CAcert
WoT User
Digitally signed by CAcert WoT User
DN: cn=CAcert WoT User, email=joao.neves@fe.up.pt
Date: 2020.06.12 00:43:14 +01'00'

SNMPv3

The extension of SNMP in Administration and Security

The Management Model

SNMPv3 maintains the Internet Network Management model with four components, as provided in SNMPv1:

- One or more nodes to manage, each containing an SNMP entity (an Agent) that allows access to node management information;
- At least one SNMP management entity (a Manager) with one or more network management applications installed;
- A network management protocol, which is used by NMS and agents to exchange management information;
- Management Information.

But contemplates additionally...

The Management Model...

SNMPv3 includes additionally four security areas that were missing in SNMPv2:

- **Authentication**: origin identification, message integrity and some aspects of security in the response;
- **Privacy**: confidentiality;
- **Authorization and Access Control**;
- Configuration and Remote Administration capability for the three previous aspects.

The SNMPv3 Framework

- In 2002 the Internet Engineering Task Force Steering Group (IESG) approved SNMPv3 as "full standard" and changed the status of SNMPv1 and SNMPv2c to "historic status"
- Defined in RFC 3411, December 2002, which is part of the STD0062
- Conceptually it is an extension of SNMP in the area of Administration and Security
- Want to have a modular architecture that allows for easy expansion (for example, new security protocols may be supported by SNMPv3 defining them as separate modules)

SNMPv3: Project Goals

- Take advantage of the work developed in SNMPv2u and SNMPv2 *;
- Resolve the security issue in SET operations (the major weakness of SNMPv1 and SNMPv2c);
- Define an architecture that guarantees longevity to the SNMP Framework;
- Keep SNMP simple;
- Ensure that SNMP does not incur high costs for minimal implementation;
- Facilitate partial SNMP update without changing the SNMP Framework;
- Enable the support of large and complex networks, but make implementation costs dependent on the added facilities.

SNMPv3: Specifications

RFC 3410 Introduction and Applicability Statements for Internet Standard Management Framework (December 2002)

RFC 3411 An Architecture for Describing SNMP Management Frameworks (December 2002)

RFC 3412 Message Processing and Dispatching (December 2002)

RFC 3413 SNMP Applications (December 2002)

RFC 3414 User-based Security Model (December 2002)

RFC 3415 View-based Access Control Model (December 2002)

RFC 3416 Version 2 of SNMP Protocol Operations (December 2002)

RFC 3417 Transport Mappings (December 2002)

RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) (December 2002)

RFC 3584 Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework (August 2003)

RFC 2578 Structure of Management Information Version 2 (SMIv2) (April 1999)

RFC 2579 Textual Conventions for SMIv2 (April 1999)

RFC 2580 Conformance Statements for SMIv2 (April 1999)

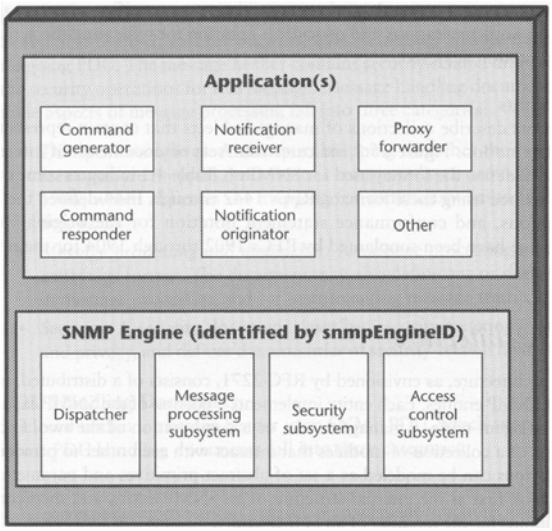
The Entity

- In previous releases there were two entities: the SNMP agent and the SNMP manager
- In this release there is an SNMP entity that is composed of two parts: the SNMP engine and the SNMP applications

SNMP Entity

RFC 3411, STD 0062

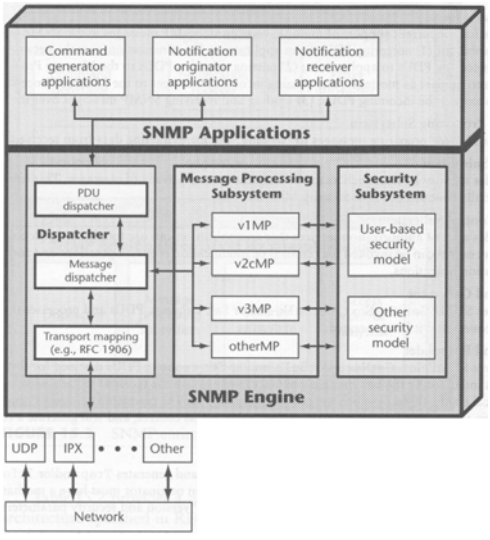
- An SNMP Entity is the implementation of SNMPv3 Architecture;
- Each Entity consists of two main elements: an SNMP Engine and one or more Applications;
- SNMP Engine **sends and receives** messages, **authenticates and encrypts** messages, and **controls access** to managed objects;
- The SNMP Engine is uniquely identified by the ***snmpEngineID*** identifier.



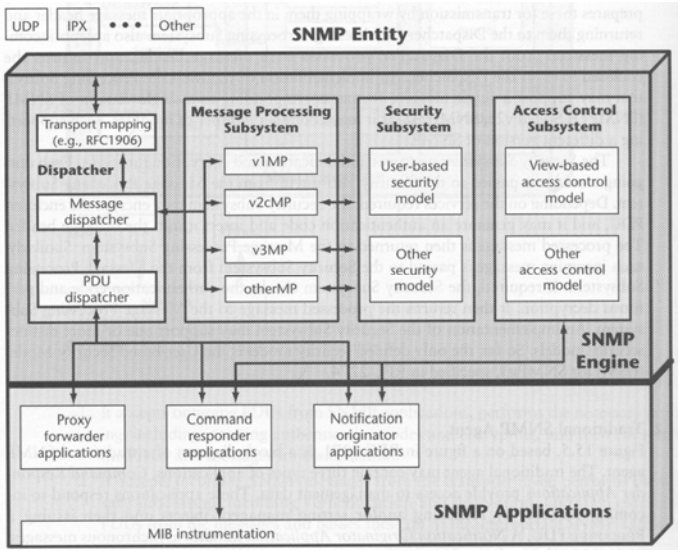
SNMP Engine Components

- ***Dispatcher*** - receives and sends messages to its Message Processing Model
- ***Message Processing Subsystem*** - consists of one or more Message Processing Models
- ***Security Subsystem***
- ***Access Control Subsystem***

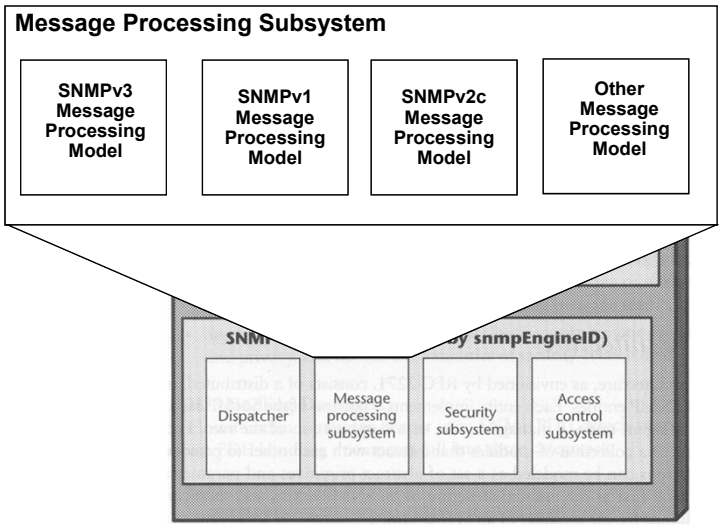
SNMP Manager



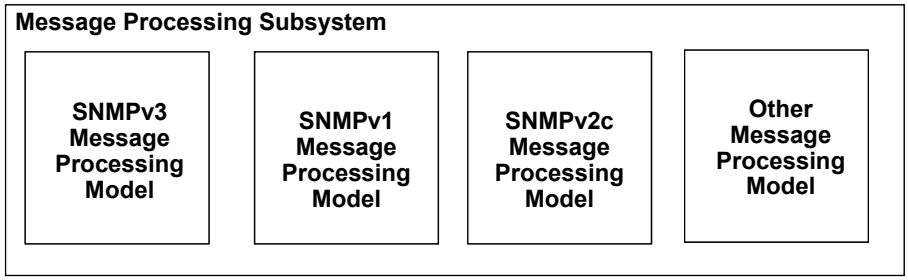
SNMP Agent



Message Processing Subsystem

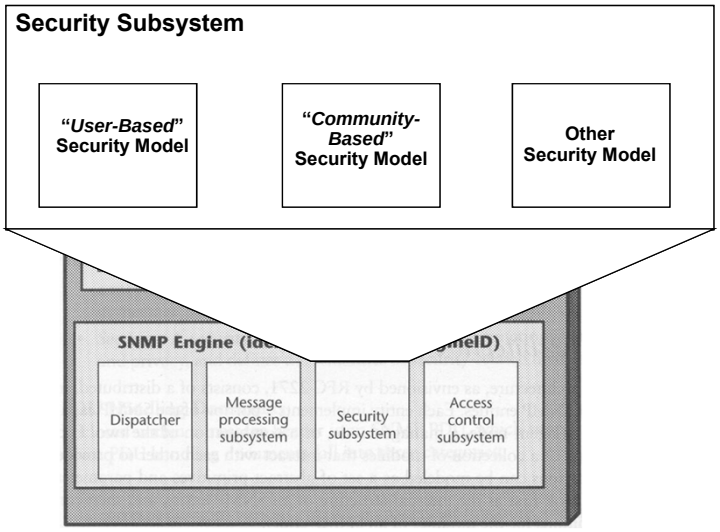


Message Processing Subsystem



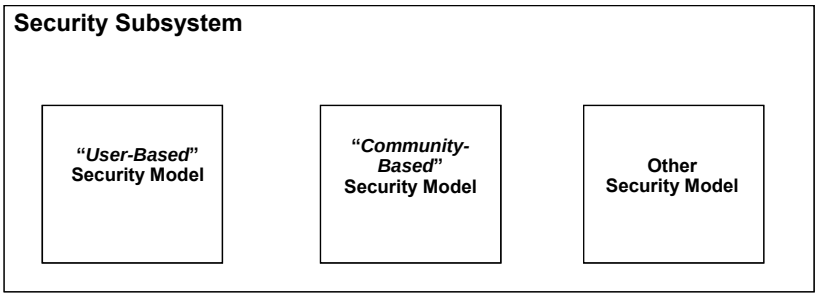
- **Supports models for SNMPv3, SNMPv2c, SNMPv1 and Others**
- **Prepare messages to send**
- **Extract data from received PDUs**

Security Subsystem



Security Subsystem

- **Authenticate messages**
- **Decrypts and encrypts private messages**



Security and Privacy

RFC 3414 - User-based Security Model

Threats are classified by severity:

- **Principal**
- **Secondary**
- **Others of lesser Importance**

Principal Threats

1. **Masquerade / Authentication of Origin**: the intruder assumes the identity of the sender to gain his privileges.
2. **Modification of Information / Data integrity:** change of messages in transit.
3. **Message Stream Modification:** the sequence is changed / reordered, messages are delayed or repeated.
4. **Disclosure / Confidentiality:** privileged information is obtained by spying on messages exchanged.
5. **Denial of Service (DoS):** denied access to the service to authorized users.
6. **Traffic Pattern Analysis:** Traffic patterns are examined in an attempt to obtain sensitive information.

Secondary Threats

1. **Masquerade / Authentication of Origin**: the intruder assumes the identity of the sender to gain his privileges.
2. **Modification of Information / Data integrity:** change of messages in transit.
3. **Message Stream Modification:** the sequence is changed / reordered, messages are delayed or repeated.
4. **Disclosure / Confidentiality:** privileged information is obtained by spying on messages exchanged.
5. **Denial of Service (DoS):** denied access to the service to authorized users.
6. **Traffic Pattern Analysis:** Traffic patterns are examined in an attempt to obtain sensitive information.

Others Threats

1. **Masquerade / Authentication of Origin**: the intruder assumes the identity of the sender to gain his privileges.
2. **Modification of Information / Data integrity:** change of messages in transit.
3. **Message Stream Modification:** the sequence is changed / reordered, messages are delayed or repeated.
4. **Disclosure / Confidentiality:** privileged information is obtained by spying on messages exchanged.
5. **Denial of Service (DoS):** denied access to the service to authorized users.
6. **Traffic Pattern Analysis:** Traffic patterns are examined in an attempt to obtain sensitive information.

Security Levels

The Architecture for SNMP Management Frameworks recognizes three levels of security (RFC 3411):

1. Without authentication and without privacy (***noAuthNoPriv***)
2. With authentication but without privacy (***authNoPriv***)
3. With authentication and with privacy (***authPriv***)

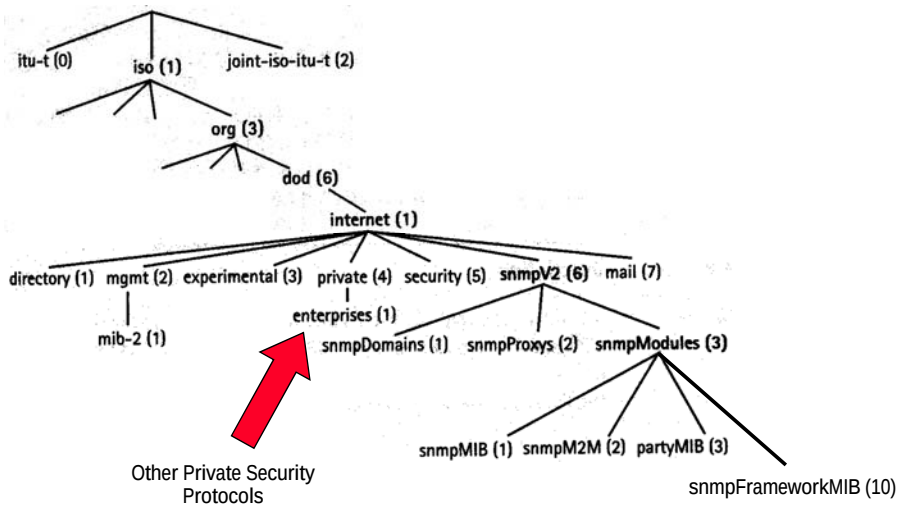
Security Mechanisms

- User-based Authentication Mechanism is based on HMAC-MD5 (Hash-based Message Authentication Code) and HMAC-SHA as optional alternative algorithm
- User-based Privacy Mechanism is based on CBC-DES (Cipher Block Chaining - Data Encryption Standard)
- Other protocols may be adopted in the future
- In SNMPv1 and SNMPv2c only authentication is implemented (*community strings)*, without privacy

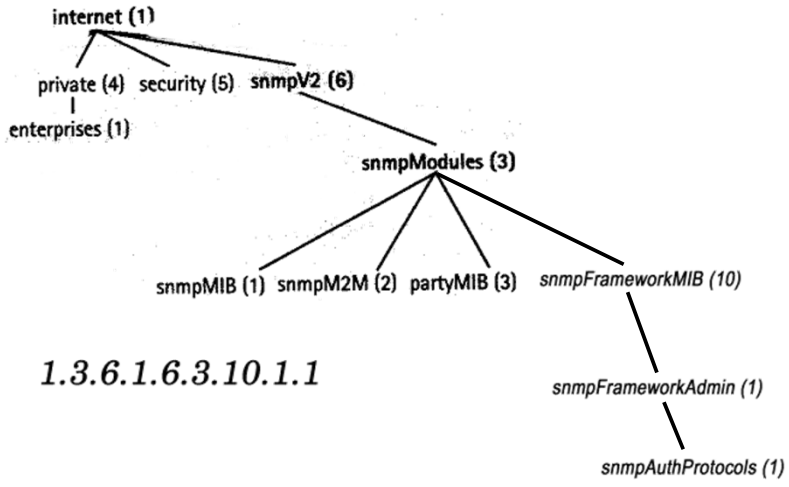
Security models and schemes

Model	Scheme	Authentication	Privacy	Action
SNMPv3	No authentication No privacy	Username (security name)	No	Username matching for authentication
SNMPv3	Authentication No privacy	MD5 or SHA	No	Provides unique authentication for each user based on the HMAC-MD5 or the HMAC-SHA algoritm
SNMPv3	Authentication Privacy	MD5 or SHA	DES	Provides unique authentication for each user based on the HMAC-MD5 or the HMAC-SHA algoritm. Provides data privacy based on the CBS-DES protocol

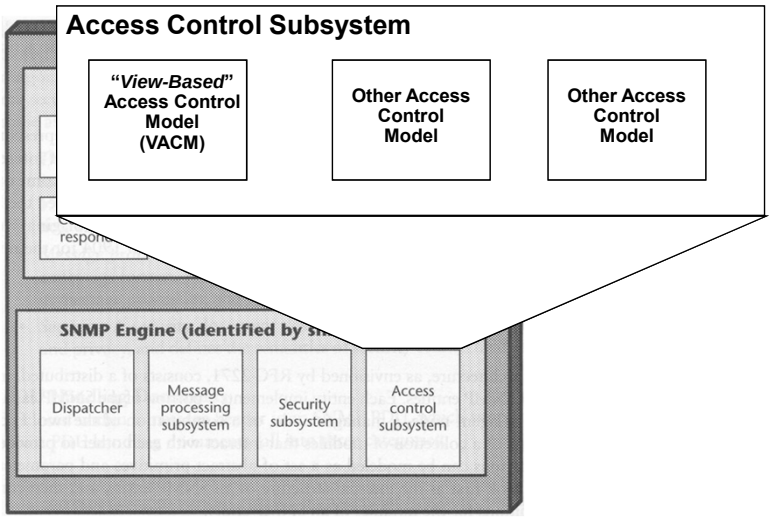
The Security subtree



snmpAuthProtocols

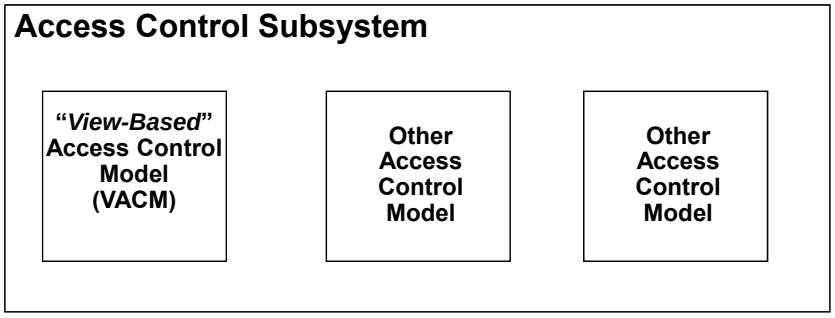


The Access Control Subsystem



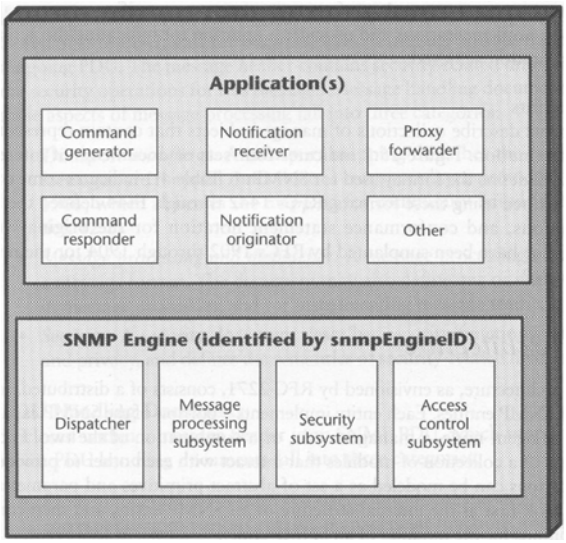
The Access Control Subsystem

- Determines permission to access a managed object
- Only the "View-Based Access Control Model" is defined



SNMPv3 Applications

- Internal applications in an SNMP entity;
- Generate SNMP messages, respond to SNMP messages, generate notifications, receive notifications, and route messages between SNMP entities.

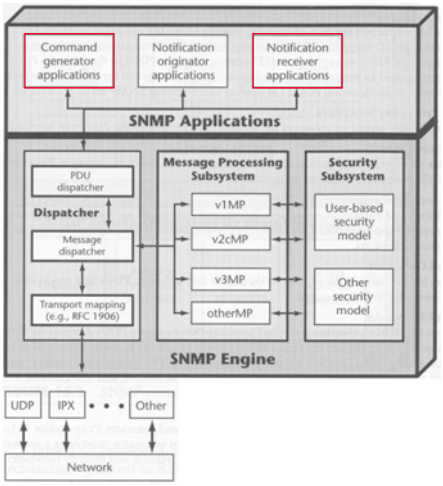


SNMPv3 Applications

- There are five types of Applications:
  - *Command Generators*: Monitor and manipulate management data
  - *Command Responders*: Facilitate Access to Management Information
  - *Notification Originators*: Initiate asynchronous messages
  - *Notification Receivers*: Handle Asynchronous Messages
  - *Proxy Forwarders*: Forward messages between entities
- Applications use the Services (Dispatcher, Message Processing Subsystem, Security Subsystem, and Access Control Subsystem) that are provided by the SNMP Engine.

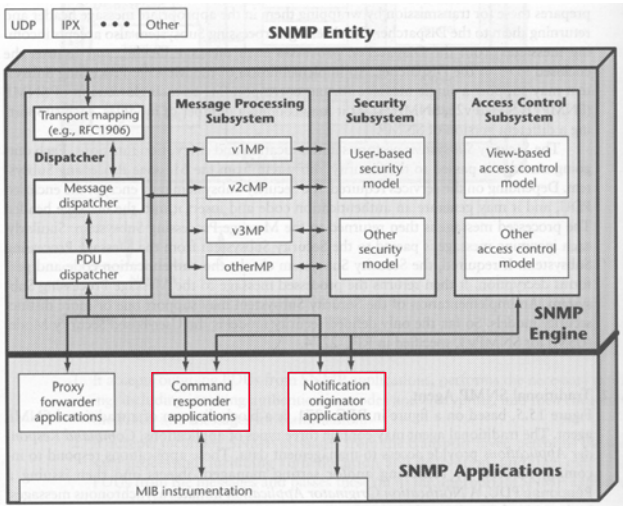
The SNMPv3 Manager

- An SNMP Entity that contains one or more, Command Generator and / or Notification Receiver Applications is called an SNMP Manager.

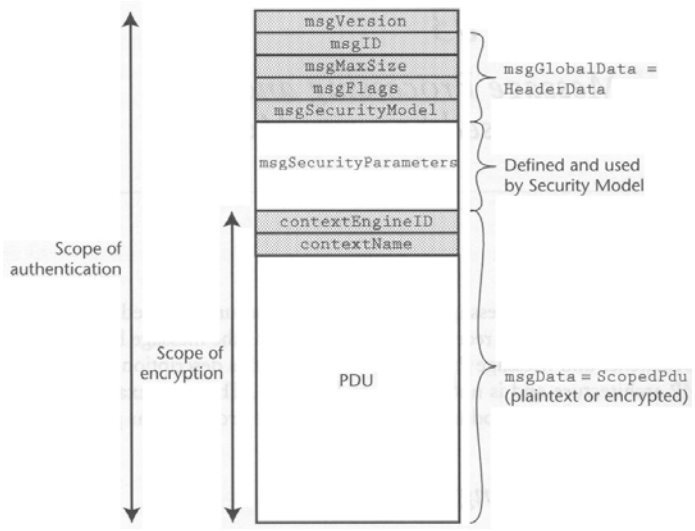


The SNMPv3 Agent

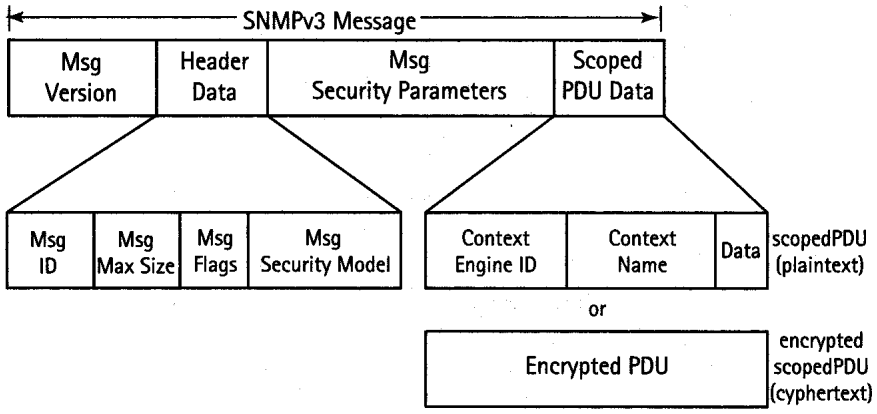
- An SNMP Entity that contains one or more Application Command and Responder or Notification Originators is called an SNMP Agent.



Message Format



Format (cont.)



Message Fields

- **msgVersion** - value 3 identifies an SNMPv3 message;
- **msgID** - integer value used to sort request and response messages between two SNMP entities;
- **msgMaxSize** - integer value that indicates the maximum message size that the originator supports; the answer depends on this value;
- **msgFlags** - an octect that contains the flags that indicate if there should be a response and what level of security is used (*reportableFlag*, *authFlag* and *privFlag*) [...];
- **msgSecurityModel** - integer value that identifies the Security template used at the source; possible values are those defined in *SnmpSecurityModel.*

msgFlags

Field	Meaning
....1	authFlag (when authFlag = 1, a process to authenticate the message is in use)
.... ..1.	privFlag (when privFlag = 1, a process to protect the message from disclosure is in use)
.... .1..	reportableFlag (when reportableFlag = 1, a Report PDU is returned to the sender under certain conditions)

Permissible values for the authFlag and privFlag are:

Field	Meaning
.... ..00	is OK, means noAuthNoPriv
.... ..01	is OK, means authNoPriv
.... ..10	reserved, must not be used
.... ..11	is OK, means authPriv

New Textual Conventions

- **SnmpEngineID**
- **SnmpSecurityModel**
- **SnmpMessageProcessingModel**
- **SnmpSecurityLevel**
- **SnmpAdminString**
- **SnmpTagValue**
- **SnmpTagList**
- **KeyChange**

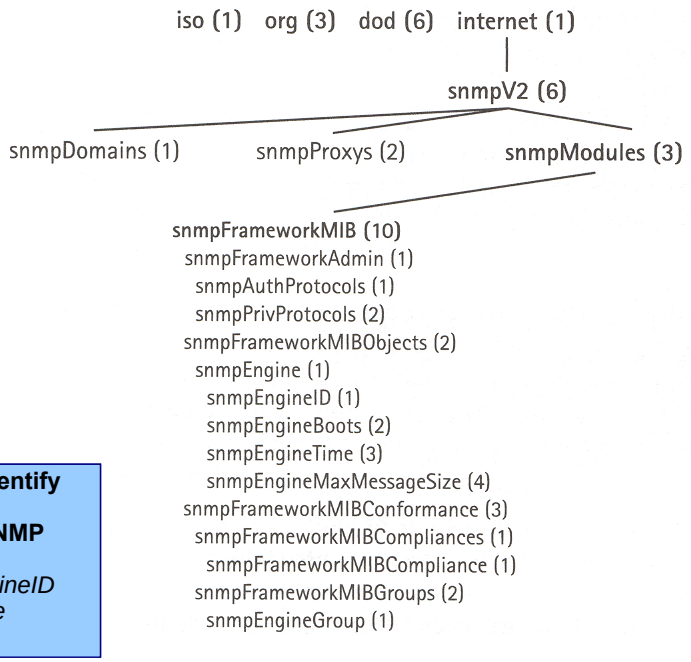
SNMP Framework MIB

RFC3411, STD0062

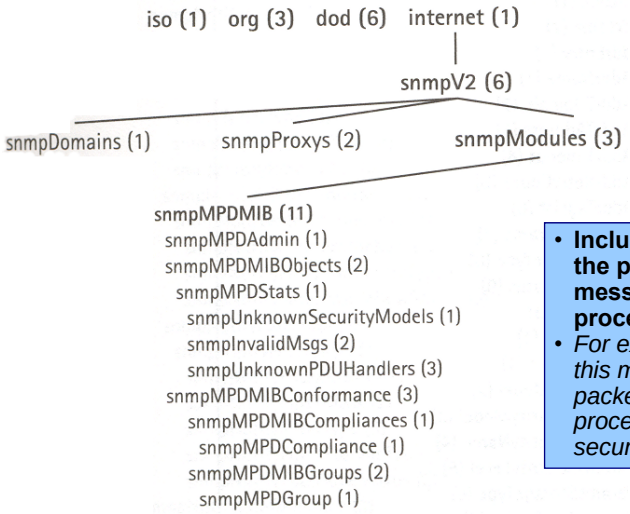
{snmpModules 10}

ou {1.3.6.1.6.3.10}

- **Includes objects to identify and determine the configuration of an SNMP engine**.
- *For example, snmpEngineID defines a unique engine identifier*



Dispatching and Message Processing MIB



SNMP-MPD-MIB
RFC3412, STD0062
{snmpModules 11}
ou {1.3.6.1.6.3.11}

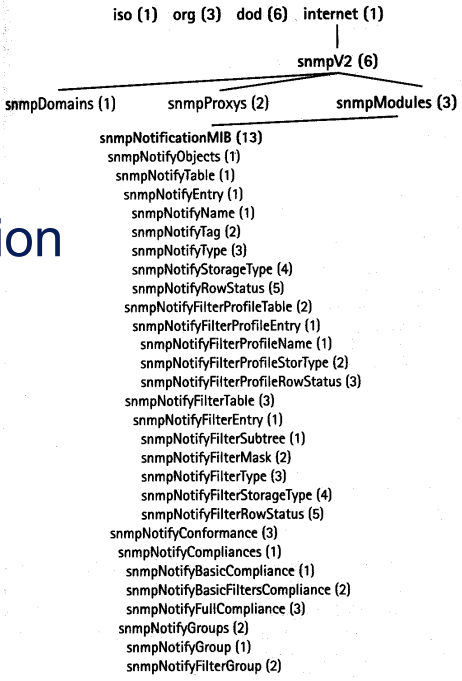
- **Includes objects to monitor the processing of SNMP messages and the Dispatch process**.
- *For example, objects defined in this module count SNMP packets received but not processed due to syntactic or security errors*

SNMP Target MIB

RFC3413, STD0062
{snmpModules 12}
ou {1.3.6.1.6.3.12}

- **Includes objects for remote configuration or management of "targets".**
- *For example, snmpTargetAddrTable sets the table of addresses to transport the generated messages.*

SNMP Notification MIB



SNMP-NOTIFICATION-MIB

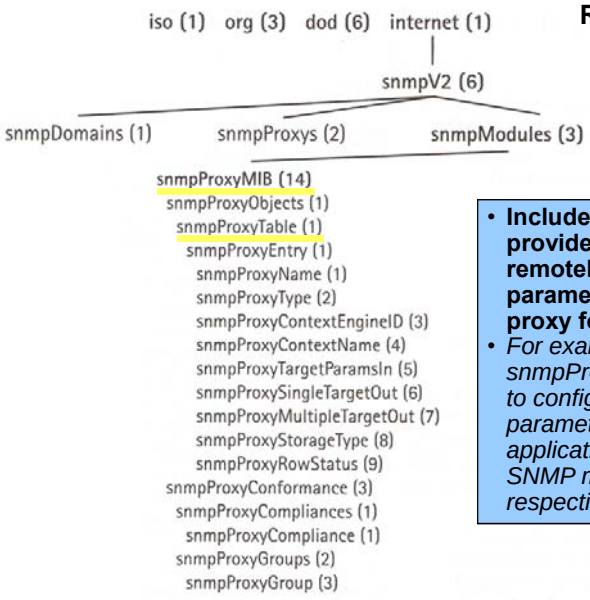
RFC3413, STD0062

{snmpModules 13}

ou {1.3.6.1.6.3.13}

- **Includes objects for remote configuration of parameters used in the notification generation process.**
- *For example, snmpNotifyTable is used to select the targets that should receive notifications, as well as the type of notifications that should receive.*

SNMP Proxy MIB



SNMP-PROXY-MIB

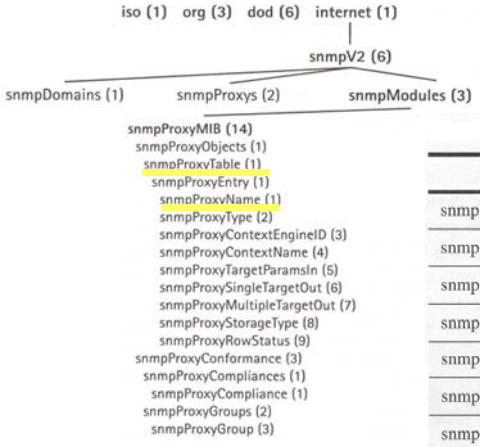
RFC3413, STD0062

{snmpModules 14}

ou {1.3.6.1.6.3.14}

- **Includes objects that provide mechanisms to remotely configure the parameters used in the proxy forwarding process.**
- *For example, snmpProxyTable allows you to configure the translation parameters used by proxy applications for forwarding SNMP messages and the respective targets.*

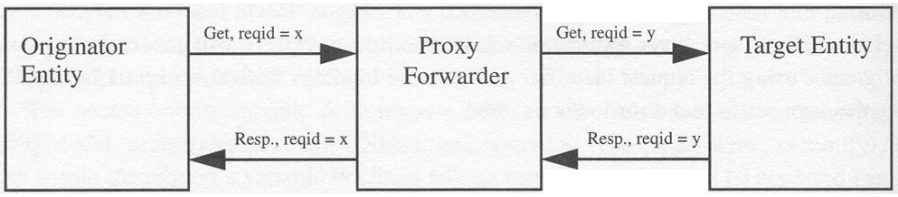
Proxy MIB (cont.)



snmpProxyTable, Indexed by snmpProxyName

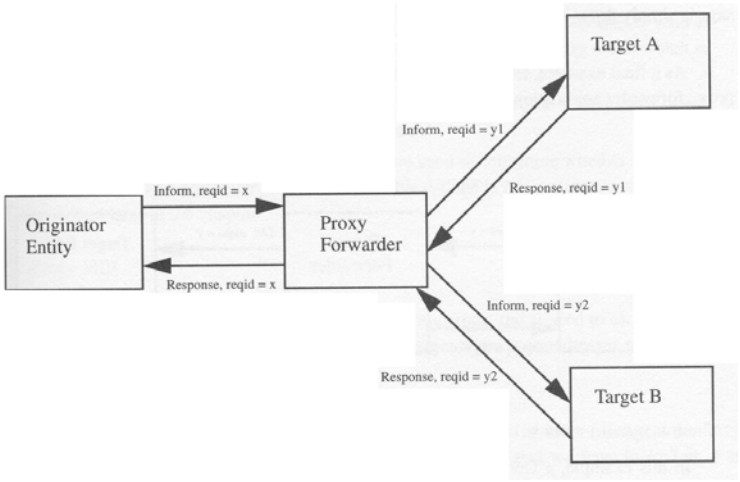
Object	Type	Access
snmpProxyName	SnmpAdminString	no-accessible
snmpProxyType	INTEGER	read-create
snmpProxyContextEngineID	SnmpEngineID	read-create
snmpProxyContextName	SnmpAdminString	read-create
snmpProxyTargetParamsIn	SnmpAdminString	read-create
snmpProxySingleTargetOut	SnmpAdminString	read-create
snmpProxyMultipleTargetOut	SnmpTagValue	read-create
snmpProxyStorageType	StorageType	read-create
snmpProxyRowStatus	RowStatus	read-create

Proxy Operation



1. The SNMP Entity sends a Get PDU with an ID = x.
2. The Proxy translates the content of the message it receives and forwards it to the respective target. This new message is assigned the unique ID = y. The SNMP version of the message you receive and the message you send can be different, which means a more complex translation.
3. The target Entity processes the Get message and responds with a PDU, ID = y.
4. The Proxy receives the PDU ID = y, verifies that it is the response to the PDU ID = x and builds the response PDU with ID = x.

Inform PDU Forwarding



Example

snmpTargetAddrTable Proxy

	addr1	addr2
snmpTargetAddrName	addr1	addr2
snmpTargetAddrTDomain	snmpUDPDomain	snmpUDPDomain
snmpTargetAddrTAddress	158.101.121.1/1061	158.101.121.2/162
snmpTargetAddrTagList	router	workstation
snmpTargetAddrParams	p1	p2
snmpTargetAddrStorageType	nonVolatile (3)	nonVolatile (3)
snmpTargetAddrRowStatus	active (1)	active (1)

- **These destinations are registered with the Proxy to forward messages to them**

snmpProxyTable

	proxy1	proxy2
Name	proxy1	proxy2
Type	1	3
snmpProxyContextEngineID	80 00 00 09 01 9e 65 79 01	80 00 00 2a 01 9e 65 79 02
snmpProxyContextName	admin	monitor
snmpProxyTargetParamsIn	p1	p2
snmpProxySingleTargetOut	addr1	
snmpProxyMultipleTargetOut		workstation
snmpProxyStorageType	nonVolatile (3)	nonVolatile (3)
snmpProxyRowStatus	active (1)	active (1)

Example (cont.)

snmpProxyTable

	proxy1	proxy2
snmpProxyName	proxy1	proxy2
snmpProxyType	1	3
snmpProxyContextEngineID	80 00 00 09 01 9e 65 79 01	80 00 00 2a 01 9e 65 79 02
snmpProxyContextName	admin	monitor
snmpProxyTargetParamsIn	p1	p2
snmpProxySingleTargetOut	addr1	
snmpProxyMultipleTargetOut		workstation
snmpProxyStorageType	nonVolatile (3)	nonVolatile (3)
snmpProxyRowStatus	active (1)	active (1)

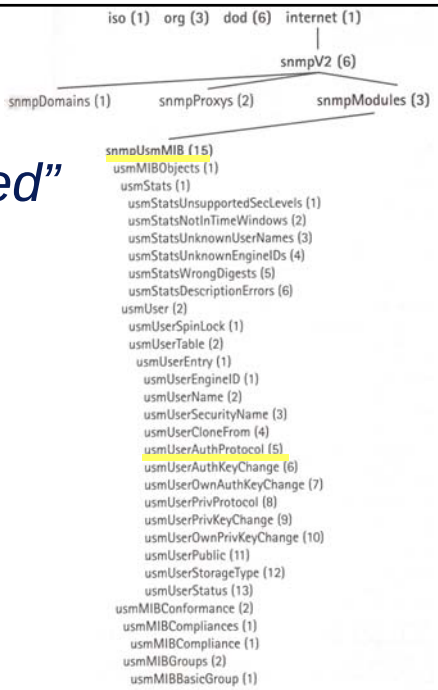
This is a Sun system

The destination is a Cisco

`snmpTargetAddrTable` says that this address is the port `161` of `158.101.121.1`

The following is an IPv4 address

"User-Based" Security Model



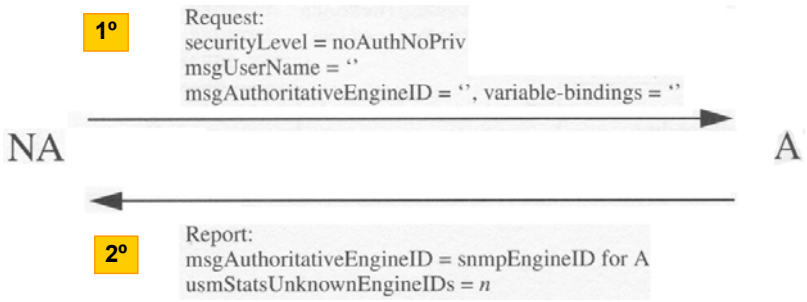
RFC3414, STD0062

{snmpModules 15}

ou {1.3.6.1.6.3.15}

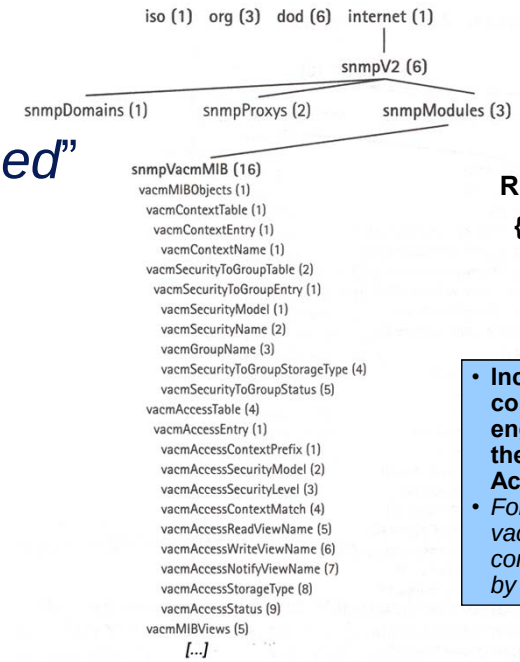
- **It includes objects to configure an SNMP engine that implements the *"User-Based"* Security Model (USM).**
- *For example, usmUserAuthProtocol specifies the type of authentication protocol.*

Discovery



- **USM allows a non-authenticating SNMP Entity to learn the identification (*snmpEngineID*) of another authenticated entity with whom it intends to communicate.**
- **The message with the response report includes the updated *usmStatsUnkownEngineID* counter in the "variable-bindings".**

"*View-Based*" Access Control Model (VACM)



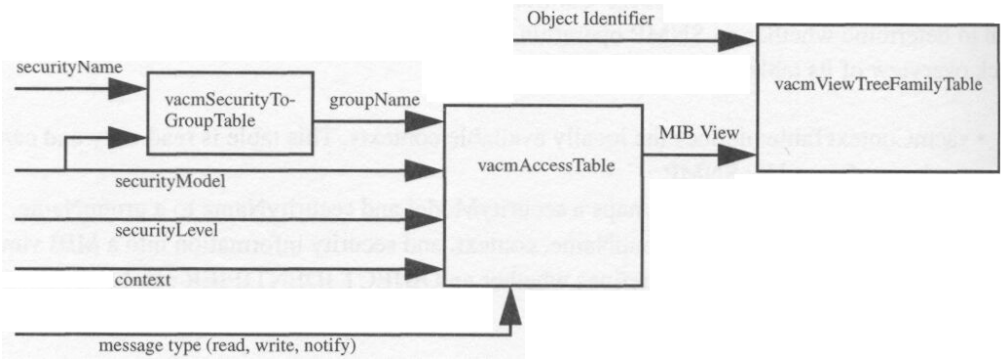
RFC3415, STD0062

{snmpModules 16}

or {1.3.6.1.6.3.16}

- **Includes objects to configure an SNMP engine that implements the "View-Based" Access Control Model**
- *For example, vacmAccessTable contains the access rights by groups.*

VACM



Example in a Cisco

- **Create an SNMPv3 view of the `internet` subtree, called** *so-leitura:*

```
router(config)# snmp-server view so-leitura internet included
router(config)# snmp-server group 4readonly v3 auth read so-leitura
router(config)# snmp-server user johnsilva 4readonly v3 auth md5 secretpwd
```

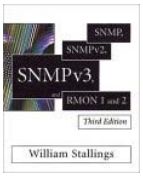
- **If wanted to limit the query to the `system` group, it would only be:**

```
router(config)# snmp-server view so-leitura system included
```

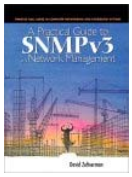
SNMP Community MIB

{snmpModules 18}
or {1.3.6.1.6.3.18}

Bibliography



- **Stallings, William**
  SNMP, SNMPv2, SNMPv3 and RMON 1 and 2
  Addison-Wesley Publishing Company, 3rd Ed.
  ISBN 0-20-148534-6



- **Zeltserman, David**
  Practical Guide to Snmpv3 and Network Management
  Prentice Hall International
  ISBN 0-13-021453-1