SNMP

Prof Brijendra Singh
Department of Computer Science,
Lucknow University, Lucknow

The Simple Network Management Protocol (SNMP) is a management protocol designed to make sure network protocols and devices not only work but work well.

SNMP is an Internet Standard protocol for collecting and organising information about managed devices on IP networks and for modifying that information to change device behaviour.

Simple Network Management Protocol is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organised in a management information base (MIB) which describe the system status and configuration.

SNMP has several goals.

The first is to simplicity SNMP function to reduce support costs and make SNMP easier to use.

Second, it must be extensible to accommodate future updates in network operation and management.

Third, the protocol must be independent of design, specifies of hosts or routers.

Three versions of SNMP have been developed and deployed. SNMPv1 is the original version of the protocol. More recent versions, SNMPv2 and SNMPv3, feature improvements in performance, flexibility and security.

In typical uses of SNMP, one or more administrative computers called *managers* have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes a software component called an *agent* which reports information via SNMP to the manager.

An SNMP-managed network consists of three key components:

- Managed devices
- Agent – software which runs on managed devices
- Network management station (NMS) – software which runs on the manager

SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as configuration changes, through remote modification of these variables.

SNMP operates in the application layer of the Internet protocol suite. All SNMP messages are transported via User Datagram Protocol (UDP).

SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol.

SNMPv1 may be carried by transport layer protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless-mode Network Service (CLNS), AppleTalk Datagram Delivery Protocol (DDP), and Novell Internetwork Packet Exchange (IPX).

Version 1 has been criticised for its poor security.

SNMPv1 and SNMPv2 use communities to establish trust between managers and agents. Most agents support three community names, one each for read-only, read-write and trap. These three community strings control different types of activities. The read-only community applies to get requests. The read-write community string applies to set requests. The trap community string applies to receipt of traps. SNMPv3 also uses community strings, but allows for secure authentication and communication between SNMP manager and agent.

SNMP version 2 introduces the option for 64-bit data counters. Version 1 was designed only with 32-bit counters which can store integer values from zero to 4.29 billion (precisely 4,294,967,295).

Security was one of the biggest weakness of SNMP until v3. Authentication in SNMP Versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent.

The security approach in v3 targets:

- Confidentiality – Encryption of packets to prevent snooping by an unauthorised source.
- Integrity – Message integrity to ensure that a packet has not been tampered while in transit including an optional packet replay protection mechanism.
- Authentication – to verify that the message is from a valid source.

SNMPv3 provides three important services: authentication, privacy, and access control.

The first two are parts of the user-based security model and the last is defined in the View-based access control model.

REFERENCE:

Book: Network Security and Management,

Author: Prof Brijendra Singh

Publisher: PHI Learning Private Limited, New Delhi,