

Protocol voor netwerk management

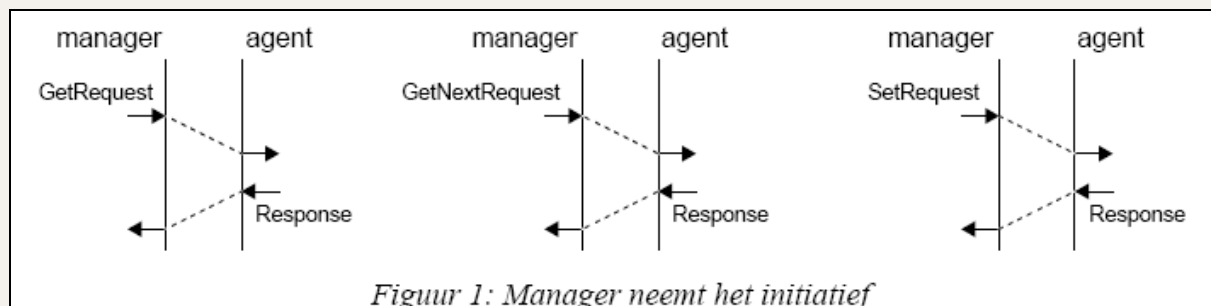
SNMP

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). De ontwikkeling van OSI management kostte 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:

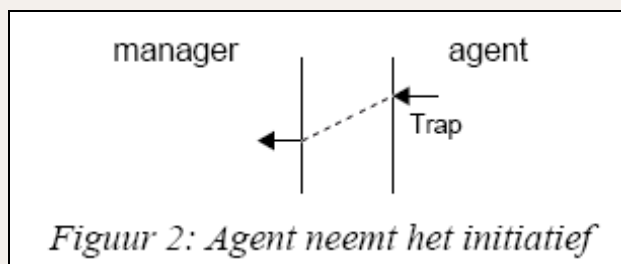
- SNMP is in principe geschikt om *alle* op het Internet aangesloten systemen te managen.
- De kosten om SNMP te implementeren zijn minimaal.
- Door nieuwe 'managed objects' te definiëren, kunnen de management mogelijkheden relatief eenvoudig vergoot worden.
- SNMP is robuust; zelfs in geval van storingen 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.



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.



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 informatie uitwisseling 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 dergelijke 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 dan ook een discussie opgang over complexiteit van SNMPv2. De discussie spitte 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 uitgekledede 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.

De SNMP implementatie in de regelaars

De SNMP implementatie in de regelaars, is een SNMP agent, V2. Deze koppeling kan gebruikt worden om alarmen, (traps) te versturen naar een SNMP manager software. Verder is er een voorziening om een aantal velden van de regelaar op te halen, voor een status overzicht. Dit alles op basis van het SNMP protocol. Deze koppeling werkt standaard op UDP poort 161, en UDP poort 162.

In het option scherm, onder configuratie, moet de SNMP vrijgegeven worden, om deze software te activeren. Verder moeten er een aantal parameters ingesteld worden in het provider scherm. Namelijk het IP nummer van de SNMP server, community string : "brcontrol", de vink box voor system traps. (aanzetten van de regelaar). Men kan hier ook kiezen voor een watchdog trap, die in verschillende tijdsspannen verstuurd wordt. Tevens bevinden zich hier de optie's voor het herhaald versturen van een alarm, en het versturen van een aparte trap als alle alarmen zijn opgeven.

In Rstree 3.2.2 en hoger, verschijnt er, na vrijgave van de SNMP, een extra icoon bij de regelaar overzicht. Als men hierop dubbelklikt, verschijnt er het overzicht scherm, van de traps die gedetecteerd en verstuurd zijn. Het ophalen van dit scherm gebeurt op basis van 5S, en duurt dus voor de eerste keer een poosje, en kan versneld worden met de knop reload !!!!! Het tweede tapblad heeft de instellingen voor elke trap, hoe en wanneer hij verstuurd wordt. In dit scherm stel je het alarmnummer in die de trigger gaat geven. (Is dus gekoppeld aan de ALARM server !!!!!)

De volgende MID en OID velden worden door de SNMP ondersteund: (dit nummer is wereldwijd geregistreerd);

1.3.6.1.4.1.30668.1.1.1 -> Cabinet Name
1.3.6.1.4.1.30668.1.1.2 -> Cabinet Nr
1.3.6.1.4.1.30668.1.1.3 -> BHCP ID
1.3.6.1.4.1.30668.1.1.4 -> Terminal Type
1.3.6.1.4.1.30668.1.1.5 -> Alarm 1
1.3.6.1.4.1.30668.1.1.6 -> Alarm 2
1.3.6.1.4.1.30668.1.1.7 -> Alarm 3
1.3.6.1.4.1.30668.1.1.8 -> Alarm 4
1.3.6.1.4.1.30668.1.1.9 -> Alarm 5
1.3.6.1.4.1.30668.1.1.10 -> Alarm 6
1.3.6.1.4.1.30668.1.1.11 -> Alarm 7
1.3.6.1.4.1.30668.1.1.12 -> Alarm 8
1.3.6.1.4.1.30668.1.1.13 -> Alarm 9
1.3.6.1.4.1.30668.1.1.14 -> Alarm 11
1.3.6.1.4.1.30668.1.1.15 -> Alarm 11
1.3.6.1.4.1.30668.1.1.16 -> Alarm 12
1.3.6.1.4.1.30668.1.1.17 -> Alarm 13
1.3.6.1.4.1.30668.1.1.18 -> Alarm 14
1.3.6.1.4.1.30668.1.1.19 -> Alarm 15
1.3.6.1.4.1.30668.1.1.20 -> Alarm 16
1.3.6.1.4.1.30668.1.1.21 -> Alarm 17
1.3.6.1.4.1.30668.1.1.22 -> Alarm 18
1.3.6.1.4.1.30668.1.1.23 -> Alarm 19
1.3.6.1.4.1.30668.1.1.24 -> Alarm 20
1.3.6.1.4.1.30668.1.1.25 -> Alarm 21
1.3.6.1.4.1.30668.1.1.26 -> Alarm 22
1.3.6.1.4.1.30668.1.1.27 -> Alarm 23
1.3.6.1.4.1.30668.1.1.28 -> Alarm 24
1.3.6.1.4.1.30668.1.1.29 -> Alarm 25
1.3.6.1.4.1.30668.1.1.30 -> Alarm 26
1.3.6.1.4.1.30668.1.1.31 -> Alarm 27

SNMP protocol aanwezig in de BRControls regelaars

1.3.6.1.4.1.30668.1.1.32 -> Alarm 28
1.3.6.1.4.1.30668.1.1.33 -> Alarm 29
1.3.6.1.4.1.30668.1.1.34 -> Alarm 30
1.3.6.1.4.1.30668.1.1.35 -> Alarm 31
1.3.6.1.4.1.30668.1.1.36 -> Alarm 32
1.3.6.1.4.1.30668.1.1.37 -> Cpu Usage

1.3.6.1.4.1.30668.1.2.37 -> Alarm Trap
1.3.6.1.4.1.30668.1.2.38 -> Alarm ID
1.3.6.1.4.1.30668.1.2.39 -> Alarm Serverity
1.3.6.1.4.1.30668.1.2.40 -> Alarm Text
1.3.6.1.4.1.30668.1.2.41 -> WatchDog Trap
1.3.6.1.4.1.30668.1.2.42 -> All Alarms Cleared Trap

Trap Field collected in a Packet

1.3.6.1.4.1.30668.1.2.37 -> Alarm Trap	
1.3.6.1.2.1.6.13.1.2 -> Ip Address	
1.3.6.1.4.1.30668.1.2.38 -> Alarm ID	Integer
1.3.6.1.4.1.30668.1.2.39 -> Alarm Serverity	Integer
1.3.6.1.4.1.30668.1.2.2 -> Cabinet Nr	Integer
1.3.6.1.4.1.30668.1.2.40 -> Alarm Text	String
1.3.6.1.4.1.30668.1.2.1 -> Cabinet Name	String

De functies kunnen uitgebreid worden door bijvoorbeeld trending, informeer naar de mogelijkheden.