groep de gegevens uit de nlHost-groep worden gebruikt. Hierdoor wordt niet langer het datalinkverkeer maar het netwerklaagverkeer gemeten. Door zowel het aantal octetten als ook het aantal berichten te meten, is het mogelijk de hoeveelheid gebruikersdata veel nauwkeuriger te bepalen. Door te meten op netwerklaagniveau, kan in een aantal gevallen het aantal benodigde probes ook lager uitvallen dan bij RMON1, waar men immers op ieder LAN-segment een eigen probe moet aansluiten.

In het geval van RMON2 is het ook mogelijk op applicatieniveau te meten. Het wordt hierdoor mogelijk voor verschillende diensten verschillende prijzen te vragen. E-mail kan bijvoorbeeld goedkoper worden aangeboden dan streaming video. De gegevens om gedifferentieerde rekeningen op te stellen worden door een RMON2 probe verzameld in de alhost-groep.

4.5 Beveiliging

RMON kan ook worden gebruikt om mogelijke aanvallen op het netwerk te detecteren. Omdat er verschillende soorten aanvallen bestaan, zijn er ook meerdere manieren om een aanval te detecteren. Stel dat een server door een beperkt aantal eindsystemen mag worden gebruikt. Door informatie te analyseren die is opgeslagen in de (nl)matrix-groep, kan eenvoudig gedetecteerd worden of de server ook door andere systemen wordt benaderd. Uit de informatie in de (nl)matrix-groep kan ook blijken dat één systeem contact zoekt met alle andere systemen. Als dit systeem geen bekende server is, is er waarschijnlijk sprake van een aanval. Bij een denial of service-aanval worden meestal door een beperkt aantal externe systemen veel korte pakketten verstuurd naar een enkele server. Uit de nlHosts-groep kan eenvoudig bepaald worden welke externe systemen een dergelijk verdacht verkeerspatroon genereren. Ook kan er bij een aanval sprake zijn van specifieke data in bepaalde pakketten. Door gebruik te maken van de filters uit de filter-groep, kan deze specifieke data worden gedetecteerd. Uiteraard kunnen de alarm-en event-groep ook in dit geval worden gebruikt voor het opslaan van

de gebeurtenissen en het versturen van trap-berichten naar de manager.

5 PRODUCTEN

De huidige RMON-producten worden meestal als probes en specifieke managersoftware geleverd. Voor de probes bestaan er echter ook goedkopere softwareoplossingen, die gebruikmaken van standaard pc's. Sommige leveranciers van hubs, switches en routers voegen RMON-functionaliteit toe aan hun producten. De meeste bekende fabrikanten, waaronder Cisco, Enterasys, Hewlett Packard, IBM en 3COM, bieden tegenwoordig RMON-producten aan.
Het is belangrijk dat de informatie die door de probes wordt verzameld correct is en dat er, ook bij hoge belasting van de probe, geen gegevens verloren gaan. Verkeerde informatie kan immers tot verkeerde conclusies leiden waardoor de problemen verergeren. Normale kopers kunnen echter onmogelijk de kwaliteit van individuele probes onderzoeken en moeten daarom bij de aanschaf vertrouwen op externe informatie. Een van de groepen die onderzoek heeft gedaan naar de kwaliteit van RMON-producten is de Syracuse University. In hun onderzoek werd ontdekt dat er problemen kunnen optreden indien de probes en de managersoftware geleverd zijn door verschillende fabrikanten. Ook traden er problemen op in het geval meerdere managers dezelfde probe probeerden te gebruiken. Wanneer RMON-functionaliteit is toegevoegd aan bestaande hubs, switches of routers, kunnen er problemen optreden in combinatie met andere managementfuncties.

5.1 Kosten

De programmatuur voor een RMON probe kan op een eigen machine draaien, of op een machine waarop ook andere software draait. De keuze is hierbij uiteraard een keuze tussen kosten en prestaties.
Indien de RMON-programmatuur op een eigen machine draait, zijn de kosten uiteraard hoger dan bij het gebruik op een non-dedicated machine, maar de prestaties zijn aanmerkelijk beter. In een drukbezet netwerk is het beslist nodig een dedicated machine te gebruiken, wil de probe het netwerkverkeer kunnen bijhouden. Dit is zeker het geval indien de volledige functionaliteit van RMON2 ondersteund moet worden. Dedicated systemen kosten vanaf een paar duizend euro tot meer dan tienduizend euro. Ze maken vaak gebruik van gemodificeerde pc-hardware. Sommige leveranciers hebben multiport probes die kunnen worden aangesloten op meerdere segmenten van het netwerk; in dit geval zijn er minder probes nodig en kunnen de kosten worden gedrukt.
In een minder druk bezet netwerk is het gebruik van een non-dedicated machine, die naast RMON ook andere programma's draait, meestal voldoende. De RMON-software kan geïnstalleerd worden

op bestaande pc's of workstations, de kosten beginnen bij een paar honderd euro. Ook zijn er veel hubs, switches en routers die door de fabrikanten reeds van RMON-programmatuur zijn voorzien. Dergelijke voorzieningen krijgt de gebruiker bijna voor niets.

LITERATUUR

Bekkers, Rudi, 'Kiezen of delen, Acht aspecten bij de selectie van een mobiel datacommunicatiesysteem', in: *Telecommagazine*, september 1996, pag. 16-21.

Bekkers, Rudi en Smits, Jan, *Mobiele Telecommunicatie: Standaarden, regulering en toepassingen*, Kluwer / Segment, Deventer, 1997.

Bekkers, Rudi en Smits, Jan, *Mobiele Telecommunicatie: Europese netwerken*, Kluwer / Segment, Deventer, 1997.

Bouman, Wim e.a., *Business Reengineering, Een onderzoek naar het regisseren van complexe organisatieverandering*, Associatie Business Engineers / Universiteit van Amsterdam, 1995.

Eekeren, Patrick van, 'Ondernemen met mobiele communicatie', in: *Tijdschrift Management & Informatie*, september 1996, pag. 4-12.

Hammer, Michael en Mangurain, Glenn, 'The changing value of communications technology', in: *Sloan Management Review*, winter 1987, pag. 65- 71.

NOTEN

1 http: / / www.auckland.ac.nz / net / NeTraMet

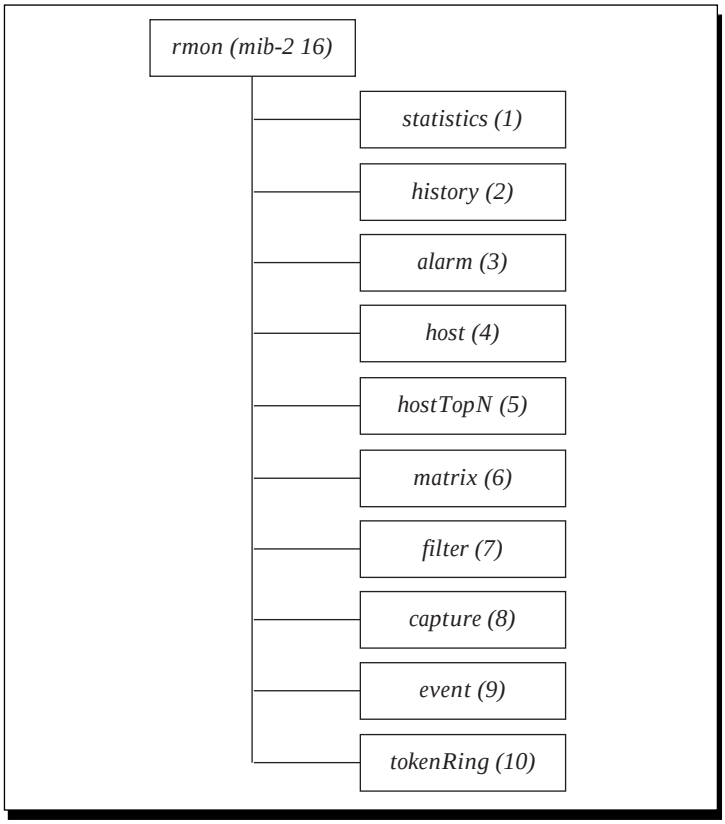
OVER DE AUTEURS

Aiko Pras is Senior researcher bij het Centrum voor Telematica en Informatie Technologie (CTIT) aan de Universiteit Twente. Paul Alexander en Peter Christian zijn studenten van de internationale Telematica masters opleiding, eveneens aan de Universiteit Twente.

4.5.2.a APPENDIX 1: Gedetailleerd overzicht van de RMON1 MIB

De oorspronkelijke RMON MIB version 1 is beschreven in RFC 2819. Deze MIB heeft de status van 'full standard' en definieert negen groepen. Deze groepen zijn bedoeld voor Ethernet LANs, alhoewel sommige onderdelen ook gebruikt kunnen worden voor andere type LANs. Voor tokenRing LANs is er een tiende groep gedefinieerd in RFC 1513; deze RFC heeft de status 'proposed standard'.

Figuur 5 laat de tien RMON-groepen zien met tussen haakjes hun object identifiers (OID's). De meeste van deze groepen zijn opgebouwd uit een tabel, in sommige gevallen ondersteund door één of meerdere controletabellen. Omdat voor ieder LAN-segment waarop de probe is aangesloten een aparte rij in de tabel wordt bijgehouden, komt de diepte van de tabel (het aantal rijen) overeen met het aantal aangesloten LAN-segmenten.



FIGUUR 5
GROEPEN VAN RMON MIB VERSION 1

Beschrijving van de groepen:

1. Statistics-groep (*statistics)*
   De *statistics*-groep houdt een aantal tellers bij voor het verkeer op datalink-niveau. Ieder LAN-segment waarop de probe is aangesloten heeft zijn eigen tellers. De tellers betreffen het aantal over het segment verstuurde data-octets, het aantal packets (opgesplitst in unicast, multicast en broadcast packets), de best mogelijke schatting van het totaal aantal botsingen (collisions), alsmede overige fouten (CRC-fouten, packets kleiner dan 64 bytes maar ook packets groter dan 1518 bytes).

   In de *statistics*-groep wordt naast het aantal verstuurde packets de afmetingen van deze packets (packet size distribution) bijgehouden. Hiertoe zijn een zestal tellers gedefinieerd: een teller voor het aantal packets met een lengte van 64 octetten (de kleinst mogelijke lengte), een teller voor lengtes tussen 65 en 127 octetten, een teller voor lengtes tussen 128 en 255 octetten, een teller voor lengtes tussen 256 en 511 octetten, een teller voor lengtes tussen 512 en 1023 octetten en tenslotte een teller voor lengtes tussen 1024 en 1518 octetten (de grootst mogelijke lengte).

2. History-groep *(history)*
   De *history*-groep wordt gebruikt voor tijdelijk opslaan van gegevens uit de *statistics*-groep. Alle tellers worden opgeslagen, behalve die betrekking hebben op de packet size distribution. Gegevens worden opgeslagen in een circulaire buffer (de *etherHistoryTable*), waarvan de grootte kan worden aangepast via de *historyControlTable*. Via deze laatste tabel kan ook het LAN-segment dat bemonsterd wordt alsmede de bemonsteringsfrequentie worden aangepast.
   Als de manager geen aanpassingen aanbrengt in de *historyControlTable*, zal een default bemonsteringsfrequentie van één monster per half uur en een default aantal buffer elementen van vijftig worden gekozen. Deze default-waarden voldoen goed als de circulaire buffer eens per dag wordt uitgelezen. Om achteraf te kunnen bepalen wanneer een bepaald element in de circulaire buffer is opgeslagen, wordt de waarde van *sysUpTime* aan ieder element toegevoegd.

3. Alarm-groep (*alarm*)
   De *alarm*-groep wordt gebruikt voor het monitoren van één of meer tellers binnen de RMON-probe. Als een teller een bepaalde grenswaarden overschrijdt, genereert de *alarm*-groep een event (de afhandeling van dit event wordt bepaald door de *event*-groep). Als voorbeeld kan gedacht worden aan het opwekken van een event indien het aantal CRC-fouten (welke geteld worden in de *statistics*-groep) hoger is dan honderd gedu-

rende één minuut. De *alarm*-groep bevat één tabel, de *alarmTable*. Deze tabel omvat onder andere het interval, in seconden, gedurende welke de data wordt bemonsterd en vergeleken met een grenswaarde, de bovengrens (die een teller in de RMON MIB niet mag overschrijden), de ondergrens (die een teller in RMON MIB niet mag onderschrijden), enzovoort.

4. Host-groep (*host*)
   De *host*-groep verzamelt statistieken voor elk systeem (host) dat op het LAN is aangesloten. Om te bepalen welke systemen dit zijn, onderschept de RMON probe elk verstuurd bericht en haalt hieruit het MAC-adres van de bron. Op deze manier kan de probe niet alleen alle actieve systemen ontdekken, maar ook statistische gegevens verzamelen. De *host*-groep omvat drie tabellen: *hostControlTable*, *hostTable*, en *hostTimeTable*.
   De *hostControlTable* legt onder andere het maximum aantal systemen vast waarvoor gegevens worden bijgehouden; dit aantal is gelijk aan de diepte (aantal rijen) van de *hostTable* en *hostTimeTable*.
   De *hostTable* bevat voor ieder systeem een aparte rij. Een rij bevat onder andere het MAC-adres van het systeem, het aantal packets en octetten dat is verzonden / ontvangen, het aantal verzonden packets met een fout, het aantal verzonden multicast en het aantal verzonden broadcast packets. De *hostTimeTable* bevat vergelijkbare informatie als de *hostTable*, maar nu gesorteerd op tijd, in plaats van de MAC-adres.

5. HostTopN-groep (*hostTopN*)
   De *hostTopN*-groep houdt de statistieken bij van een groep hosts die bovenaan staan wat betreft bepaalde parameters, bijvoorbeeld de tien hosts die de meeste foute berichten verzenden. De gegevens in deze groep worden afgeleid van de bovenbesproken *host*-groep. De *hostTopN*-groep bestaat uit twee tabellen: *hostTopNControlTable* en *hostTopNTable*.
   Via de *hostTopNControlTable* kunnen onder andere de parameters voor het bepalen van de rangorde worden vastgelegd. Een voorbeeld van een mogelijke parameter is het aantal verstuurde packets met een fout. Verder kan met de hostTopNTable het interval waarover wordt gemeten, het maximaal aantal te beschouwen hosts, enzovoort worden gemeten.
   De *hostTopNTable* houdt wederom per systeem een aparte rij bij. Een rij bevat naast het MAC-adres van het systeem ook de waarde van de parameter die de rangorde bepaalt.

6. Matrix-groep (*matrix*)
   De *matrix*-groep wordt gebruikt voor het bijhouden van het verkeer tussen hostparen in een subnetwerk. De gegevens kunnen bijvoorbeeld worden gebruikt om te bepalen welke host een an-

dere host heeft overspoeld met packets. De groep bestaat uit één controle tabel, *matrixControlTable*, en twee data tabellen, *matrixSDTable* en *matrixDSTable*. De *matrixSDTable* omvat de bron en bestemmings MAC-adressen, het aantal verzonden packets van de bron naar de bestemming, het aantal octetten alsmede het aantal berichten met een fout. De *matrixDSTable* bevat identieke informatie, maar is gesorteerd op volgorde van bestemmings- en daarna bronadres.

7. Filter-groep (*filter*)
   De *filter*-groep wordt door de manager gebruikt om de probe in te stellen op het vinden van packets die aan specifieke voorwaarden voldoen. Er zijn twee soorten filters: datafilters die een bitpatroon met een deel van de data vergelijken en statusfilters die werken op basis van de status van de packets: valid, CRC error, enzovoort. Een stroom packets die door het filter gaat, hierna *kanaal* genoemd, kan een gebeurtenis initiëren (ingesteld in de *event*-groep) en / of afgevangen worden (ingesteld in de *capture*-groep; zie ook figuur 3). De filterlogica, kanaaldefinitie en werking van de kanalen worden beschreven met programma-achtige if-then-else statements, boolse logica, enzovoort.
   Deze groep omvat twee tabellen: *filterTable* en *channelTable*. De *filterTable* omvat onder andere het kanaal waar het filter op wordt toegepast, en de data of status waarop wordt gefilterd, enzovoort. De *channelTable* omvat onder andere de gebeurtenissen om kanalen in en uit te schakelen, het aantal packets dat overeenkomt met een event, enzovoort.

8. Capture-groep (*capture*)
   De *capture*-groep wordt gebruikt voor het bufferen van packets die zijn afgevangen uit één van de kanalen van de *filter*-groep.
   De *capture*-groep bevat een data-tabel, *captureBufferTable*, en een controle-tabel, *bufferControlTable*.
   De data-tabel beschrijft onder andere de volgorde waarin en het tijdstip waarop packets zijn afgevangen, de inhoud van het packet dan wel een deel daarvan, de lengte van het packet of het deel dat is opgeslagen, de eventuele foutstatus van het packet, enzovoort.
   De controle-tabel wordt door de manager gebruikt om de capture-logica in te stellen. Deze tabel bepaalt onder andere uit welke kanalen packets moeten worden afgevangen, de status van de buffers (vol of ruimte beschikbaar), enzovoort.

9. Event-groep (*event*)
   De *event*-groep bepaalt wat er moet gebeuren nadat:
   – de *alarm*-groep een alarm heeft afgegeven;
   – de *filter*-groep een specifiek bitpatroon heeft gedetecteerd;

– de *filter*-groep een bepaalde conditie heeft gedetecteerd (bijvoorbeeld een packet met een fout).

Mogelijke acties die de *event*-groep kan initiëren zijn het versturen van een SNMP-trapbericht en / of het vastleggen van de gebeurtenis in een logTabel. De *eventTable* beschrijft voor ieder soort gebeurtenis welke van deze acties moet worden uitgevoerd. Voor het vastleggen van gebeurtenissen wordt de *logTable* gebruikt; deze tabel omvat onder andere een unieke identificatie van de logentry, de waarde van *sysUpTime* ten tijde van het maken van de logentry, logbeschrijving, enzovoort.

10. TokenRing-groep (*tokenRing*)
    De *tokenRing*-groep (gedefinieerd in RFC 1513) bevat een aantal tabellen voor het monitoren van tokenRing-subnetwerken. De *ringStationTable* bevat statusinformatie en statistieken voor elk station op de ring. De *ringStationOrdertable* beschrijft de volgorde van de stations in de ring. De *ringStationConfigTable* wordt gebruikt voor het configureren of zelfs verwijderen van stations uit de ring. Ook is er een *sourceRoutingStatsTable* waarin routeringsinformatie kan worden opgeslagen.