Simple Network Management Protocol

(SNMP)

Organismos de estandarización

- **ISOC (Internet Society)**

Es responsable de promover el desarrollo, evolución y uso abierto de Internet en todo el mundo.
También facilita el desarrollo abierto de estándares y protocolos para la infraestructura técnica de Internet, incluida la supervisión del Internet Architecture Board (IAB)

*fuente: http://ecovi.uagro.mx/ccna1/course/module3/3.2.3.2/3.2.3.2.html

IAB (Internet Architecture Board, Comité de Arquitectura de Internet)

Es responsable de la administración y el desarrollo general de los estándares de Internet.
También supervisa la arquitectura para los protocolos y los procedimientos que utiliza Internet.
El IAB consta de 13 miembros, entre los cuales se encuentra el presidente del IETF (Internet Engineering Task Force).

*fuente: http://ecovi.uagro.mx/ccna1/course/module3/3.2.3.2/3.2.3.2.html

IETF (Internet Engineering Task Force)

Se encarga de desarrollar, actualizar y mantener Internet y las tecnologías TCP/IP. (corto plazo)
Una de sus principales responsabilidades es producir documentos RFC (Request For Comments) que contienen especificaciones de protocolos, procesos y tecnologías para Internet.

Consta de Grupos de Trabajo (WG) encargados de desarrollar las especificaciones.

*fuente: http://ecovi.uagro.mx/ccna1/course/module3/3.2.3.2/3.2.3.2.html

IESG (Internet Engineering Steering Group, Comité Directivo de Ingeniería de Internet)

Es responsable de la administración técnica del IETF y el proceso de los estándares de Internet.

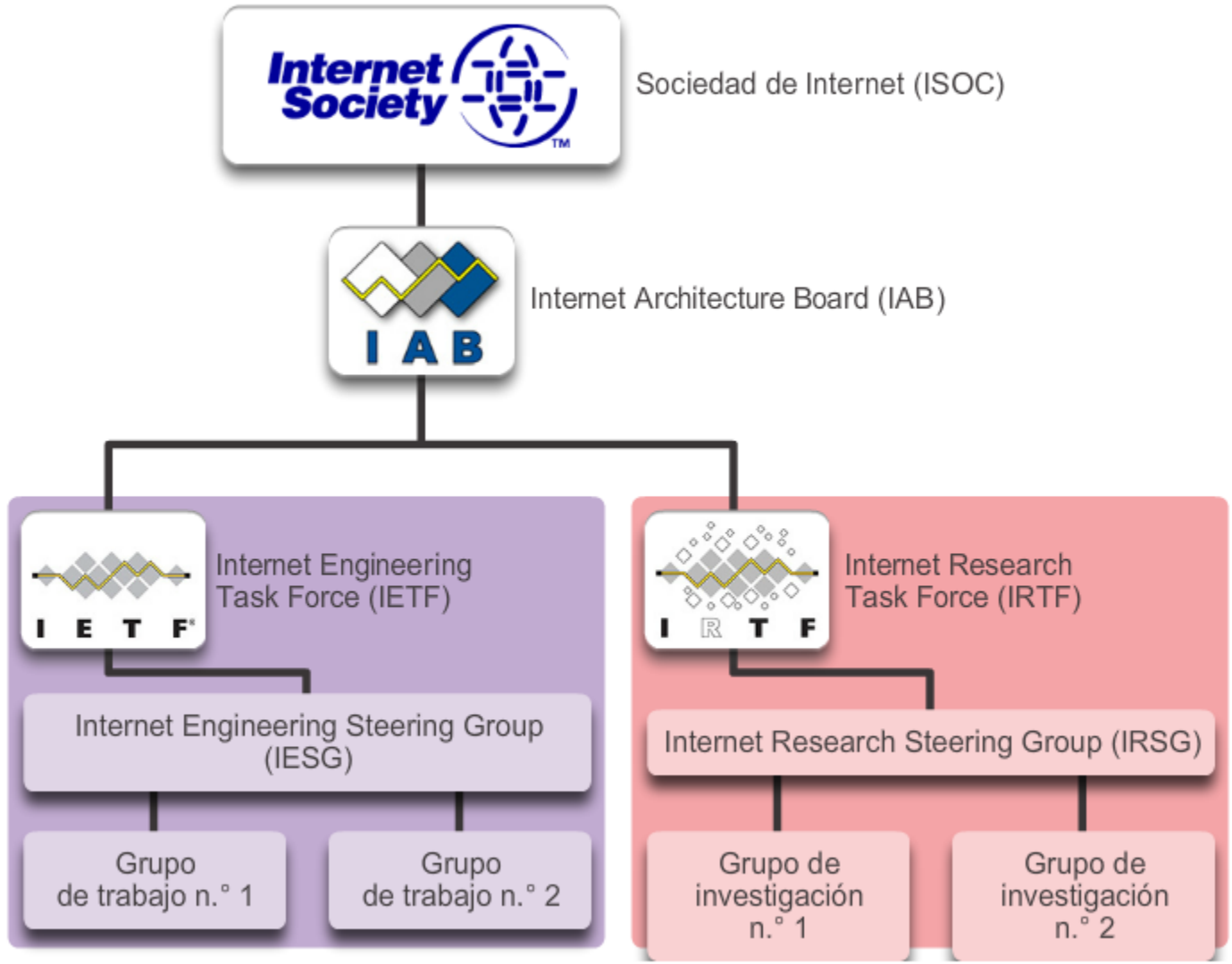
*fuente: http://ecovi.uagro.mx/ccna1/course/module3/3.2.3.2/3.2.3.2.html

IRTF (Internet Research Task Force)

Se centra en la investigación a largo plazo relacionada con los protocolos, aplicaciones, arquitecturas y tecnologías de TCP/IP y de Internet.

*fuente: http://ecovi.uagro.mx/ccna1/course/module3/3.2.3.2/3.2.3.2.html

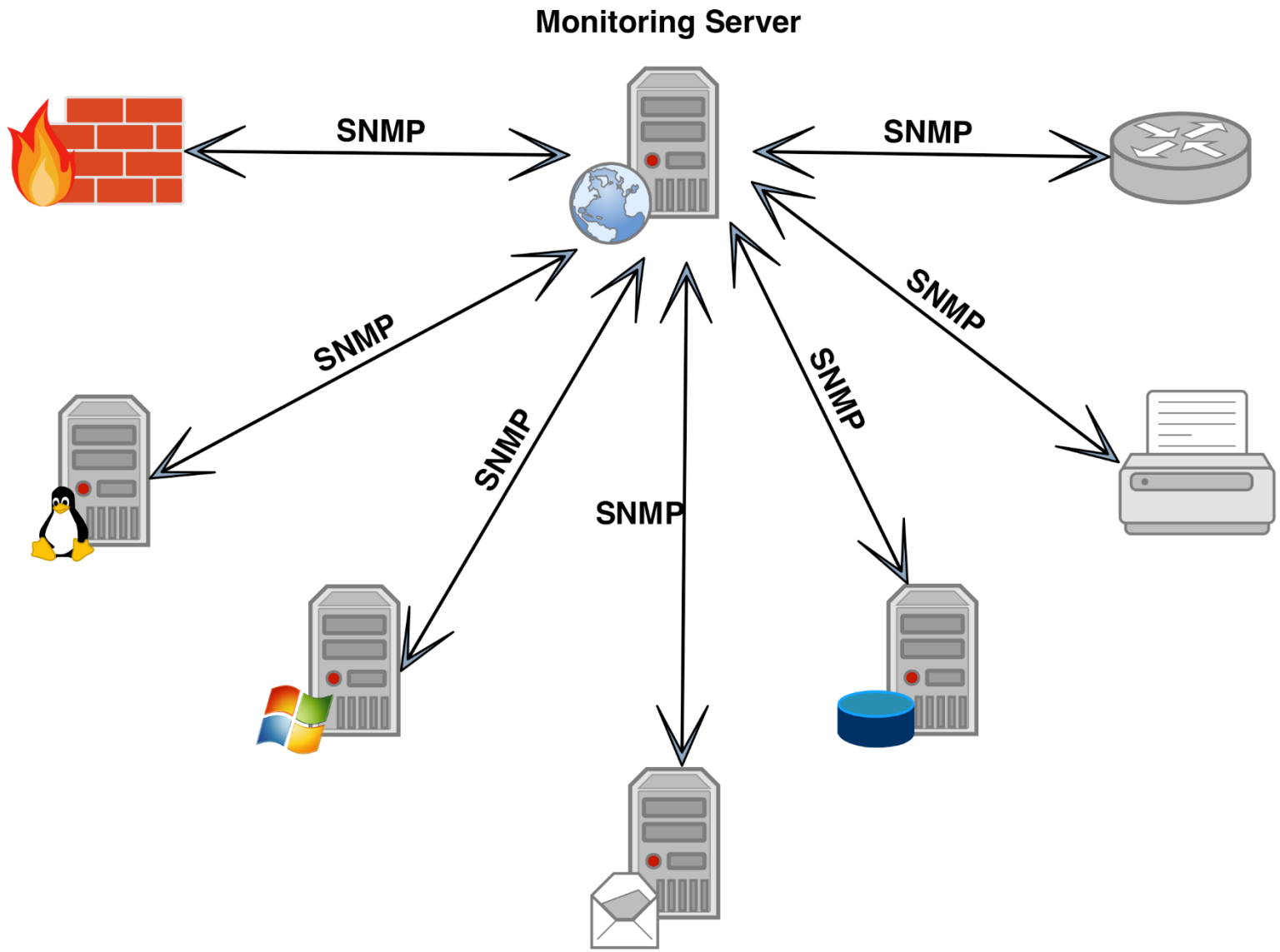
ISOC, IAB, IETF e IRTF



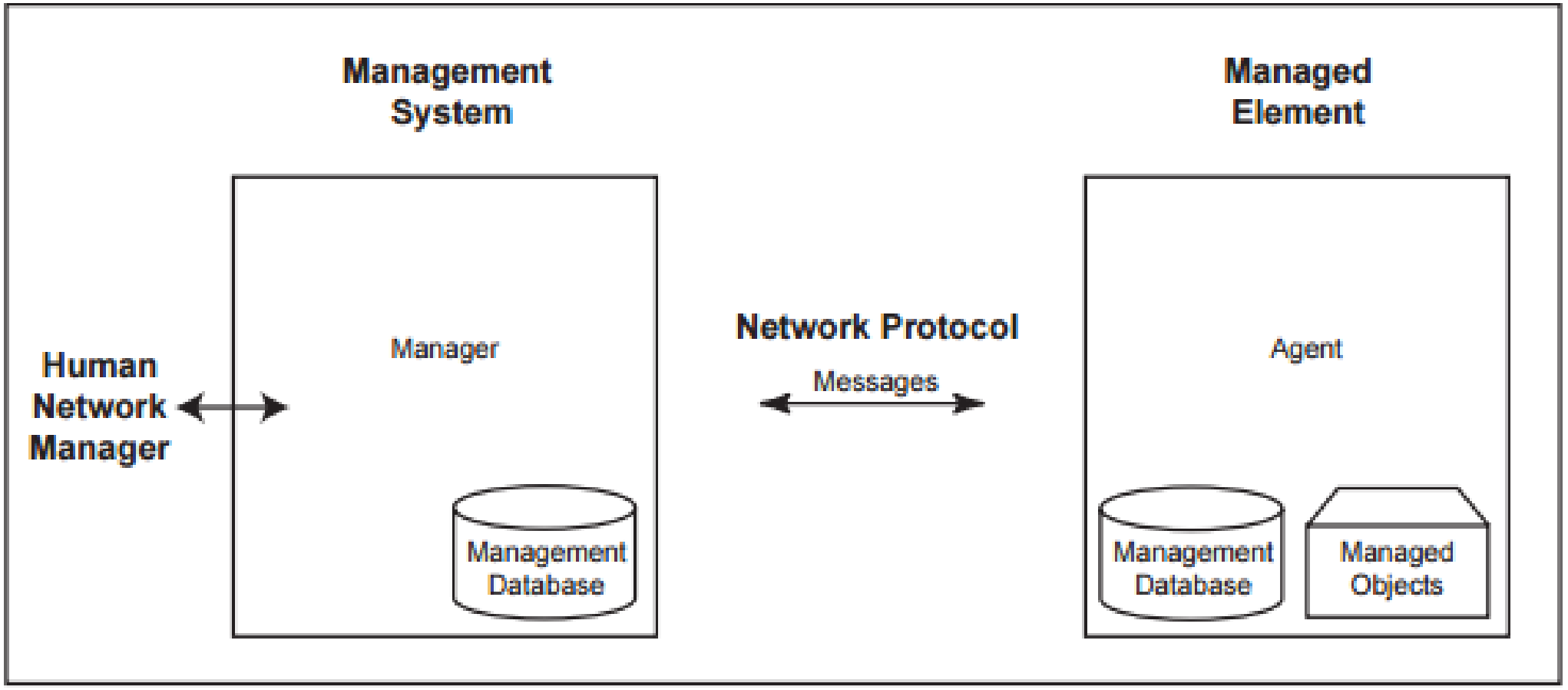
*fuente: http://ecovi.uagro.mx/ccna1/course/module3/3.2.3.2/3.2.3.2.html

Simple Network Management Protocol

- SNMP es un protocolo implementado sobre la capa de aplicación
- Definido por la Internet Arhitecture Board(IAB) en el RFC 1157 en 1988
- Creado para intercambiar información de gestión y monitoreo entre dispositivos de red.

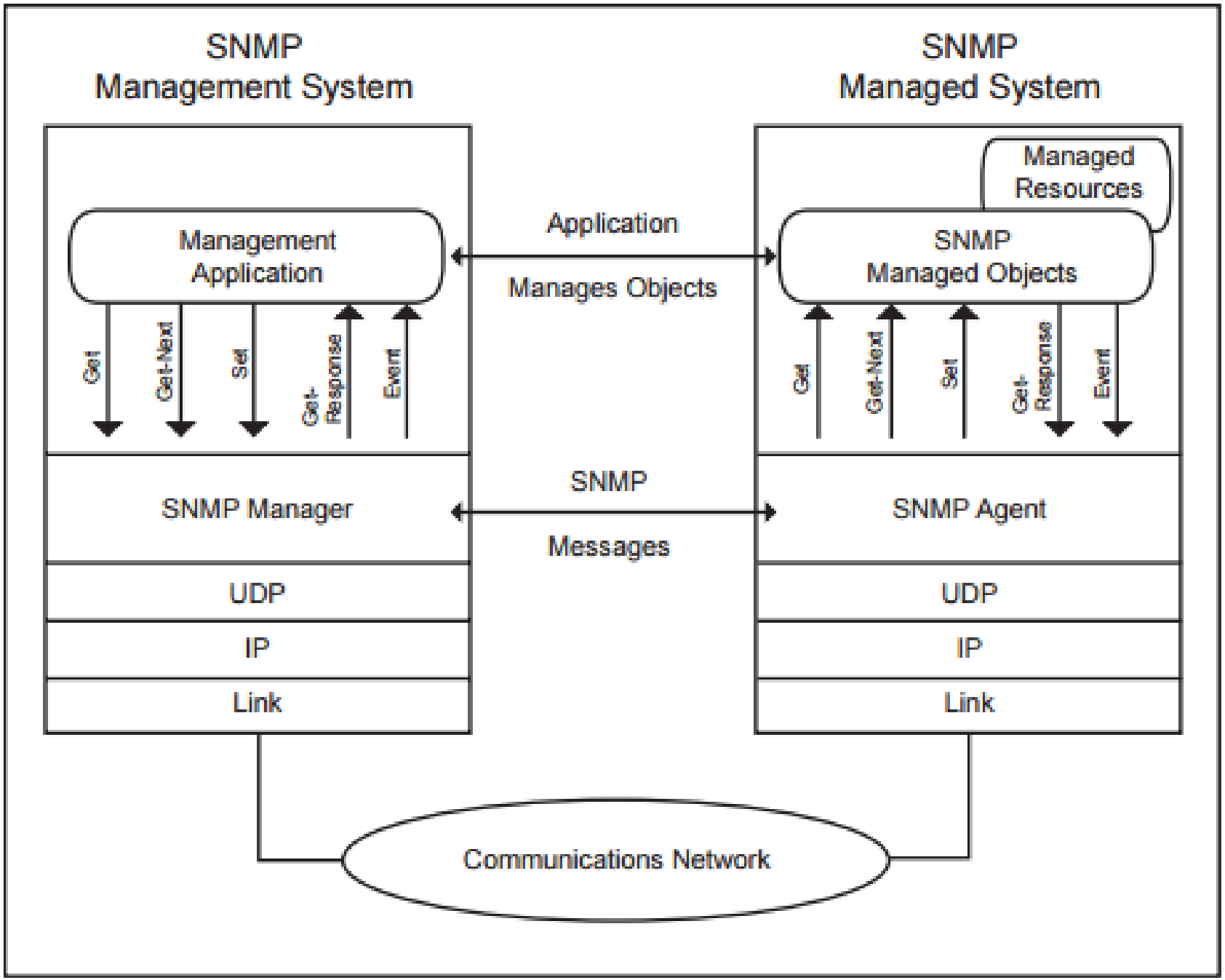

Monitoring Server
SNMP
SNMP
SNMP
SNMP
SNMP
SNMP
SNMP

Arquitectura de SNMP



SNMP uses a manager/agent architecture. Alarm messages (Traps) are sent by the agent to the manager.

*fuente: http://www.dpstelecom.com


SNMP
Management System
SNMP
Managed System
Managed
Resources
Management
Application
Application
Manages Objects
SNMP
Managed Objects
Get
Get-Next
Set
Get-
Response
Event
SNMP Manager
SNMP
Messages
SNMP Agent
UDP
IP
Link
UDP
IP
Link
Communications Network

Componentes de SNMP

- Administrador SNMP
- Dispositivos administrados
- Agente SNMP
- Management Information Base (MIB)

Administrador SNMP

El administrador o sistema de administración SNMP es responsable de comunicarse con el agente SNMP implementado en los dispositivos administrados. Sus principales funciones son:

- Consultar a los agentes SNMP
- Obtener respuestas de los agentes
- Establecer variables en los agentes
- Acusar eventos asíncronos de los agentes (traps)

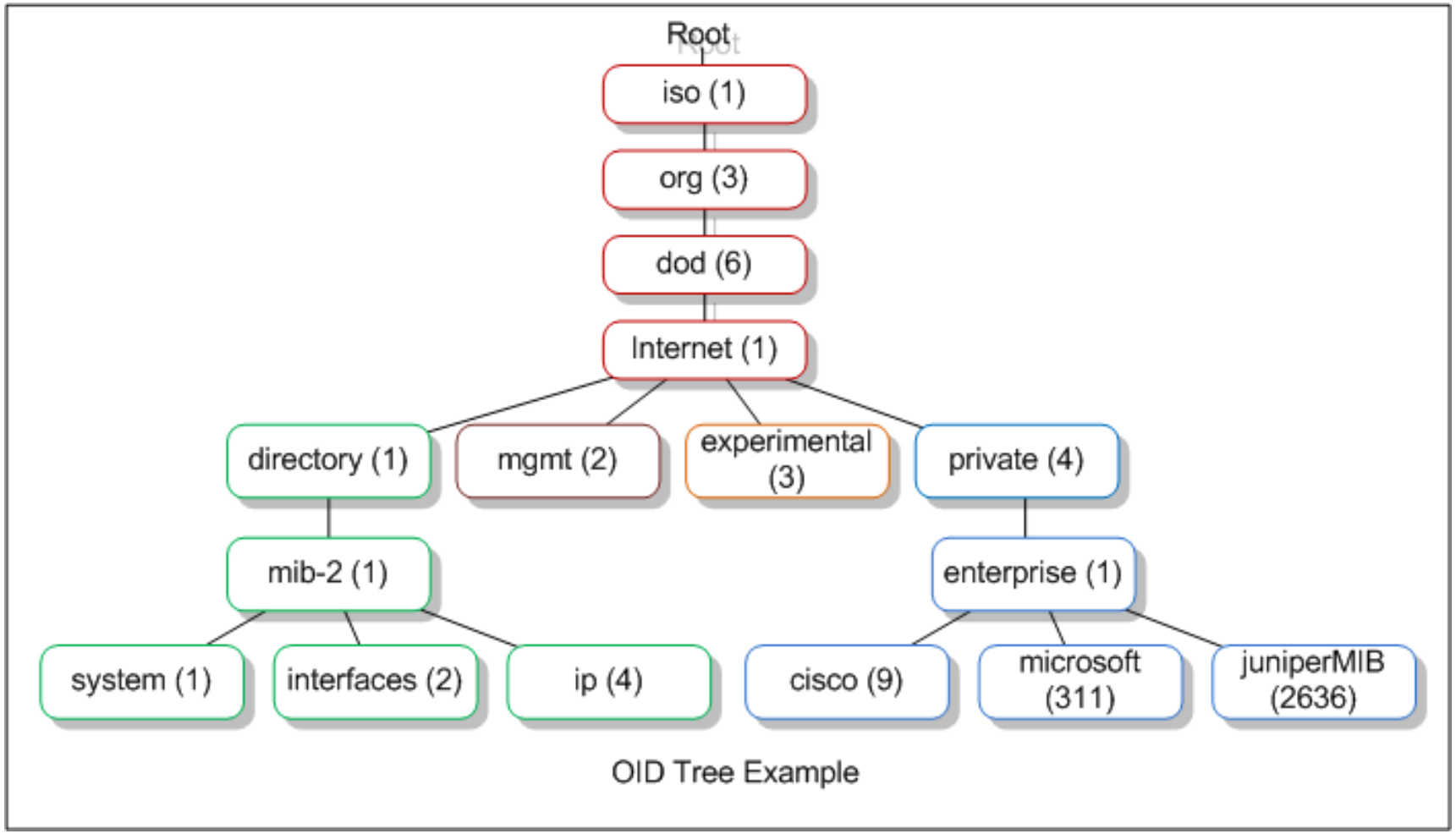
Management Information Base (MIB)

- Es un archivo de texto que describe los elementos de red SNMP como una lista de objetos de datos.
- Contiene información jerárquica, estructurada en forma de árbol con variables individuales (estado, descripción) de los dispositivos gestionados en una red.
- Su principal función es traducir cadenas numéricas en texto entendible a los humanos.
- Es parte de la gestión de red definida en el modelo OSI
- Un número entero largo es usado como ID de Objeto (OID) para distinguir cada variable de forma única

OID(Object Identier)

- Es una dirección utilizada para identificar dispositivos y su estado.
- Ej.
  - Ancho de banda utilizado por un dispositivo
  - Cantidad de memoria disponible
  - Dirección IP
- Tiene una estructura de árbol donde cada número define un nivel de direccionamiento distinto

Estructura del árbol OID



*fuente: http://rcp100.sourceforge.net/snmp.html

Ejemplo de OID (público)

1.3.6.1.2.1.1.4

Número	Etiqueta	Explicación
.1	iso	ISO es el grupo que estableció el estándar OID
.3	org	Una organización será especificada a continuación
.6	dod	Departamento de Defensa de los Estados Unidos de Norteamérica
.1	internet	Comunicación será vía Internet/Red
.2	mgmt	Este es un dispositivo de gestión definido por el IETF
.1	MIB-2	El OID está definido en la versión 2 de la especificación de MIB
.1	System	Éste es un parámetro de sistema
.4	sysContact	Éste parámetro es la información de contacto para el administrador de un sistema

Ejemplo de OID (privado)

1 . 3 . 6 . 1 . 4 . 1 . 2682 . 1 . 4 . 5 . 1 . 1. 99 . 1 . 1 . 6

Número	Etiqueta	Explicación
.1	iso	ISO es el grupo que estableció el estándar OID
.3	org	Una organización será especificada a continuación
.6	dod	Departamento de Defensa de los Estados Unidos de Norteamérica
.1	internet	Comunicación será vía Internet/Red
.4	private	Este es un dispositivo manufacturado por una entidad privada (no gubernamental)
.1	enterprise	El fabricante está catalogado como una empresa

Ejemplo de OID (privado)

1 . 3 . 6 . 1 . 4 . 1 . 2682 . 1 . 4 . 5 . 1 . 1. 99 . 1 . 1 . 6

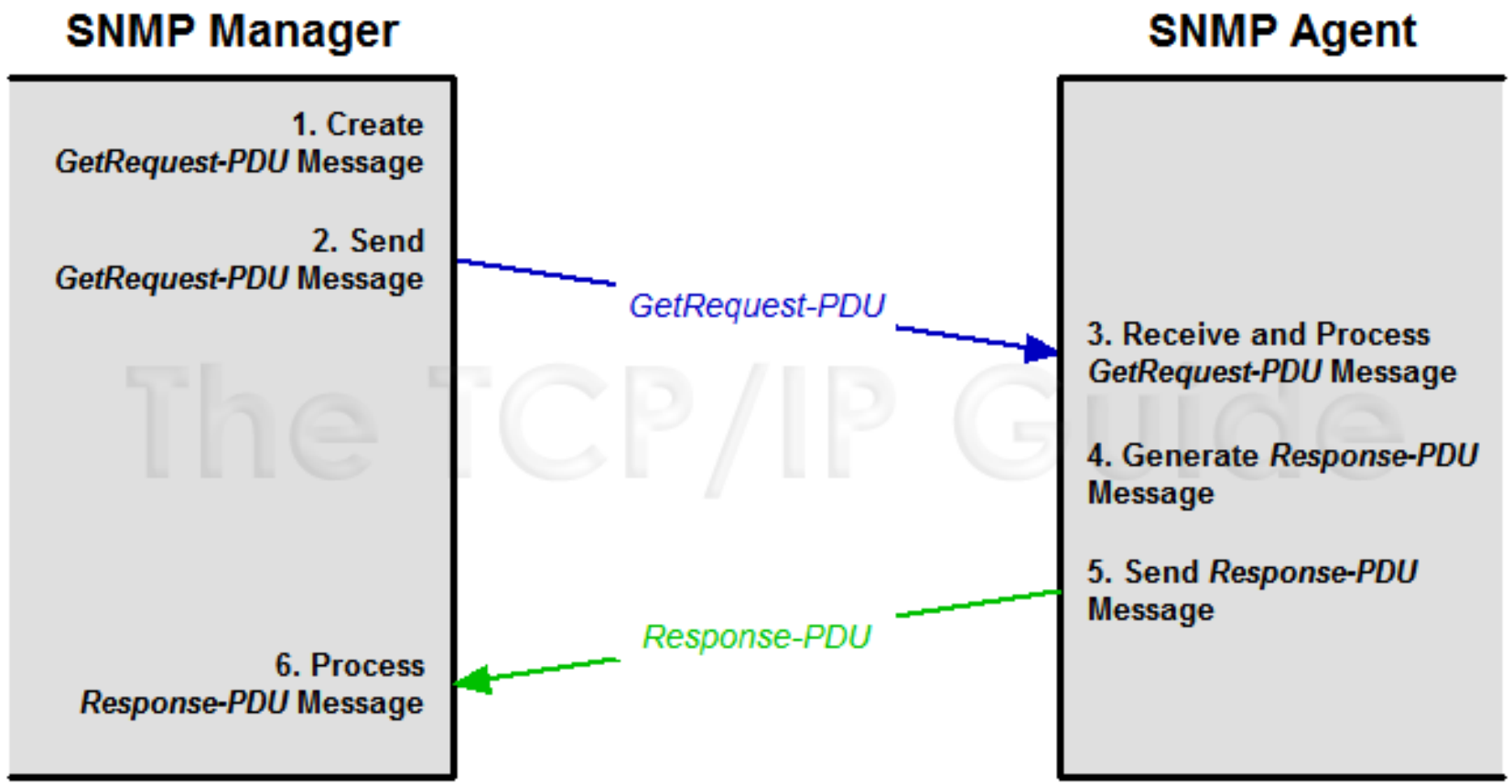
Número	Etiqueta	Explicación
.2682	dpsInc	El fabricante es DPS Telecom Inc.
.1	dpsAlarmControl	Ésta es una alarma y dispositivo de control fabricado por DPS
.4	dpsRTU	Ésta es una Unidad Terminal Remota (RTU)
.5	AlarmGrid	Se trata de un punto de alarma discreta
.1	AlarmEntry	Un punto de alarma será especificado a continuación
.1	Port	Éste es el puerto para este punto de alarma
.99	Address	Ésta es la dirección de éste punto de alarma
.1	Display	Éste es el display para este punto de alarma
.1	Point	Éste es el número de punto de alarma
.6	dpsRTUAState	Éste es el estado del punto de alarma(set, clear, etc.)

Subtree Name	OID	RFC	Description
system	1.3.6.1.2.1.1	RFC1213	System information.
interfaces	1.3.6.1.2.1.2	RFC2863	Interface information.
at	1.3.6.1.2.1.3	RFC1213	Translation MIB, deprecated
ip	1.3.6.1.2.1.4	RFC4292, RFC4293	Internet Protocol
icmp	1.3.6.1.2.1.5	RFC1213, RFC4293	Internet Control Message Protocol
tcp	1.3.6.1.2.1.6	RFC4022	Transmission Control Protocol
udp	1.3.6.1.2.1.7	RFC4113	User Datagram Protocol
snmp	1.3.6.1.2.1.11	RFC1213	Simple Network Management Protocol
host	1.3.6.1.2.1.25	RFC2790	Host Resources
event	1.3.6.1.2.1.88	RFC2981	DISMAN Event
notification log	1.3.6.1.2.1.99	RFC3014	Notification log

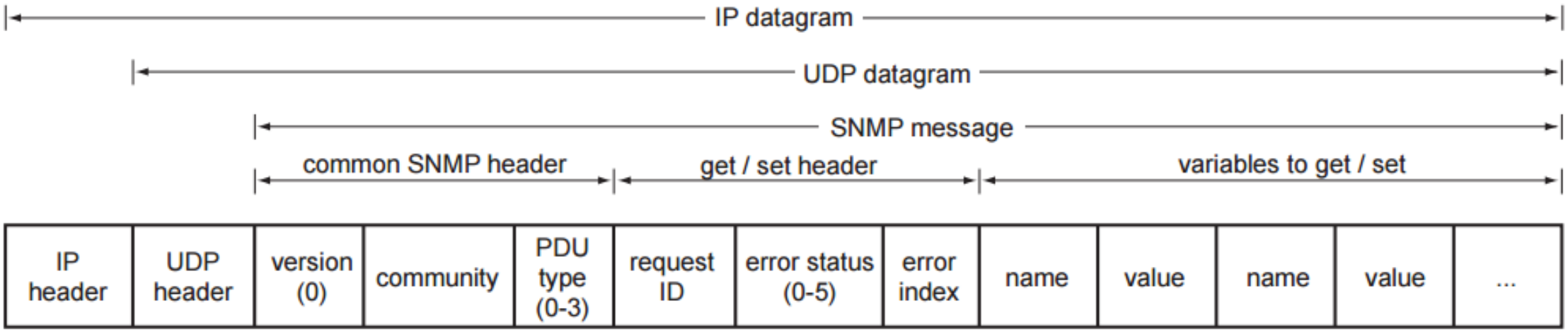
*fuente: http://rcp100.sourceforge.net/snmp.html

Mensajes SNMP

- 5 diferentes tipos de mensajes:
  - **Get**: Usado por el gestor SNMP para consultar una MIB
  - **GetNext**: usado por el gestor SNMP para leer secuencialmente a través de la MIB
  - **GetResponse**: usado por el agente SNMP para responder una petición
  - **Set**: usado por el gestor SNMP para fijar un valor en la MIB
  - **Trap**: usado por el agente SNMP para reportar eventos


SNMP Manager
SNMP Agent
1. Create GetRequest-PDU Message
2. Send GetRequest-PDU Message
GetRequest-PDU
3. Receive and Process GetRequest-PDU Message
4. Generate Response-PDU Message
5. Send Response-PDU Message
Response-PDU
6. Process Response-PDU Message

Formato de mensaje



versión
- 0=versión 1
- 1=versión 2

Tipo De PDU
- 0=Get
- 1=GetNext
- 2=Response
- 3=Set
- 4=Trap

Error status
- 0=No error
- 1=Too big
- 2=No such name
- 3=Bad value
- 4=Read only
- 5=General error

*Tamaño máximo del PDU = MTU

Implementaciones de SNMP (linux)

- **snmpd**: agente snmp
- **snmp**: gestor snmp

#sudo apt-get update
#sudo apt-get install snmp
#sudo apt-get install snmpd

*FUENTE: https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-an-snmp-daemon-and-client-on-ubuntu-14-04

Archivo /etc/snmp/snmp.conf

```
#mibs :
```

Archivo /etc/snmp/snmpd.conf

```
###############
#
#  AGENT BEHAVIOUR
#

#  Listen for connections from the local system only
agentAddress  udp:127.0.0.1:161
#  Listen for connections on all interfaces (both IPv4 *and* IPv6)
#agentAddress udp:161,udp6:[::1]:161
```

Archivo /etc/snmp/snmpd.conf

```
###############################################################################
#
#  ACCESS CONTROL
#

                                #  system + hrSystem groups only
#view   systemonly  included   .1.3.6.1.2.1.1
#view   systemonly  included   .1.3.6.1.2.1.25.1

                                #  Full access from the local host
 rwcommunity public  localhost
```

Verificación del servidor

- sudo service snmpd stop/start/restart
- sudo service snmpd status
- sudo netstat –nao –udp //n=numeric, a=todo pts abiertos y cerrados
  //o=info relacionada a timers

Aplicaciones

- **snmpwalk**:lee secuencialmente a través de la MIB

Ej. snmpwalk -v 1 -c public 127.0.0.1

- **snmpget**: obtiene una entrada de la MIB

Ej. snmpget -v 1 -c public localhost 1.3.6.1.2.1.1.4.0

- **snmpset**: modifica una entada de la MIB

Ej. snmpset -v 1 -c public 127.0.0.1 1.3.6.1.2.1.1.4.0 s Escuela

OID’s de interés:

CPU Statistics

-Load
  1 minute Load: .1.3.6.1.4.1.2021.10.1.3.1
  5 minute Load: .1.3.6.1.4.1.2021.10.1.3.2
  15 minute Load: .1.3.6.1.4.1.2021.10.1.3.3

-CPU
  percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0
  raw user cpu time: .1.3.6.1.4.1.2021.11.50.0
  percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0
  raw system cpu time: .1.3.6.1.4.1.2021.11.52.0
  percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0
  raw idle cpu time: .1.3.6.1.4.1.2021.11.53.0
  raw nice cpu time: .1.3.6.1.4.1.2021.11.51.0

OID’s de interés:

-Memory Statistics

Total Swap Size: .1.3.6.1.4.1.2021.4.3.0
Available Swap Space: .1.3.6.1.4.1.2021.4.4.0
Total RAM in machine: .1.3.6.1.4.1.2021.4.5.0
Total RAM used: .1.3.6.1.4.1.2021.4.6.0
Total RAM Free: .1.3.6.1.4.1.2021.4.11.0
Total RAM Shared: .1.3.6.1.4.1.2021.4.13.0
Total RAM Buffered: .1.3.6.1.4.1.2021.4.14.0
Total Cached Memory: .1.3.6.1.4.1.2021.4.15.0

-System uptime

System Uptime: .1.3.6.1.2.1.1.3.0

OID’s de interés:

-Disk Statistics

The snmpd.conf needs to be edited. Add the following (assuming a machine with a single ‘/' partition):

disk / 100000 (or)

includeAllDisks 10% for all partitions and disks

The OIDs are as follows

Path where the disk is mounted: .1.3.6.1.4.1.2021.9.1.2.1
Path of the device for the partition: .1.3.6.1.4.1.2021.9.1.3.1
Total size of the disk/partion (kBytes): .1.3.6.1.4.1.2021.9.1.6.1
Available space on the disk: .1.3.6.1.4.1.2021.9.1.7.1
Used space on the disk: .1.3.6.1.4.1.2021.9.1.8.1
Percentage of space used on disk: .1.3.6.1.4.1.2021.9.1.9.1
Percentage of inodes used on disk: .1.3.6.1.4.1.2021.9.1.10.1

OID’s de interés:

-Disk Statistics

Path where the disk is mounted: .1.3.6.1.4.1.2021.9.1.2.1
Path of the device for the partition: .1.3.6.1.4.1.2021.9.1.3.1
Total size of the disk/partion (kBytes): .1.3.6.1.4.1.2021.9.1.6.1
Available space on the disk: .1.3.6.1.4.1.2021.9.1.7.1
Used space on the disk: .1.3.6.1.4.1.2021.9.1.8.1
Percentage of space used on disk: .1.3.6.1.4.1.2021.9.1.9.1
Percentage of inodes used on disk: .1.3.6.1.4.1.2021.9.1.10.1

Get available disk space for / on the target host

#snmpget -v 1 -c "community" target_name_or_ip .1.3.6.1.4.1.2021.9.1.7.1

this will return available disk space for the first entry in the ‘disk' section of snmpd.conf; replace 1 with n for the nth entry

Get the 1-minute system load on the target host

API SNMP4J