



F5 White Paper

SNMP: Simplified

The Simple Network Management Protocol defines a method for managing devices that connect to IP networks. The “simple” in SNMP refers to the requirements for a managed device, not the protocol. This white paper defines the history, frequently used terms, and implementation of SNMP.

by Peter Murray and Paul Stalvig
Technical Marketing Managers



Contents

| | |
|-----------------------|----------|
| Introduction | 3 |
| History | 3 |
| Definitions | 5 |
| Implementation | 8 |
| Perspective | 9 |
| Conclusion | 9 |



Introduction

It's no secret that managing networks and applications are complex tasks. Multiple technologies are in use today, often by the same organization. This article presents an overview of one technology: the Simple Network Management Protocol (SNMP).

SNMP offers a method to monitor and manage network devices and hosts. This document offers a simplified view of SNMP fundamentals and explains how the fundamental components work together. We'll look at concepts including network elements, the Network Management Station (NMS), SNMP and RMON probes, the Management Information Base (MIB), Object Identifiers (OID), and more.

Reading this can help you to achieve two objectives: 1) to better understand SNMP's purpose and history, and 2) to help you better understand how its components work together to deliver management information and control network devices.

History

Prior to SNMP, most network devices were managed as individual elements by proprietary network management software. These software point products could only manage a single vendor's devices, and some were merely text-based command-line utilities.

The lack of functionality and interoperability resulted in overly complex management implementations. Using a multitude of management systems and network-related commands made troubleshooting network-related issues extremely difficult, and prevented IT administrators from being able to see a single, more complete view of the end-to-end network.

Defined by the Internet Engineering Task Force (IETF) in the late '80s, SNMP was designed to help monitor complex multi-vendor networks. Since then, two more SNMP versions have been ratified by the Internet Engineering Task Force (IETF). SNMP v1 provided the basic structure and process required to define network management information, retrieve information from network devices, control devices, and allow unsolicited messages—called Traps—to be sent to a NMS.

The public, or generic, portion of the SNMP MIB defines generic device information, some limited performance information, and higher level performance information. The public portion defines information that is primarily useful for



end stations. Device information and limited network information is available in the public MIB.

The lasting power of SNMP developed out of the capability for other organizations to extend the MIB. Most network equipment manufacturers have added private extensions to the SNMP MIB that define proprietary equipment information. For example, an Ethernet switch manufacturer may offer a private MIB extension that includes per-port traffic, user, and error information.

SNMP Versions

SNMP v1 has been extended several times to incorporate new features, SNMP v2 added several features, including the capability to retrieve data in bulk rather than individually, and added the capability for the NMS to acknowledge a trap message. SNMP v3 added encryption both for the community strings that are used to access to a network device and the SNMP data transmitted between devices.

SNMP Data Collection

SNMP was primarily used for device-based management, and was designed to be as non-invasive as possible. An important requirement for SNMP was to minimize managed-element processing overhead. SNMP was therefore designed to collect and report information, but not to provide sophisticated information processing. For example, an SNMP-managed node doesn't report information such as link throughput; rather, SNMP defines the information to be collected and relies on the NMS to retrieve and process the information to produce a derived value.

In this example, determining link throughput requires an NMS to collect two items from a managed node—the packet count from a network interface, and system time. Collection must be performed twice. The NMS then calculates the number of bits sent or received over the specified time period.

RMON MIB Extensions

The Remote MONitoring (RMON) extensions to SNMP, including RMON 1 and RMON 2, were defined by the IETF to add “flow-based” monitoring, as opposed to “device-based” monitoring, which is what SNMP primarily delivers. The first version, RMON 1, defined ten management groups that focused on OSI Layer 1 and Layer 2 information in Ethernet and Token Ring networks, which help to monitor LANs. The second version, RMON 2, included ten more groups that added support for network protocol- and application-layer monitoring. Compared to standard SNMP agents, agents that fully support RMON management require more processing capability. Because of this requirement, full RMON management is typically carried out by one or more probes designed specifically for RMON.



When implemented fully, RMON can provide many of the features and functionality offered by network analyzers. The disadvantage to RMON is that RMON agents shoulder a greater management burden because they must collect information from managed elements and process that information to provide higher-level data.

Many network devices lack the processing horsepower required for extensive processing and instead implement only a small subset of the RMON groups. In fact, a device must only support statistics, history, alarms and events, the first four RMON 1 groups, to be labeled as RMON-compliant.

SMON MIB Extensions

The Switch MONitoring (SMON) definition further extended RMON to include detailed (typically Ethernet-based) LAN switch information. SMON enabled device-wide reporting and control for the one or more virtual LANs (VLANs) defined on the switch.

Definitions

Often technologies like SNMP change over time due to proprietary vendor extensions and implementations, requiring users to learn numerous new terms. Oddly, SNMP terms have remained true to the initial terminology. While this may seem irrelevant, it actually shows the full commitment and support vendors have made to SNMP. Below are the necessary definitions for understanding how SNMP works.

Network Element(s): “Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations” (J. Case, 1990). Quite simply, a network element is a monitored device. An element is often referred to as a node or a managed node. The (managed) node construct allows SNMP administrators to reference network elements without the complexity normally associated with other system administrators. SNMP administrators may use agent to refer to the software running on a given network element.

Network Management Station (NMS): A server that runs the network management application. It is the primary recipient that network elements communicate with to relay the management and control information; it also provides the methods and means to analyze and report significant information.



SNMP Relay Device (also known as SNMP Probe, SNMP Collection Point, SNMP Proxy Agent): A node that polls Network Elements to collect information as a proxy for one or more NMSs. The collecting device may itself be an NMS, for example, residing in a regional data center. An SNMP Relay Device helps localize SNMP polling and trap reception, thereby reducing SNMP traffic across enterprise backbones and WAN links. An SNMP Relay Device may do local processing to summarize data that can then be sent in bulk to the NMS.

RMON Probe: An RMON probe, which resides on a specific LAN, collects information for that LAN, performs more sophisticated processing than an SNMP agent, and reports more complex information such as link and individual Layer 2 throughput.

Stand-alone RMON probe appliances are another solution that often delivers more complete RMON feature support than that found in most network equipment. RMON and SMON enabled administrators to place probes in the network to perform remote polling, logging, and trap forwarding functions. Probes typically have the extra processing power to analyze and distill information before it is transferred to an NMS.

Management Information Base (MIB): The MIB is a database containing Object Identifier (OID) information. The MIB can be depicted as a hierarchical tree-based structure where the MIB is the “tree” and each individual object is a “leaf.” Each individual object is identified by an OID. Levels within the MIB are assigned by different organizations. The top-level MIB OIDs belong to various standards organizations, while lower-level OIDs belong to associated organizations such as Network Equipment Manufacturers, who assign OIDs that extend the MIB with proprietary values.

Object Identifier (OID): Object Identifiers identify individual entries, or objects, within the MIB. OIDs are specified using an “x,y” naming convention, defined by Abstract Syntax Notation One (ASN.1). In this naming convention, “x” is a numeric value identifying an OID’s position within the MIB tree and “y” is a human-readable OID name, also called a *variable name*. The numerical OIDs make searching through the MIB and reporting “human readable information” an easier process. Figure 1 represents the F5 OID hierarchy, which defines all OIDs that reside below the string beginning with 1.3.6.1.4.1.3375.

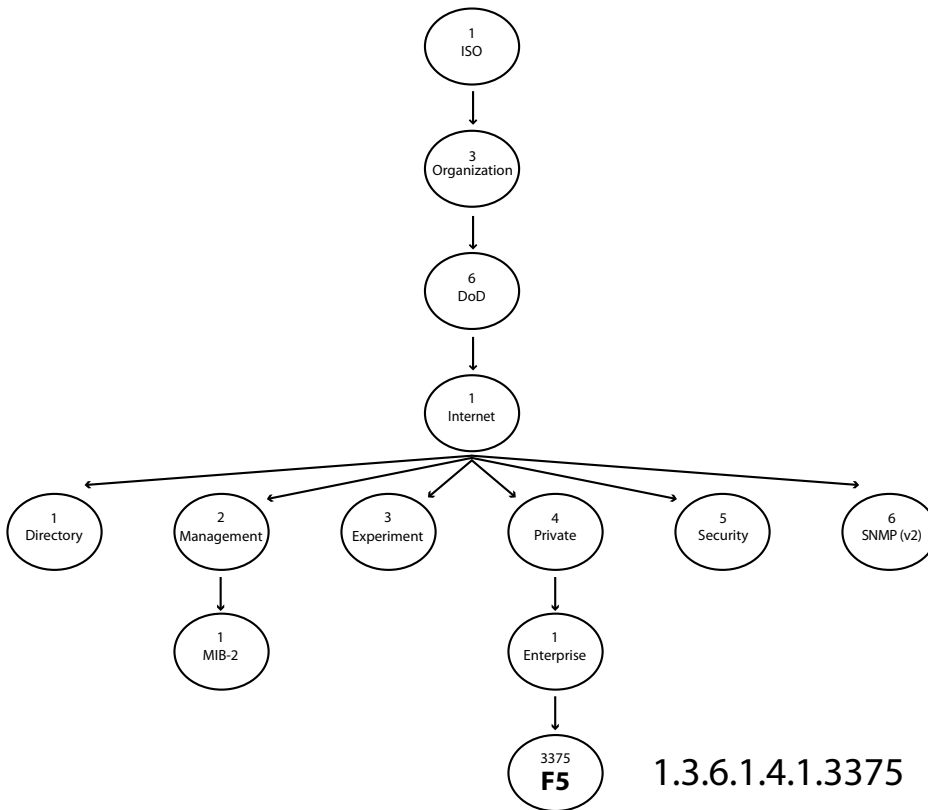


Figure 1: F5 OID hierarchy

Protocol Data Unit (PDU): A PDU tells the NMS and/or the agent what SNMP action to take. SNMP version 1 contained the five following PDUs: GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap. SNMP version 2 added GetBulk Request and Inform (which acknowledges a Trap). GetResponse is the only PDU used to respond to GetRequest, GetNextRequest, GetBulk, and SetRequest PDUs. All PDUs except Trap are sent via User Datagram Protocol (UDP) on Port 161. Traps are sent on UDP Port 162.

Traps or Alerts: Traps or alerts are the method by which important, unsolicited information is reported to an NMS by a network element to an NMS or probe. No trap response is defined in SNMP v1, and each managed element must have one or more Trap receivers defined for the Trap to be effective.

In SNMP version 2 and higher, the concept of a Trap was extended using another SNMP message called Inform. Like a Trap, an Inform message is unsolicited. However, Inform enables an NMS running SNMPv2 (or higher) to send a Trap to another NMS, and can also be used by a SNMP v2 (or higher) managed node to send an SNMP v2 Trap. The receiving node sends a response telling the sending NMS that the receiving NMS received the Inform message. Both messages are sent on UDP Port 161.

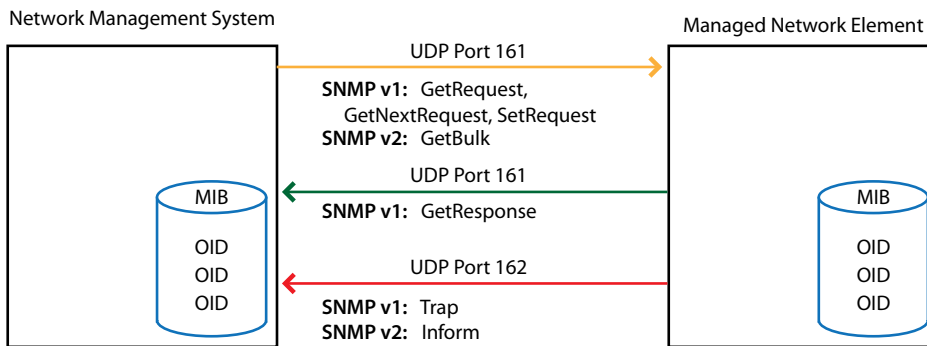


Figure 2: SNMP Communication

Community: SNMP specifies two groups, called communities, to enable access to the OIDs on a managed element. SNMP community strings function as passwords to secure access to an element's OIDs. The read-community string, named *public* by default, allows read-only access, while the write-community string, named *private* by default, allows write access. Both community strings must be defined for full management access to an element, and common community strings must be defined on all elements, probes, and NMSs for full management in an SNMP domain. Note that until SNMP v3, community strings were sent in clear text, reducing SNMP security. Version 3 specified encrypted community strings and PDUs.

Implementation

Now that we've looked at definitions, it's easier to see how SNMP operates in a network. In its simplest form, an SNMP agent is loaded on a host with the appropriate MIB components. MIB components include the SNMP MIB, and may include RMON extensions, SMON extensions, private MIB extensions, or a combination.

The agent is configured to communicate with one or more NMSs using specific SNMP community strings. The NMS IP address is also configured to enable the agent to send Traps or Notifications. The agent contains the SNMP MIB and typically, the manufacturer's private MIB extensions. The agent may also contain RMON or SMON extensions.

The NMS is configured with the same community strings as the elements it manages. The NMS is also configured with the appropriate combination of the SNMP MIB, RMON extensions, SMON extensions, and private MIB extensions required to manage the agents for which it is responsible. The NMS is also configured, either manually or through automatic discovery, with the IP addresses of the agents it is to manage. Note that SNMP communication requires network devices to open UDP Ports 161 and 162 for polling and Traps/Notifications.



After initial configuration is complete, the agent collects information. The NMS periodically polls the agent. When appropriate, the agent sends Traps to the NMS. The NMS can also be used to modify agent configuration as appropriate.

In a more complicated network, probes or multiple NMSs may be used in remote sites to limit WAN-based SNMP communication. Probes typically collect SNMP, RMON, or SMON MIB and process the data as appropriate (RMON and SMON only). Remote NMSs may also relay information to one or more centralized NMSs.

The central NMS polls probes and remote NMSs for agent data, enabling local administration (where appropriate), centralized administration for a complete network overview, and summarized (bulk) data transfer from remote sites to reduce WAN utilization.

Perspective

Compared to previous monitoring and management methods, SNMP reduces the amount of overhead on the network element. Reduced processing overhead and a common platform enables growth and platform independence. This allows SNMP to be used on almost every IP network, often using a single, centralized NMS. While larger IP networks may require SNMP proxies to minimize WAN-based SNMP traffic, the reduction in the number of NMSs compared to previous methods enabled IT to focus on the other issues and to simplify the management network.

Conclusion

Through the use of SNMP agents, probes, and NMSs, information technology systems-monitoring has grown dramatically and has drastically reduced the requirement for administrators to manually monitor individual network components. The ability to have systems inform an NMS, and ultimately humans, of error conditions has led to increased uptime and availability. While not perfect, SNMP provides many of the tools necessary to collect and analyze data to enable system tuning for optimum performance and to identify when and where future growth in the network is required.



F5 Networks, Inc.
Corporate Headquarters

401 Elliott Avenue West
Seattle, WA 98119
+1-206-272-5555 Voice
(888) 888IGIP Toll-free
+1-206-272-5556 Fax
www.f5.com
info@f5.com

F5 Networks
Asia-Pacific

+65-6533-6103 Voice
+65-6533-6106 Fax
info.asia@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa

+44 (0) 1932 582 000 Voice
+44 (0) 1932 582 001 Fax
emeainfo@f5.com

F5 Networks
Japan K.K.

+81-3-5114-3200 Voice
+81-3-5114-3201 Fax
info@f5networks.co.jp