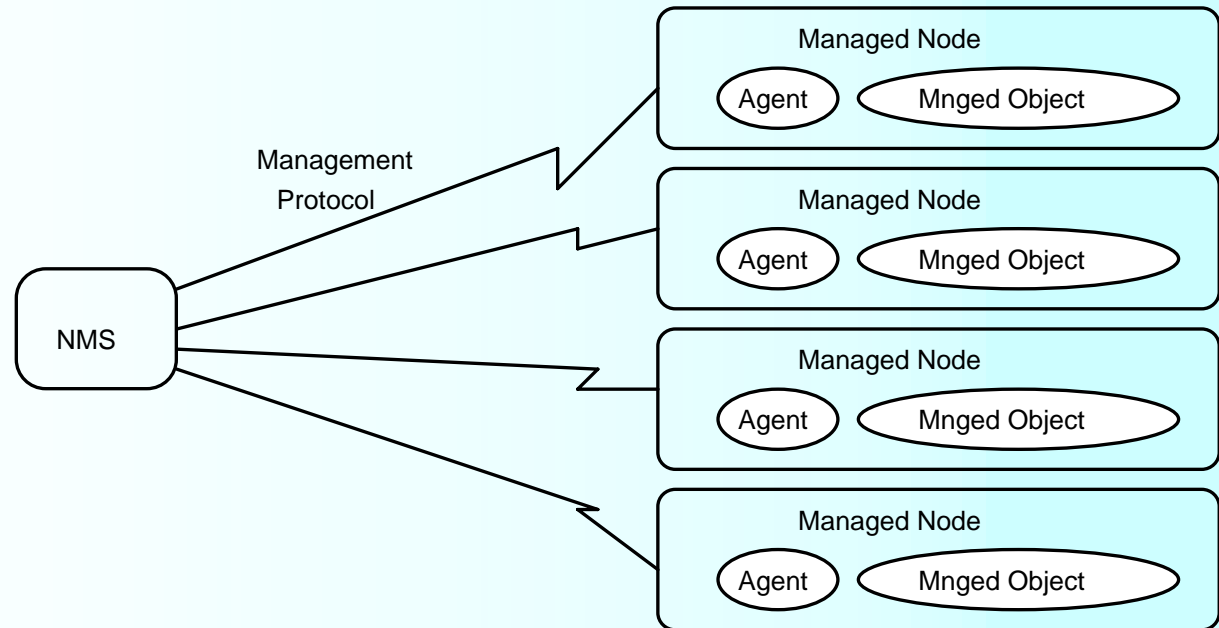


SNMP

Simple Network Management Protocol

- Protocolo de gestión remota de dispositivos



SNMP

Simple Network Management Protocol

- Managed Nodes
 - hosts, servers, routers, hubs, bridges
- **Agent**
- **NMS "Network Management Station"**
- Management Protocol **SNMP**
- Managed Objects & Management Information Base **MIB**
- Management Operations
 - Read, Write, Traversal, Trap
- Proxy Agents

SNMP

Data Representation

- **ASN.1 (Abstract Syntax Notation One)**

- Abstract Syntax

- Utilizados para definir formatos de PDUs

- Utilizados para definir estructuras de datos asociadas a objetos administrables

- **Types**

- Define tipos de datos. Los labels empiezan con letra mayúscula.

- **Values**

- Instancias de un tipo de datos. Los labels empiezan con letra minúscula.

- **Macros**

- Para cambiar la gramática del lenguaje. Los labels llevan todas mayúsculas.

SNMP

Data Representation - Types

- Define tipos de datos. Los labels empiezan con letra mayúscula.
- Tipos elementales:
- INTEGER: Número entero
 - Para valores lógicos usar: up(1) o down(2)
- OCTET STRING: 0 o más octetos que pueden tomar valores 0..255
- OBJECT IDENTIFIER: denota un authoritatively (único) named object
 - Secuencia de enteros no negativos
 - Ej: 1.3.6.1.2.1 o sea iso.org.dod.internet.mgmt.mib
- NULL: Tipos estructurados (constructed types):
- SEQUENCE: Secuencia ordenada de 0 o más ASN.1 types
- SEQUENCE OF TYPE: Secuencia ordenada de 0 o más elementos de un ASN.1 type
- Sub-Tipos (subtypes):
 - IpAddress: String de 4 octetos
 - Counter: Entero positivo $0..2^{32}$

SNMP

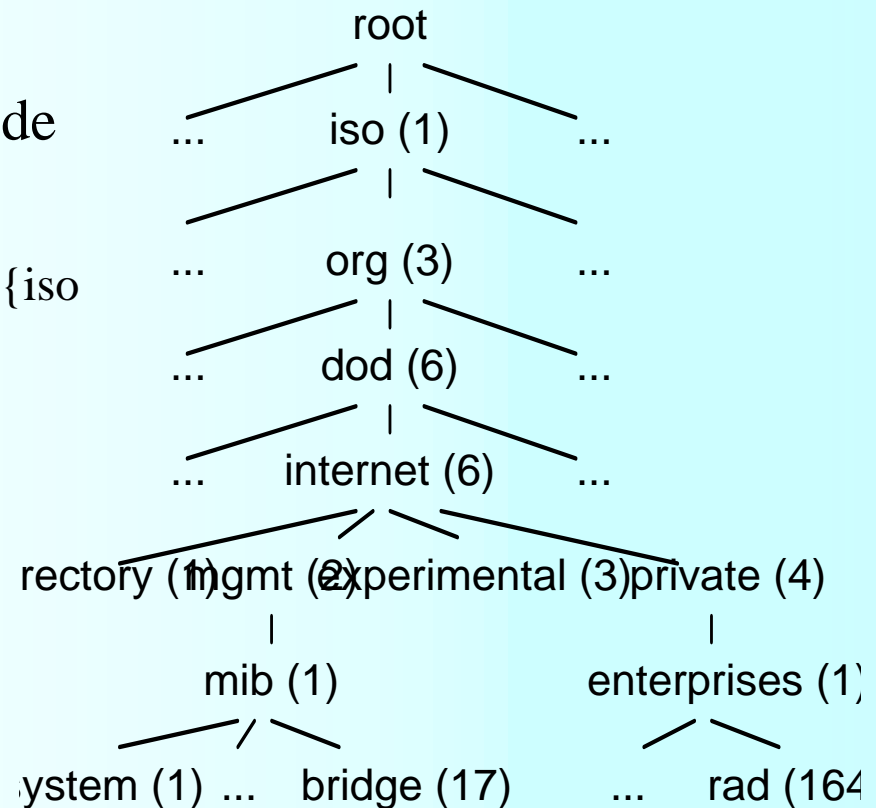
Managed Objects

- **SMI (Structure of Management Information)**
 - Define las reglas para describir objetos administrables (managed objects)
 - Todo objeto administrable tiene asociada una sintáxis y una semántica
 - Una variable es una instancia de un objeto
 - SMI define el esquema para la database de los objetos administrables
- **MIB (Managed Information Base)**
 - Es la database de los objetos administrables
 - Cada objeto tiene:
 - name (Object Identifier)
 - type (Object Type)
 - access (read-write, read-only, not-accessible, write-only) ;
 - status (mandatory, optional, obsolete)
- Ej:
 - sysDescr OBJECT-TYPE
 - SYNTAX OCTET STRING
 - ACCESS read-only
 - STATUS mandatory
 - ::= {system 1 }

SNMP

Object Names

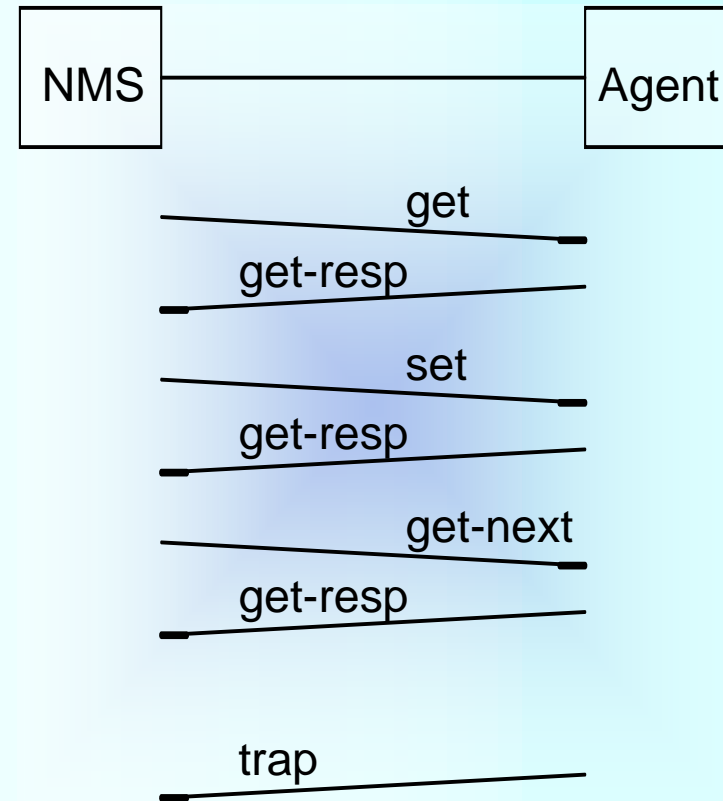
- **Object Name:**
 - Es el OBJECT IDENTIFIER de los objetos administrables.
- Ej: Internet OBJECT IDENTIFIER ::= {iso org(3) dod(6) 1} (o sea 1.3.6.1)



SNMP

Protocolo SNMP

Operación	Descripción
Get	para recuperar el valor de una variable MIB
Set	para modificar el valor de una variable MIB
get-Next	para recuperar el valor de una variable MIB pero en modo de acceso "traversal"
get-Response	para devolver el valor de una variable MIB
Trap	para reportar eventos extraordinarios



SNMP

Autenticación y Acceso

Autenticación en SNMP

View: subset of manageable objects

Access Mode: read-only, read-write

Community profile: View + Access Mode

SNMP entities: NMS & Agent

Community name

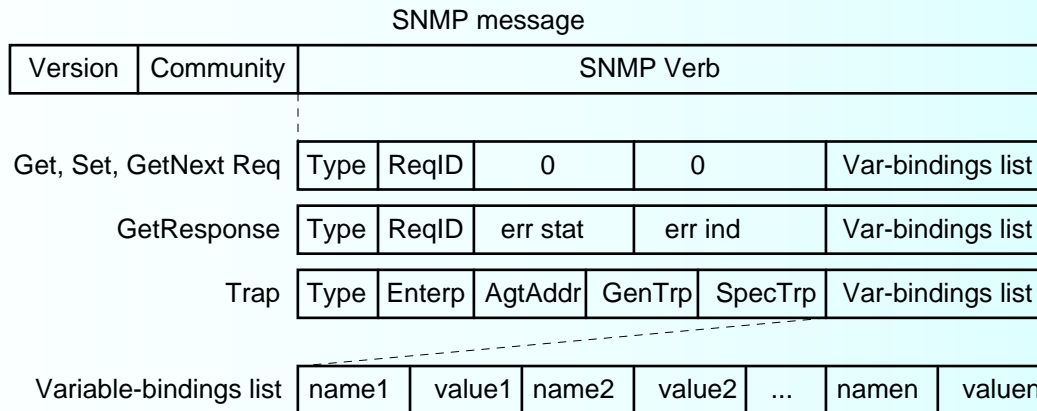
Authentic SNMP messages

Authetication failure

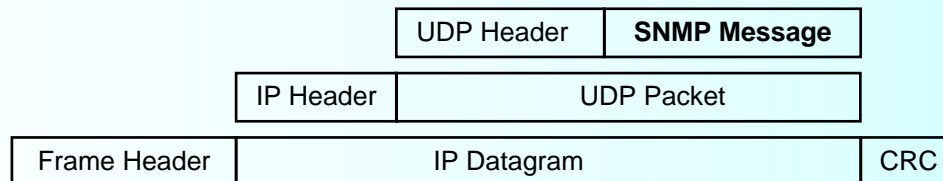
community name	IP address	access	traps	view name
public	0.0.0.0	read-only	no	all
public	192.9.200.1	read-only	yes	all
priv1	192.9.200.17	read-write	yes	all
priv2	150.30.25.4	read-write	yes	interfaces

SNMP

Formato de mensaje SNMP



- Version: SNMP o SNMPv2
- ReqID: utilizado para matchear responses con requests
- P.S.: La SNMP PDU no tiene longitud máxima. Si $SNMPPDU > MTU \implies$ Error "Too big"



SNMP

MIB II

```
-- MIB-II groups
system      OBJECT IDENTIFIER ::= { mib-2 1 }
interfaces  OBJECT IDENTIFIER ::= { mib-2 2 }
at          OBJECT IDENTIFIER ::= { mib-2 3 }
ip          OBJECT IDENTIFIER ::= { mib-2 4 }
icmp       OBJECT IDENTIFIER ::= { mib-2 5 }
tcp        OBJECT IDENTIFIER ::= { mib-2 6 }
udp        OBJECT IDENTIFIER ::= { mib-2 7 }
egp        OBJECT IDENTIFIER ::= { mib-2 8 }
-- cmot    OBJECT IDENTIFIER ::= { mib-2 9 }
transmission OBJECT IDENTIFIER ::= { mib-2 10 }
snmp       OBJECT IDENTIFIER ::= { mib-2 11 }
-- system group
sysDescr OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..255))
ACCESS read-only
```

SNMP

Traps

- Un trap es enviado por un Agent a una NMS.
- El mensaje de tipo trap es enviado indicando:
 - **sysObjID** del agent que lo generó (enterpriseID)
 - **network address** del agent que lo generó
 - **Generic Trap number**
 - **Specific Trap Number**
 - **timestamp** que es el sysUpTime de cuando se produjo el evento
 - **variable list** que provee información adicional relacionada con el trap
- Hay 7 generic trap numbers:
 - **coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborLoss, enterpriseSpecific**
- Hay una enorme cantidad de **Enterprise Traps**, por ejemplo:
 - "Temperature has reached danger point"
 - "Load balance conflict"
- En el agent se pueden definir niveles de **threshold** para decidir si un evento debe o no generar un trap.

SNMP

Extensiones MIB

- **RMON**
 - RFC 1271
 - Remote Network Management Goals
 - for Remote Monitoring of Networks:
 - network traffic statistics, hosts address table, hosts statistics, historical statistics, thresholds, packet/protocol analysis, ...
 - mgmt.mib.rmon(16) groups:
 - Statistics, History, Alarms, Hosts, HostTopN, TrafficMatrix, PacketCapture, Events.
- **REPEATER**
 - RFC 1516
 - for link testing, network traffic statistics, MAC address table, hosts statistics
- **BRIDGE**
 - RFC 1493
 - for link testing, network traffic statistics, STP performance, WAN Link performance
- **HOST**
 - RFC 1514
 - for host job counts, host file system info

SNMP

NMS Applications

- Varias “Generic NMS Applications” que trabajan con SNMP:
 - **OpenView** (HP)
 - **SunNetManager** (Sun)
 - **NetView/6000** (IBM)
 - PC/SNMP Tools (FTP Soft)
 - IT Metro (U&R Consultores)

SNMP

Otros Network Management Protocols

- **Otros protocolos de Network Management**
 - La ISO propuso una serie de protocolos de Network Management conformes a su modelo de referencia OSI.
 - Estos se denominan **CMIS** (Common Management Information Service) y **CMIP** (Common Management Information Protocol).
 - El protocolo **CMOT** es la implementación de CMIS/CMIP sobre conexiones TCP (CMis/ip Over Tcp)