PAESSLER

WHITE PAPER

Quo Vadis, SNMP?

White Paper Part 1: Introducing SNMP

PRTG NETWORK MONITOR

Authors: Jens Rupp, Lead Developer at Paessler AG
Daniel Zobel, Head of Software Development at Paessler AG

Published: August 2010 – Last Update: March 2014

Contents

Introduction

As business efficiency becomes more and more dependent on connected computer systems, monitoring and ensuring their reliability in performance is absolutely necessary. Because of the huge amount of devices on the market, supplied by various manufacturers, it was imperative to introduce a standard for this kind of monitoring. That is why IETF[1] developed Simple Network Management Protocol (SNMP) towards the end of the 80s. Today, the third generation of SNMP is still the standard for network management—not least because there is no practical alternative. However, the use of this protocol as a basis for extensive network management is not unproblematic—it requires comprehensive know-how and sometimes the ability to improvise.

SNMP Professionally Monitors Networks

SNMP is a protocol to monitor network devices. In addition, with SNMP it is possible to deal with configuration tasks and to change settings from a distance. SNMP-compatible hardware typically includes routers, switches and servers. Also printers, environmental sensors (temperature, humidity, etc.) and many other devices can be checked and controlled using this standard protocol.

It is a prerequisite that the device is available through a network connection (Ethernet, TCP/IP) and has access to an SNMP server. It must also be an active device which can react to requests. Looking at the current offer of network switches, it can be claimed that for many of the cheaper devices (below 100 Euros, largely consumer products), the access to SNMP was 'saved' away. Most of the professional devices by known brand producers (i.e. Cisco, Linksys and HP; each from circa 200 Euros) offer SNMP support—a quality feature of professional network hardware.

Different Development Stages

The first SNMP version (V1) was defined in 1988[2]. Although this version doesn't contain any wiretapping prevention via encoding or other mechanisms due to its simplicity, it is still the most frequently used variant in 'private LANs' behind a firewall. Yet use of this version is not recommended for public nets. Nevertheless, even today many simple devices still only offer SNMP V1.

The security problem shifted into focus in 1993[3] and 1996[4]. The solutions that were then discussed never really took off. Only one slightly enhanced follow on version[5] was partly able to establish itself. When speaking of SNMP V2, what is usually meant is version "V2c".

The current version is SNMP V3 which increases the security of SNMP. However, as the use of SNMP V3 is relatively complex and demanding, this version has not really managed to establish itself for use in intranets since its specification in 2002.

[1] "The Internet Engineering Task Force" is focused on improving the internet by creating high-quality and important documents that influence the way people design, use, and manage the internet.

[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

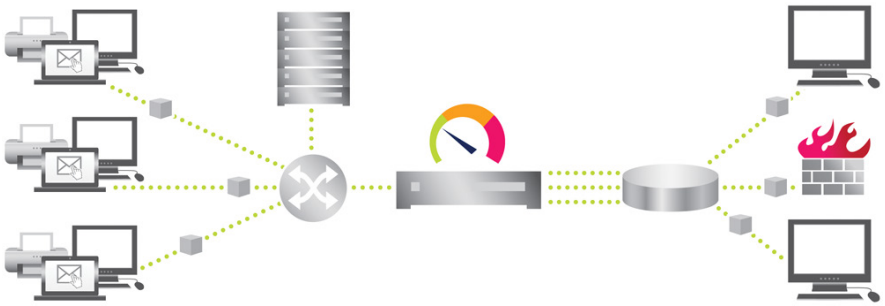
[5] SNMP V2c, RFC 1901, RFC 1905, RFC 1906

How Does SNMP Work?

BASIC COMMUNICATION VIA SNMP

Through SNMP, client-server communication can take place via the "User Datagram Protocol" (UDP): A monitoring or management software sends (as a client) a UDP packet to the SNMP server, the so-called "agent" which is normally a piece of software running within a device. This in turn reacts by sending an SNMP packet as an answer. Each single question-answer-cycle enables the client to retrieve one "measurement" from the device, for example network traffic, CPU-load, temperature, etc. Depending on the inquiry method, several measurements can be transferred at a time.

FIGURE 1:
Client-server communication via SNMP



CONTROL COMMANDS AND SNMP TRAPS

Beyond the pure exchange of information, control commands are transferred via SNMP. With these the client can set certain measurements and options within the device and change its settings.

While in classic communication the client always actively requests information from the server, SNMP allows the additional use of so-called "traps." These are data packages that are sent from the SNMP server to the client without being explicitly requested. If a device (or the server in this device) is configured correspondingly, an SNMP trap is sent to the client as soon as something specific happens on the server.

Management software can therefore react immediately without delay to incidents, regardless of any set scanning intervals at which the server is regularly checked.

COMPLEX DESCRIPTION LANGUAGE

So far the process is relatively simple and straightforward. Unfortunately, however, the creation of the data packages is very complex. The packages are created in a description language that is based on the fairly complicated "Abstract Syntax Notation One" (ASN.1). As the whole procedure is pretty complex, many implementations contain faults, especially in the embedded area (e.g. routers and switches). These range from small slips to complete misinterpretations of the RFCs[6], which in turn lead to problems with the client programs.

Budding software developers writing their first implementation of SNMP must first of all gain sound knowledge, experience, and know-how of the individual manufacturers' devices by studying a growing group of customers with varied hardware setups. Through this, the developer gradually gets to know the different problems the various hardware manufacturers have. So, via remote-debugging, it can build workarounds into its programs to intercept faults. Network specialist Paessler has faced this challenge with its network management solution PRTG. Today, the software can intercept many different SNMP variations from several manufacturers which have actually been implemented incorrectly.

[6] RFC "Request for Comments" are technical documents that are published by the Internet Engineering Task Force (IETF). Many RFCs have become commonly accepted standards.

MANAGEMENT INFORMATION BASE (MIB)

So that SNMP clients and servers can exchange the corresponding measurements, the available SNMP objects must have clear addresses that are known to both sides. This is an implicit necessity for a successful transfer of the measurements and network monitoring using SNMP. The "Management Information Base" (MIB) was created as an independent format for the storage of device information so that the access can work—regardless of the manufacturer and with different client-server combinations.

An MIB is a text-file in which all searchable SNMP objects of a device are listed in a standardized tree hierarchy. It contains at least one "Object Identifier" (OID) that delivers not only the necessary unique address and name, but also information on type, access rights and a description of the respective object. MIB files are written in SMIv2, an ASCII text format based on ASN.1. They can be easily upgraded with specific OIDs by the manufacturers of SNMP compatible devices, using additional text files. The current standard is the MIB-II, which has expanded the original MIB to include types that are urgently needed[7].

ABOUT OIDS

SNMP capable devices allow access to their standard OIDs at the following branch: 1.3.6.1.2.1.[…]

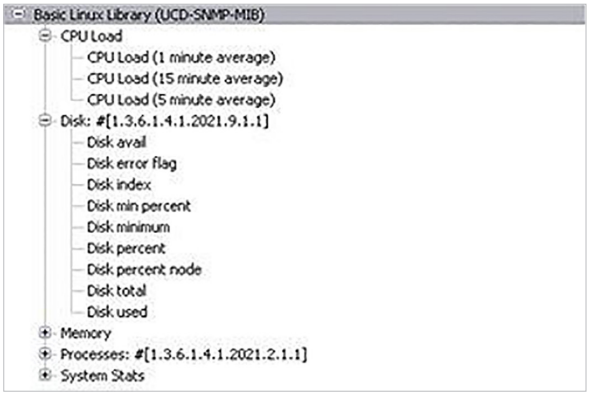
This corresponds to another spelling of the following chain of figures which can be used as an alternative to the number code: iso.org.dod.internet.mgmt.mib.[…]

Producer-specific OIDs on the other hand always begin with the following chain of figures (see figure 2):
1.3.6.1.4.1.[manufacturer number].[…]

Each manufacturer can register a unique manufacturer number in this number branch at the "Internet Assigned Numbers Authority" (IANA) free of charge, and make his own additions available there.

Each knot in the tree structure of the MIB contains a unique ID and a name that identify the underlying branch. To find out the address of a specific knot one has to move through the tree structure from the "root" to the bottom. The number of every knot is noted. If all the numbers of all the knots are strung together and are each separated by a dot, you can get the address of a desired object. The number is called the "OID" of an SNMP object.

FIGURE 2:
The MIB tree structure of a Linux MIB



[7] These definitions are described in RFC 2578, RFC 1155, RFC 1213, and RFC 1157.

Challenges in Connection with SNMP

Network monitoring with SNMP works very reliably in most cases. Besides the compatibility problems mentioned previously, small glitches and obstacles arise when using it in practice, which complicate a successful usage of SNMP—especially when installing it for the first time. Suitable software can help to avoid many problems right from the start. One of the greater challenges is, for example, load problems. These occur when the SNMP client triggers too many enquiries within a very short time period because of a too "optimistic" configuration and thereby temporarily disturbs or even paralyzes the network. A good solution provides sensible default-values. The overall effort needed for setup is often underestimated and it can be especially time consuming when MIBs are missing or faulty. Additionally, the RFCs explicitly allow devices to change the SNMP objects' unique address (OID) at any reboot.

An intelligent auto-discovery function in the SNMP management program (Client) takes the pressure off the administrator, as it automatically recognizes the given devices in the network and the SNMP objects contained therein. It can also make sure that devices with changing OIDs are automatically re-recognized after a reboot. You can find an elaborate description of the challenges with SNMP in the second part of this White Paper.

ALTERNATIVES TO SNMP

Looking at the slightly cumbersome first configuration, the automatic question is whether there are any other monitoring options in the network. Whether there are alternatives depends on what is to be monitored and on which systems. With PCs, there is the option to install special software (so-called "probes" or "agents"). But if a router is to be monitored, frequently the only option is to use the manufacturer's own firmware. This often is only SNMP. More expensive devices frequently have more extensive options.

NetFlow (xFlow) to Measure Bandwidth

An interesting alternative for capturing traffic information is NetFlow/IPFIX (Cisco) or sFlow and variations thereof (we will now call all of these xFlow). In these xFlow systems, the router gathers the data together into "Flows" and sends them in a bundle to the monitoring software. What is interesting is that not only the volume, but also the IP-addresses and ports, are transmitted. This allows far more detailed analyses.

However, it is a prerequisite that the router supports the xFlow-Export (e.g. only the bigger Cisco routers and switches can export NetFlow).

Packet Sniffing to Measure Bandwidth

A further option to complete data traffic within a network is the direct traffic analysis of all data packages. But in doing so, two big problems arise: extremely high demands on the system and the suitable network topology. Because each and every data package must be analyzed, an analysis computer that is capable of processing the whole network load, even with very high traffic, is needed. And this computer must be integrated into the network in such a way that it receives all the data packages. But by default, in a "switched" network, every host sees only those packages which are meant for it.

This requires a technology which can mirror all the data to be monitored to one network card. For example, this can be done with the help of "Port Mirroring," a "Monitoring-Port" or "Span" (as the technology is called with Cisco devices).

Windows Management Instrumentation (WMI)

"Windows Management Instrumentation" is Microsoft's implementation of a standard for managing IT systems. Using WMI, almost all data can be retrieved from a Windows computer. Included in this data is information on hardware and the system, entries in the events protocol, information on services and processes, registry entries, etc. Everything can be monitored via WMI, from hard disk free space to an Exchange Server's performance. As with SNMP, it is possible to get write-access on the client through the WMI protocol and set options there. By doing so not only can settings be changed, but also services stopped, values set or computers restarted. All WMI functions are controllable from remote computers via the network if the configuration is set up correspondingly.

However, this is purely a Windows standard and therefore requires special software, normally a Windows operating system no older than XP. Depending on the Windows version used and the size of the network, load problems can arise when using WMI. And the setup for remote connections, especially via a WAN, does not always work immediately.

Agent-based Systems (Usually Specific to Manufacturers)

For Windows– and Linux-based systems, it is possible to install an agent software. This little background program acts on the computer as a data server and provides the values to monitor in a format which the monitoring software can process. However, consistent standards are often missing, so the user has to decide on a certain monitoring solution in the long term. This solution will then only work with one specific agent software. Moreover, the administrator must install an agent on each system, which can be very costly—depending on the size of the network.

The Future of SNMP

Despite many problems and security risks, SNMP V1 in particular is widely used; not least because of a lack of mainstream alternatives. SNMP can be used universally and a great number of devices provide it as the sole standard to readout values. There is admittedly great potential for a new, modern, and flexible standard, but no-one can achieve it single-handedly. In the past few years, different approaches have emerged, but none of them could be established until today. It would take real cooperation among different manufacturers to develop a new standard, which is the main reason it has not happened. It is something of a chicken and egg scenario. On the one hand, a manufacturer will not worry about supporting an (experimental) protocol that he did not contribute to. On the other hand, the administrators will not be happy about a proprietary protocol that is supported by a single manufacturer only.

Indeed, SNMP (especially with V3) covers all necessary areas of application, but the setup is somewhat cumbersome and complex. Yet, it is still not complex enough to warrant the introduction of a new standard. This will not be an issue to the manufacturers; however it will be troublesome primarily for those who have to deploy SNMP. What could help here is a monitoring solution which significantly reduces the user's "perceived complexity".

Despite its numerous shortcomings, SNMP will be with us for a long time yet, even if a new standard is established. Billions of well-performing monitoring systems will not be replaced by new ones over night—as the saying goes, "Never touch a running system." This protocol may not be the best solution, but it is widely accepted and established. Once a network monitoring via SNMP is set up, it runs efficiently in most cases.

More information can be found in a Paessler article "How do SNMP, MIBs and OIDs work?" at: www.paessler.com/knowledgebase/en/topic/653

Read more about how to use SNMP in the second part of this White Paper: "Putting SNMP into practice"

ABOUT PAESSLER AG

Paessler AG leads the industry in providing the most powerful, affordable and easy-to-use network monitoring and testing solutions. The company's suite of just-right software products deliver peace of mind, confidence and convenience for businesses of all sizes – from Small Office/Home Office (SOHO) to large enterprises, including more than 70% of the Fortune 100 companies. Based in Nuremberg, Germany, Paessler's global reach includes more than 150,000 active installations of its products. Founded in 1997, Paessler AG remains a privately held company and is recognized as both a member of the Cisco Developer Network and a VMware Technology Alliance Partner.

Freeware and Free Trial versions of all products can be downloaded from www.paessler.com/prtg/download.

Paessler AG
Bucher Str. 79a, 90419 Nuremberg, Germany, www.paessler.com, info@paessler.com

VAT-ID: DE 217564187
TAX-ID: FA Nuremberg 241/120/60894
Registration: Amtsgericht Nuremberg HRB 23757

CEO/COO: Dirk Paessler, Christian Twardawa
Chairman: Dr. Marc Roessel