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 Product Development at Paessler AG

Published: August 2010 – Last Update: June 2017

# Contents

# Introduction

As business efficiency depends on connected computer systems ever more, 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 designed to monitor network devices. In addition, with SNMP you have the possibility to deal with configuration tasks and to change settings from a distance. SNMP-compatible hardware typically includes routers, switches, and servers. But you can also check and control printers, environmental sensors (temperature, humidity, etc.), and many other devices, and even powered off devices as long as they provide a lights-out management possibility, and support SNMP, of course.

Further prerequisites are that the device is connected to the network via a TCP/IP connection (supporting also User Datagram Protocol (UDP), what it normally does), and can be reached by your network monitoring tool.

Looking at the current offer of network switches, it can be claimed that for many of the cheaper devices, largely consumer products, the access to SNMP was omitted to reduce costs. Most of the professional devices by known manufacturers (for example, Cisco, Linksys and HP) offer SNMP support—a quality feature of professional network hardware.

**SNMP support is still a quality feature of professional hardware.**

# Different Development Stages

The first SNMP version (V1) was defined in 1988[2]. Although this version doesn't contain any wiretapping prevention via encryption or other security mechanisms, due to its simplicity it is still frequently used in private LANs behind a firewall. Yet use of this version is not recommended for public networks.

The lack of security shifted into focus in 1993[3] and 1996[4]. The solutions that were then discussed never really took off. Only one slightly enhanced follow-up version[5] was partly able to establish itself. When speaking of SNMP V2, what is usually meant is version "V2c". However, it has the same security system as SNMP V1, which means that it has modifiable passwords, the so-called community strings, but they are sent in clear text.

---

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

So use of version 2 is not recommended for public networks either. Nevertheless, even today many simple devices still only offer SNMP V1, or V2.

**SNMP was constantly developed further. Still, even today, not all modern devices support encrypted connections.**

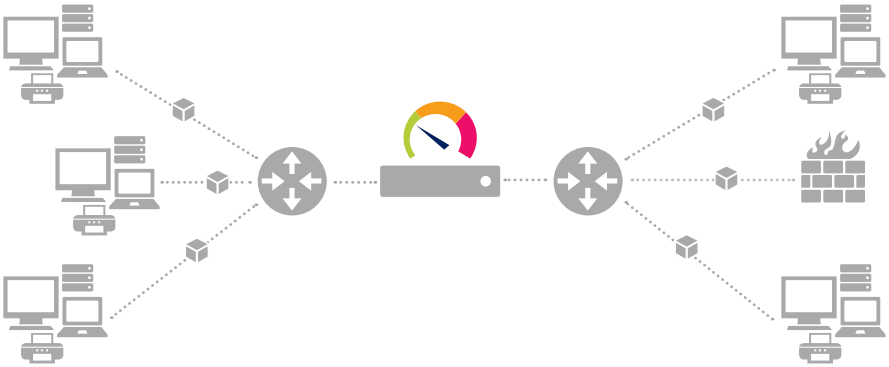
The current version is SNMP V3, which increases the security of SNMP by providing authentication and encryption methods. However, as the use of SNMP V3 is relatively complex and demanding, this version has not yet really managed to establish itself for use in intranets since its specification in 2002.

# 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 server, the so-called SNMP "agent", which is normally a piece of software running on a device. This in turn reacts by sending a UDP packet containing the SNMP message as an answer. Each single question-answer cycle enables the client to retrieve one "measurement" from the device, for example network traffic, CPU load, or temperature. Depending on the inquiry method, you can also get several measurements at a time.

**PICTURE 1:**
Client-server communication via SNMP



## CONTROL COMMANDS AND SNMP TRAPS

Beyond the pure exchange of information, you can also transfer control commands via SNMP. With these the client can set certain values and options within the device and change its settings.

**Via SNMP, it is also possible to change the configuration of a device.**

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

**Using SNMP traps, management software and admins can react much faster to new events.**

And the network management software can therefore immediately react to incidents, by sending alarms to inform the network admin, for example.

## COMPLEX DESCRIPTION LANGUAGE

So far the process is relatively simple and straightforward. Unfortunately, however, the creation of the SNMP data packages is very complex. The packages are created in a description language that is based on the fairly sophisticated Abstract Syntax Notation One (ASN.1). As the whole procedure is pretty complex, many implementations contain faults, especially in the embedded area, concerning, for example, 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 like your network management solution.

**SNMP "suffers" from its complex description language: Hardware manufacturers frequently implement the protocol incorrectly.**

As a budding monitoring software developer writing your first implementation of SNMP, you need to gain, first of all, sound knowledge, experience, and know-how of the individual manufacturers' devices by studying a growing group of customers with varied hardware setups. Through this, you gradually get to know the different problems the various hardware manufacturers have. So, via remote-debugging, you can build workarounds into your network monitoring software to smooth out the faults implemented by the hardware vendors. Network specialist Paessler has faced this challenge with its network management solution PRTG Network Monitor. Today, the software can offset many different SNMP variations from several manufacturers that are actually implemented incorrectly.

## MANAGEMENT INFORMATION BASE (MIB)

For successful network monitoring using SNMP, you need the transfer of the measurements regarding your network devices to be successful. Firstly, the available SNMP objects, standing for the "things that can be measured", must therefore be known to both the client and the server. So both the SNMP manager included in your monitoring software and the SNMP agent on your network device need to know that, for example, for your device "Server Rack" there is a monitoring object "temperature". If they do, they will be able to communicate about measurements like 36.2° and 39.6°.

Secondly, every monitoring object needs to have a unique address that the SNMP manager (client) uses in order to request a measurement and that the SNMP agent (server) uses in order to answer a request. Because so many manufacturers and many different client-server combinations exist, there needs to be an independent format for storing and accessing device information—the Management Information Base (MIB).

An MIB is a text-file, usually ending in *.mib* or *.my*, in which all searchable SNMP objects of a device are listed in a standardized tree hierarchy. An MIB contains at least one Object Identifier (OID) that delivers not only the necessary unique object address and its name, but also information on type, access rights and a description of the respective object.

### INFORMATION BOX: OIDS

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

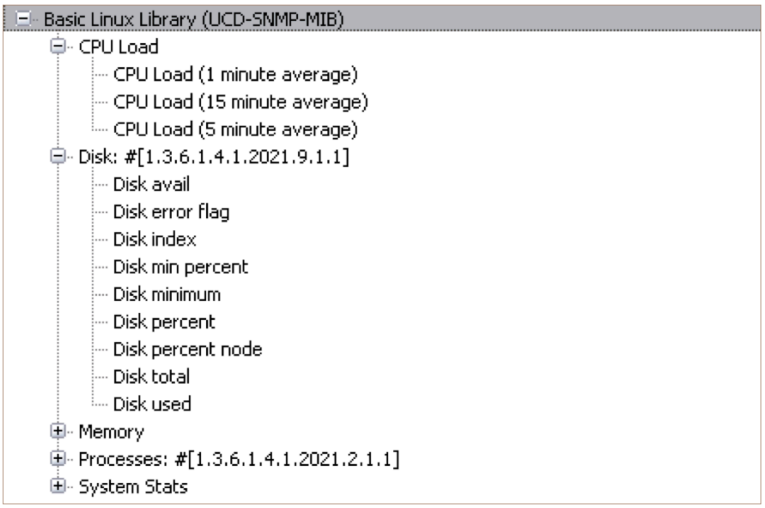
This corresponds to another spelling of the following chain of figures which can be used as an alternative to the number code: **Iso.org.dod.internet.mgmt.mib.[...]**

Producer-specific OIDs on the other hand always begin with the following chain of digits (see picture 2): **1.3.6.1.4.1.[Producer 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 their own additions to the SNMP monitoring objects to be available.

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.

**PICTURE 2:**
The MIB tree structure of a Linux MIB




MIB files are written in SMIv2, version 2 of the Structure of Management Information, an ASCII text format based on ASN.1. The current standard MIB for SNMP is the MIB-II, which has expanded the original MIB to include data types that are urgently needed.[7] Hardware manufacturers can easily upgrade MIB files with specific OIDs for their SNMP compatible devices by using additional MIB text files. Normally, they provide their specific MIBs for their customers in the internet or via their support.

## Challenges You May Face with SNMP

Network monitoring with SNMP works very reliably in most cases. However, during the setup and use in practice some small glitches and obstacles may arise, besides the compatibility problems mentioned previously, especially when installing SNMP monitoring for the first time. Suitable software like a good network monitoring tool 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 manager (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 monitoring 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 (re-) recognizes the given devices in the network and their respective SNMP objects. 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 of SNMP, you might automatically want to know whether there are any other monitoring options in the network. The answer is yes, there are alternatives, that, however, depend on what you want to monitor and on which systems. With PCs, you often have 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.

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

## NETFLOW (XFLOW) TO MEASURE BANDWIDTH

An interesting alternative for capturing traffic information is NetFlow (Cisco) or sFlow and their variations (we will now call all of them xFlow). In xFlow systems, the router gathers the data into "Flows" and sends them in a bundle to the monitoring software. What is interesting is that you do not only get the volume, but also the IP-addresses and ports. This allows you to analyze far more in detail.

**Flows allow very precise analyses of the network traffic, but they are only available for certain devices.**

However, it is a prerequisite that the router supports the xFlow-Export. For example, only the bigger Cisco routers and switches can export NetFlow.

## PACKET SNIFFING TO MEASURE BANDWIDTH

A further option to measure data traffic within a network is "Packet Sniffing", the direct traffic analysis of all data packages. But if you do so, two big problems arise: You will set extremely high demands on the analyzing system and you need a suitable network topology. Because each and every data package will be analyzed, you need an analysis computer that is capable of processing the whole network load, even with very high traffic. And this computer needs to 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 the packages that are meant for it.

**Packet sniffing delivers exact analyses, but requires very efficient computers for data calculation and a special network topology.**

This requires a technology that can mirror all the data to be monitored to only one network card. For example, you can achieve this 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, for example, information on hardware and the system, entries in the events protocol, information on services and processes, and registry entries. You can monitor nearly everything via WMI, from hard disk free space to an Exchange Server's performance. As with SNMP, you have the possibility to get write-access on the client through the WMI protocol and set options there. By doing so you can not only change settings, but also stop services, set values or restart computers. All WMI functions are controllable from remote computers via the network if the configuration is set up correspondingly.

**WMI has a large range of functions but is restricted to Windows systems.**

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, you can 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 as a user you have to decide on a certain monitoring solution in the long term. This solution will then only work with one specific agent software. Moreover, as an administrator you will have to install an agent on every system, which can be very costly—depending on the size of the network.

**Agent-based systems need an agent on each individual system.**

# The Future of SNMP

Despite many problems and security risks, SNMP, in particular V1 and V2, is still 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 establish themselves until today. It would take real cooperation among different manufacturers to develop a new standard, which is the main reason it has not happened. This is something like the chicken-and-egg dilemma. On the one hand, the manufacturers will not worry about supporting an (experimental) protocol that they 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 may be 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 can help here is a network monitoring solution that significantly reduces the user's "perceived complexity".

**A good monitoring solution reduces the "perceived complexity" of SNMP by supporting the user with setup and configuration.**

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 overnight—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.

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 200,000 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 Solution Partner Program 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** · www.paessler.com · info@paessler.com