

Overview of SNMPv3

Addicam.V.Sanjay

Abstract

This paper attempts to present an overview of SNMPv3. This paper will attempt to address the issues like what is SNMPv3. This paper attempts to describe the architecture of SNMPv3 along with the various components, which make up the building blocks of SNMPv3. This paper will also address the shortcomings of SNMPv3. This paper will also look into the future of SNMPv3.

Assumption

This paper explores SNMPv3. It assumes the reader to have a basic knowledge of SNMP, its commands and Network Management. For more information about SNMP, please refer to this web site <http://www.cisco.com/warp/public/535/3.html>

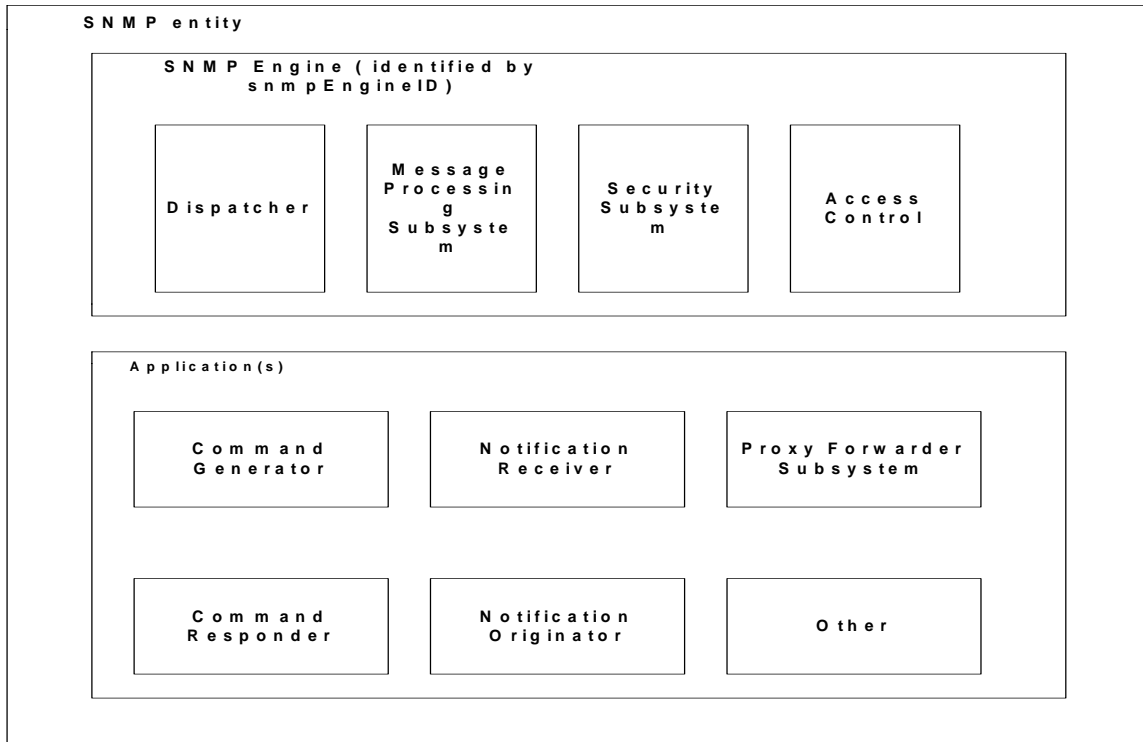
What is SNMPv3???

SNMP is simple network management protocol. It is a protocol, which is used to test whether the various equipments (routers, computers, bridges) etc in a network are working fine. If they are not working fine, SNMP can be used to set these equipments right.

SNMPv1, the first version of the SNMP protocol had no security features. To fill this Void SNMPv2, the second version of the SNMP protocol was developed. This version had security features, but the protocol as a whole turned out to be very complex and difficult to implement. It was also not backward compatible with SNMPv1.

SNMP v3, the third version of SNMP protocol, added to the security infrastructure present in SNMPv2. SNMP v3 also ensured that it is backward compatible with both SNMP v1 and snmpv2. SNMP v3 also had a modular architecture. SNMP v3 has proved to be popular and is now widely used and implemented.

How does the architecture of SNMPv3 look???



Can you give an explanation of each of these components???? Sure !!!!

SNMP Engine: An SNMP engine provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects. There is a one-to-one association between an SNMP engine and the SNMP entity, which contains it. [rfc 2271]

Dispatcher: There is only one Dispatcher in an SNMP engine. It helps in Sending and receiving SNMP messages to/from the network, determining the version of an SNMP message and interacting with the corresponding Message Processing Model and in providing an abstract interface to SNMP applications for delivery of a PDU to an application.[rfc 2271]

Message Processing Subsystem: The Message Processing Subsystem is responsible for preparing messages for sending, and extracting data from received messages. [rfc 2271]

Security Subsystem: The Security Subsystem provides security services such as the authentication and privacy of messages. User-Based security model is the most popular Security Subsystem in use.

Here is a description of the User-Based Security (usm) model.....

The User-Based Security Model needs to provide protection against the following type of threats

- Modification of Information

The modification threat is the danger that some unauthorized entity may alter in-transit SNMP messages generated on behalf of an authorized user in such a way as to effect unauthorized management operations, including falsifying the value of an object.

- Masquerade

The masquerade threat is the danger that management operations not authorized for some user may be attempted by assuming the identity of another user that has the appropriate authorizations.

- Disclosure

The disclosure threat is the danger of eavesdropping on the exchanges between managed agents and a management station.

Protecting against this threat may be required as a matter of local policy.

- Message Stream Modification

The SNMP protocol is typically based upon a connection-less transport service which may operate over any sub-network service.

The re-ordering, delay or replay of messages can and does occur through the natural operation of many such sub-network services.

The message stream modification threat is the danger that messages may be maliciously re-ordered, delayed or replayed to an extent which is greater than can occur through the natural operation of a sub-network service, in order to effect unauthorized management operations.[rfc 2274]

The goal of the USM is to provide authentication and privacy services, which can be translated to the following goals:

- 1) Provide for verification that each received SNMP message has not been modified during its transmission through the network.
- 2) Provide for verification of the identity of the user on whose behalf a received SNMP message claims to have been generated.
- 3) Provide for detection of received SNMP messages, which request or contain management information, whose time of generation was not recent.
- 4) Provide, when necessary, that the contents of each received SNMP message are protected from disclosure.[rfc 2274]

Goals 1,2 and 3 are related to providing authentication. Goal 4 is related to providing privacy.

Here is a brief description of the authentication module:

The basis for security in the use of authentication schemes is the secret keys shared keys shared by sender and receiver for authentication. The secret keys for the USM are developed from the user password. Two algorithms are recommended in SNMPv3 for developing keys from the password: HMAC-MD5-96 and HMAC-SHA-96. The first letter in the designation stands for the cryptographic hash function (H) used for generating message access code (MAC). The second part of the designation is the hashing algorithm used, the first being the MD5 hashing algorithm, and the second being the SHA-1 hashing algorithm used to generate MAC. The MAC is derived by truncating the hashing code generated to 96 bits, as indicated by the last set of characters in the designation.

The secret key for authentication is derived from a password chosen by the user. The user in our case is the nonauthoritative SNMP engine, which is generally a network management system. In both MD5 and SHA-1 algorithms, the password is repeated until it forms a string of 2^{20} (1048576 octets), truncating the last repetition, if necessary.

This result is called digest0. In the second step, the digest0 is hashed by using either MD5 or SHA-1 algorithm to derive digest1. The MD5 algorithm yields a 16-octet digest1, and SHA-1 results in a 20-octet digest1. Concatenating the authoritative SNMP engine ID and digest1 forms a second string. This string is fed into the respective hashing algorithm to derive digest2. The derived digest2 is the user's authentication key, authkey, that is input

to the authentication modules. The choice between the 16-octet MD5-based authkey and the 20-octet SHA-1 based authKey depends on the implementation. Breaking the code in the 20-octet key is more difficult than for the 16-octet key. However, processing is faster with the 16-octet key.

A user has only one password and hence one secret key, digest1. However it communicates with all the authoritative SNMP engines (all the agents in the network). The shared information is again a secret between the two communicating engines. The concept of a localized key is introduced to avoid having to store a separate password for each authoritative engine with the user communicates. A has function, which is the same as that used to generate the secret key, is used to generate the localized key:

$$\text{Localized Key} = H(\text{secret}, \text{authoritativeSnmEngineID}, \text{secret})$$

Where secret is the secret key (digest1) and the authoritativeSnmEngineID is the SNMP engine ID of the authoritative SNMP engine with which the local user is communicating. This localized key is different for each authoritative engine and is localized for the user at the authoritative SNMP engine. It is stored in each authoritative engine with which the user communicates.

SNMPv3 permits the operation of change and modification in keys, but not the creation of keys, to ensure that the secret key does not become stale. Note that the localized key is the same as authkey.[Subramanian]

Now for the privacy module....

The privacy module generates non readable ciphertext from readable plain text. The SNMPv3 recommendation for data confidentiality is to use the cipher block chaining mode of the data encryption standard (CBC-DES) symmetric encryption protocol. The USM specifications require that only a portion of the message be encrypted. A secret value in combination with a timeliness value is used to create the encryption/decryption key and initialization vector (IV). Again, the secret value is user-based, and hence is associated typically with a network management system. The 16-octet privacy key, `privkey`, is generated from the password is described in the generation of authentication code with the MD-5 hashing algorithm.

The first 8 octets of the 16-octet privacy key are used in creating the DES key. It is only 56 bits long, so the least significant bit of each octet in the privacy key is discarded. The 16-octet IV is made up of two parts: an 8-octet pre-IV concatenated with an 8-octet salt. The pre-IV comprises the last eight octet of the privacy key. The salt is added to ensure that two identical instances of ciphertext are not generated from two different plaintexts that are using the `snmp` key. The salt is generated by an SNMP engine by concatenating a 4-octet `snmpEngineBoots` with a locally generated integer. The salt constitutes the privacy parameters.

The encryption process first divides the plaintext of a scoped Protocol data unit into 64-bit blocks. The plaintext of each block is XOR-ed with the ciphertext of the previous block, and the result is encrypted to produce a ciphertext for the current block. For the first block, the IV is used instead of the ciphertext of the previous block. [subramanian]

Now back to the access control subsystem, which is one of the core subsystems of a SNMP entity...

Access control deals with the problem of who can access network management components and what they can access. In SNMPv3 access control has been made more secure and more flexible by introduction of the View-based Access control model (VACM). VACM defines a set of services that an application in an agent can use to validate command requests and notification receivers. It validates sending sources and their access privilege for command requests. One of the assumptions made is that the authentication of the source has been done by the authentication module. In order to perform the services, a local database containing access rights and policies, called the local configuration datastore (LCD), has been created in the SNMP entity. The LCD is typically in an agent or in a manager functioning in an agent's role when it communicates with another manager. [subramanian]

The elements which make up the View based Access control model are

Groups: A group is a set of zero or more <securityModel, securityName> tuples on whose behalf SNMP management objects can be accessed. A group defines the access rights afforded to all securityNames which belong to that group. The combination of a securityModel and a securityName maps to at most one group. A group is identified by a groupName. [rfc 2275]

The Access Control module assumes that the securityName has already been authenticated as needed and provides no further authentication of its own. The View-based Access Control Model uses the securityModel and the securityName as inputs to the Access Control module when called to check for access rights. It determines the groupName as a function of securityModel and securityName. [rfc 2275]

Security Level : Different access rights for members of a group can be defined for different levels of security, i.e., noAuthNoPriv, authNoPriv, and authPriv. The securityLevel identifies the level of security that will be assumed when checking for access rights. The View-based Access Control Model requires that the securityLevel is passed as input to the Access Control module when called to check for access rights. [rfc 2275]

Contexts: An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context. An SNMP entity potentially has access to many contexts. The View-based Access Control Model defines a vacmContextTable that lists the locally available contexts by contextName. [rfc 2275]

MIB views and View Families: For security reasons, it is often valuable to be able to restrict the access rights of some groups to only a subset of the management information in the management domain. To provide this

capability, access to a context is via a "MIB view" which details a specific set of managed object types (and optionally, the specific instances of object types) within that context. For example, for a given context, there will typically always be one MIB view which provides access to all management information in that context, and often there will be other MIB views each of which contains some subset of the information. So, the access allowed for a group can be restricted in the desired manner by specifying its rights in terms of the particular (subset) MIB view it can access within each appropriate context. [rfc 2275]

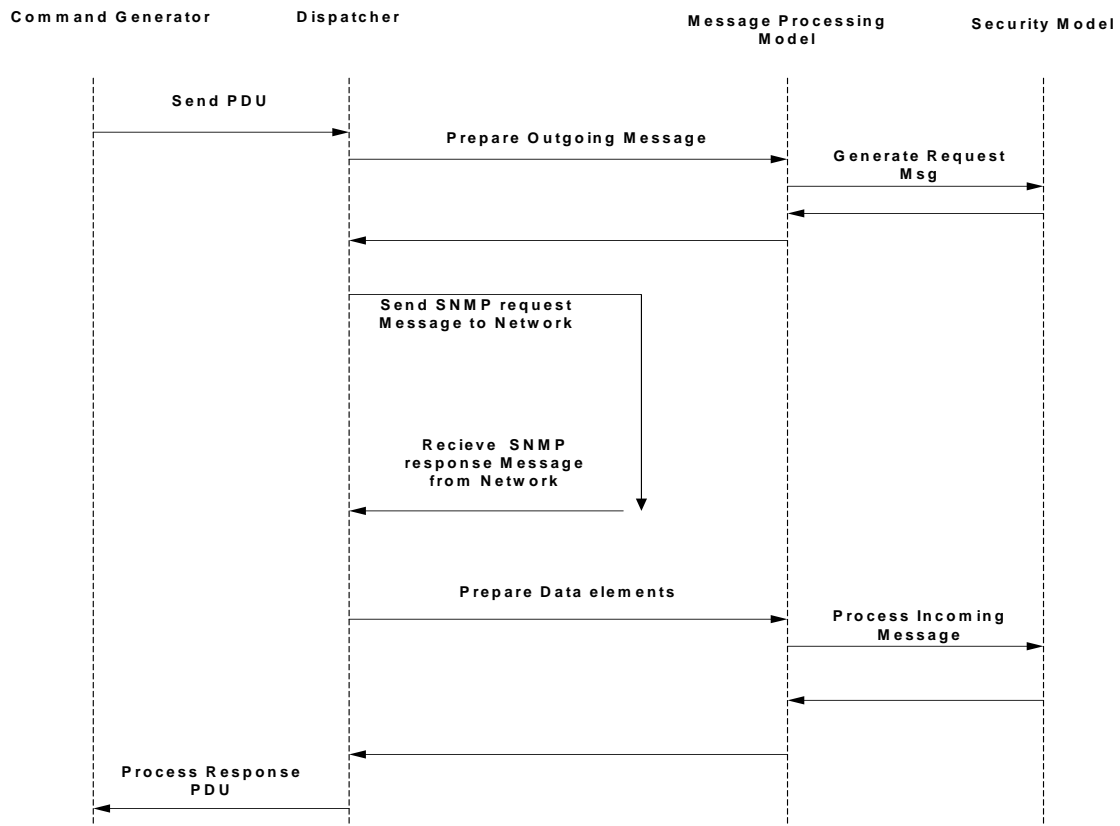
Access Policy: The View-based Access Control Model determines the access rights of a group, representing zero or more securityNames which have the same access rights. For a particular context, identified by contextName, to which a group, identified by groupName, has access using a particular securityModel and securityLevel, that group's access rights are given by a read-view, a write-view and a notify-view. The read-view represents the set of object instances authorized for the group when reading objects. Reading objects occurs when processing a retrieval (for example a GetRequest, GetNextRequest, GetBulkRequest) operation. The write-view represents the set of object instances authorized for the group when writing objects. Writing objects occurs when processing a write (for example a Set) operation.

The notify-view represents the set of object instances authorized for the group when sending objects in a notification, such as when sending a notification (for example an Inform or SNMPv2-Trap).

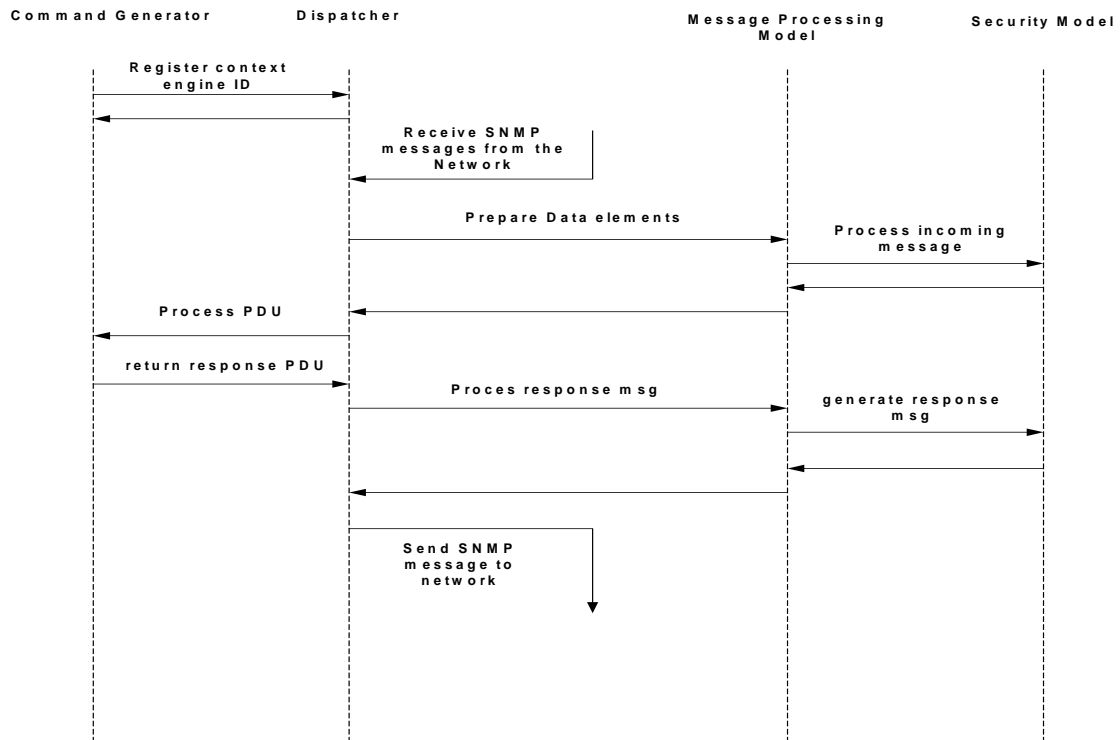
Now let us consider some of the applications present in the SNMP entity....

The applications present in the SNMP entity are :

Command Generator: The command generator application is used to generate get-request, get-next-request, get-bulk and set-request messages. It also processes the response to the command sent. Typically, the command generator application is associated with the network manager process. [subramanian] Scenario diagram of a command generator application is as shown in the diagram [rfc 2271]



Command Responder: The command responder processes the get and set requests destined for it from a legitimate remote entity. The scenario diagram of command responder application is shown below.



[rfc 2271]

Notification originator: The notification originator application generates either a trap or an inform message. Its function is somewhat similar to that of the command responder, except that it needs to find out where to send the message and what SNMP version and security parameters to use.[subramanian]

Notification receiver: The notification receiver application receives SNMP notification messages. It registers with the SNMP engine to receive these messages, just as the command responder application does to receive get and set messages.

Proxy forwarder: The proxy forwarder application forwards SNMP requests, notifications, and responses without regard for the managed objects contained in those messages.

Shortcomings of SNMPv3....

SNMP is not a particularly efficient protocol. There is a number of useless information and the information in some of the directives is oversized. Because of this Network bandwidth is wasted.

Future of SNMPv3....

SNMP v3, the latest version of SNMP is undergoing a lot of improvements to make it future proof. These improvements include changes to.

- Accommodate a wide range of operating environments.
- Facilitate the need to transition from previous multiple protocols to SNMP v3.
- Facilitate the ease of setup and maintenance activities.

Conclusion

SNMP is here to stay. It is a very helpful and simple tool in managing and monitoring the network. It's unique selling point is it's simplistic design and architecture. •The future versions of SNMP will have QOS (quality of service)considerations. It will also have provisions for “self healing network management”.•The need for SNMP in managing complex network will only increase in the future.

References

(I have cited articles from these two references in my research paper.)

Cisco (2002). Network Management Basics. Retrieved Feb 20 2004, from the World Wide Web:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm#xtocid3

Subramanian, Mani. (2000). Network Management: Principles and practice, Addison Wesley, Massachusetts.

(I have referred these references, when researching my paper, but I did not find an opportunity to cite from the articles at these references.)

Comer, Douglas. (1997). Computer Networks and Internets, Prentice Hall, New Jersey.

Guild Soft. (2000). Network Management –Scope of a CMIP stack. Retrieved Feb 20 2004, from the World Wide Web:

<http://www.guildsoftindia.com/nms.htm>

Stevenson, Douglas. (1995). Network Management: What it is and what it isn't. Retrieved Feb 20 2004, from the world wide web:<http://netman.cit.buffalo.edu/Doc/Dstevenson/>

Stevens, Richards. (1999). TCP/IP Illustrated Volume 1: The protocols, Addison Wesley, Massachusetts.

Tabor, Daniel. (1995). Network Management Lesson 27. Retrieved Feb 20 2004, from the World Wide Web:

<http://www.cs.njit.edu/~cis456/protected/lesson27/single27.html>

Unknown. (????). SUMMARY: Retrieved Feb 20 2004, from the World Wide Web: <http://www.geocities.com/SiliconValley/Horizon/4519/work.html>