Protocollen voor netwerk management

Deel 2: SNMP, NMF en CMOL

Aiko Pras
Vakgroep Tele-Informatica en Open Systemen
Faculteit Informatica
Universiteit Twente
email: pras@cs.utwente.nl

In een vorig artikel is de ontwikkeling van OSI en TMN management besproken. Dit tweede artikel gaat in op de management protocollen die ontwikkeld zijn voor de Internet wereld, het Network Management Forum (NMF) en de IEEE.

SNMP

In de tweede helft van de jaren tachtig concludeerde de IETF (Internet Engineering Task Force, de organisatie die verantwoordelijk is voor de ontwikkeling van de internet protocollen) dat het snel groeiende Internet niet meer op ad-hoc basis gemanaged kon worden. Na enige discussie werd besloten gebruik te gaan maken van OSI's CMIP. Om dit protocol te kunnen toepassen in het op TCP/IP gebaseerde Internet, waren een aantal kleine aanpassingen nodig. Het resultaat van deze aanpassingen kreeg de naam CMOT (Common Management Over TCP/IP).
Zoals eerder besproken koste de ontwikkeling van OSI management veel tijd. Omdat de IETF niet werkloos wilde toezien totdat deze ontwikkeling eindelijk tot resultaat zou leiden, werd besloten het reeds bestaande SGMP (Simple Gateway Monitoring Protocol) verder te ontwikkelen en op korte termijn te gebruiken als noodoplossing. Het was de bedoeling na verloop van tijd deze oplossing te vervangen door een structurele oplossing op basis van OSI.

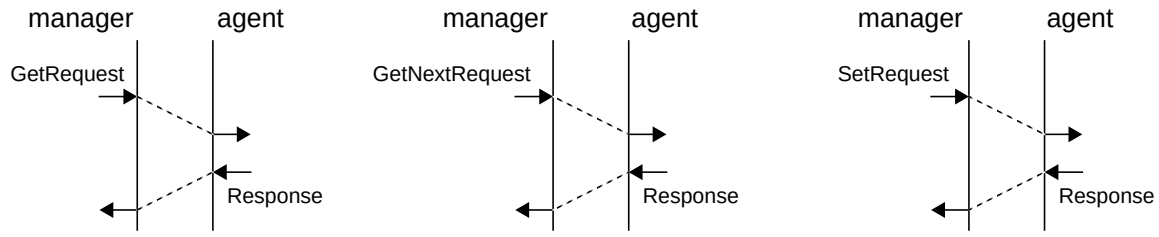
Het op basis van SGMP ontwikkelde management protocol kreeg de naam SNMP (Simple Network Management Protocol) en voldeed aan de volgende criteria:
- SNMP is in principe geschikt om *alle* op het Internet aangesloten systemen te managen.
- De kosten om SNMP te implementeren zijn minimaal.
- Door nieuwe 'managed objects' te definiëren, kunnen de management mogelijkheden relatief eenvoudig vergoot worden.
- SNMP is robuust; zelfs in geval van storingen kan de manager verder werken (alhoewel hiervoor misschien wat meer moeite nodig is).

Achteraf beschouwd was SNMP de juiste oplossing op het juiste moment. Binnen enkele jaren bleek het inderdaad mogelijk het merendeel van de op het Internet aangesloten apparatuur via SNMP te beheren. Tegenwoordig bouwen fabrikanten van datacommunicatie apparatuur SNMP standaard in en is dit protocol uitgegroeid tot de belangrijkste norm voor netwerk management.

Het overweldigende succes van SNMP was door niemand voorzien, zelfs niet door de IETF. In het licht van dit succes werd het oorspronkelijke plan om SNMP op termijn te vervangen door CMOT in 1992 dan ook verlaten. Op dit moment lijkt het onwaarschijnlijk dat OSI ooit nog gebruikt gaat worden voor het managen van TCP/IP netwerken. Het is eerder zo dat SNMP's positie steeds sterker wordt, wat blijkt uit de toenemende toepassing van dit protocol in netwerken die niet op TCP/IP zijn gebaseerd. Voorbeelden hiervan zijn Novell's Netware en ATM.

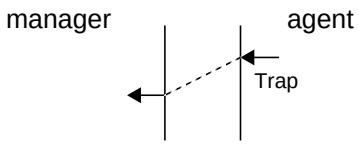
SNMP operaties

Bij SNMP ligt het initiatief om management gegevens te versturen meestal bij de manager. Om bepaalde informatie te verkrijgen, zal de manager een *'GetRequest'* of *'GetNextRequest'* naar de agent sturen (Figuur 1). De gevraagde informatie zal vervolgens door de agent als onderdeel van de *'Response'* worden teruggestuurd. Indien de manager informatie in de agent wil veranderen, zal een 'SetRequest' worden verstuurd. Om eventuele fouten te kunnen terugmelden, zal ook in dit geval de agent met een 'Response' reageren.



Figuur 1: Manager neemt het initiatief

In uitzonderingsgevallen kan ook de agent het initiatief om gegevens te versturen nemen. Hiertoe verstuurt de agent een 'Trap' (Figuur 2), die in tegenstelling tot de vorige operaties door de ontvanger niet wordt bevestigd. Voorbeelden van uitzonderingsgevallen zijn het actief worden van nieuwe systemen, het resetten van systemen en het uitvallen van verbindingen tussen systemen.



Figuur 2: Agent neemt het initiatief

Een belangrijke eigenschap van SNMP is dat de berichten die tussen manager en agent worden uitgewisseld verloren kunnen gaan. Alhoewel dit in eerste instantie een ongewenste eigenschap lijkt, hebben de ontwerpers toch bewust hiervoor gekozen. Om de informatieuitwisseling betrouwbaar te maken, hadden ze namelijk gebruik moeten maken van protocol functies die op zich weer bij bepaalde netwerk problemen kwetsbaar zijn. Zo zouden er bijvoorbeeld functies moeten komen die de opbouw van een verbinding tussen manager en agent verzorgen. Indien het netwerk overbelast wordt, kan een dergelijke verbinding echter verbroken worden. De overbelasting kan er vervolgens voor zorgen dat een nieuwe managementverbinding niet meer kan worden opgebouwd. Het resultaat is dat de manager niet meer met de agent kan communiceren en dat effectief management onmogelijk wordt.
Om dergelijk problemen te voorkomen, hebben de ontwerpers van SNMP bewust gekozen voor een aanpak waarbij de manager zelf verantwoordelijk is voor het opnieuw versturen van een management bericht indien het eerdere bericht verloren is gegaan. Bericht verlies kan door de manager gedetecteerd worden door te controleren of de *Response* op het eerdere bericht wel tijdig is ontvangen.

SNMPv2

Vanaf het moment dat de SNMP protocol norm was vastgelegd, zijn er meerdere voorstellen tot verbetering verschenen. In 1992 heeft de IETF een aantal van deze voorstellen samengenomen en begon de ontwikkeling van een nieuwe versie van deze norm: SNMP versie 2 (SNMPv2). In

vergelijking tot de originele versie van SNMP, zou deze nieuwe versie de volgende mogelijkheden moeten bieden:
- management informatie op efficiëntere wijze te vervoeren (dankzij de nieuwe *'GetBulk'* operatie)
- management te beveiligen (via authenticatie,versluiering en toegangscontrole per object),
- een hiërarchie van managers te bouwen (met behulp van de Manager-to-Manager MIB).

Daarnaast zou SNMPv2 nog een groot aantal kleinere verbeteringen moeten bevatten.

In 1993 werd SNMPv2 'Proposed Standard'. Ondertussen waren meerdere onderzoeksgroepen (waaronder één van de Universiteit Twente) begonnen met de bouw van prototypes. Vrij snel werd duidelijk dat SNMPv2 veel ingewikkelder in elkaar zat dan men oorspronkelijk had aangenomen. Toen de IETF in 1994 de vraag opriep of er voldoende steun was om SNMPv2 tot 'Draft Standard' te promoveren, kwam er danook een discussie opgang over complexiteit van SNMPv2. De discussie spitste zich toe op het zogeheten administratieve model, waarin beschreven wordt hoe de gegevens die voor de beveiliging van SNMPv2 nodig zijn (zoals 'access control lists' en sleutels voor authenticatie en versluiering) geadministreerd moeten worden. Hiertoe introduceert het model zogeheten 'parties' en 'contexts', grootheden waarvan de identifiers in ieder management bericht meegestuurd moeten worden. In een poging de ontstane impasse te doorbreken, stelden in juni 1995 twee van de vier oorspronkelijke ontwerpers een nieuw administratief model voor.

Ondanks het feit dat dit nieuwe model veel beter te begrijpen is, bleek snelle overeenstemming niet mogelijk. Toen in september 1995 het mandaat van de werkgroep ten einde liep, kon de IETF leiding dan ook niet veel anders besluiten dan alle controversiële punten uit SNMPv2 te verwijderen en verder te gaan vanuit een uitgeklede versie. Deze versie staat bekend onder de naam SNMPv1.5 of SNMPv2t (de 't' slaat op 'transitional') en bevat geen mogelijkheden meer om management te beveiligen of een hiërarchie van manager systemen te bouwen. Het is op dit moment nog niet mogelijk een zinvolle uitspraak te doen over de acceptatie van dit uitgeklede protocol door de markt.

Network Management Forum

In 1988 is het 'OSI Network Management Forum' (NMF) opgericht met het doel de ontwikkeling, acceptatie en implementatie van de OSI management normen te bevorderen. Het Forum wordt gevormd door fabrikanten, netwerk operators en onderzoekslaboratoria en heeft geen winst oogmerk. Reeds snel besloot het Forum zich niet meer tot de OSI management normen te beperken; een gevolg hiervan was dat het voorvoegsel 'OSI' uit de naam verdween.

Onderwerpen waaraan het NMF tevens aandacht ging besteden waren:
- SNMP.
- De 'Distributed Management Environment' (DME) van de 'Open Software Foundation' (OSF).
- De 'Management Protocol API' (XMP) en de 'OSI-Abstract Data Manipulation API' (XOM) van de X/Open groep.
- De 'Common Object Request Broker Architecture' (CORBA) van de 'Object Management Group' (OMG).

Al deze onderwerpen kregen een plaats in het zogeheten OMNI*Point* programma, waarvan het doel was tot normen, specificaties, implementaties, test methoden, test gereedschappen alsmede bibliotheken van managed objects te komen. Buiten de telecom industrie heeft het OMNI*Point*

programma nog maar weinig effect gehad. Redenen waarom OMNIPoint nog niet echt van de grond is gekomen:

- De DME is grotendeels mislukt. Op een belangrijke netwerk management conferentie die begin dit jaar in de VS werd gehouden, werd gesteld dat de DME zich teveel richt op object georiënteerde technieken en te weinig oog heeft voor protocol aspecten. Het tracht met name gedistribueerd management van objecten mogelijk maken, maar beseft onvoldoende dat deze objecten zelf gedistribueerd zijn. Verder probeert het niet compatibele informatie modellen te integreren (één van OSI, één van SNMP en één op CORBA gebaseerd). In feite is DME te ambitieus en maakt teveel gebruik van technieken die in de praktijk hun nut nog niet hebben bewezen.
- XOM is in gebruik te complex. In een aantal implementaties heeft men XOM dan ook al vervangen door andere, niet genormeerde APIs.
- De ontwikkeling van CORBA heeft meer tijd gekost dan verwacht. Het NMF kon daarom het deel van de implementatie dat op CORBA is gebaseerd niet op tijd leveren.

IEEE

Het ‘Institute of Electrical and Electronics Engineers’ (IEEE) is een organisatie van experts die proberen onder andere normen voor elektrotechnische systemen te ontwikkelen. Eén van de belangrijkste wapenfeiten van de IEEE zijn de zogeheten 802 normen, die de toegangsprotocollen voor Local en Metropolitan Area Networks (LANs en MANs) beschrijven. In deze normen wordt echter ook aandacht besteed aan management van LANs en MANs.
De IEEE netwerk management normen vertonen sterke overeenkomst met de OSI management normen. Het belangrijkste verschil is echter dat IEEE voor het vervoer van management informatie gebruik maakt van de data link service, terwijl OSI hiervoor een presentatie service verkiest. Het IEEE management protocol staat bekend onder de naam ‘Common Management over LLC’ (CMOL) en heeft als nadeel dat de manager alleen systemen kan managen die op hetzelfde lokale net zijn aangesloten; het feit dat management informatie wordt verstuurd over een data link service impliceert immers dat routers management informatie niet kunnen doorsturen. In de praktijk blijkt CMOL geen enkele rol van betekenis te spelen.