Global Information Assurance Certification Paper

SNMP Security Enhancement
Jose Luis Camacho
March 28, 2001- GSEC Practical Assignment Version 1.2b

SNMP Architecture

SNMP (Simple Network Management Protocol) has become the most widely protocol used in network management for TCP/IP based networks. The SNMP system consists of the following three parts:

- An SNMP manager
- An SNMP agent
- A Management Information Base (MIB)

The SNMP Manager is part of a Network Management System (NMS) such as Spectrum, HP Open View and Cisco Works. Information is exchanged between NMS and elements of a network. NMS will control and monitor the network, using the data gathered from the network. The data gathered from monitoring a network falls into three categories:

- Statistics
- Current status
- Alerts

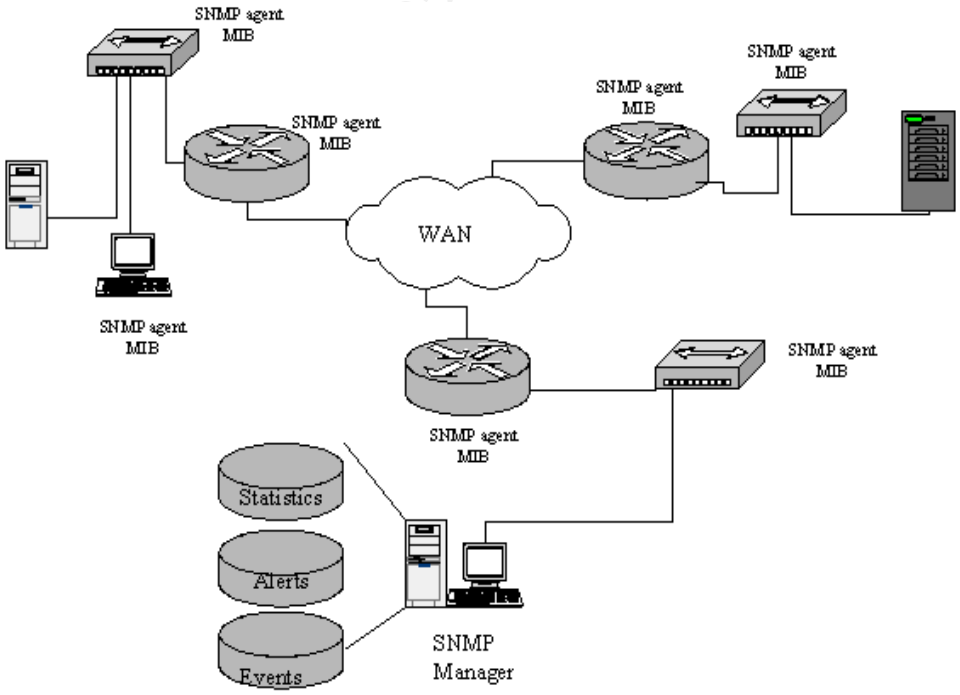


Figure 1.SNMP elements.

Network statistics are sent on regular basis to the NMS where they are collected and stored. For example traffic levels, cpu process and so on. Data is also collected on the current status of devices. For example link status. The third type of data collected is about

alerts or alarms. Alerts are reports of any unusual activity in the network.
Any node in the network that is to be managed, including PCs, workstations, servers, switches and routers, and so on, includes an SNMP agent. The agent is responsible for

- Collecting and maintaining information about its local environment locate in MIBs (Model Information Base)
- Providing that information to a manager, either in response to a request or in an unsolicited fashion when something noteworthy happens. Responding to a manager commands to alter the local configuration or operating parameters

The SNMP agent contains MIBs. MIB is a virtual information that represents parameters of the network device such traffic, cpu process, management information etc. These values are integers, strings, counters etc. A manager can request or store a value into that MIB agent. Figure 1 illustrates the relationship between the SNMP manager and agents.

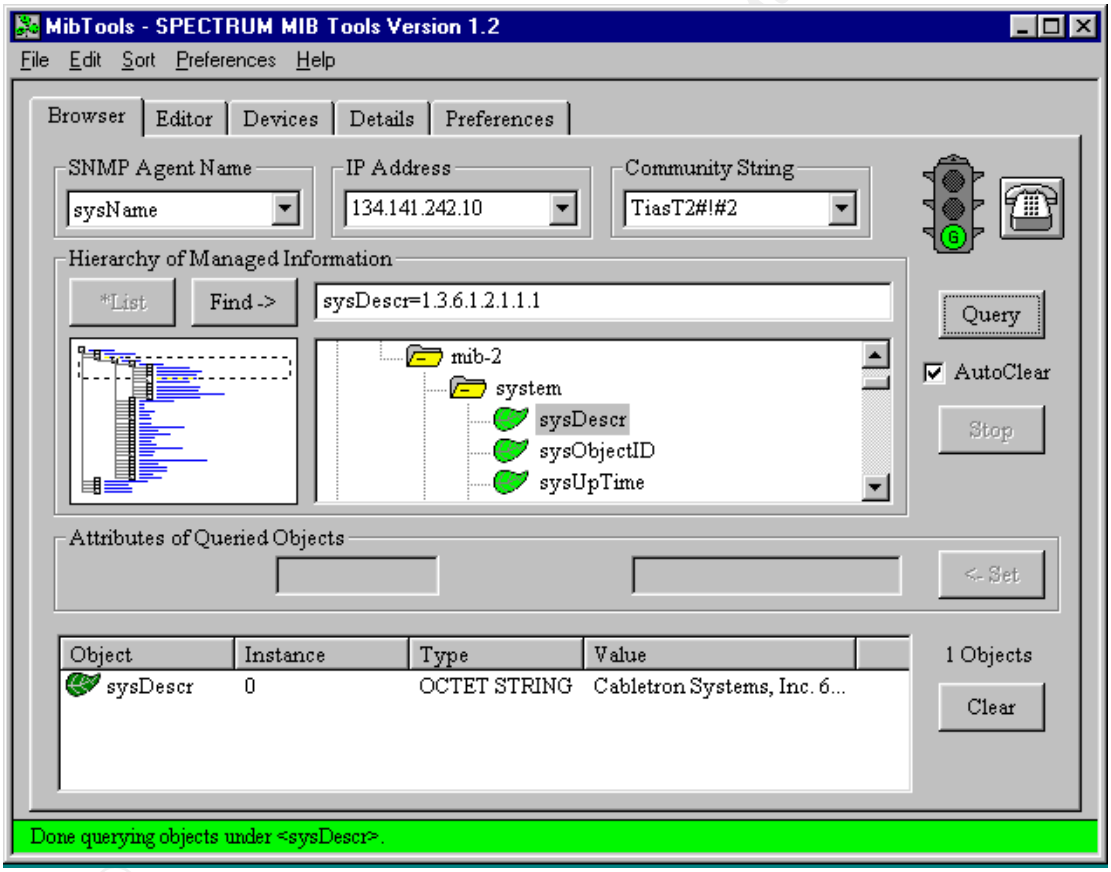


Figure 2. Spectrum MIB-Tools (Commercial Tool from Cabletron Systems) shows a MIB SysDescr

Figure 2 illustrate a Cabletron Ethernet Switch 6E123-50 SysDescr MIB OID (Object Identifier) = 1.3.6.1.2.1.1.1. This is a MIB that belongs to MIB-II group and contains a string value that show a description of this network device " Cabletron Systems, Inc. 6E123-50 Rev 04.10.22 08/21/00 –15:45 ofc"
The OID is the position of this MIB in the ISO/CCITT tree. The OID is the series of

integers that mark the path from the root of the tree to the object. A friendly form of an identifier is often written as a series of text labels separated by dots:
OID Textually = iso.org.dod.internet.mgmt.mib-2.system.sysdescr
OID String Numerically = 1.3.6.1.2.1.1.1
Figure 3 illustrates the tree ISO and CCITT structure.

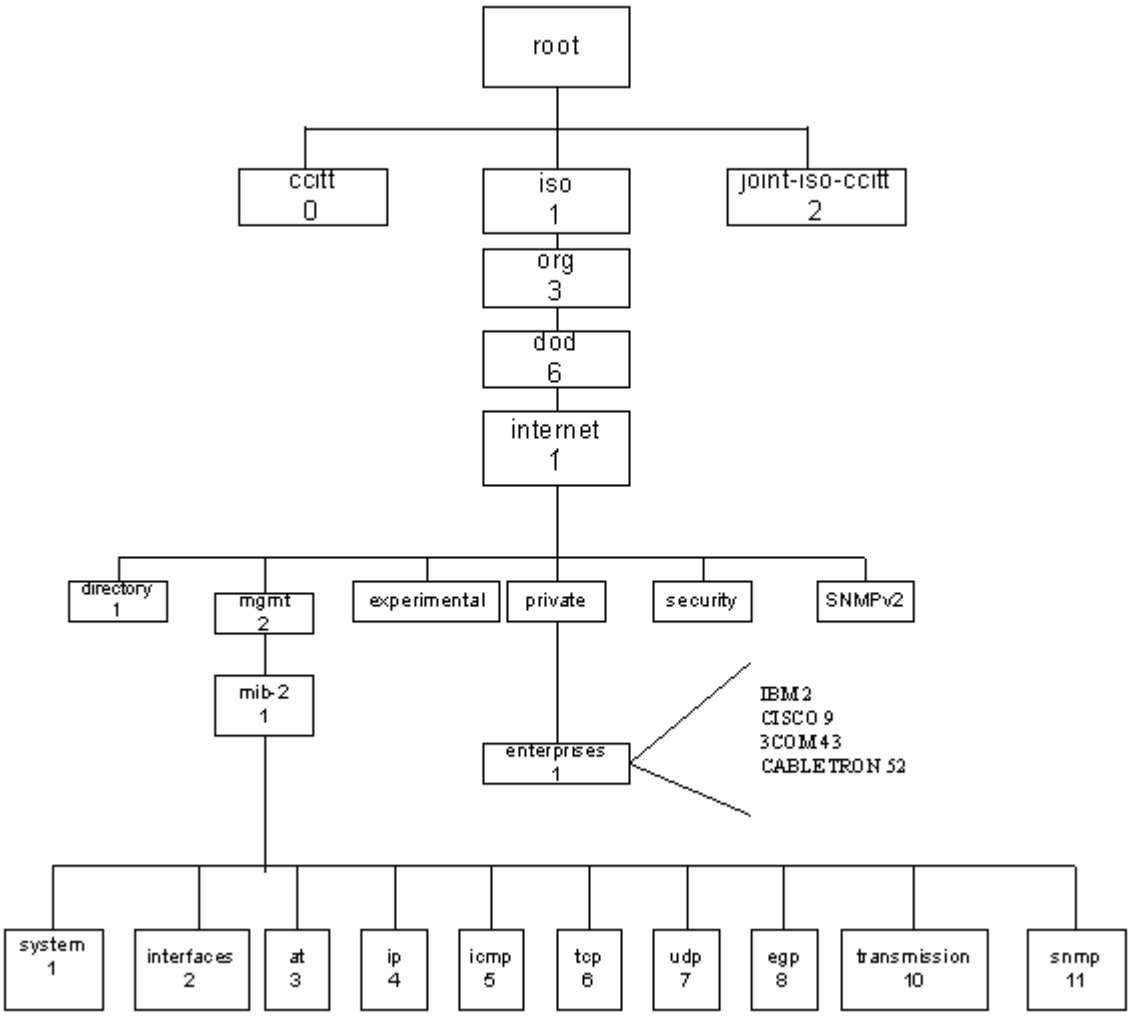


Figure 3. ISO-CCITT tree

There are MIBs for many technologies such Ethernet, Token Ring, Routing, ATM, FDDI, Frame Relay, Host Management, Directory Services etc. There are enterprise's MIBs that allows better control in their devices such Cisco, Cabletron, 3com etc.
As you can see we have total control of the network with SNMP architecture.

Security in SNMP versions

- SNMPv1-A full Internet Standard, defined in RFC 1157. Security is based in

community Strings.

- SNMPv2c-The community-string based Framework for SNMPv2. SNMPv2c is an Experimental Internet Protocol defined in RFC 1901, RFC 1905, and RFC1906. SNMPv2c is an update is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic), and uses the community-based security model of SNMPv1.
- SNMPv3- Version 3 of SNMP. SNMPv3 is an interoperable standards-based protocol defined in RFCs 2273-2275. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.
  The security features provided in SNMPv3 are:
  - ✓ Message integrity – Ensuring that a packet has not been tampered with in transit.
  - ✓ Authentication – Determining the message is from a valid source.
  - ✓ Encryption – Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

Figure 4 illustrated Security Models and Levels.

Model	Level	Authentication	Encryption	What Happens
SNMPv1	NoAuthNoPriv	Community String	No	Uses a community string match for authentication.
SNMPv2c	NoAuthNoPriv	Community String	No	Uses a community string match for authentication.
SNMPv3	NoAuthNoPriv	Username	No	Uses a username match For authentication.
SNMPv3	AuthNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	AuthPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on CBC-DES (DES-56) standard.

Figure 4.

Control access in SNMPv1

SNMPv1 uses a community string match for authentication. Where community string is a password used to control access to node information. There is a read only community string that allows only read MIB's value in the SNMP agent and read-write community string that allows read and change values in SNMP agent MIB.

Security flaw in SNMPv1

SNMPv1 transmit all information in clear text. Anyone monitoring the network can grab the community name from passing traffic. SNMP usually uses the UDP transport and destination ports 161 and 162 when communicating.

Figure 5 illustrates a Sniffer capture, as you can see a central management station 134.141.242.32 is changing community strings in the switch 134.141.242.10.

I did the laboratory with a Cabletron SS6000 6E123-50, the following description show you some of the keys for exploit this flaw.

```
SNMP:
SNMP: SNMP Version      = 1          ----→ SNMP Version
SNMP: Community         = TiasT2#1#2----→ Community with RW
privilegies
SNMP: Command           = Set Request---→ SNMP Command Set
SNMP: Request ID        = 2
SNMP: Error Status      = 0 (No error)
SNMP: Error Index       = 0
SNMP:
OID Read Only community string
SNMP: Object = {1.3.6.1.4.1.52.4.1.1.9.5.1.0}
{Cabletron.4.1.1.9.5.1.0}
SNMP: Value  = networkwizard---→RO password value
OID Read and Write Community String
SNMP: Object = {1.3.6.1.4.1.52.4.1.1.9.5.2.0}
{Cabletron.4.1.1.9.5.2.0}
SNMP: Value  = son2123#145---→RW password value
OID Superuser access
SNMP: Object = {1.3.6.1.4.1.52.4.1.1.9.5.3.0}
{Cabletron.4.1.1.9.5.3.0}
SNMP: Value  = TiasT2#1#2---→SU password value
```

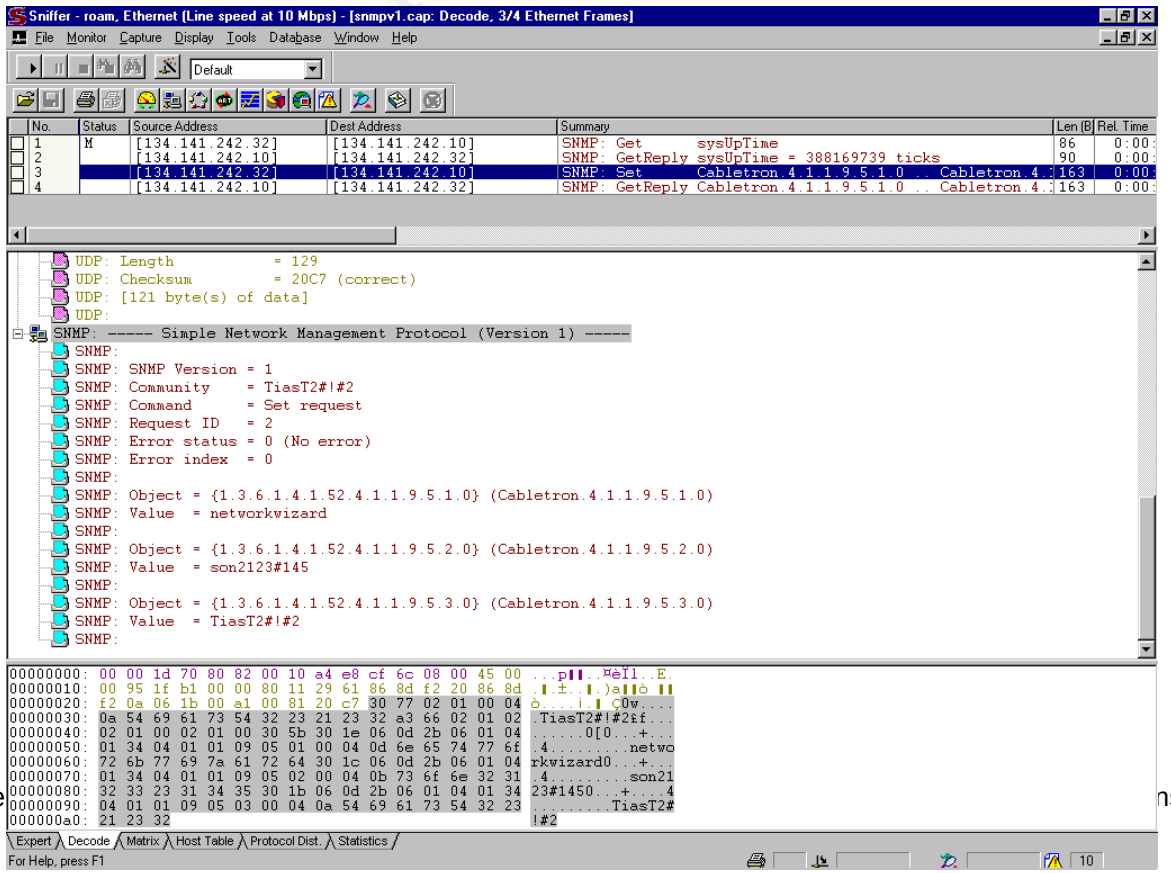


Figure 5. Sniffer Expert Capture of SNMP traffic.

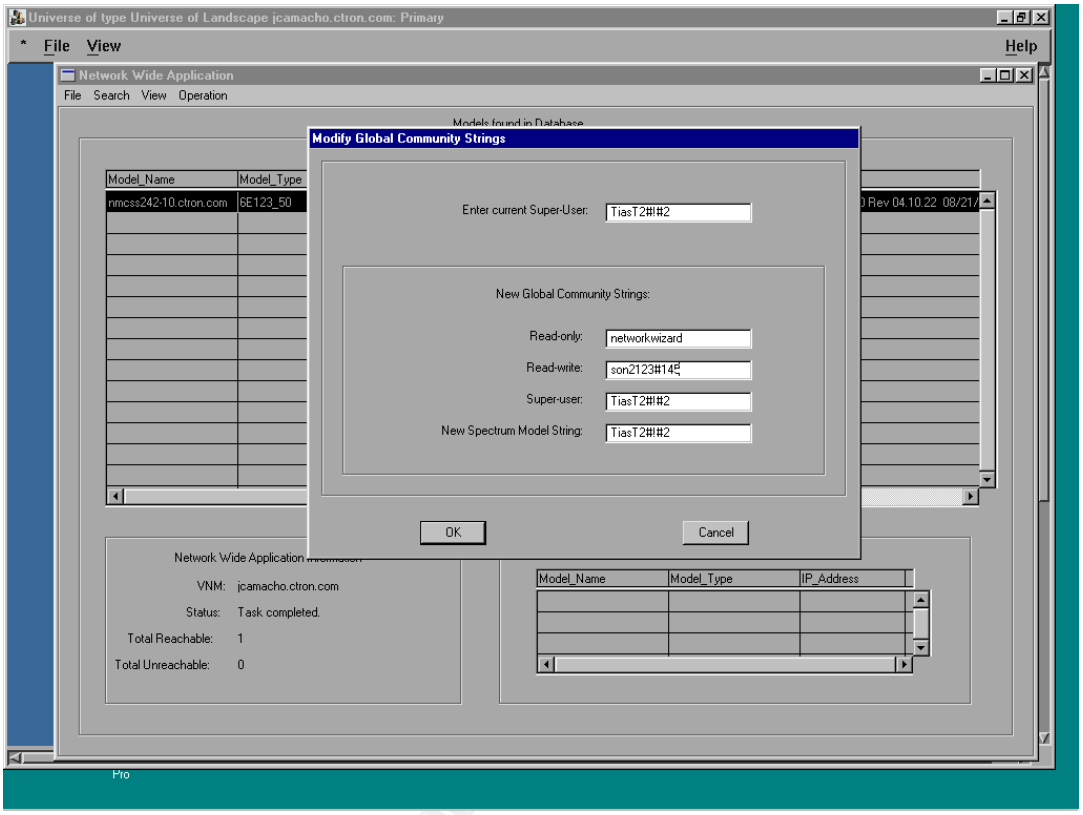
Obtaining community string RW string anyone can change the configuration of our network devices or with R permission read the configuration and anyone tries to gain access to our Network backbone. In Details from the menu of Spectrum MIB Tools we can see the ASN.1 (Abstract Language Notation) of each MIB.
For each Enterprise there are certain MIBs that are supporting the community names.

```
contROCommStr  OBJECT-TYPE
          SYNTAX  OCTET STRING
          ACCESS  read-write
          STATUS  mandatory
          DESCRIPTION
        "This is defined as the base read only community string to
             access MIBs in this container or on this module. A write
             to this object will change all instances of
             contLogicalEntryROCommStr."
          :: =  { contCommStr 1 }
          --1.3.6.1.4.1.52.4.1.1.9.5.1

contRWCommStr  OBJECT-TYPE
          SYNTAX  OCTET STRING
          ACCESS  read-write
          STATUS  mandatory
          DESCRIPTION
        "This is defined as the read write community string to
             access MIBs in this container or on this module.A write
to
             this object will change all instances of
             contLogicalEntryRWCommStr."
          :: =  { contCommStr 2 }
          --1.3.6.1.4.1.52.4.1.1.9.5.2

contSUCommStr  OBJECT-TYPE
          SYNTAX  OCTET STRING
          ACCESS  read-write
          STATUS  mandatory
          DESCRIPTION
        "This is defined as the super user community string to
             access MIBs in this container or on this module.A write
to
             this object will change all instances of
             contLogicalEntrySUCommStr."
          :: =  { contCommStr 3 }
          --1.3.6.1.4.1.52.4.1.1.9.5.3
```

Minimum security conditions in SMPv1.

Well the first step is avoids our network devices of the usual community strings such public, admin, private or blank space. Try to write 10 characters strong password. Solarwinds is management software that provides a SNMP brute force attack that can be used to test your passwords.
Second step, many Management tools provides a way to change the community strings

frequently. Figure 6 shows an example with SPECTRUM 5.0 rev 1 using NetWideApp from the spectrum Menu. We can use this option to change the community string by



zone and not use the same community for all the network devices.

Figure 6. NetWideApp. Using NetWideApp the community string change in network devices and Spectrum Database at the same time.

Third step, It's important that software management allows permission level of users in order to protect the access to our Network Management Workstation. In this way only the network manager can change network devices configuration and the others only have permissions to see alarms or get reports.

Control Access in SNMPv2 and derived.

SNMPv2 included a security facility that was not widely accepted. SNMPv2 was issued in 1996 with functional enhancements but without security facility. This version used the simple and insecure password-based authentication feature, provided in SNMPv1 and is referred to as SNMPv2c.
To remedy the lack of security, a number of independent groups began to work on a security enhancement as a result emerged SNMPv2u and SNMPv2*. These two approaches served as input to SNMPv3.

SNMPv3: A security enhancement for SNMP.

SNMPv3 is not a replacement for SNMPv1 and/or SNMPv2. SNMPv3 defines a security capability to be used in conjunction with SNMPv2 or SNMPv1.
The RFC 2271 reflects a key design requirement for SNMPv3. Each SNMP entity includes a single SNMP engine. An SNMP engine implement functions for sending and receiving messages, authenticating and encrypting /decrypting messages, and controlling access to managed objects. Base in RFC 2271 the next text gives us a clear idea of the security enhancement for SNMPv3.Figure 7 illustrates SNMPv3 Security Features.

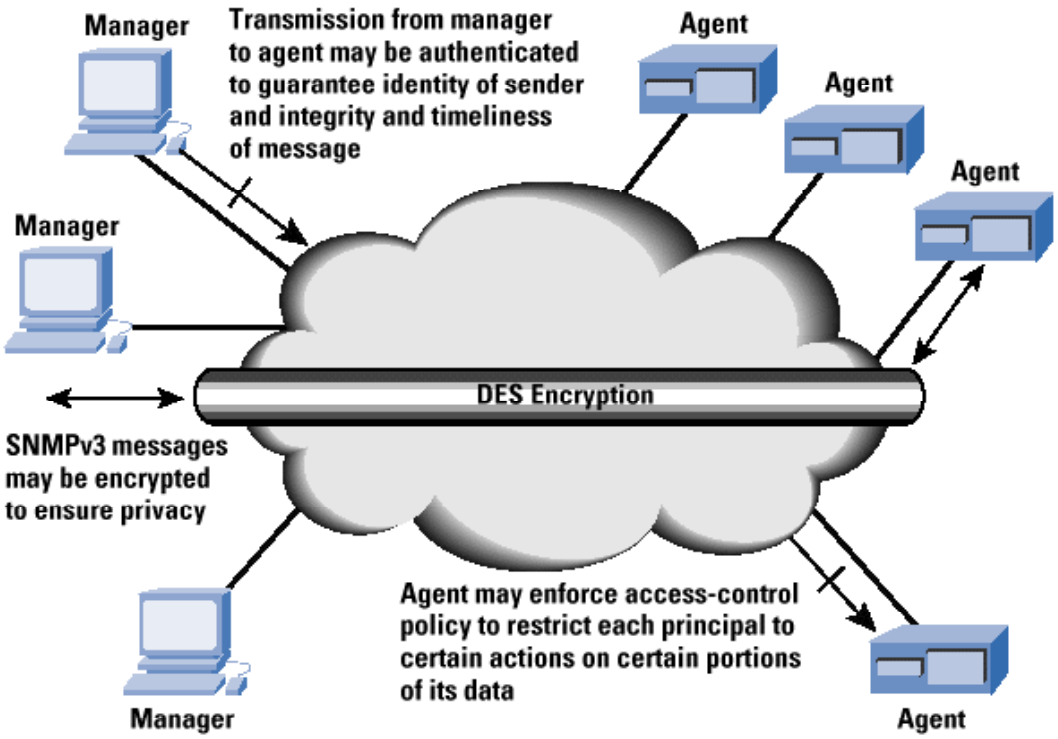


Figure 7. SNMPv3 Security Features.

Several of the classical threats to network protocols are applicable to the management problem and therefore would be applicable to any Security Model used in an SNMP Management Framework. Other threats are not applicable to the management problem. This section discusses principal threats, secondary threats, and threats which are of lesser importance. The principal threats against which any Security Model used within this architecture SHOULD provide protection are:

Modification of Information
The modification threat is the danger that some unauthorized SNMP entity may alter in-transit SNMP messages generated on behalf of an authorized principal 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 principal may be attempted by assuming the identity of another principal that has the appropriate authorizations. Message
Stream Modification
The SNMP protocol is typically based upon a connectionless transport service by which may operate over any subnetwork service. The re-ordering, delay or replay of messages can and does occur through the natural operation of many such subnetwork 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 subnetwork service, in order to effect unauthorized management operations.

Disclosure
The disclosure threat is the danger of eavesdropping on the exchanges between SNMP engines. Protecting against this threat may be required as a matter of local policy.

There are at least two threats against which a Security Model within this architecture need not protect.

Denial of Service
A Security Model need not attempt to address the broad range of attacks by which service on behalf of authorized users is denied. Indeed, such denial-of-service attacks are in many cases indistinguishable from the type of network failures with which any viable management protocol must cope as a matter of course.

Traffic Analysis
A Security Model need not attempt to address traffic analysis attacks. Many traffic patterns are predictable - entities may be managed on a regular basis by a relatively small number of management stations - and therefore there is no significant advantage afforded by protecting against traffic analysis.

SNMPv3 Architecture

Figure 8 represent a SNMP Manager based in RFC 2271.
The SNMP Manager includes SNMP Applications. A Command Generator Application- Monitor and Manipulate management data at remote agents; they make use make use of SNMPv1 or SNMPv2 PDUs, including Get, GetNext, GetBulk, and Set. A Notification Originator Application initiates asynchronous messages (traps). A Notification Receiver Application- Processes incoming asynchronous messages (traps).
The SNMP Engine performance two overall functions:

- It accepts outgoing PDUs from SNMP applications, performs the necessary processing including inserting authentication codes and encrypting, and then encapsulates the PDUs in to messages for transmission.

- It accepts incoming SNMP messages from the transport layer, performs the necessary processing, including authentication and decryption , and the extracts the PDU from the messages and passes these on to the appropriate SNMP application.

The Security Subsystem provides security services such as the authentication and privacy of messages and potentially contains multiple Security Models.

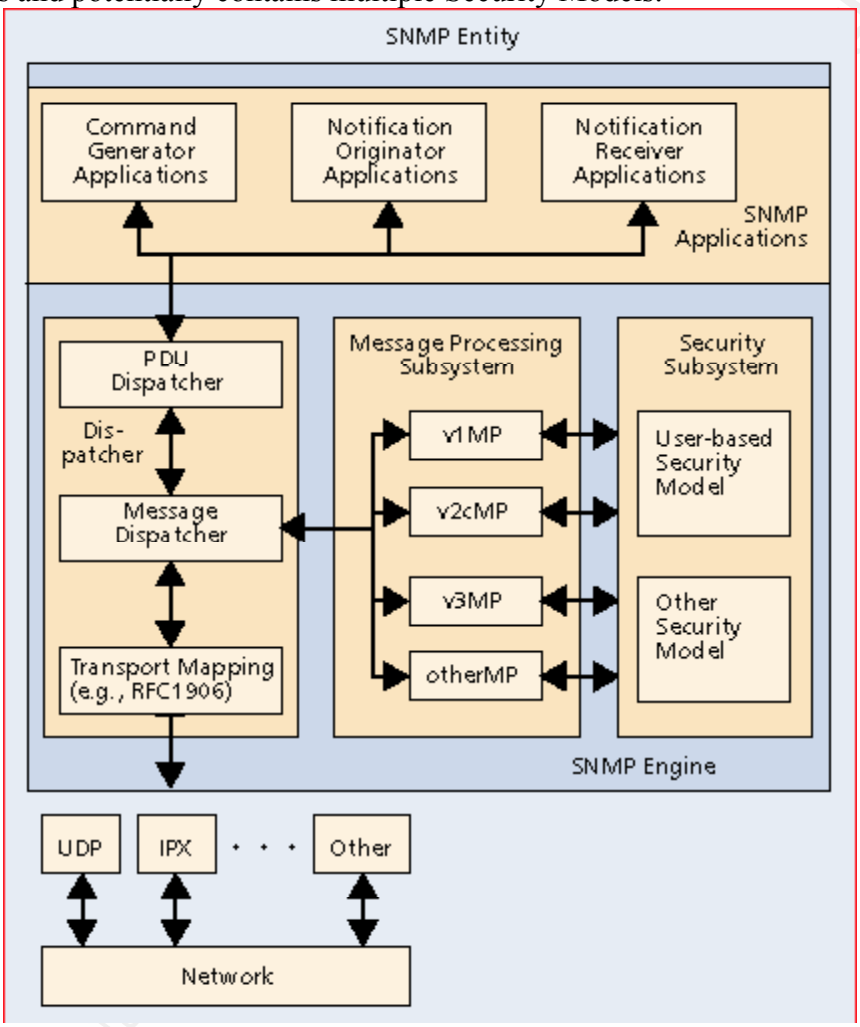


Figure 8. SNMPv3 Manager from RFC 2271

The SNMP engine for a SNMP agent has all the components found in SNMP engine for SNMP Manager plus an Access control Subsystem. The Security Subsystem is concerned with privacy and authentication, and operates on SNMP messages. The Access Control Subsystem is concerned with authorized access to management information (MIBs). Figure 8 illustrates a SNMP agent and its SNMP engine.

User-Bases Security Model

User Security Model provides authentication and privacy services for SNMP.

USM allows the use of one of two alternative authentication protocols: HMAC-MD5-96 and HMA-SHA-96.
HMAC-MD5-96 authentication protocol is the first defined for the User-based Security Model. This protocol uses the MD5 [MD5] message digest algorithm. A 128-bit MD5 digest is calculated in a special (HMAC) way over the designated portion of an SNMP message and the first 96 bits of this digest is included as part of the message sent to the recipient. The size of the digest carried in a message is 12 octets. The size of the private authentication key (the secret) is 16 octets.

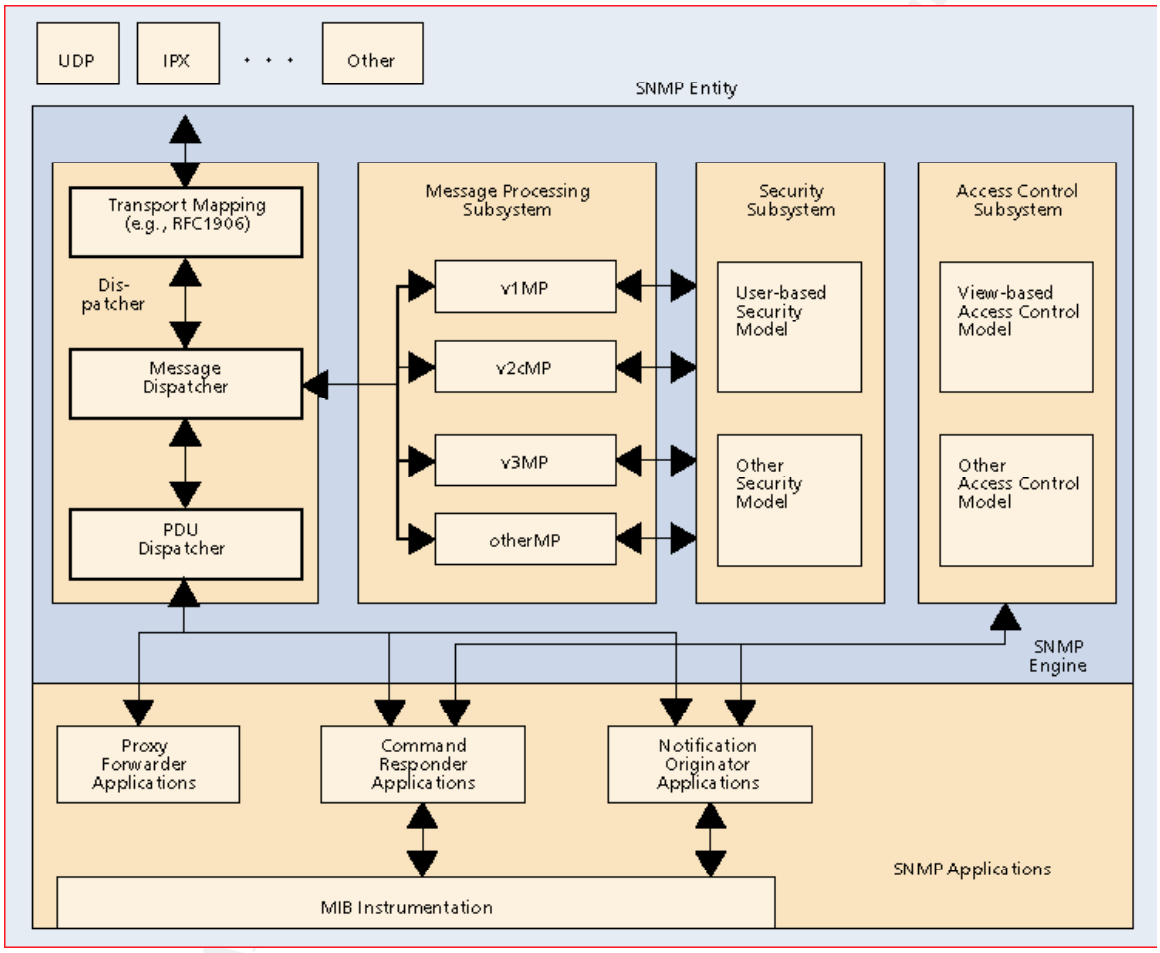


Figure 9. SNMPv3 Agent from RFC 2271

HMA-SHA-96 this mechanism uses the SHA [SHA-NIST] message digest algorithm. A 160-bit SHA digest is calculated in a special (HMAC) way over the designated portion of an SNMP message and the first 96 bits of this digest is included as part of the message sent to the recipient. The size of the digest carried in a message is 12 octets. The size of the private authentication key (the secret) is 20 octets.
USM uses the cipher block chaining (CBC) mode of the Data Encryption Standard (DES) for encryption .A 16-octect privKey is provided as a input to the encryption protocol. The first eight octets (64 bits) of this privKey are used as a DES key. For CBC mode, a 64-bit

Initialization Vector (IV) is required. The last eight octets of the priKey contain a value that is used to generate this IV.
For more information see *www.snmpworld.com* search RFC 2274 and RFC 2271.

Authoritative and Non-Authoritative Engines

When an SNMP message contains a payload by which expects a response (for example, a Get, GetNext, GetBulk, Set, or Inform PDU), the receiver of such messages is authoritative. When an SNMP message contains a payload by which does not expect a response (for example, an SNMPv2-Trap Response), then the sender of such message is authoritative. These designation servers have two purposes:

1. The timeliness of message is determined with respect to a clock maintained by the authoritative engine. When an authoritative engine sends a message (Trap, Response), it contains the current value of its clock, so that the non-authoritative recipient can synchronize on that clock. When a non-authoritative engine sends a message (Get, GetNext, GetBulk, Set, Inform), it includes its current estimate of the time value at the destination, allowing the destination to assess the message's timeliness.

1. A key localization process, enables a single principal to own keys stored in multiple engines are localized to the authoritative engine in such a way that the principal is responsible for single key but avoids the security risk of storing multiples of the same key in a distributed network. This means that these keys are not stored in a MIB and are not accessible via SNMP.

View-Based Access Control

Access control is a security function performed at the PDU level. An access control document defines mechanisms for determining whether access to a managed object in a local MIB by a remote principal should be allowed. The SNMPv3 documents define the view-based access control (VACM) model.
VACM has two important characteristics:

- VACM determines whether access to a managed object in a local MIB by a remote principal should be allowed.
- VACM makes use of a MIB that:
  Defines the access control policy for this agent.
  Makes it possible for remote configuration to be used.

More information http://www.comsoc.org/pubs/surveys/4q98issue/stallings.html

Summary

SNMP is the most widely protocol used for management. A security enhancement in SNMP guarantee reliability. As you can see SNMPv3 has better security than its predecessors. SNMPv4 probably will take in count that today DES Encryption is not considered secure. It is crackable in a short period of time. Maybe triple DES will be used.

References:

SNMPv3: A Security Enhancement for SNMP by William Stalling
http://www.comsoc.org/pubs/surveys/4q98issue/stallings.html

SNMP WORLD
www.snmpworld.com

Cisco SNMPv3
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/snmp3.pdf

Configuring SNMP
www.cisco.com

Securing your Cisco Router when using SNMP
http://www.sans.org/y2k/GSEC.htm

Cisco Publications
The New SNMPv3 Proposed Internet Standards by William Stalling
http://www.cisco.com/warp/public/759/ipj_1-3/ipj_1-3_snmpv3.html

SNMP A guide to Network Management
Dr. Sidnie Feit
McGraw-Hill 1995

Mastering Network Security
Chris Brenton 2000
SYBEX