Gestión

Area de Ingeniería Telemática
http://www.tlm.unavarra.es

Grado en Ingeniería en Tecnologías de Telecomunicación, 4º

Ejemplo

- En línea de comandos con net-snmp
- A un router nuestro (10.4.0.2)
- Veamos si los interfaces están levantados:

```
snmpget -c public 10.4.0.2 1.3.6.1.2.1.2.2.1.7.1
snmpget -c public 10.4.0.2 1.3.6.1.2.1.2.2.1.7.2
snmpget -c public 10.4.0.2 1.3.6.1.2.1.2.2.1.7.3
snmpget -c public 10.4.0.2 1.3.6.1.2.1.2.2.1.7.4
```

- El número de paquetes que ha intentado reenviar:

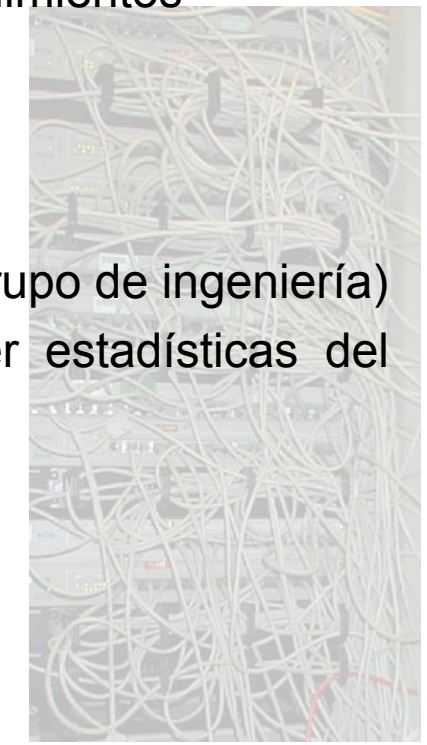
```
snmpget -c public 10.4.0.2 1.3.6.1.2.1.4.6.0
```

- Y todos los datos que nos ofrece por SNMP:

```
snmpwalk –c public 10.4.0.2
```

OAM&P

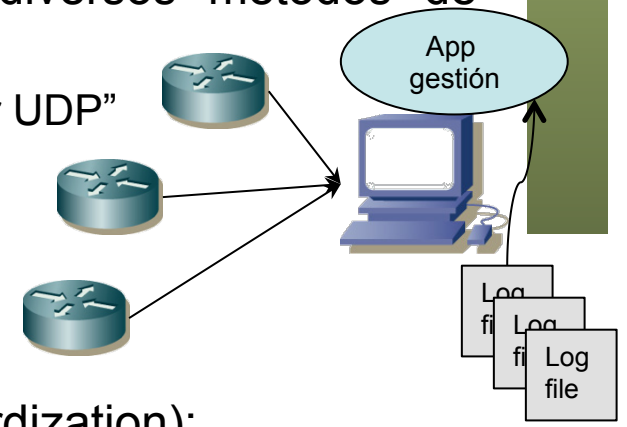
- *Operations, Administration, Maintenance and Provisioning*
- Operación
  - Tareas diarias para dar el servicio
  - Responsabilidad del grupo de operaciones desde el NOC (*Network Operations Center*)
- Administración
  - Establecer y gestionar objetivos, políticas, procedimientos
- Instalación y Mantenimiento
- *Provisioning*
  - Planificación y diseño de red
  - Configuración de circuitos (responsabilidad del grupo de ingeniería)
  - Emplean herramientas de gestión para obtener estadísticas del tráfico para planificación



Una implementación básica

Obtener información: syslog

- RFC 5424 “The Syslog protocol” (versión moderna estandarizada)
- Permite emitir mensajes de texto para quedar registrados (log)
- Soportado por gran cantidad de equipos (routers, switches)
- Permite identificar el host origen del mensaje, el dispositivo o aplicación, la fecha, el nivel de importancia
- Suelen rotarse los ficheros y comprimirse o borrarse
- De cliente a servidor con la posibilidad de diversos métodos de transporte
  - RFC 5426 “Transmission of Syslog Messages over UDP”
  - RFC 3195 “Reliable Delivery for syslog”
  - Puerto UDP 514, puerto TCP 601
  - Puede emplear TLS (puerto TCP/UDP 6514)
  - Puede usar relays
- Ejemplo (hay muchas variantes pre-IETF-standardization):




```
Aug 14 09:12:32 tlm34 rtkit-daemon[2160]: Supervising 4 threads of 2 processes of 1 users.
Aug 14 09:12:32 tlm34 pulseaudio[2183]: [pulseaudio] pid.c: Daemon already running.
Aug 14 09:17:01 tlm34 CRON[2201]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Aug 14 09:17:21 tlm34 anacron[1481]: Job `cron.daily' started
Aug 14 09:17:21 tlm34 anacron[2207]: Updated timestamp for job `cron.daily' to 2013-08-14
```

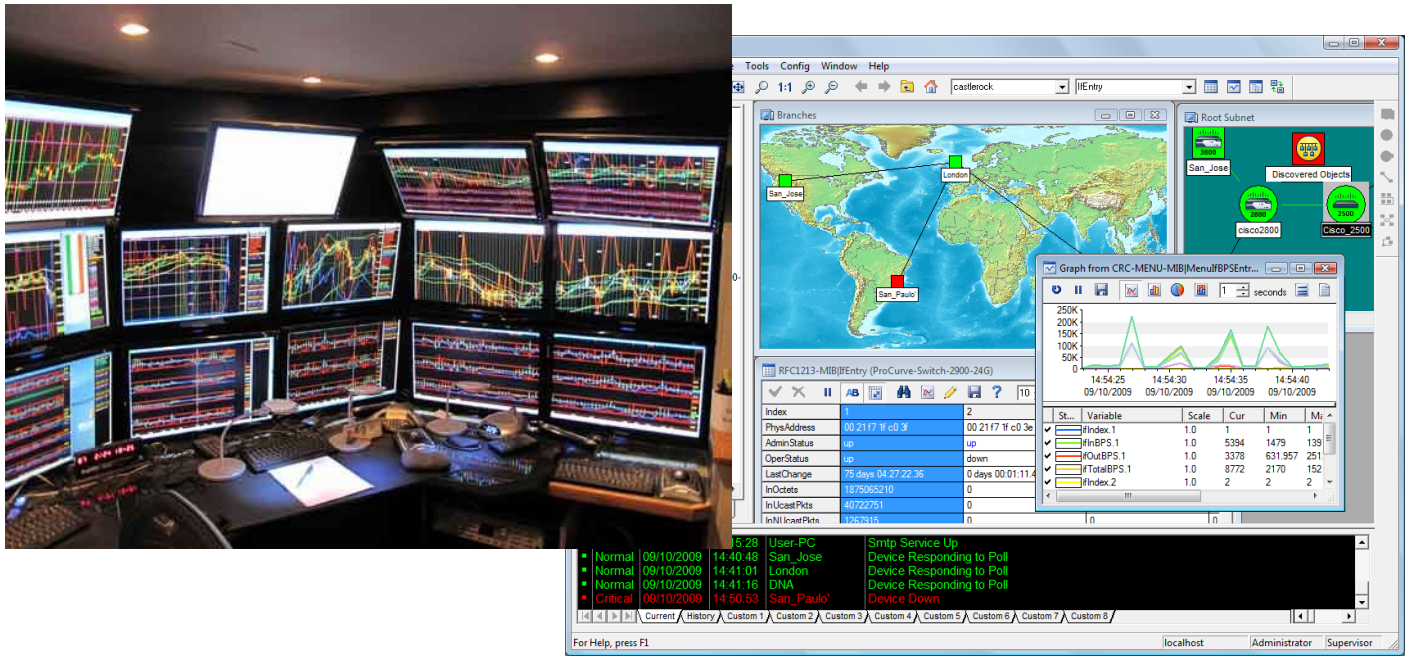
Configuración: CLI

- *Command Line Interface*
- Soportado por la mayoría de conmutadores y routers
- Sin coste adicional de software de gestión
- Reminiscencia del terminal UNIX
- Y de que los primeros routers eran máquinas UNIX
- No hay un CLI estandarizado aunque es frecuente:
  - Ayuda (?)
  - Autocompletado (tab)
  - Modos y submodos
  - El *prompt* marca el *command mode*
  - Su salida está pensada para humano y no es simple de procesar por script

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/4
Router(config-if)# ip address 172.20.52.106 255.255.255.248
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

NMS

- *Network Management System*
- Herramientas para la monitorización y el control de la red
- Hardware y software:
  - desde *ping*
  - hasta una sonda de monitorización y análisis de tráfico
  - pasando por una consola de monitorización (un ordenador) con un soft para la recogida de logs o parte del S.O. de un switch
- Gestión *in-band* o *out-of-band*



Información

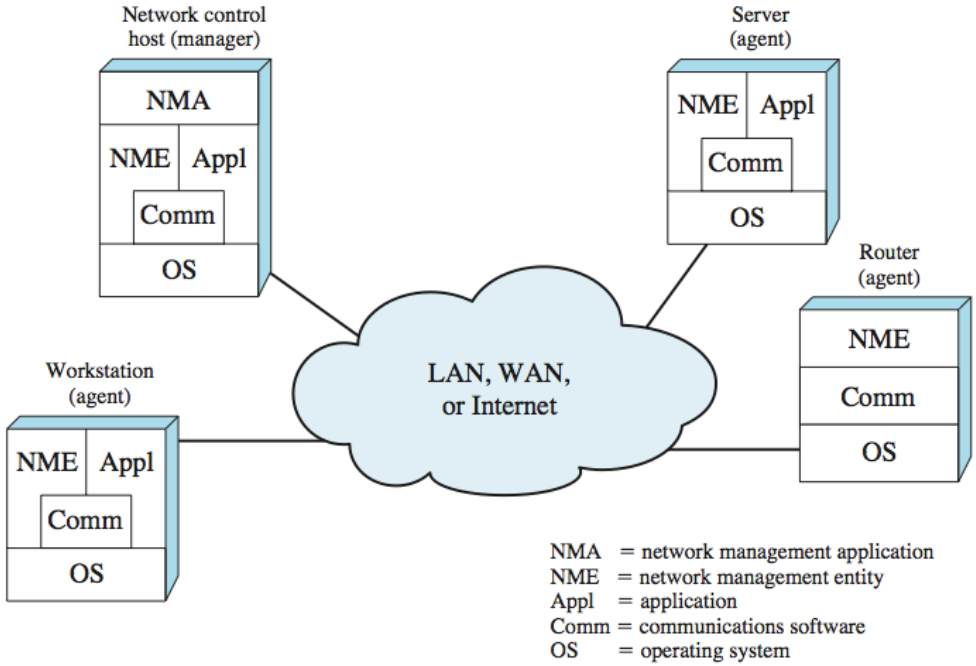
- Para todas estas tareas es clave la recogida de información
- Esta suele venir de los propios equipos de infraestructura de red
- O servidores o servicios
- Aunque también se puede generar de forma activa (ej: ping)
- La información la produce un agente
- La recoge un gestor (*manager*)
- Empleando un protocolo
- Y una forma de representar la información

Tipos de información

- Estática: caracteriza a los elementos y su configuración (ej. Número de puertos de un switch)
- Dinámica: relacionada con sucesos (ej. Número de conexiones TCP)
- Estadística: derivada de la dinámica (ej. Número medio de paquetes transmitidos por segundo)

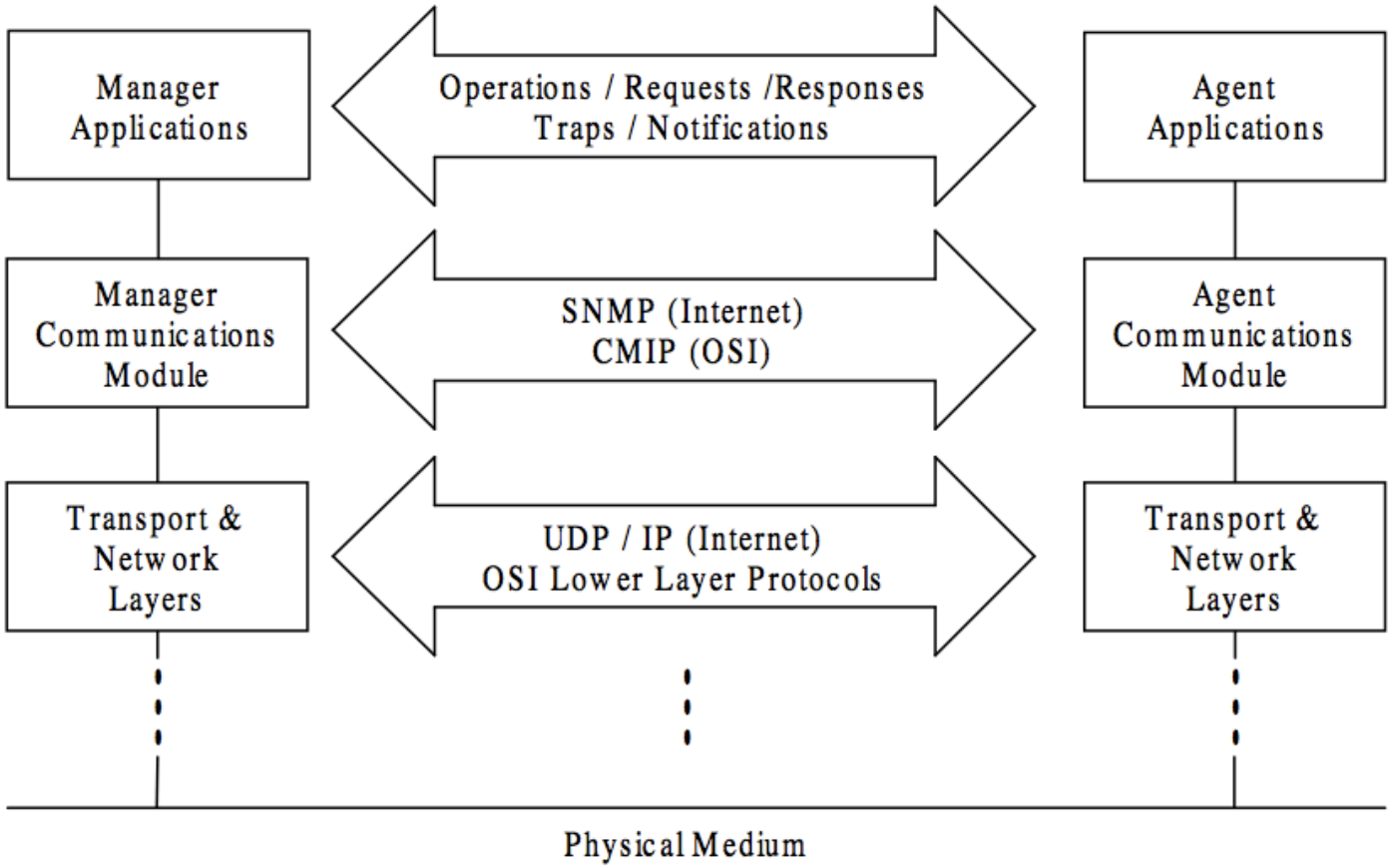
NMS: elementos

- Network elements: Hosts, hubs, switches, routers..., gestionados o no
- *Agents*
  - Proceso corriendo en un elemento de red gestionado
  - Contesta a preguntas del manager y puede enviar alarmas
- Manager: Consulta al agente, recibe datos, los procesa y almacena en una base de datos



"Business Data Communications", William Stallings

Comunicaciones



Estándares

CMIP: Common Management Information Protocol

- OSI management standard (para 7 niveles)
- Orientado a objetos (clases, herencia...)
- Complejo para especificar esos objetos
- Desde sus comienzos ha tenido elevados requerimientos de memoria en las estaciones lo cual ha obstaculizado su implantación
- CMIP over TCP/IP (CMOT RFC 1189, histórica)

TMN: Telecommunications Management Network

- Estándar de ITU-T
- Para gestión de red de operadora
- Basado en CMIP (OSI)

SNMP: Simple Network Management Protocol

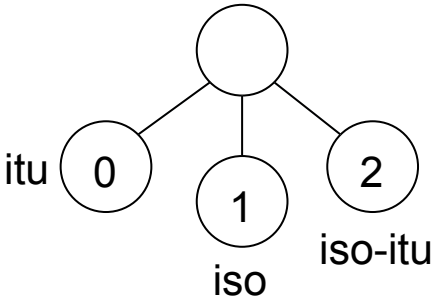
- Gestión para Internet (redes TCP/IP)
- Nombre del protocolo y del framework

Modelo para la información

- **SMI** (Structure of Management Information): los mecanismos para describir y nombrar los objetos
- **MIB** (Management Information Base): Es donde se almacena (los objetos) esa información (en agente o gestor), el *schema*
- **MDB** (Management Database) es la base de datos con los datos medidos o introducidos por administración
- Ejemplo:
  - La SMI define cómo especificar un número de puertos de un puente
  - En la MIB dice que un switch del model X del fabricante Y tiene un parámetro que es el número de puertos.
  - En la MDB dice que el switch Z del modelo X del fabricante Y que se está gestionando en la red tiene 12 puertos

MIB

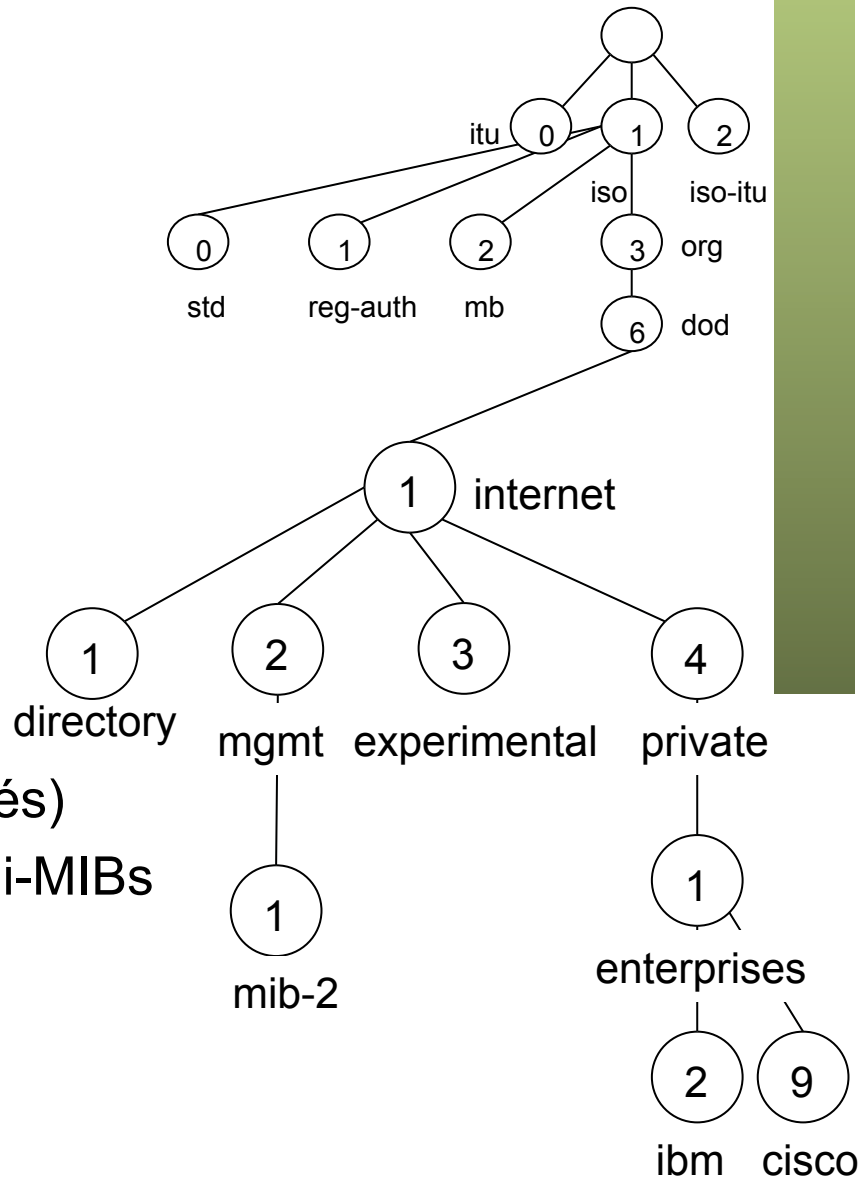
- *Virtual information store* (el schema)
- Estructura en árbol
- Especificada por ISO pero empleada también en Internet
- Objetos definidos empleando ASN.1
- Cada objeto tiene: nombre, sintaxis y codificación
- Nombre:
  - OBJECT IDENTIFIER (OID), secuencia de números de nodos de un árbol
  - Raíz sin etiqueta, sub-árboles delegados en gestión



Nota: Podéis encontrar ccitt en lugar de itu

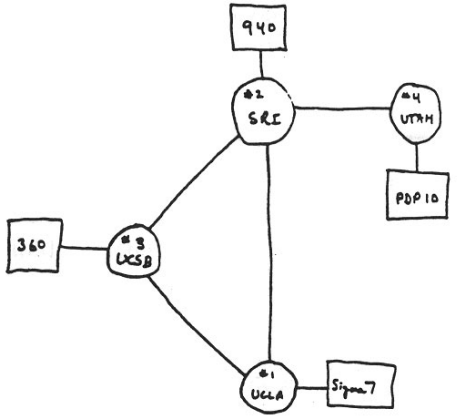
MIB OIDs para Internet

- IANA gestiona:
  1.3.6.1 = iso.org.dod.internet
- 1.3.6.1.4 = private
  - Definidos unilateralmente
  - 1.3.6.1.4.1 = enterprises
  - Ahí un subárbol por empresa
- 1.3.6.1.2 = mgmt
  - Objetos estándar
- 1.3.6.1.2.1 = MIB-II
  - RFC 1213 (actualizada después)
  - Más una gran cantidad de mini-MIBs
  - MIB-I histórica (RFC1156)



Gestión en Internet

- *Internet Standard Management Framework*
- Última versión (v.3) RFC 3410 (podéis leer ahí sobre su evolución desde v.1)
- *SNMPv3 Management Framework*
- Como con gran parte de Internet, al final su simplicidad es parte del motivo de su éxito (a S es de Simple)
- Simple para no dedicar mucho esfuerzo dado que, total, TCP/IP se acabaría cambiando por los protocolos OSI
- Claro claro…



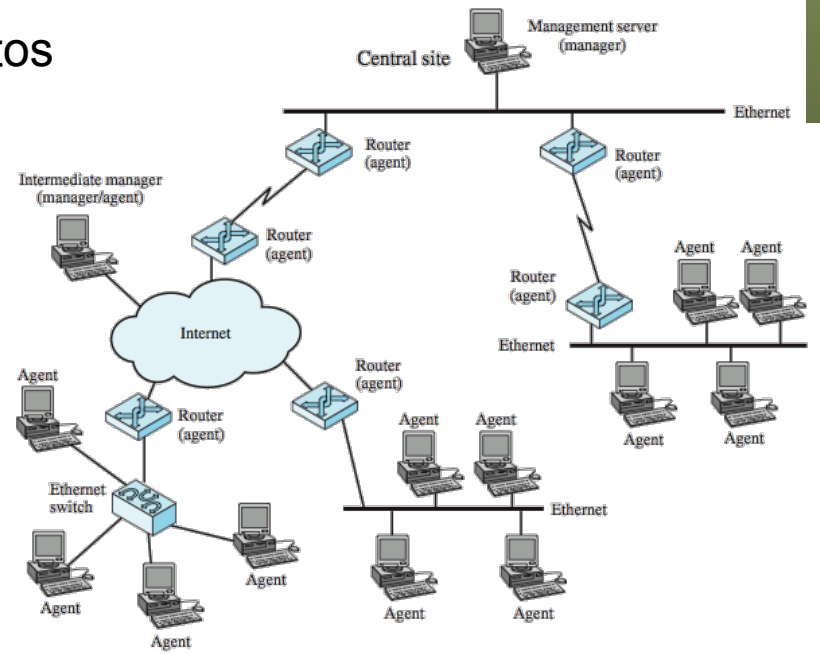
THE ARPA NETWORK

DEC 1969

4 NODES

Gestión en Internet

- Hoy en día la gran mayoría de equipos de red implementan alguna versión de SNMP
- También ha influido que los estádares han sido siempre gratuitos y accesibles por www/ftp
- Pero no le quitemos importancia a la simplicidad
- CMOT? (CMIP over TCP/IP) para una época de transición que aún no ha llegado ;-)
- El framework de gestión consiste en:
  - Un lenguaje de definición de datos
  - La MIB
  - Un protocolo
  - Seguridad y administración

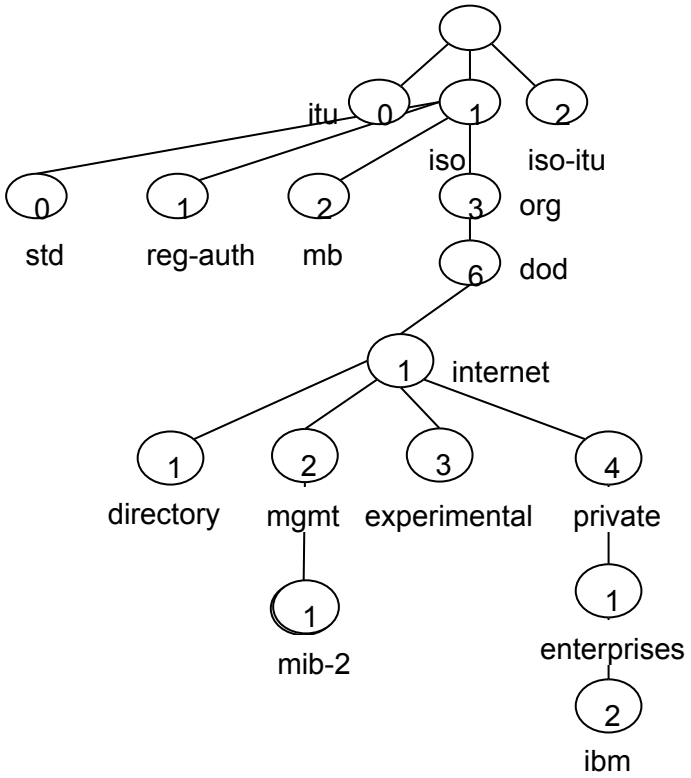


SMIv2

- El lenguaje para definir los tipos de datos
- RFC 2578 “Structure of Management Information Version2 (SMIv2)”
- Es un subconjunto de ASN.1
  - *Abstract Syntax Notation One*
  - Estándar OSI e ITU-T
- SMIv2 es la forma actual de escribir MIBs
- SMIv1 no ha dejado de ser estándar por todos los que dependen de él

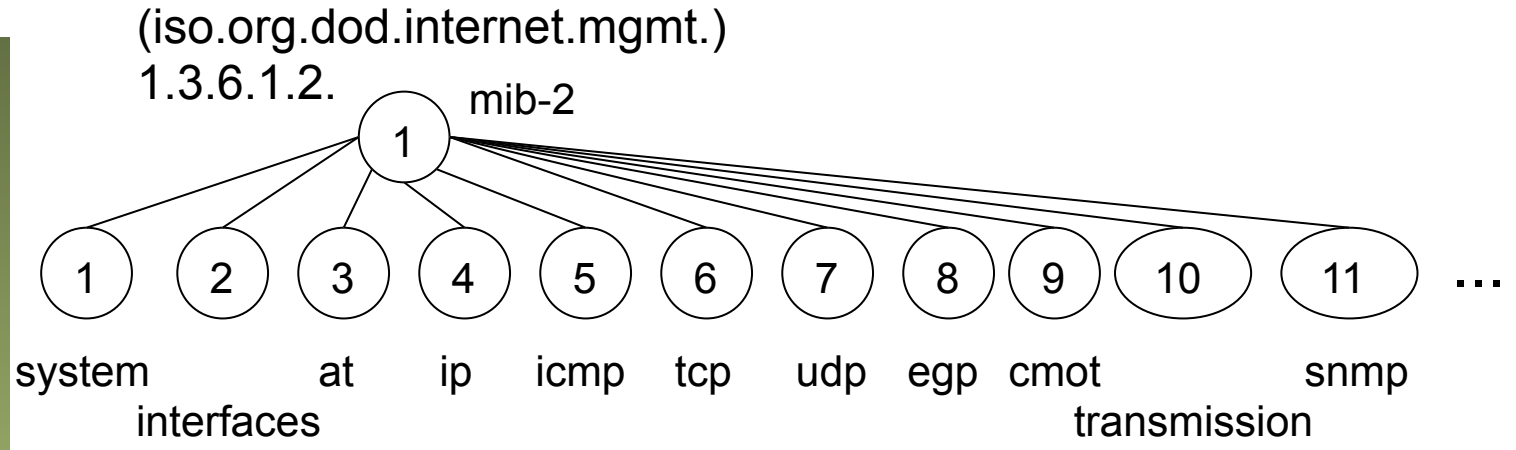
MIB-II

- RFC 1213 “Management Information Base for Network Management of TCP/IP-based internets: MIB-II”
  - Grupos: System, Interfaces, Address Translation (IP a MAC), IP, ICMP, TCP, UDP, EGP, Transmission, SNMP



MIB-II

- RFC 1213 “Management Information Base for Network Management of TCP/IP-based internets: MIB-II”
  - Grupos: System, Interfaces, Address Translation (IP a MAC), IP, ICMP, TCP, UDP, EGP, Transmission, SNMP



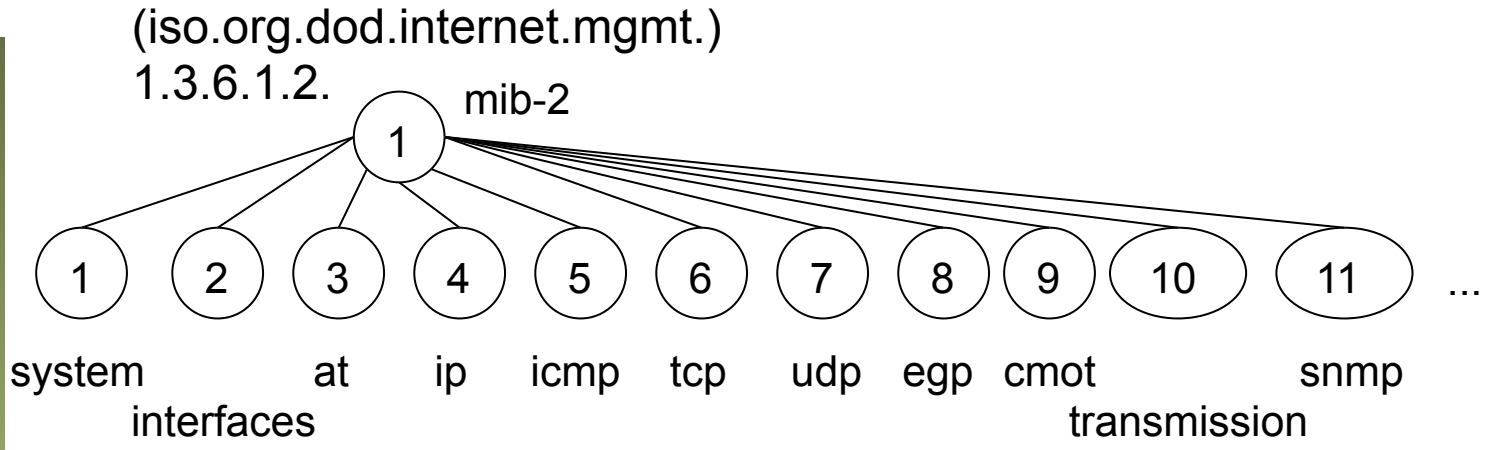
Ejemplos MIB-II (RFC 1213)

```
ifOutOctets OBJECT-TYPE
    SYNTAX  Counter
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
            "The total number of octets transmitted out of the
            interface, including framing characters."
    ::= { ifEntry 16 }


ipDefaultTTL OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-write
    STATUS  mandatory
    DESCRIPTION
            "The default value inserted into the Time-To-Live
            field of the IP header of datagrams originated at
            this entity, whenever a TTL value is not supplied
            by the transport layer protocol."
    ::= { ip 2 }
```

MIB-II

- RFC 1213 "Management Information Base for Network Management of TCP/IP-based internets: MIB-II"
  - Grupos: System, Interfaces, Address Translation (IP a MAC), IP, ICMP, TCP, UDP, EGP, Transmission, SNMP



- RFC 2011 "SNMPv2 Management Information Base for the Internet Protocol using SMIv2"
  - Actualiza objetos empleando SMIv2
  - Para los grupos IP e ICMP

Ejemplo (RFC 2011)

```
ipInDelivers OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
          "The total number of input datagrams successfully delivered
          to IP user-protocols (including ICMP)."
    ::= { ip 9 }
```

MIB-II

- Se actualizan con SMIv2 e independizan:
  - RFC 2011 “SNMPv2 Management Information Base for the **Internet Protocol** using SMIv2”
  - RFC 2012 “SNMPv2 Management Information Base for the **Transmission Control Protocol** using SMIv2”
  - RFC 2013 “SNMPv2 Management Information Base for the **User Datagram Protocol using** SMIv2”
- Pero…
- Obsoletas por:
  - RFC 4293 ”Management Information Base for the Internet Protocol (IP)” (2006)
  - RFC 4022 “Management Information Base for the Transmission Control Protocol (TCP)” (2005)
  - RFC 4113 “Management Information Base for the User Datagram Protocol (UDP)” (2005)
- Que actualizan objetos, mejoran soporte de IPv6, recogen objetos de otras RFCs, etc.

Ejemplo

```
ipInDelivers OBJECT-TYPE
    SYNTAX     Counter32
    MAX-ACCESS read-only
    STATUS     deprecated
    DESCRIPTION
            "The total number of input datagrams successfully delivered
            to IPv4 user-protocols (including ICMP).
            This object has been deprecated as a new IP version neutral
            table has been added.  It is loosely replaced by
            ipSystemStatsIndelivers."
    ::= { ip 9 }


ipSystemStatsInBcastPkts OBJECT-TYPE
    SYNTAX     Counter32
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
            "The number of IP broadcast datagrams received.
           Discontinuities in the value of this counter can occur at
            re-initialization of the management system, and at other
            times as indicated by the value of
            ipSystemStatsDiscontinuityTime."
    ::= { ipSystemStatsEntry 42 }
```