Int. Conf. on Signal, Image Processing Communication & Automation, ICSIPCA

Literature Survey on SNMP

Pallavi Awasthi[1], Divya M.N[2] and Sudeshna Roy[3]
[1]M.Tech Scholar, School of ECE, Reva University
awasthi8394@gmail.com
[2]Professor, School of ECE, Reva University
divya.mn@reva.edu.in
[3]R&D Engineer, Logic-Fruit Technologies
sudeshna.roy@logic-fruit.com

***Abstract*— Simple Network Management Protocol (SNMP) is widely used network management protocol on the TCP/IP-based network. SNMP has been recommended by the Internet Activities Board (IAB) as it is full Internet standard and will be used for the management of the nodes over the internet. The usefulness of SNMPv1 was improved by the SNMPv2c, yet at the same time, both the variants needed security highlights which were additionally incorporated into the later form that is SNMPv3.This overview fundamentally concentrates on the near contrasts between the distinctive variants of SNMP that is primarily SNMPv1 and SNMPv3, their further act of spontaneities and future degrees.**

***Index Terms*— SNMPv1, SNMPv3, MIB, SMI, TCP/IP.**

I. Introduction

In today's system of switches, switches, servers and other system network equipments make an exceptionally complex system. It is an difficult task to manage all the network devices in an expansive system effectively. The broadly useful of Network Management is to monitor the system successfully and effectively by using different system management tools. The fundamental motivation behind system administration is to catch all the approaching and active traffics from/to a system and investigate this and creating a report which will mirror the aggregate soundness of a system. SNMP is a protocol through which any network can be checked. It is an extremely straightforward protocol and easy to implement.

Figure 1 demonstrates the SNMP comprises of Manager, Managed devices, SNMP agents, Management Information Database Otherwise called as Management Information Base (MIB).

SNMP works in simple straightforward customer server pattern, where, customers are the SNMP agents who report the obliged data to the server where SNMP manager gets and controls or deals with the application. SNMP agent gets the required data from the MIB which must be installed according to the requirements.

An SNMP agent is running in all SNMP managed network devices. The principle of this agent is to constantly gather the data that the manager may request and react to the request from at least one or more management stations with suitable information. In the actual implementation, the agent is any system which response to the SNMP request. At the time of system re-boot or illegal access or in the situations, where the quick correspondence is required, SNMP agent can send trap messages to the manager directly without waiting for the request information.

Grenze ID: 02.ICSIPCA.2017.1.19

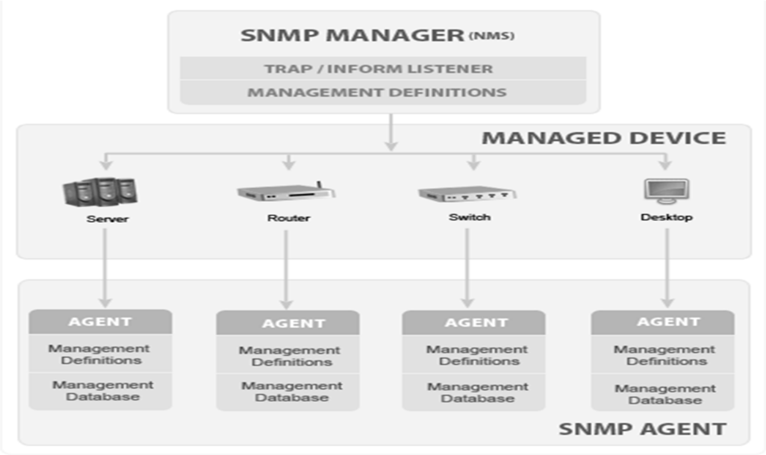

Figure1. Basic SNMP Communication Diagram

II. SNMP

Simple Network Management Protocol is a set of protocols for managing and monitoring network devices. There are three primary functions with SNMP utilized by the administrators of the Network Management System (NMS), the SNMP GET operation which gets information from a device with SNMP support, the SNMP SET operation which changes values in a device for managing it, additionally there is a probability of telling the network on the system to send data if a specific parameter is met, this is known as a TRAP message.

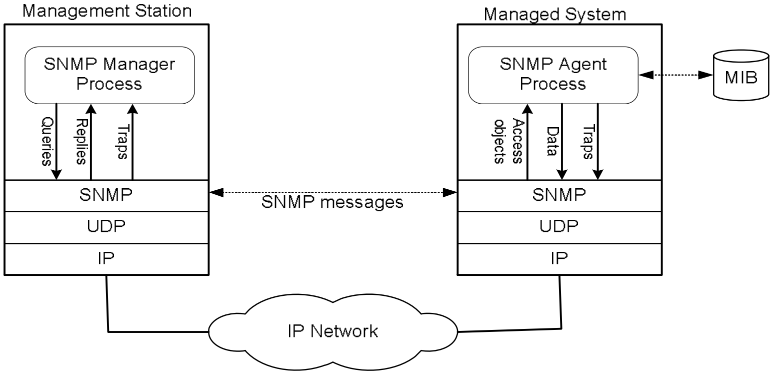

Figure 2. Interactions in SNMP

The figure 2 demonstrates the interaction in SNMP by management station and managed station. The interaction is performed by using the SET, GET, and TRAP which performs the respective operations as discussed above.

A. SNMPv1

SNMPv1 was the first standardized protocol for Simple Network Management Protocol. It was standardized in 1988 by IETF and is defined in the RFC 1157. The greatest concern in this variant of the convention is the absence of security; it is only on communities plain-content passwords that permit all devices with the community string to communicate with each other.

B. SNMPv2

SNMPv2c is the successor of the SNMPv2 protocol and is used in large portions of today's SNMP monitoring. It was defined in RFC 3416, RFC 3417 and RFC 3418. SNMPv2 introduced the Protocol Data

Unit (PDU) Inform Request which is much similar to the TRAP notifications but with an acknowledgement that the packet has been received; if no acknowledgement is received by the sending manager then the notification will be re-sent. This version of the protocol also includes upgrades in e.g. error handling, performance and set commands.

C. SNMPv3

SNMPv3 is the most up to date form of the SNMP protocol. This version of the protocol fundamentally focuses on security; thusly this is most well known for using SNMP over the insecure internet. SNMPv3 encrypts its packets with DES encryption to guarantee privacy and moreover it uses the standardized User-bases Security Model (USM) in its architecture. Not all devices support SNMPv3 and this together with the complexity of installing SNMPv3 result in many organisations using SNMPv2 as their protocol for SNMP communication. Every agent inside the network devices which use SNMPv3 has its own unique identifier called engine ID, the engine ID can be set by the administrator or be configured by the manufacturing company. This consolidated with passwords and encryption represents the biggest security changes implemented by SNMPv3.

D. Management Information Base

MIB is a database which stores all the information depicting the managed devices. This database is used by the SNMP manager to query the required information from the agent. MIB, for the most part, contains factual and control values for the hardware node on a network. SNMP as a matter, of course, has fundamental MIB supporting the capacity of minimum necessary values. However, MIB can be extended by writing our own SNMP handlers. These SNMP handlers are required for deciphering the information as required by the manager.

MIB is virtual databases utilized for managing the entities in a communications network. Generally introduced on present day network equipment before shipped from the manufacturer but can also be supplemented with more MIBs by the administrator; this indicates that SNMP is adaptable and safe for future updates. The objects in the MIB are characterised utilizing a subset of Abstract Syntax Notation One (ASN.1) and the database containing these objects are hierarchical (tree-structured). The entries in the databases are addressed through Object Identifiers (OID), different diverse items have distinctive MIBs pre-programmed in their system and OIDs are used distinguish the distinctive MIBs and entries.

E. Structure of Management Information

SMI is an RFC standard that characterizes how MIBs is named and specifies their related data types, SMI has been released in two versions, SMIv1 (RFC 1155) and SMIv2 (RFC 2578). SMIv2 was standardized to give improvements to SNMPv2. Coding in SMIv1 implements the syntax attribute of ASN.1; ASN.1 follows Basic Encoding Rules (BER). BER characterizes how the objects are encoded and decoded so that they can be transmitted over a transport medium such as Ethernet. SMIv2 adds a new leaf to the OID tree under the internet sub tree which is called SNMPv2. SMIv2 likewise includes various fields which give prominent control on how an object is accessed.

III. SNMP Vulnerability and Solution

A. Description

By enabling SNMP services, devices can monitor the network statistics such as port utilization, device connectivity, errors, packet drops, packet discards, and other critical network health statistics. By enabling SNMP services it is easy to administrate any network adequately and productively yet enabling it will make a network defenseless to security attacks. It could enable an intruder to gain unapproved access to the system on which the SNMP software is running, launch denial of service attacks that bring the framework down, or cause unstable behavior.

B. Type of Threats

Several classical threats can harm a network which may cause closing down of a network by other unapproved persons, getting the authority to access the secret information and secret information of a system. Underneath are few threats that are described by which unauthorized access to a network can happens.

Masquerading: When attacker plays a role of a network manager by spoofing, thus he can gain manager's access to all confidential data and can carry out each employment in the system that a system supervisor is approved to do.

Modification of Information: In network management, a legitimate network manager can create a valid management PDU. If an attacker succeeds to intercept the transmission, the whole PDU can be changed while keeping the validation data unaltered. This can happen if the PDU is not marked, nor encrypted.

Message Stream Modification: This implies that the stream of SNMP messages is changed. As the messages could be recorded and replayed. An attacker could case record the valid management message that orders the router to close down. At that point, later on, the attacker could utilize the captured message to perform the router shutdown whatever point he needed to do as such.

Disclosure: The threat of disclosure implies that the confidential data is leaked to the people who shouldn't see it. In this way, if an attacker spies the management traffic on a network segment, he could get some vital information. That data could be used as the basis for other attacks, such as masquerading. An approach to fight the threat of disclosure is to encrypt the messages.

Denial of Service (DoS): In the network management, the DoS can likewise be a outcome if the other threats take place. For example, if an attacker succeeds to masquerade and act as the network manager, he can possibly give the shutdown command to a particular switch. Furthermore, this is, a denial-of-service type of threat taking place.

Traffic Pattern Analysis: It is a risk where the information contents of the SNMP messages are overlooked. Rather, the essential data about the system is extracted from the usual patterns of the traffic flow.

IV. SNMPv3 Security

The problems with SNMPv1 & v2 are discussed above and the SNMPv3 mechanisms to implement security are discusses below:

A. User-Based Security Model (USM)

- Individual messages can be authenticated to the known SNMP authorities, such as a specific Network Management System.
- Messages contain multiple timing mechanisms to prevent the capture and the replay.

B. Authentication and Integrity

For authentication of the sender and checking the integrity of messages the USM supports different authentication protocols, which are based on a widely used HMAC.

C. Strong Privacy

- Data encryption choices strengthen message security or privacy.

D. Timeliness Verification of Messages

Message delay or message replay attacks can occur in the network. To make the SNMPv3 secure against these kinds of flow manipulating attacks the USM has a timing mechanism. SNMPv3 demands that the messages or information, then it must be received within a reasonable time window. The timeliness mechanism is based on the two counters associated with each single SNMP engine that is the snmp Engine Boots and snmp Engine Time.

E. Privacy through Encryption

For security, the USM utilizes Data Encryption Standard for ciphering messages. The secret key needed for encryption is gained by taking the first eight octets of the privacy key (privKey) related with the user.

The key creation, update and management are portrayed in RFC-2274. The idea is to generate a unique key (called localized key) for each of the user-SNMP-engine pair by using the user's password and snmpEngineID, which is the id of the target SNMP engine.

F. View-Based Access Control (VBAC)

The access control mechanism intended to be used with the SNMPv3; it is portrayed in RFC-2575. It is specified to determine the access rights as per group basis. This is different from USM which specifies the authentication of the users individually. In VBAC each user should be included in some group and then the different groups can then be granted different levels of security.

V. Functional Areas Where SNMP Work

A. Fault Management

The purpose of fault management is to inform the users or monitoring system's of the frame when a fault occurs. Fault management involves with failure detection, resolving the fault that has been detected, Keeping records of the faults and logging the prevention mechanism. SNMP features can be used for the failure detection service.

B. Configuration Management

The purpose of Configuration Management is to administrate the network and system configurations. It monitors all the network devices in the system and its configurations. If any hardware or software fault occurs then it tracks, manages and notifies the fault.

C. Accounting Management

The purpose of accounting management is to administrate whether networks and its resources are being used effectively or not. Proper Accounting Management can easily reduce the network problems.

D. Performance Management

The goal of performance management is to measure, monitor and report on various aspects of the network or the system performance of the frame.

E. Security Management

The purpose of security management involves securing the network and its hosts and resources from threats or unapproved access. This includes network security systems as well as the physical securities of the network equipments by authorizing the users in the frame.

VI. Comparative Study

The table 1 beneath shows the comparison between SNMPv1 and SNMPv3. The study shows that as the security of the data over the network is an important criterion nowadays and in future hence, SNMPv3 has a lot of future scope over network.

TABLE I
Comparative Study of SNMPv1 & SNMPv3

SNMPv1	SNMPv3
For SNMP v1 &2c we need to set the snmp.community	For SNMPv3 we need to set the snmp.security, auth, authToken, priv,privToken
Uses a community string match for authentication	Security for message and Access Control
"Community string" is used, which is very insecure	The AES and 3-DES Encryption are Supported for security.
It supports 32 bit counters, and that it has little security	It supports 64 bit counters

VII. Conclusion

SNMP is an extraordinary approach to monitor the network devices. Past adaptations of SNMP gave an uncertain approach to get to this information. In spite of the fact that the attempts were made to upgrade the security in the second version of SNMP, the improvements proved to be more complex that the developers thought, and the protocol was not adopted as a result. SNMPv3 addresses the security deficiencies with the addition of a user-based system for access control, a means to properly authenticate the users, and a method for encrypting SNMP traffic between agent and host

On the whole, SNMPv3 provides the best of both worlds: ready access to system monitoring information, and complicated security. As security of the data over the network is an important criterion nowadays hence, in future SNMPv3 has a lot of future scope over network. As with most good things, SNMP has its demerits, it builds very complex software agents, and sometimes it reduces the bandwidth of the network. Due to its simple nature and the features it possesses, the SNMP protocol exhibits shortcomings when operated in very huge or rapidly increasing networks.

ACKNOWLEDGMENT

I would like to express my profound gratitude to the complete team of Logic-Fruit Technologies, for their valuable support, supervision, encouragement and their continuous guidance throughout this work.
I would like to thankfully acknowledge the School of ECE, REVA University, Bangalore, for their constant support throughout this work.

REFERENCES

[1] SNMP Version 3 Tools Implementation Guide: http://www.cisco.com/c/en/us/td/docs/security/asa/snmp/snmpv3_tools.pdf

[2] Migrating from SNMPv1 to SNMPv3: http://www.ibm.com/support/knowledgecenter/en/ssw_aix_61/com.ibm.aix.networkcomm/HT_commadmn_snmpv1_to_snmpv3.htm#snmpv1_to_snmpv3

[3] Configuring SNMP: http://www.cisco.com/c/en/us/td/docs/routers/ir910/software/release/1_1/configuration/guide/ir910scg/swsnmp.pdf

[4] AES and 3-DES Encryption Support for SNMP Version3: http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/configuration/guide/12_2sx/nm_12_2sx_book/nm_encrypt_snmp_sup.pdf

[5] Mib file creation: http://net-snmp.sourceforge.net/tutorial/tutorial-4/agent/02-mib.html

[6] User-based Security Model (USM) for v3 of SNMPv3 Protocol: https://tools.ietf.org/html/rfc3414#page-55

[7] Net-SNMP Tutorial – Toolkit: http://www.net-snmp.org/tutorial/tutorial-5/toolkit/

[8] Message format: http://verticalhorizons.in/snmp-message-format-snmp-pdu-format/

[9] LWIP 2.0.0: http://www.nongnu.org/lwip/2_0_0/upgrading.html

[10] K. McCloghrie & M. Rose,” Management Information Base for Network Management of TCP/IP-based internets:MIB-II”, RFC1213, 1991

[11] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol", RFC 1157, SNMP Research, Performance Systems International, Performance Systems International, MIT Laboratory for Computer Science, May 1990.

[12] R. Presuhn, J. Case, K. McCloghrie, M. Rose & S. Waldbusser, “Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)”, RFC3418, 2002