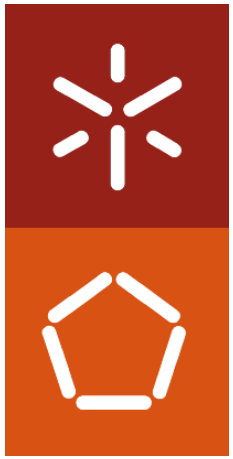
GESTÃO DE REDES / NETWORK MANAGEMENT

Notas complementares / Complementary notes

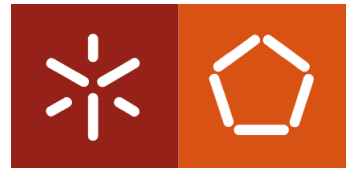
User-based Security Model
View-based Access Control Model



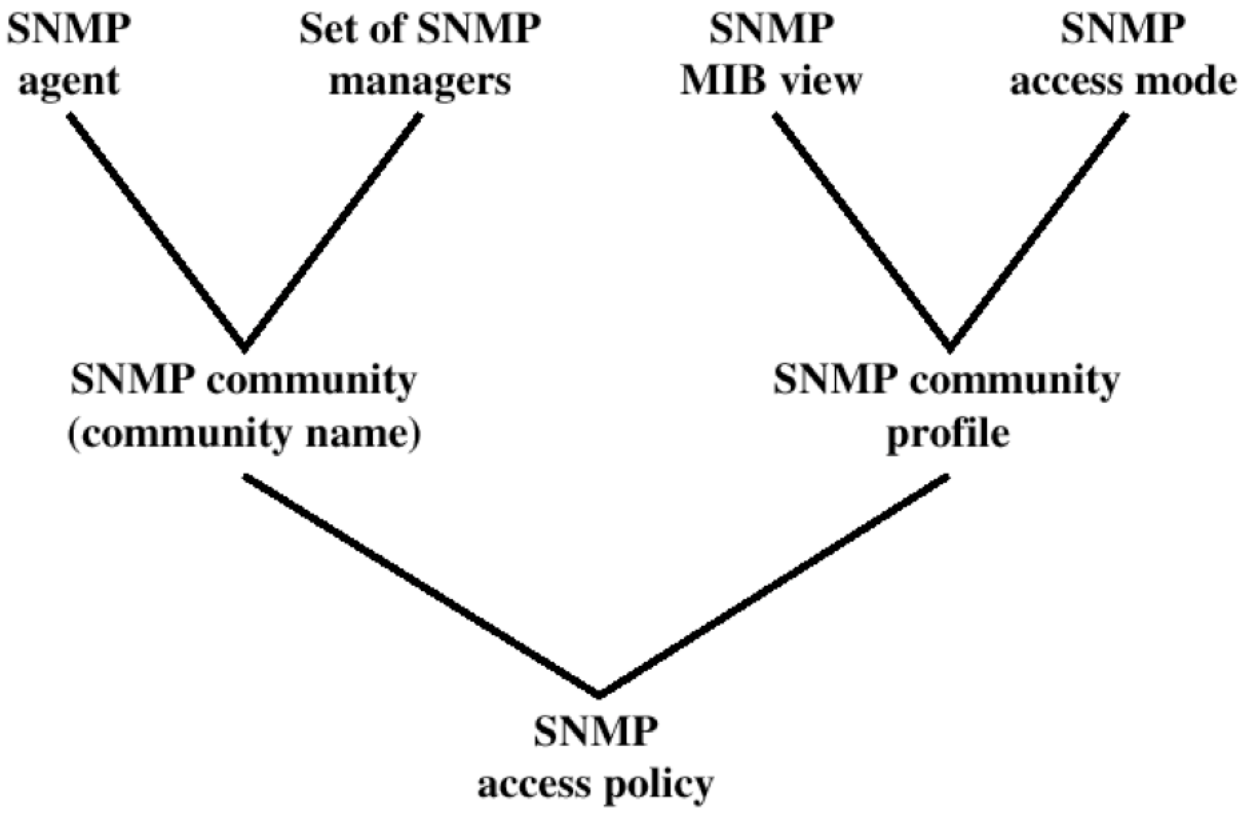
SNMP v1/v2 Security

- **v1 / v2c**
  - "Community" String sent in all protocol messages
  - Actually acts as a "password"
  - The agent only responds if the password is correct
- **Pros and cons:**
  - Simple, very simple, to implement ....
  - It is not encrypted!
  - Very weak security
  - requires secure "channel"
  - There is no concept of "user" but rather of “community” of managers (dilute responsibilities)

SNMP v1/v2 Security



- **v1 / v2c: community-based access model**



SNMP v3 Security Model

- **V3**
  - No use of "community strings" ... !
  - Users authentication (agents can verify user identity)
  - One "Shared secret" for each user (used in authentication)
  - Messages are sent with a calculated *hash* of the message with the shared secret ... the *hash* can be validated at the destination
  - Message content (payload) can optionally be encrypted with a second "Shared secret" (used for confidentiality)
  - Properties: authentication, integrity, confidentiality
  - Two models and a clear separation between: Authentication (**User-Based Security Model**) and Access Control (**View-Based Access Control Model**)

USM – User-Based Security Model

- **Principal Threats:**
  - Modification of Information: The modification threat is the danger that some unauthorized entity may alter in-transit SNMP messages (...)
  - Masquerade: The masquerade threat is the danger that management operations (...) may be attempted by assuming the identity of another user
- **Secondary Threats:**
  - Disclosure: The disclosure threat is the danger of eavesdropping on the exchanges between managed agents and a management station.
  - Message Stream Modification: The message stream modification threat is the danger that messages may be maliciously re-ordered, delayed or replayed (...) SNMP protocol is typically based upon a connection-less transport service
- **Threats not considered:**
  - Denial of Service
  - Traffic Analysis: (...) traffic patterns are predictable ...

USM – User-Based Security Model

- **Security requirements:**
  - Data Integrity: provision of the property that data has not been altered or destroyed in network
  - Data Origin Authentication: the claimed identity of the origin is corroborated
  - Data Confidentiality: information is not available to unanthorized entities
  - Limited stream integrity: message whose generation time is outside of a specified time window is not accepted
- **and constraints:**
  - If management network stress is inconsistent with security, give preference to the former (!)
  - No dependency on other services (ex: NTP, key manag. Like PKI)
  - security mechanism should entail no changes to the basic SNMP network management philosophy....

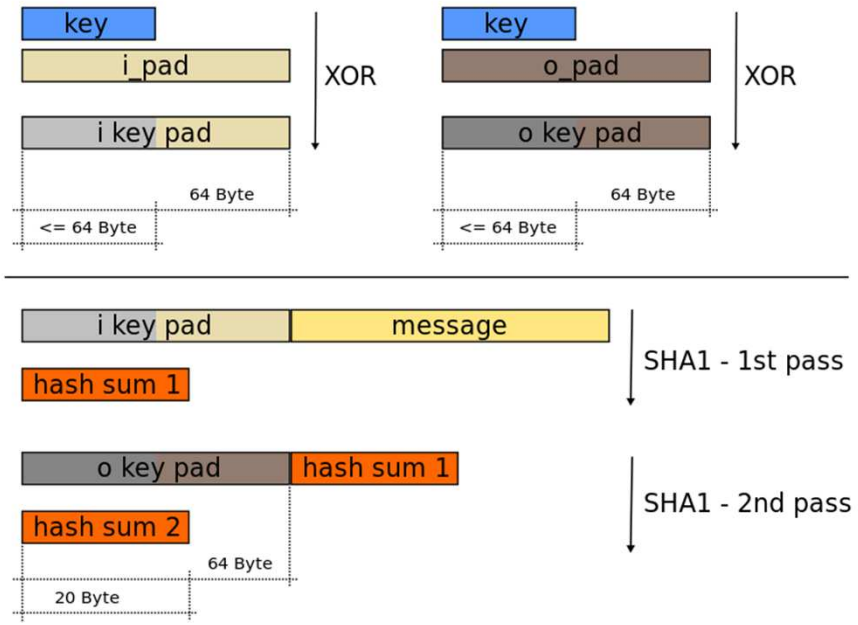
USM: HMAC – RFC2104

$$\mathrm{HMAC}(K, m) = \mathrm{H}\left((K' \oplus opad) \parallel \mathrm{H}\left((K' \oplus ipad) \parallel m \right) \right)$$

$$K' = \begin{cases} \mathrm{H}(K) & K \text{ is larger than block size} \\ K & \text{otherwise} \end{cases}$$

where

H	is a cryptographic hash function,
m l	s the message to be authenticated,
K	is the secret key,
K'	is a block-sized key derived from the secret key, *K*; either by padding to the right with 0s, up to the block size, or by hashing down to the block size,
‖	denotes concatenation,
⊕	denotes bitwise exclusive or (XOR),
opad	is the outer padding, consisting of repeated bytes, valued 0x5c, up to the block size, and
Ipad	Is the inner padding, consisting of repeated bytes, valued 0x36, up to the block size.



(images from Wikipedia: https://en.wikipedia.org/wiki/HMAC)

USM: CBC-DES and Others

- **RFC 3414 defines DES as the only required method of message encryption for SNMP Version 3 authPriv mode**
  - The data is encrypted in Cipher Block Chaining mode.
  - The plaintext is divided into 64-bit blocks.
- **RFC 3826**
  - provides support for the 128-bit key in the Advanced Encryption Standard (AES).
  - included in the SNMP-USM-AES-MIB
- **And CISCO extensions:**
  - The extended options of AES with 192- or 256-bit keys and 3-DES are supported as extensions in the Cisco-specific MIB—CISCO-SNMP-USM-EXT-MIB.

USM: Security Level

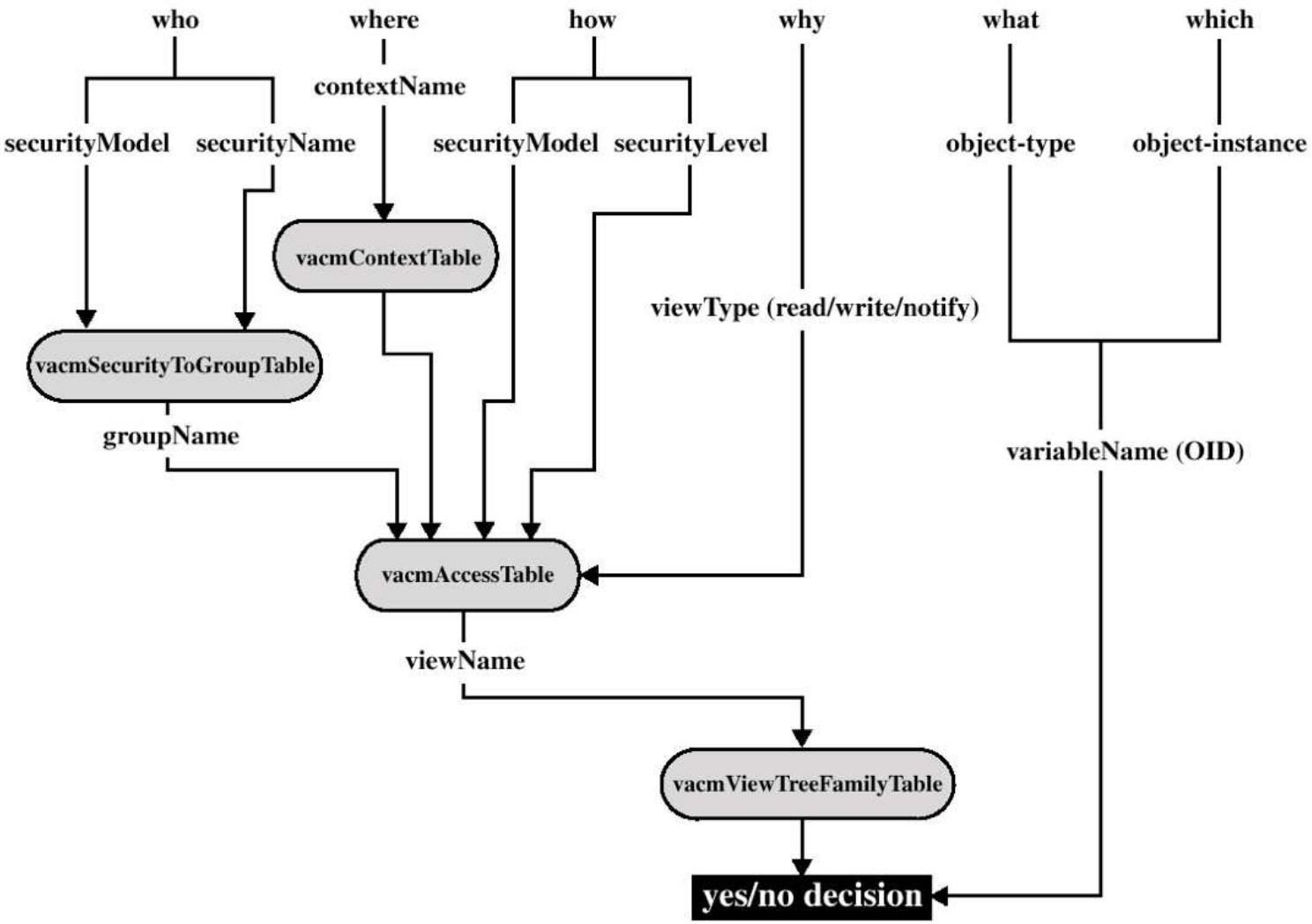
- **Confidentiality & Authentication services**

Auth \ Priv	[Yes]	[No]
[Yes]	authPriv	authNoPriv
[No]	noAuthPriv	noAuthNoPriv

→ **noAuthPriv** doesn't make sense and is not used! Why??

VACM – View-Based Access Control Model

- **RFC3414 (https://tools.ietf.org/html/rfc3415)**



VACM – View-Based Access Control Model

- **Abstract primitive for Access Control:**

```
statusInformation =     -- success or errorIndication      isAccessAllowed(
                         securityModel      -- Security Model in use
                         securityName       -- principal who wants access
                         securityLevel      -- Level of Security
              viewType          -- read, write, or notify view
              contextName       -- context containing variableName
              variableName      -- OID for the managed object          )
```

- **Results:**

  accessAllowed

  notInView

  noSuchView, noSuchContext, noGroupName, noAccessEntry

  otherError

VACM MIB (RFC3415)

vacmContextTable OBJECT-TYPE

SYNTAX SEQUENCE OF VacmContextEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION "The table of locally available contexts.

vacmSecurityToGroupTable OBJECT-TYPE

SYNTAX SEQUENCE OF VacmSecurityToGroupEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION "This table maps a combination of securityModel and

securityName into a groupName which is used to define an access control policy for a group of principals."

VACM MIB (RFC3415)

vacmAccessTable OBJECT-TYPE

SYNTAX SEQUENCE OF VacmAccessEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION "The table of access rights for groups. Each entry is indexed by a groupName, a contextPrefix, a securityModel and a securityLevel. To determine whether access is allowed, one entry from this table needs to be selected and the proper viewName from that entry must be used for access control checking.

VACM MIB (RFC3415)

vacmViewTreeFamilyTable OBJECT-TYPE

SYNTAX SEQUENCE OF VacmViewTreeFamilyEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION "Locally held information about families of subtrees within MIB views.

SNMP CISCO Config.: example 1

snmp-server contact Maria Admin <maria@uminho.pt>

snmp-server location Azurém, Guimarães

snmp-server view mib2 mib-2 **included**

snmp-server community public **ro**

snmp-server community comaccess **rw** 4

snmp-server host 172.16.1.27 **informs** version 2c public alarms

...

access-list 4 **permit** 192.168.100.0 0.0.0.255

SNMP CISCO Configuration

Passos:

1. **enable**
2. **configure terminal**
3. **snmp-server group** [group-name {v1 | v2c | v3 [auth | noauth | priv]}] [**read** read-view] [**write** write-view] [**notify** notify-view] [**access** access-list]
4. **snmp-server engineID** {local engine-id | remote ip-address [udp-port udp-port-number] [vrf vrf-name] engine-id-string}
5. **snmp-server user** user-name group-name [remote ip-address [udp-port port]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access access-list]
6. **end**

SNMP CISCO Config: example 2

snmp-server view *vista-ro* internet included

snmp-server group *ReadGroup* v3 **auth read** *vista-ro*

snmp-server user admin *ReadGroup* v3 **auth** md5 *zy22zy56*

snmp-server user maria *ReadGroup* v3 **auth** md5 *ola12345* **priv** des56 *DXPT##23*

See manual:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.html

NET-SNMP Config

Ver: http://net-snmp.sourceforge.net/wiki/index.php/Vacm

```
#        sec.name  source          community
com2sec local     localhost       secret42
com2sec custom_sec 192.168.1.0/24  public

#                 sec.model  sec.name
group custom_grp v1          custom_sec
group custom_grp v2c         custom_sec
group incremental usm        myuser      # SNMPv3 username == sec.name

#            incl/excl subtree                          mask
view all     included  .1
view custom_v excluded  .1
view custom_v included  sysUpTime.0
view custom_v included  interfaces.ifTable

#                context sec.model sec.level match  read     write  notif
access MyRWGroup ""      any       noauth    exact  all      all    none
access custom_grp ""     any       noauth    exact  custom_v none   none
access incremental ""    usm       noauth    exact  custom_v none   none
```