PAESSLER

WHITEPAPER

Quo Vadis, SNMP?

Whitepaper Teil 1: Einführung in SNMP

PRTG NETWORK MONITOR

Jens Rupp, Lead Developer bei der Paessler AG
Daniel Zobel, Head of Software Development bei der Paessler AG

Erstveröffentlichung: August 2010 – Stand: März 2014

Inhalt

Einleitung

Da die geschäftliche Effizienz zunehmend von vernetzten Computersystemen abhängt, ist es unabdingbar, deren Funktionsfähigkeit zu überwachen und zu steuern. Auf Grund der zahlreichen Geräte verschiedener Hersteller auf dem Markt war die Einführung eines Standards für diese Überwachung unumgänglich. Daher entwickelte die IETF[1] bereits Ende der 80er Jahre das Simple Network Management Protocol (SNMP). Mittlerweile ist SNMP in der 3. Generation nach wie vor Standard im Netzwerk-Management – nicht zuletzt in Ermangelung einer praktikablen Alternative. Denn der Einsatz des Protokolls als Basis für ein umfassendes Netzwerk-Management ist nicht unproblematisch und erfordert umfassendes Know-how und Improvisationsvermögen.

SNMP zur professionellen Netzwerküberwachung

SNMP ist ein Protokoll zur Überwachung von Netzwerkgeräten. Darüber hinaus lassen sich über diesen Standard auch Konfigurationsaufgaben abwickeln und Einstellungen aus der Ferne tätigen. SNMP-fähige Hardware sind üblicherweise Router, Switches und Server. Auch Drucker, Umgebungssensoren (Temperatur, Luftfeuchtigkeit etc.) und viele andere Geräte können mittels dieses Standardprotokolls abgefragt und gesteuert werden.

Voraussetzung ist, dass das Gerät über eine Netzwerkverbindung (Ethernet, TCP/IP) erreichbar ist und über einen SNMP-Server verfügt. Es muss also ein aktives Gerät sein, das auf Anfragen reagieren kann. Bei Betrachtung des heutigen Angebots von Netzwerk-Switchen lässt sich feststellen, dass bei vielen günstigeren Geräten (Sub-100-Euro Klasse, Consumer-Hersteller) am Zugriff per SNMP „gespart“ wurde. Die meisten professionellen Geräte der Markenhersteller (z.B. Cisco, Linksys und HP; jeweils ab ca. 200 Euro) bieten dagegen SNMP-Unterstützung an – ein Qualitätsmerkmal professioneller Netzwerkhardware.

Verschiedene Entwicklungsstufen

Die erste SNMP-Version (V1) wurde bereits 1988[2] definiert. Obwohl diese Version keine „Abhörsicherheit“ durch Verschlüsselung oder ähnliche Mechanismen beinhaltet, ist sie auf Grund ihrer einfachen Nutzbarkeit noch immer die am häufigsten verwendete Variante in „privaten LANs“ hinter einer Firewall. Für öffentliche Netze empfiehlt sich die Verwendung dieser ersten Version jedoch nicht. Trotzdem bieten viele einfache Geräte auch heute noch lediglich SNMP V1 an.

Das Sicherheitsproblem rückte 1993[3] und 1996[4] in den Fokus. Die damals diskutierten Lösungen haben sich aber nie wirklich durchgesetzt. Lediglich eine um einige Funktionen erweiterte Nachfolgerversion[5] konnte sich halbwegs etablieren. Wenn man von SNMP V2 spricht, meint man üblicherweise die Version „V2c“.

Die aktuelle Version ist SNMP V3, die insbesondere die Sicherheit von SNMP steigert. Da die Verwendung von SNMP V3 allerdings recht komplex und aufwändig ist, hat sich diese Version seit ihrer Spezifikation 2002 besonders bei der Verwendung in Intranets kaum durchgesetzt.

[1] „The Internet Engineering Task Force“ hat es sich zur Aufgabe gemacht, das Internet zu verbessern, indem es qualitativ hochwertige und bedeutende technische Dokumente erstellt, welche die Art und Weise beeinflussen, wie Menschen das Internet gestalten, einsetzen und verwalten.

[2] RFC 1155, RFC 1156, RFC 1157

[3] SNMP V2p, RFC 1441, RFC 1445, RFC 1446, RFC 1447

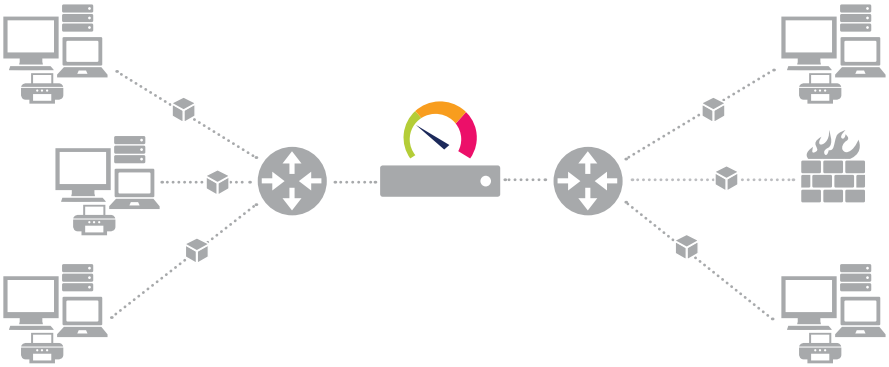
[4] SNMP V2p, RFC 1909, RFC 1910

[5] SNMP V2c, RFC 1901, RFC 1905, RFC 1906

Wie funktioniert SNMP?

Mittels SNMP findet eine Client-Server-Kommunikation über das „User Datagram Protocol“ (UDP) statt: Eine Überwachungs- oder Managementsoftware sendet (als Client) ein UDP-Paket an den SNMP-Server, den so genannten „Agenten“, der sich in der Regel in einem Gerät befindet. Dieser reagiert wiederum mit einem SNMP-Paket als Antwort. Mit jedem einzelnen Anfrage-Antwort-Zyklus kann der Client einen „Messwert“ von dem Gerät abrufen, beispielsweise Netzwerk-Traffic, CPU-Auslastung, Temperatur etc. Je nach Abfragemethode können auch mehrere Werte gleichzeitig übertragen werden.

ABBILDUNG 1:
Client-Server-Kommunikation mittels SNMP



GRUNDSÄTZLICHE KOMMUNIKATION ÜBER SNMP

Über den reinen Informationsaustausch hinaus werden über SNMP auch Steuerungsbefehle übertragen. Mit diesen kann der Client im Gerät bestimmte Werte setzen und Optionen sowie Einstellungen verändern.

Während bei der klassischen Kommunikation immer der Client aktiv Informationen vom Server abfragt, ermöglicht SNMP zusätzlich die Verwendung von sogenannten „Traps“. Dies sind Datenpakete, die vom SNMP-Server zum Client versandt werden, ohne dass diese explizit angefordert werden müssen. Wenn ein Gerät (bzw. der Server in diesem Gerät) entsprechend konfiguriert ist, wird auf diese Weise ein SNMP-Trap an den Client gesendet, sobald auf Serverseite ein bestimmtes Ereignis eintritt.

Eine Managementsoftware kann damit ohne Zeitverzögerung auf Ereignisse reagieren, unabhängig von einem etwaigen Scanning-Intervall, in welchem sie den Server regelmäßig abfragt.

STEUERUNGSBEFEHLE UND SNMP-TRAPS

Soweit ist der Prozess recht einfach und gradlinig. Leider ist aber das Erzeugen der Datenpakete sehr aufwändig. Die Pakete werden in einer Beschreibungssprache erstellt, die auf der ziemlich komplizierten „Abstract Syntax Notation One“ (ASN.1) basiert. Da der ganze Vorgang relativ komplex ist, enthalten viele Implementierungen Fehler, insbesondere im Embedded-Bereich (z.B. in Routern und Switches). Diese reichen vom kleinen Lapsus bis zu handfesten Falschinterpretationen der RFCs[6], die dann zu Problemen bei den Client-Programmen führen.

AUFWÄNDIGE BESCHREIBUNGSSPRACHE

„Junge“ Software-Hersteller, die ihre ersten Implementierungen von SNMP schreiben, müssen daher oft erst anhand eines wachsenden Kundenkreises mit unterschiedlichen Hardware-Umgebungen einen fundierten Erfahrungsschatz gewinnen und Kompetenzen für die Geräte der einzelnen Hersteller aufbauen. Dabei lernt das Unternehmen nach und nach die Probleme der verschiedenen Hardware-Hersteller kennen. So kann es durch ein Fern-Debugging ggf. Workarounds in seine Programme einbauen, um Fehler abzufangen. Auch der Netzwerkspezialist Paessler stellt sich seit Jahren mit seiner Netzwerkmanagement-Lösung PRTG dieser Herausforderung. Mittlerweile kann die Software sehr viele SNMP-Varianten verschiedener Hersteller abfangen, die eigentlich fehlerhaft implementiert sind.

[6] Als RFC (engl. „Request for Comments“, dt. „Bitte um Kommentare“) werden technische Dokumente bezeichnet, die von der Internet Engineering Task Force (IETF) herausgegeben werden. Viele RFCs haben sich zum allgemein akzeptierten Standard entwickelt.

MANAGEMENT INFORMATION BASE (MIB)

Damit SNMP-Client und -Server die jeweiligen Werte austauschen können, müssen die verfügbaren SNMP-Objekte über eindeutige Adressen verfügen, die auf beiden Seiten bekannt sind. Dies ist unbedingte Voraussetzung für eine erfolgreiche Übermittlung der Werte und eine Netzwerküberwachung mittels SNMP. Damit der Zugriff auch herstellerübergreifend und mit unterschiedlichen Client-Server-Kombinationen funktioniert, wurde die „Management Information Base“ (MIB) als unabhängiges Format zur Speicherung von Geräteinformationen geschaffen.

Eine MIB ist eine Textdatei, in der alle abfragbaren SNMP-Objekte eines Gerätes in einer standardisierten Baumhierarchie aufgelistet sind. Sie enthält mindestens einen „Object Identifier“ (OID), der neben der notwendigen eindeutigen Adresse und einem Namen auch Informationen über Typ, Zugriffsrechte und eine Beschreibung des jeweiligen Objektes liefert. MIB-Dateien sind in SMIv2 geschrieben, einem auf ASN.1 basierenden ASCII-Textformat. Sie können von den Herstellern SNMP-fähiger Geräte mit Hilfe zusätzlicher Textdateien auf einfache Weise um spezifische OIDs erweitert werden. Momentaner Standard ist die MIB-II, welche die ursprüngliche MIB unter anderem um dringend benötigte Typen erweitert hat [7].

ÜBER OIDS

SNMP-fähige Geräte stellen ihre Standard-OIDs immer unter dem folgenden Zweig bereit: 1.3.6.1.2.1.[…]

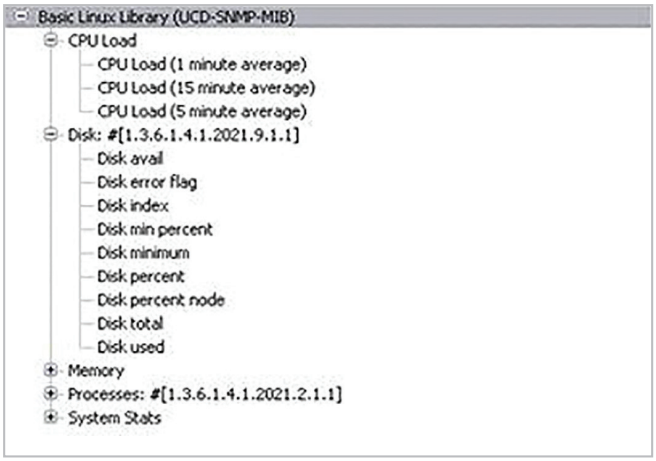
Dies entspricht in einer anderen Schreibweise der folgenden Zeichenkette, die alternativ zum Zahlencode verwendet werden kann: iso.org.dod.internet.mgmt.mib.[…]

Herstellerspezifische OIDs beginnen dagegen immer mit folgender Zeichenkette (siehe Abbildung 2): 1.3.6.1.4.1.[Herstellernummer].[…]

Jeder Hersteller kann sich in diesem Nummernzweig bei der „Internet Assigned Numbers Authority“ (IANA) kostenlos eine eindeutige Herstellernummer registrieren, unter der er seine eigenen Erweiterungen zur Verfügung stellt.

Jeder Knoten in der Baumstruktur der MIB enthält eine eindeutige ID und einen Namen, die den dahinter liegenden Zweig identifizieren. Um die Adresse eines spezifischen Knotens zu ermitteln, bewegt man sich in der Baumstruktur von der Wurzel („Root“) nach unten. Dabei wird die Zahl jedes Knotens notiert. Hängt man nun die Zahlen aller Knoten aneinander und trennt diese mit einem Punkt, so erhält man die Adresse des gewünschten Objektes. Die so zusammengesetzte Zahl wird als „OID“ eines SNMP-Objektes bezeichnet.

ABBILDUNG 2:
Die Baumstruktur der MIB am Beispiel einer Linux MIB



[7] Beschrieben sind diese Definitionen in RFC 2578, RFC 1155, RFC 1213 sowie RFC 1157.

Herausforderungen im Zusammenhang mit SNMP

ALTERNATIVEN ZU SNMP

Eine Netzwerküberwachung mit SNMP funktioniert in den meisten Fällen sehr zuverlässig. Neben den bereits erwähnten Kompatibilitätsproblemen ergeben sich bei der praktischen Arbeit jedoch kleine Tücken oder Hindernisse, die den erfolgreichen Einsatz von SNMP erschweren – vor allem bei der Ersteinrichtung. Eine geeignete Software kann helfen, viele Probleme von vornherein auszuschließen. Zu den größeren Herausforderungen zählen beispielsweise Lastprobleme. Diese treten auf, wenn der SNMP-Client auf Grund einer zu „optimistischen" Konfiguration in sehr kurzen Abständen viele Anfragen erzeugt und damit das Netzwerk zeitweise stört oder gar lahmlegt. Eine gute Lösung unterstützt hier mit sinnvollen Default-Werten. Auch der Einrichtungsaufwand durch nicht vorhandene oder fehlerhafte MIBs wird häufig unterschätzt. Die RFCs sehen zudem die Möglichkeit vor, dass Geräte mit jedem Neustart die eindeutige Adresse (OID) ihrer SNMP-Objekte ändern dürfen. Eine intelligente Auto-Discovery Funktion im SNMP-Managementprogramm (Client) entlastet den Administrator, da sie die im Netzwerk vorhandenen Geräte und die darin enthaltenen SNMP-Objekte automatisch erkennt. Sie kann auch dafür sorgen, dass Geräte mit wechselnden OIDs nach einem Neustart automatisch wieder erkannt werden. Eine ausführlichere Beschreibung der Herausforderungen mit SNMP finden Sie im zweiten Teil dieses Whitepapers.

NetFlow (xFlow) zur Bandbreitenmessung

Eine interessante Alternative für Traffic-Informationen ist NetFlow (Cisco) bzw. sFlow und deren Variationen (wir bezeichnen das zusammenfassend als xFlow). Bei diesen xFlow-Systemen fasst der Router die Daten in „Flows" zusammen und schickt sie gebündelt an die Monitoring-Software. Interessant ist hierbei, dass nicht nur das Volumen, sondern auch IP-Adressen und Ports übermittelt werden. Dies ermöglicht weitaus genauere Analysen. Voraussetzung ist allerdings, dass der Router den xFlow-Export unterstützt (z.B. können nur die größeren Cisco-Router und -Switches NetFlow exportieren).

Packet Sniffing zur Bandbreitenmessung

Eine weitere Möglichkeit, den gesamten Datenverkehr eines Netzwerks zu analysieren, ist die direkte Traffic-Analyse aller Datenpakete. Dabei ergeben sich allerdings zwei große Probleme: sehr hohe Systemanforderungen und die passende Netzwerktopologie. Da jedes einzelne Datenpaket analysiert werden muss, wird hierzu ein Analyse-Rechner benötigt, der auch bei hohen Netzwerklasten in der Lage ist, den Netzwerkverkehr vollständig zu bearbeiten. Außerdem muss dieser Rechner so in das Netzwerk integriert sein, dass er alle Datenpakete erhält. In einem „ge-switchten" Netz sieht jeder Rechner aber nur die Pakete, die für ihn bestimmt sind. An dieser Stelle ist eine Technik gefragt, mit der alle zu überwachenden Daten auf eine Netzwerkkarte gespiegelt werden. Dies geschieht z.B. mit Hilfe von „Port Mirroring", einem „Monitoring-Port" oder „Span", wie die Technik bei Cisco-Geräten bezeichnet wird.

Windows Management Instrumentation (WMI)

„Windows Management Instrumentation" ist Microsofts Implementierung eines Standards für das Management von IT-Systemen. Mit WMI können nahezu alle Daten eines Windows-Rechners abgefragt werden. Dazu zählen unter anderem Hardware- und Systeminformationen, Einträge im Ereignisprotokoll, Dienste und Prozesse, Registry-Einträge usw. Vom Festplattenfüllstand bis zur Exchange Server Performance lässt sich via WMI alles überwachen. Wie mit SNMP kann auch über das WMI-Protokoll schreibend auf den Client zugegriffen werden, um dort Optionen einzustellen. Dabei können nicht nur Einstellungen verändert, sondern auch Dienste beendet, Werte gesetzt oder Rechner neu gestartet werden. Alle WMI-Funktionen sind bei entsprechender Konfiguration auch über das Netzwerk von entfernten Rechnern aus (Remote) zu steuern.

Allerdings handelt es sich um einen reinen Windows-Standard und erfordert daher spezielle Software, meist ein installiertes Windows-Betriebssystem ab Version XP. Je nach verwendeter Windows-Version und Netzwerkgröße kann es bei der Verwendung von WMI auch zu Lastproblemen kommen. Zudem kommt es vor, dass die Einrichtung von Remote-Verbindungen, insbesondere über ein WAN, nicht immer auf Anhieb funktioniert.

Agent-basierende Systeme (meist herstellerspezifisch)

Für Windows- und Linux-basierende Systeme besteht die Möglichkeit, eine Agent-Software auf dem System zu installieren. Dieses kleine Programm fungiert auf dem Rechner (im Hintergrund) als Datenserver und stellt die zu überwachenden Messwerte in einem Format zur Verfügung, das die Monitoring-Software verarbeiten kann. Allerdings fehlen oft einheitliche Standards, sodass man sich langfristig auf eine bestimmte Monitoring-Lösung festlegen muss, die nur mit einer bestimmten Agent-Software funktioniert. Zudem ist es erforderlich, auf allen Systemen einen Agenten zu installieren, was – je nach Netzwerkgröße – sehr aufwändig sein kann.

Die Zukunft von SNMP

Trotz der vielen Probleme und Sicherheitsrisiken ist insbesondere SNMP V1 sehr weit verbreitet, nicht zuletzt aus Mangel an etablierten Alternativen. SNMP ist universell einsetzbar. Sehr viele Geräte stellen es als einzigen Standard zum Auslesen von Werten zur Verfügung. Hier steckt viel Potenzial für einen neuen, modernen und flexiblen Standard, allerdings kann das niemand im Alleingang realisieren. In den vergangenen Jahren gab es hierzu verschiedene Ansätze, von denen sich aber bis heute keiner durchsetzen konnte. Das liegt vor allem daran, dass für einen neuen Standard verschiedene Hardware-Hersteller miteinander kooperieren müssten. Dabei erinnert diese Problematik ein wenig an die Henne-Ei Metapher. Kein Hersteller wird sich die Mühe machen, ein (experimentelles) neues Protokoll zu unterstützen, an dem er nicht selbst mitgearbeitet hat. Entschließt sich wiederum ein Hersteller dazu, ein proprietäres Format zu entwickeln, dann stößt dieses in der Regel auf wenig Akzeptanz bei den Administratoren.

SNMP deckt (insbesondere mit V3) funktional zwar alle notwendigen Anwendungsgebiete ab, ist jedoch im Einsatz sehr umständlich und aufwändig einzurichten. Für die Einführung eines neuen Standards ist der Leidensdruck aber offenbar nicht hoch genug. Der liegt nicht bei den Herstellern, sondern vor allem bei denen, die SNMP anwenden müssen. An dieser Stelle öffnet sich ein interessantes Einsatzfeld für Netzwerküberwachungs-Software, der es gelingt, die „erlebte Komplexität“ für den Benutzer deutlich zu vereinfachen.

SNMP wird uns trotz seiner zahlreichen Mängel noch lange begleiten, selbst wenn ein neuer Standard eingeführt werden sollte.

Millionen laufender und funktionierender Monitoring-Systeme werden nicht von heute auf morgen durch etwas Neues ersetzt werden – getreu dem Motto: „Never Touch a Running System“. Das Protokoll mag zwar nicht die beste Lösung sein, aber es ist weit verbreitet, bekannt und etabliert. Und wenn eine Netzwerküberwachung mittels SNMP erst einmal eingerichtet ist, dann läuft sie meist zuverlässig.

Paessler hat zu diesem Thema einen kurzen Artikel im Internet veröffentlicht: http://www.paessler.com/knowledgebase/en/topic/653

Informationen zur praktischen Anwendung von SNMP finden Sie im zweiten Teil dieses Whitepapers: „SNMP praktisch anwenden“.

ÜBER DIE PAESSLER AG

Die Paessler AG ist seit Jahren führend in der Entwicklung von leistungsfähiger, bezahlbarer und benutzerfreundlicher Netzwerk-Monitoring-Software. Paessler Produkte sorgen für Ruhe und Sicherheit in IT-Abteilungen von Unternehmen aller Größen - von SOHOs über KMUs bis hin zu global tätigen Konzernen – umfassend, unkompliziert und zuverlässig. Vom Firmensitz in Nürnberg aus betreut Paessler über 150.000 Installationen seiner Produkte, die weltweit im Einsatz sind. Das 1997 gegründete Unternehmen ist bis heute privat geführt und sowohl Mitglied des Cisco Solution Partner Program als auch ein VMware Technology Alliance Partner.

Freeware und Testversionen aller Produkte können unter www.paessler.de/prtg/download heruntergeladen werden.

Paessler AG · www.paessler.de · info@paessler.com