

SCHNELLES NETZWERK-MONITORING

Gibt es eine Alternative zu SNMP?

Warum sollte jemand angesichts klar dominierender Standards im Bereich Netzwerk-Monitoring auf den Gedanken kommen, nach einer Alternative für die Überwachung und Verwaltung von LANs und WANs zu suchen?

Obwohl nicht für den klassischen Markt der Applikationen erdacht, hat das Simple-Network-Management-Protokoll (SNMP) zweifelsfrei eine Traumkarriere hinter sich. Neben HTTP, Telnet oder FTP erreichte kaum ein anderes Protokoll innerhalb der "IP-Familie" eine vergleichbare Popularität wie SNMP. In kürzester Zeit faszinierte die in Aussicht gestellte Vision, selbst große heterogene Netzwerke auf einer zentralen Managementplattform administrieren zu können, ganze Heerscharen von IT-Verantwortlichen. Hersteller begannen damit, zumindest teilweise über den eigenen Tellerrand

hinweg zu schauen und fanden es überaus angenehm, ihre Produkte mit dem Stempel "SNMP-konform" zu veredeln. In gewisser Weise ist SNMP neben den bereits etablierten LAN-Standards mit dafür verantwortlich, dass die Mixtur von Netzwerkkomponenten verschiedener Hersteller heute Normalität ist.

SNMP existiert weltweit in Millionen von Systemen. Es lebt in Form von mehr oder weniger intelligenten Agenten, die in den aktiven Komponenten hauptsächlich mit der Sammlung von Informationen über Ereignisse, Fehler oder der Fortschreibung von zahlreichen Zählerständen beschäftigt

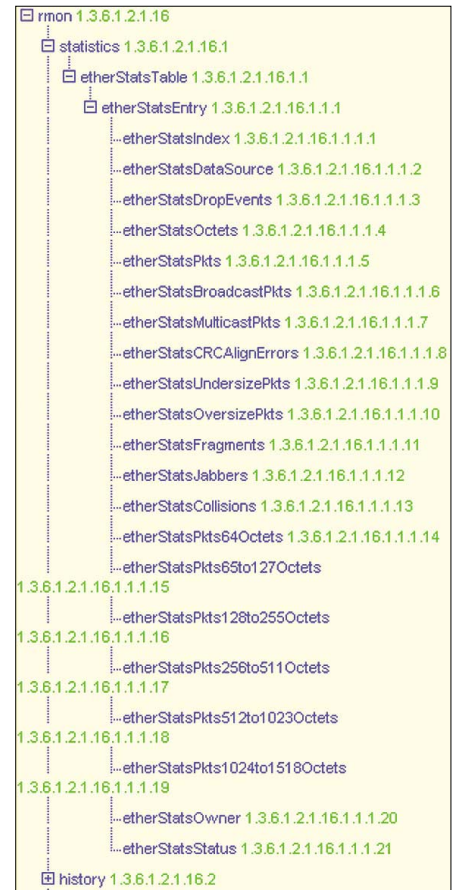


Bild 2. Erläuterung der Struktur eines Eintrags der RMON-1-Ethernet-Statistiken; auch diese werden je Interface im Agenten gespeichert. Schnell wird bei genauem Hinsehen die Fülle von Parametern pro Segment sichtbar.

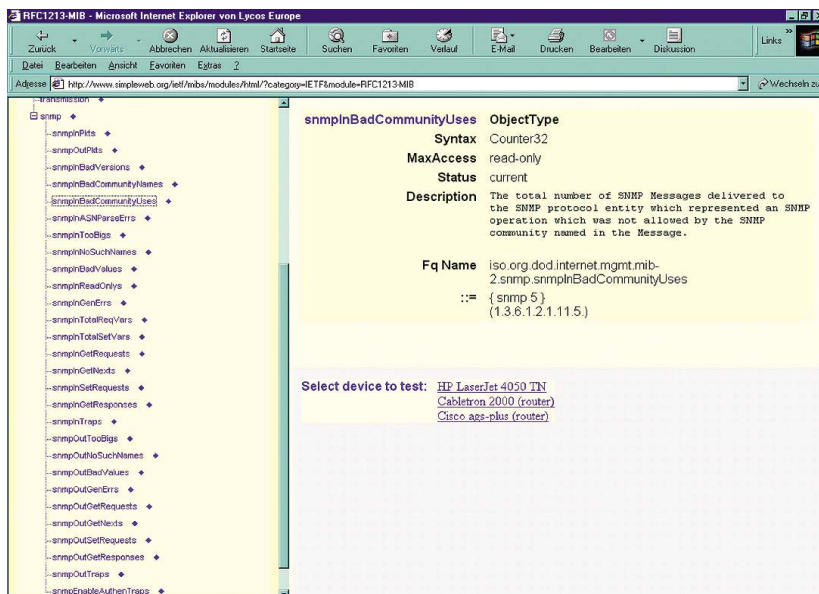


Bild 1. Der beispielhafte partielle Ausdruck zeigt eine SNMP-MIB-II-Information für einen Port innerhalb eines abgefragten Systems. Auf der Internet-Seite <http://www.simpleweb.org/ietf> kann man sich über die Baumstruktur der Datenbanken ein genaueres Bild machen.

sind. Ähnlich einer Wasseruhr registrieren die Agenten die vom Prozessor des Systems gelieferten Vorkommnisse. Gespeichert werden die Zählerstände von SNMP in Registern von 4 Byte Breite (bei SNMP Version 1). Also lassen sich rund vier Milliarden Increments (genau: 4.294.967.296) mit den Registern zählen, bevor diese wieder bei null beginnen. Liest der Administrator mit der Managementplattform die Zähler nicht rechtzeitig aus, besteht die Gefahr der Verwischung von Statistiken, da man unter Umständen nicht mehr genau sagen kann, wie oft die Counter bereits in der Zwischenzeit überdreht wurden. Wie schnell das in modernen Highspeed-LANs geschehen kann, ist bei einer Gigabit-Verbindung leicht vorstellbar. Die Register werden in einheitliche Standard-MIBs (Management-Information-Base) und in herstellereigenen Private-MIBs unterteilt.

So klar wie die Struktur der MIBs sind auch die Prinzipien der Übertragung: Jede Variable wird durch die Managementplattform einzeln vom Agenten per SNMP-Request und dem SNMP-Reply angefordert. Verbesserungen dieser Methode durch so genannte Bulk-Requests sind erst seit SNMP ab der Version 2 möglich. Moderne Netzwerkverwaltung ist bestrebt, möglichst viele Details in möglichst kurzen Zeitabständen zu beschaffen, um eine umfassende Überwachung in Echtzeit zu erreichen. Zur Ergänzung der ersten MIBs (MIB I/MIB II) wurden im Verlauf der Weiterentwicklung weitere Datenbasen für die detaillierte Analyse von LANs erdacht (RMON-MIBs I und II). RMON (Remote Monitoring) 1 und 2 bietet bereits insgesamt 19 Objektgruppen an, für die jeweils pro Schnittstelle wiederum eine Fülle von Datensätzen für die Abholung per Managementstation vorgehalten werden. Neben den Polling-Verfahren sind zur Da-

tenaufzeichnung Filter- und Capture-Gruppen verfügbar.

Trotz der Verbreitung und auch der unbestreitbaren Vorteile des SNMPs gibt es einige Punkte, die den Glanz seiner Erfolgsgeschichte trüben. SNMP wurde für die Verwaltung von aktiven Komponenten eines lokalen Netzwerks erdacht. Von WAN-spezifischen Parametern (zum Beispiel Frame-Relay, ATM etc.) war bei der Planung der SNMP Version 1 noch keine Rede. Zudem sind moderne LAN-Strukturen heute mit Switching, VLANs und so weiter wesentlich komplexer, als dies bei der Konzeption von SNMP überhaupt vorstellbar war. Mit anschwellender Informationsflut braucht es zunehmend Speicherplatz und Prozessorleistung. Folglich werden die aktiven Komponenten damit leistungshungriger und teurer. Mit jeder Erweiterung der SNMP-MIBs, also MIB 1, MIB 2, RMON1, RMON2 und so weiter, addieren sich erschreckend viele Informa-

tionen, die alle vom Agenten zur Managementstation übertragen werden müssen. Wer frei nach Orwells Big Brother "alles über seine Netzwerke wissen möchte", der muss auch eine entsprechend große Zahl von Informationen transportieren und verwalten können.

Das wohl größte Problem des SNMPs liegt in dem sehr ineffektiven Prinzip, Messdaten zu beschaffen. Bei der meistverbreiteten Version 1, und oft unterstützten Geräte nur diesen Standard, wird jede SNMP-Variable einzeln in einem Datenpaket angefragt und beantwortet. Die Variablen werden zudem jeweils für jeden Port des aktiven Systems extra abgerufen, also alle Variablen für den LAN-Port, dann alle für den WAN-Port eines Routers und so weiter. Bei einer durchschnittlichen Paketgröße von rund 250 Byte addiert sich sowohl die Menge als auch das für die Übertragung der Daten notwendige Zeitfenster schnell zu einer "behäbigen

Größe". Kommen nun zu den Standard-MIB-Abfragen umfassende RMON-Diagnosen hinzu, wächst die zu übertragende Menge der Messinformationen weiter rasant an. In einem Beispiel-Setup, bei dem der Administrator einen zentralen Ethernet-Switch mit rund 120 Ports via (MINI-)RMON erfasst, führt dies zu einem Datenvolumen von rund 180 KByte pro Polling. Schnell wird bei diesem Beispiel sichtbar, dass hier von Echtzeit-Monitoring keine Rede mehr sein kann. Die Betonung bei SNMP muss daher bei genauerem Hinsehen nach wie vor auf Simple-Network-Management-Protokoll lauten. Es eignet sich aus den erwähnten Gründen eher schlecht für die Kontrolle und Steuerung von Systemen oder Applikationen.

HSRMON (High-Speed-Remote-Monitoring) wurde von Chevin bereits gegen Ende der 80er Jahre entwickelt, also zu einem Zeitpunkt, zu dem es noch keinen SNMP-Standard oder gar RMON gab. Es hat während der vergangenen Jahre zahlreiche Erweiterungen und weitere Verbesserungen erfahren. HSRMON wird typischerweise für die Sammlung und die Analyse von LAN-spezifischen Details genutzt. Die Inhalte unterscheiden sich im Informationsgehalt nicht zu den von

SNMP und RMON gelieferten Daten. HSRMON ist zunächst proprietär und schreckt den standardgläubigen IT-Verwalter ab. Doch in der Praxis muss das keineswegs ein Nachteil sein. Im Gegensatz zu SNMP setzt das HSRMON-Protokoll auf das TCP (Transmission Control Protocol) und nicht auf UDP (User Datagram Protocol) auf. Mit Hilfe von HSRMON können sowohl Endgeräte als auch dedizierte Mess-Probes ausgestattet werden. Hierzu wird ein schlankes und erstaunlich prozessorschonendes Agentenmodul direkt im Zielsystem installiert. Als Zielsystem kommen derzeit alle Windows-basierenden Plattformen, Workstations wie auch Server in Frage. Eine Unix-beziehungswise Linux-kompatible Version wird derzeit entwickelt. Als sehr vorteilhaft erweisen sich die Agenten speziell in geschwitten Netzwerken. Durch Multiuser-Technologie erlauben die HSRMON-Agenten zusätzlich den Zugriff von mehreren Plattformen aus zum gleichen Zeitpunkt. Neben der reinen Übertragung von Messdaten gestattet das HSRMON wie auch der Standard die Realisierung von Filter- und Capture-Betrieb sowie die Generierung von Alarmen, basierend auf frei definierbaren Grenzwerten.

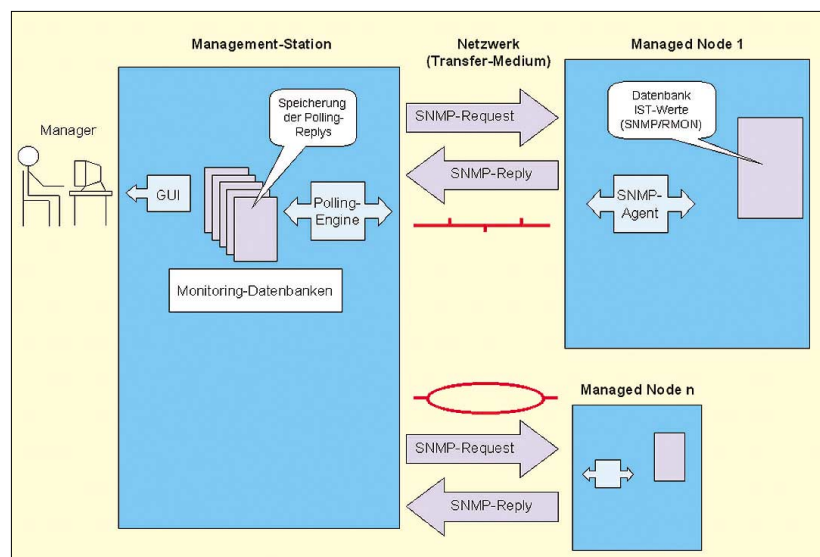


Bild 3. Prinzipschaubild des Polling-Verfahrens durch SNMP/RMON: Alle Messdaten, die der Agent aus seinem Interface gewinnen kann, werden in einer Online-Datenbank registriert und deren Zähler Parameter für Parameter in Einzelpaketen durch die Managementplattform abgefragt. Hierdurch entsteht je nach "Tiefe" der Messdaten ein nicht unerheblicher Overhead. Zudem wird Echtzeitkontrolle von Netzwerken erheblich erschwert, unter Umständen (insbesondere bei langsamen WAN-Verbindungen) unmöglich gemacht.

Wie SNMP-Agenten benötigt auch der HSRMON-Agent eine lokale Intelligenz, die mit dem Registrieren von Daten wie Paketaufkommen, Netzwerklast, Protokollstatistik und so weiter betraut ist. Die gesammelten Detailinformationen werden für die Abholung durch die Managementstation in Form einer Datenbank vorgehalten. Während SNMP-Systeme lediglich "die Datenbank" bereithalten, bereitet HSRMON die Messdaten auf eine besondere Weise zum Transport zur Plattform vor. Anstatt alle Messwerte einzeln zu übertragen, konsolidiert HSRMON sie in kompakten und bereits verdichteten Datenreihen. Redundante Messinformationen machen oftmals bis zu 80 Prozent des Management-Traffic aus. Ein Beispiel hierzu: SNMP/RMON-Agenten erkennen in einem fehlerhaften Datenstrom so genannte Phantomadressen, für die jeweils separate Knoten- und Konversationsstatistiken angelegt sind. Selbst wenn von dieser physikalisch nicht existenten Station kein einziges Paket mehr ausgeht, wird ein SNMP/RMON-Agent diesen von nun an, also praktisch "für immer", im Auge behalten und die sich nicht mehr verändernden Daten pausenlos bei jedem Polling erneut übertragen. HSRMON hingegen stellt bei jeder Abfrage seitens der Managementstation nur diejenigen Werte zur Verfügung, die sich seit dem letzten Polling tatsächlich verändert haben. In der Praxis bedeutet dies, dass sich durch HSRMON eine wesentliche Effizienzsteigerung beim Transport erreichen lässt.

Wer einmal in der Verlegenheit war, über eine WAN-Verbindung Netzwerk-Monitoring zu betreiben, wird sicherlich mit dem Problem konfrontiert gewesen sein, dass echtes Monitoring oder gar Analyse von Datenströmen mit SNMP oder RMON aufgrund der unerhörten Overheads nahezu unmöglich ist. Um so

verblüffender die Effektivität mit HSRMON. Es überträgt selbst bei sehr kurzen Zeitintervallen die notwendigen Daten zur Managementstation und gestattet Messintervalle von zwei Sekunden zu verwenden, ohne eine normale ISDN-Verbindung mit Management-Overhead zu saturieren. Selbst bei Versuchen mit GSM-Datenverbindungen von 9,6 kBit/s ist eine Online-Messung via HSRMON noch realisierbar. Ideal ist HSRMON überall dort einsetzbar, wo bei der begrenzten Bandbreite oder aber bei hunderten von geswitchten LAN-Segmenten (= LAN-Ports) Messungen zu betreiben sind.

Durch die zusätzliche Implementierung der Standardprotokolle SNMP und RMON kann der Netzwerkverwalter als "Zugabe" die in Endgeräten aktiven HSRMON-Agenten "missbrauchen", um als Relay-Agenten zu fungieren. Das heißt, er kommuniziert über die schmalbandige ISDN-Strecke zwischen Managementstation und

dem Agenten via HSRMON. Seitens des Agenten und damit lokal fragt er einen SNMP/RMON-Agenten ab und überträgt dessen Analysedetails in der schlankeren HSRMON-Technologie auf die Plattform.

HSRMON erhebt nicht den Anspruch der seligmachenden und allumfassenden Komplettlösung für Netzwerk-Monitoring und Analyse. Bestehend ist jedoch die enorme Effektivität des Protokolls, wenn es um den Datentransport zwischen Managementstation und Agenten geht. Die Sichtweise der Erfinder von HSRMON, in einer "voll geswitchten Welt" die Intelligenz der Agenten bis in die Endgeräte zu bringen, findet zunehmenden Zuspruch, da die möglichen Alternativen allesamt mit kleineren oder größeren Nachteilen einhergehen. Dieses Verfahren bietet der Netzwerkverwaltung ohne weiteres einen praktikablen Lösungsansatz für modernes Netzwerkmanagement.

(Uli Weller Magellan Netzwerke/rkf)

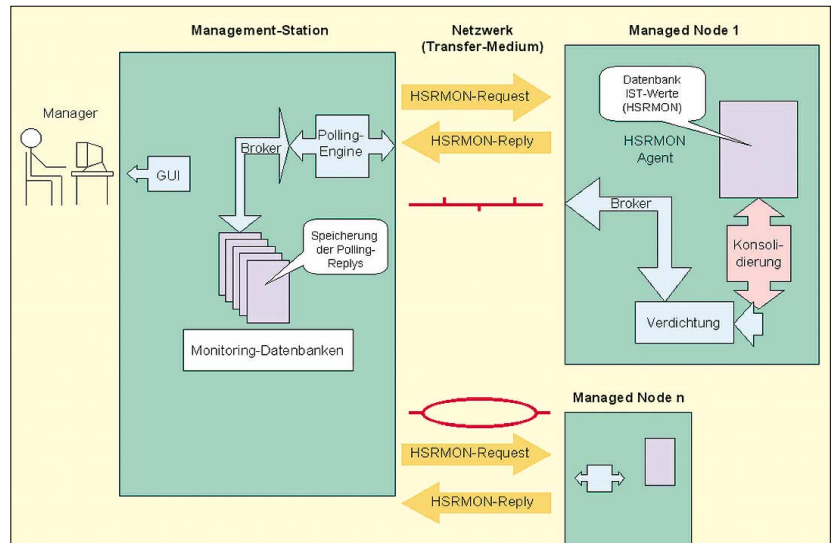


Bild 4. Auf den ersten Blick unterscheidet sich HSRMON nur unwesentlich vom Prinzip des SNMP/RMON-Standards. Durch die Konsolidierung und Verdichtung der Messinformationen können allerdings enorme Vorteile im Bereich der Übertragungseffektivität sowie des Management-Overheads erzielt werden. Insbesondere bei WAN-Verbindungen kann dies für das Monitoring von entscheidendem Vorteil sein.