SNMP (Simple Network Management Protocol)

Article Number: 49 | Rating: 5/5 from 1 votes | Last Updated: Tue, Feb 9, 2016 at 10:29 PM

Target Audience

SNMP is a powerful tool that Nagios can use to check and monitor your computer, device, and network.

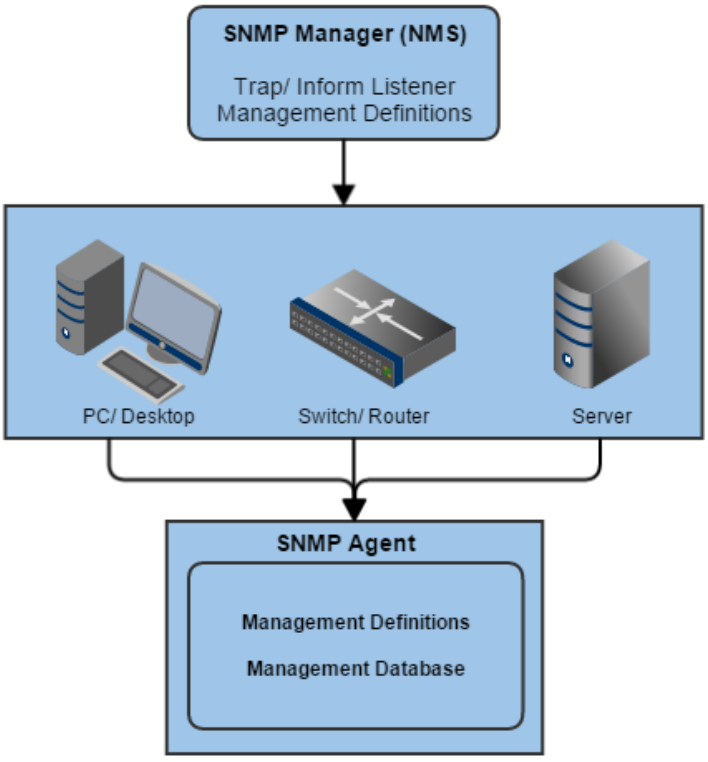
SNMP (Simple Network Management Protocol) is a protocol defined by the IETF (Internet Engineering Task Force) to help manage and monitor equipment connected to a network. This document will give you a brief overview, and links to additional documentation.

SNMP

SNMP stands for Simple Network Management Protocol, but it is not so simple, the concept of it is really simple- send a few packets of information out to a device across the network and get a few packets of information back. The original definition documents are pretty straight forward. But as computers/networks/devices evolved so did SNMP. One of the notable evolutions in SNMP has been Authentication.

In addition because this is a "standard" it is implemented by different companies, naturally each implementation will have differences in the way they work. Which leads to differences in how to work with them. Because this "standard" is implemented by different companies, each implementation can vary in how they respond and what data they communicate/produce. This naturally leads to some differences in how to interact with the different implementations. This means that often what has worked with one device may need to be altered some to work with a different device by a different vendor.

SNMP Workflow



The **SNMP Manager** (Network Management System) will send a get request to the devices then they will get to the device, populate the request and send it back to the SNMP agent where the Management Definitions and Management Database are updated. The second block is the **Managed Devices** (can be routers, switches, workstations, printers, USPs, etc.) that will be monitored and send SNMP data back to the Agent. The last block is the **SNMP Agent** will accept any SNMP communication and read the current Management Definitions and database and store any Management Information as defined by the **MIB**.

SNMP Commands

GET: Generated by Manager to managed device. Retrieves one or more values from the managed device.

GET NEXT: Same as the regular GET, but it retrieves the value of the next OID in the MIB tree.

GET BULK: Retrieve large MIB table data in volume.

SET: Used by manager to adjust or assign a value on the Managed Device.

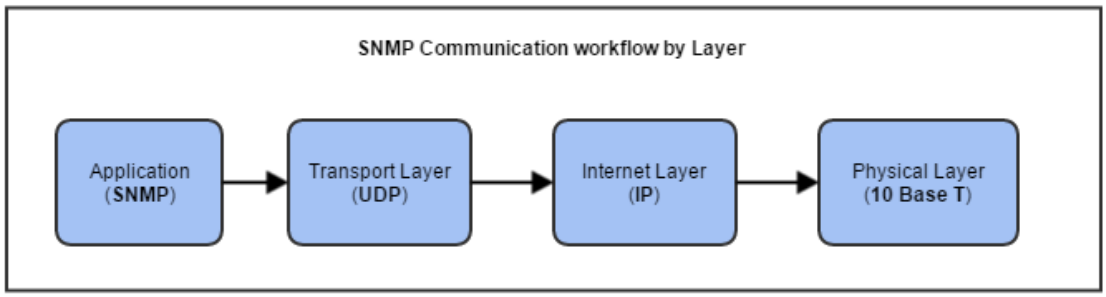
TRAPS: Initiated by AGENT to Manager to signal the occurence of an event.

INFORM: Similar to TRAP, initiated by AGENT, but includes a confirmation that the Manager received the message.

RESPONSE: The command used to carry back values or action signals directed by the Manager.

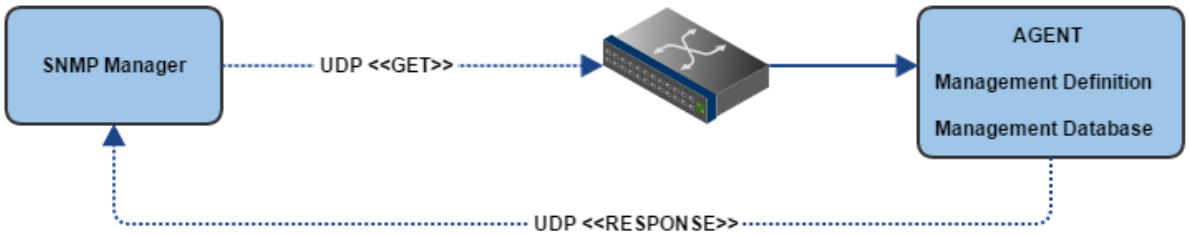
SNMP Communication

SNMP is part of the TCP/IP protocol suite and is wrapped before it is sent. Here is the basic four-layer model developed by the Department of Defense (DoD):



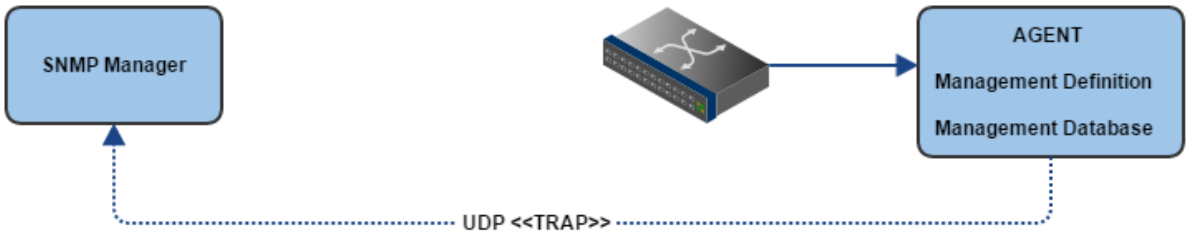
By Default SNMP uses port **161** and TRAP/INFORM uses port **162** for communication. Here is the basic communication flow for each type of action:

GET (GET NEXT/GET BULK/GET SET)



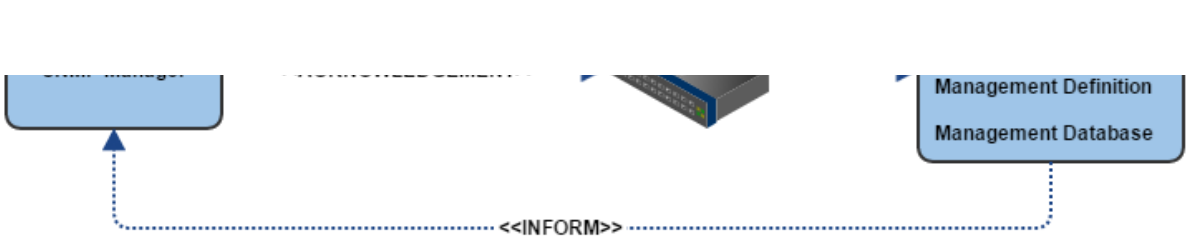
GET operations are a request for one or more values of information from the Managed Device.

TRAP



The **TRAP** is sent from the device back to the manager on the occurrence of an event.

INFORM



INFORM start at the device which will use the Management Definitions to create an INFORM message and send it the SNMP Manager. If it is received successfully the Manager will send an ACKNOWLEDGEMENT message back to the device.

SNMP Terminology

There are a lot of parts involved in SNMP, but going over each term and defining it briefly can help troubleshooting problems in the future or just allow for better understanding of SNMP in general. (alphabetical)

ASN.1 - Abstract Syntax Notation One. A description language used to describe SNMP data types in machine architecture-independent format. Used to write MIBs.

Community - The term community refers to the SNMPv1 or SNMPv2c configured request name. A community is used when making SNMPv1 or SNMPv2c requests to an SNMP agent.

IETFT - The Internet Engineering Task Force. A standards body that forms Working Groups to develop technology for the Internet community. When protocol is deemed ready to move forward in the standards process, the IETF sends its recommendations to the IESG.

MIB - Management Information Base: The structure that describes the management data of a device using OID's

MIB Family - For the purpose of writing method routines, SNMP variables are separated into families. A family consists of all of the leaf MIB variables with the same immediate parent node, or root (the Object Identifier without the instance information). For example, in MIB-II the following variables form a single family since they are all children of ifEntry (1.3.6.1.2.1.2.2.1):

```
ifIndex 1.3.6.1.2.1.2.2.1.1
ifDescr 1.3.6.1.2.1.2.2.1.2
...skipping entries between...
ifOutQLen 1.3.6.1.2.1.2.2.1.21
ifSpecific 1.3.6.1.2.1.2.2.1.22
```

Note that ifNumber (1.3.6.1.2.1.2.1) is also a member of the interfaces group, but it is not a member of the same family since it is not a child of ifEntry.

NSTI - Nagios SNMP Trap Interface

OID - Object Identifier: Identifies a variable that can be read or set by SNMP.

Security Level (SNMPv3) - users can be configured to use one of the following security levels:

- No authentication and no privacy (**noAuthNoPriv**)
- Authentication and no privacy (**authNoPriv**)
- Authentication and privacy (**authPriv**)

SNMP - Simple Network Management Protocol

SNMP Trap - Asynchronous notification from *agent to manager*.

SNMPv1 - The first incarnation of the Simple Network Management Protocol- deprecated.

SNMPv2c - Community-based SNMPv2. A historic protocol published in RFC 1901 which combines SNMPv2c operations (such as GetBulk) with SNMPv1 trivial authentication.

SNMPv3 - Simple Network Management Protocol version 3. The specification for this Full Standard protocol is published in RFCs 3410 and 3418. SNMPv3 provides a Full Standard administrative framework (authorization, access control, etc.) and a remote configuration/administration MIB.

TCP - The Transmission Control Protocol is a connection-oriented transport-layer protocol. It attempts to achieve reliability through retransmission.

UDP - The User Datagram Protocol is a connectionless end-to-end transport-layer protocol.

User - The term "user" refers to the SNMPv3 USM users configured on an SNMP agent. The user is used when making an SNMPv3 request to an agent that supports SNMPv3.

Additional Informational Links

See SNMP Tools on Nagios KB

See SNMP Traps on Nagios KB

snmp.com Glossary of Terms

IETF RFC1098 - "A Simple Network Management Protocol (SNMP)"

Wikipedia SNMP Page

The Internet Engineering Task Force (IETF®)

Final Thoughts

For any support related questions please visit the Nagios Support Forums at:

http://support.nagios.com/forum/

Posted by: **bdgoecke** - Mon, Feb 2, 2015 at 3:56 PM. This article has been viewed 7969 times.

Online URL: https://support.nagios.com/kb/article/snmp-simple-network-management-protocol-49.html