A Brief Tour of the Simple Network Management Protocol

Ian A. Finlay, CERT® Coordination Center

Have you ever remotely configured or monitored a device connected to the Internet? If you have, you may have used the Simple Network Management Protocol (SNMP).

SNMP is the most popular protocol used to manage networked devices. It was designed in the late 1980s to facilitate the exchange of management information between networked devices operating at the application layer of the ISO/OSI model. SNMP is formally defined in RFC 1157:

> *Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. 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. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements.*

Network Configuration

One of the most common uses of SNMP is for remote management of network devices. SNMP is popular because it is flexible. Vendors can easily add network-management functions to their existing products.

An SNMP-managed network typically consists of three components: *managed devices, agents,* and one or more *network management systems.*

A *managed device* can be any piece of equipment that sits on your data network and is SNMP compliant. Routers, switches, hubs, workstations, and printers are all examples of managed devices.

An *agent* is typically software that resides on a managed device. The agent collects data from the managed device and translates that information into a format that can be passed over the network using SNMP.

A *network-management system* monitors and controls managed devices. The network-management system issues requests, and devices return responses.

Network-management systems and agents communicate using messages. SNMPv1 supports five different types of messages: *GetRequest, SetRequest, GetNextRequest, GetResponse,* and *Trap.* A single SNMP message is referred to as a Protocol Data Unit (PDU). These messages are constructed using Abstract Syntax Notation One (ASN.1) and translated into binary format using Basic Encoding Rules (BER). Each message type has a different purpose:

GetRequest is typically used by the network-management system to retrieve one or more values from an agent.

SetRequest is used by the network-management system to set the values within a device.

GetNextRequest is used by the network-management system to retrieve the next value in a table or a list within an agent.

GetResponse informs the management station of the results of a *GetRequest* or *SetRequest* by returning an error indication and a list of variable/value bindings.

Trap messages are sent from agents to managers. *Trap* messages are unsolicited (the manager does not issue a request message) and may indicate a warning or error condition or otherwise notify the manager about the agent's state. In essence, *Trap* messages provide an immediate notification for an event that might only be discovered during infrequent polling.

Network Monitoring

SNMP runs on a multitude of devices and operating systems, including, but not limited to,

- core network devices (routers, switches, hubs, bridges, and wireless network access points)
- operating systems
- consumer broadband network devices (cable modems and DSL modems)
- consumer electronic devices (cameras and image scanners)
- networked office equipment (printers, copiers, and FAX machines)
- network and systems management/diagnostic frameworks (network sniffers and network analyzers)
- Uninterruptible Power Supplies (UPS)
- networked medical equipment (imaging units and oscilloscopes)
- manufacturing and processing equipment

The SNMP protocol enables network and system administrators to remotely monitor and configure devices on their network, such as routers, switches, hubs, and servers. For example, if a system administrator wants to know how much traffic is flowing through a network device, she might poll the device using SNMP. Once the data is pulled from the router or switch, it can be interpreted in a number of different ways. Network traffic throughput is not the only thing you can monitor using SNMP. It is also used to monitor

CPU usage, device voltage and attributes, and environmental conditions. For example, a system administrator could monitor the temperature of a router chassis based on information obtained through use of SNMP. Monitoring environmental conditions of routers is imperative because if the temperature climbs to high, the device could be damaged.

SNMP and Security

SNMPv1 uses something called a community string for authentication purposes. The community string is really a password that is used to control access to information residing on a managed device. There are two types of community strings: read only and read-write. The read only community string allows you to query the device and only read values, while the read-write community string allows you to not only read values but make changes to those values as well. The problem is that community string names are transmitted in clear text. Any attacker sniffing the network can ascertain the community name from passing traffic. Once this community name is known, the attacker can then potentially read values off of the managed device or make configuration changes.

In many cases, an attacker does not even need to sniff the network traffic to obtain a community name. They can **guess** them. History has shown that many network administrators use easy to guess or well known community names (such as 'public,' 'admin,' or 'private') and sometimes no password at all.

There are also other ways in which attackers can access information. SNMP messages are typically passed over the network using UDP (a connectionless transport service). Because UDP is a connectionless transport, the delay, replay, and reordering of packets is a possibility. As such, it's possible for an attacker to maliciously reorder, replay, and delay packets. As a result, an attacker may be able to influence the behavior of a managed device.

Later versions of SNMP attempt to address these security issues. Quoting from RFC 2271:

> *The Security Subsystem [within the SNMP protocol] provides security services such as the authentication and privacy of messages…*

Recently, numerous vulnerabilities have been reported in multiple vendors' SNMPv1 implementations. These vulnerabilities are as a result of implementation errors, not problems in the protocol itself. The vulnerabilities in the decoding and subsequent processing of SNMP messages by both managers and agents may result in denial-of-service conditions, format string vulnerabilities, and buffer overflows. Some vulnerabilities do not require the SNMP message to use the correct SNMP community string. For more information, see CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP) (http://www.cert.org/advisories/CA-2002-03.html).

Appendix: References and additional information

Web pages

http://www.cert.org/advisories/CA-2002-03.html
http://www.kb.cert.org/vuls/id/854306
http://www.kb.cert.org/vuls/id/107186
http://www.cisco.com/warp/public/535/3.html
http://www.comsoc.org/livepubs/surveys/public/4q98issue/stallings.html
http://www.snmplink.org/
http://www.solarwinds.net/Tools/SNMP.htm

RFCs

RFC 1212 *Concise MIB Definitions*
RFC 1213 *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*
RFC 1215 *A Convention for Defining Traps for use with the SNMP*
RFC 1270 *SNMP Communications Services*
RFC 2570 *Introduction to Version 3 of the Internet-standard Network Management Framework*
RFC 2571 *An Architecture for Describing SNMP Management Frameworks*
RFC 2572 *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*
RFC 2573 *SNMP Applications*
RFC 2574 *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
RFC 2575 *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*
RFC 2576 *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*
RFC 3000 *Internet Official Protocol Standards*